SOPHOS

simple + secure

Sophos UTM

administration guide

Product version: 9.200

Document date: Tuesday, February 18, 2014

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to nsg-docu@sophos.com.

Contents

1 Installation

This section provides information on installing and setting up Sophos UTM on your network. The installation of Sophos UTM proceeds in two steps: first, installing the software; second, configuring basic system settings. The initial setup required for installing the software is performed through a console-based installation menu. The internal configuration can be performed from your management workstation through the web-based administrative interface of Sophos UTM called WebAdmin. Before you start the installation, check if your hardware meets the minimum system requirements.

Note – If you are employing a Sophos UTM hardware appliance, you can skip the following sections and directly jump to the *Basic Configuration* section, as all Sophos UTM hardware appliances ship with UTM Software preinstalled.

The following topics are included in this chapter:

1.1 Recommended Reading

Before you begin the installation, you are advised to read the following documents that help you setting up Sophos UTM, all of which are enclosed within the package of your Sophos UTM hardware appliance unit and which are also available at the Sophos UTM Resource Center:

- Quick Start Guides Hardware
- Operating Instructions

1.2 System Requirements

The minimum hardware requirements for installing and using UTM are as follows:

- **Processor:** Pentium 4 with 1.5 GHz (or compatible)
- **Memory:** 1 GB RAM
- **HDD:** 20 GB IDE or SCSI hard disk drive
- **CD-ROM Drive:** Bootable IDE or SCSI CD-ROM drive
- **NIC:** Two or more PCI Ethernet network interface cards
- **NIC** (optional): One heart-beat capable PCI Ethernet network interface card. In a high-availability system, the primary and secondary system communicate with one another through so-called heart-beat requests. If you want to set up a high-availability system, both units need to be equipped with heart-beat capable network interface cards.
- **USB** (optional): One USB port for communications with a UPS device
- **Switch** (optional): A network device that connects (and selects between) network segments. Note that this switch must have jumbo frame support enabled.

Sophos provides a list of hardware devices compatible with UTM Software. The *Hardware Compatibility List* (HCL) is available at the Sophos Knowledgebase. To make the installation and operation of UTM Software less error-prone, you are advised to only use hardware that is listed in the HCL. The hardware and software requirements for the client PC used to access WebAdmin are as follows:

- **Processor:** Clock signal frequency 1 GHz or higher
- **Browser:** Latest version of Firefox (recommended), latest version of Chrome, latest version of Safari, or Microsoft Internet Explorer 8 onwards. JavaScript must be enabled. In addition, the browser must be configured not to use a proxy for the IP address of the UTM's internal network card (eth0).

1.2.1 UPS Device Support

Uninterruptible Power Supply (UPS) devices maintain a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available. Sophos UTM supports UPS devices of the manufacturers MGE UPS Systems and APC. The communication between the UPS device and Sophos UTM is made via the USB interface.

As soon as the UPS device runs in battery operation, a notification is sent to the administrator. If the power failure persists for a longer period and the voltage of the UPS device approximates a critical value, another message will be sent to the administrator—Sophos UTM will be shut down automatically.

Note – Please read the operation manual of the UPS device to connect the devices to Sophos UTM. UTM will recognize the UPS device when booting via the USB interface. Only boot Sophos UTM when you have connected the USB interfaces to each other.

1.2.2 RAID Support

A RAID (*Redundant Array of Independent Disks*) is a data storage scheme using multiple hard drives to share or replicate data among the drives. To ensure that the RAID system is detected and properly displayed on the Dashboard, you need to use a RAID controller that is supported by Sophos UTM. Check the HCL to figure out which RAID controllers are supported. The HCL is available at the Sophos Knowledgebase. Use "HCL" as search term to locate the corresponding page.

1.3 Installation Instructions

What follows is a step-by-step guide of the installation process of Sophos UTM Software.

Before you begin the installation, please make sure you have the following items available:

- The Sophos UTM CD-ROM
- The license key for Sophos UTM

The setup program will check the hardware of the system, and then install the software on your PC.

1.3.1 Key Functions During Installation

In order to navigate through the menus, use the following keys (please also note the additional key functions listed at the bottom of a screen):

- F1: Displays the context-sensitive help screen.
- Cursor keys: Use these keys to navigate through the text boxes (for example, the license agreement or when selecting a keyboard layout).
- Tab key: Move back and forth between text boxes, lists, and buttons.
- Enter key: The entered information is confirmed, and the installation proceeds to the next step.

- Space key: Select or unselect options marked with an asterisk.
- Alt-F2: Switch to the installation console.
- Alt-F4: Switch to the log.
- Alt-F1: Switch to the interactive bash shell.
- Alt-F1: Return to the main installation screen.

1.3.2 Special Options During Installation

Some screens offer additional options:

View Log: Opens the installation log.

Support: Opens the support dialog screen.

To USB Stick: Writes the installation log as zip file to a USB stick. Remember to insert a USB stick before confirming this option. The zip file can be used to solve installation problems, e.g. by the Sophos UTM Support Team.

Back: Returns to the previous screen.

Cancel: Opens a confirmation dialog window to abort the installation.

Help: Opens the context-sensitive help screen.

1.3.3 Installing Sophos UTM

1. **Boot your PC from CD-ROM drive.**
   The installation start screen is displayed.

   Note – You can always press F1 to access the help menu. Pressing F3 in the start screen opens a troubleshooting screen.

2. **Press Enter.**
   The *Introduction* screen is displayed.
3. **Select *Start Installation*.**
   The *Hardware Detection* screen is displayed.

   The software will check the following hardware components:

- CPU
- Size and type of hard disk drive
- CD-ROM drive
- Network interface cards
- IDE or SCSI controllers

If your system does not meet the minimum requirements, the installation will report the error and abort.

As soon as the hardware detection is completed, the *Detected Hardware* screen is displayed for information purposes.

4. **Press Enter.**
   The *Select Keyboard* screen is displayed.
5. **Select your keyboard layout.**
   Use the Cursor keys to select your keyboard layout, e.g. *English (UK)*, and press Enter to continue.

   The *Select Timezone* screen is displayed.
6. **Select your area.**
   Use the Cursor keys to select your area, e.g. *Europe*, and press Enter to continue.
7. **Select your time zone.**
   Use the Cursor keys to select your time zone, e.g. *London*, and press Enter to continue.

   The *Date and Time* screen is displayed.
8. **Set date and time.**
   If date and time are not correct, you can change them here. Use the Tab key and the Cursor keys to switch between text boxes. You can unselect the *Host clock is UTC* option by pressing the Space key. Invalid entries will be rejected. Confirm your settings with the Enter key.

   The *Select Admin Interface* screen is displayed.
9. **Select an internal network card.**
   In order to use the WebAdmin tool to configure the rest of Sophos UTM, select a network interface card to be the internal network card (eth0). Choose one of the available network cards from the list and confirm your selection with the Enter key.

Note – Interfaces having an active connection are marked with *[link]*.

The *Network Configuration* screen is displayed.

10. **Configure the administrative network interface.**
Define the IP address, network mask, and gateway of the internal interface which is going to be the administrative network interface. The default values are:

Address: `192.168.2.100`

Netmask: `255.255.255.0`

Gateway: `none`

You need to change the gateway value only if you wish to use the WebAdmin interface from a workstation outside the subnet defined by the netmask. Note that the gateway itself must be within the subnet.[1]

Confirm your settings with the Enter key.

If your CPU supports 64 bit the *64 Bit Kernel Support* screen is displayed. Otherwise the installation continues with the *Enterprise Toolkit* screen.

11. **Install the 64-bit kernel.**
Select *Yes* to install the 64-bit kernel or *No* to install the 32-bit kernel.

The *Enterprise Toolkit* screen is displayed.

12. **Accept installation of the Enterprise Toolkit.**
The Enterprise Toolkit comprises the Sophos UTM Software. You can decide to install Open Source software only. However, we advise to also install the Enterprise Toolkit to be able to use the full functionality of Sophos UTM.

Press Enter to install both software packages or select *No* to install the Open Source software only.

[1] For example, if you are using a network mask of `255.255.255.0`, the subnet is defined by the first three octets of the address: in this case, `192.168.2`. If your administration computer has the IP address `192.168.10.5`, it is not on the same subnet, and thus requires a gateway. The gateway router must have an interface on the `192.168.2` subnet and must be able to contact the administration computer. In our example, assume the gateway has the IP address `192.168.2.1`.

The *Installation: Partitioning* screen is displayed.

13. **Confirm the warning message to start the installation.**
Please read the warning carefully. After confirming, all existing data on the PC will be destroyed.

    If you want to cancel the installation and reboot instead, select *No*.

    Caution – The installation process will delete all data on the hard disk drive.

    The software installation process can take up to a couple of minutes.

    The *Installation Finished* screen is displayed.

14. **Remove the CD-ROM, connect to the internal network, and reboot the system.**
When the installation process is complete, remove the CD-ROM from the drive and connect the `eth0` network card to the internal network. Except for the internal network card (`eth0`), the sequence of network cards normally will be determined by PCI ID and by the kernel drivers. The sequence of network card names may also change if the hardware configuration is changed, especially if network cards are removed or added.

    Then press Enter in the installation screen to reboot UTM. During the boot process, the IP addresses of the internal network cards are changed. The installation routine console (Alt+F1) may display the message "No IP on eth0" during this time.

After Sophos UTM has rebooted (a process which, depending on your hardware, can take several minutes), ping the IP address of the `eth0` interface to ensure it is reachable. If no connection is possible, please check if one of the following problems is present:

- The IP address of Sophos UTM is incorrect.
- The IP address of the administrative computer is incorrect.
- The default gateway on the client is incorrect.
- The network cable is connected to the wrong network card.
- All network cards are connected to the same hub.

1.4 Basic Configuration

The second step of the installation is performed through WebAdmin, the web based administrative interface of Sophos UTM. Prior to configuring basic system settings, you should have a

plan how to integrate Sophos UTM into your network. You must decide which functions you want it to provide, for example, if you want to operate it in bridge mode or in standard (routing) mode, or how you want it to control the data packets flowing between its interfaces. However, you can always reconfigure Sophos UTM at a later time. So if you do not have planned how to integrate Sophos UTM into your network yet, you can begin with the basic configuration right away.

1. **Start your browser and open WebAdmin.**
   Browse to the URL of Sophos UTM (i.e., the IP address of eth0). In order to stay consistent with our configuration example above, this would be `https://192.168.2.100:4444` (note the HTTPS protocol and port number 4444).

   Deviating from the configuration example, each Sophos UTM ships with the following default settings:

   - **Interfaces:** Internal network interface (eth0)
   - **IP address:** 192.168.0.1
   - **Network mask:** 255.255.255.0
   - **Default gateway:** none

   To access WebAdmin of any Sophos UTM, enter the following URL instead:

   `https://192.168.0.1:4444`

   To provide authentication and encrypted communication, Sophos UTM comes with a self-signed security certificate. This certificate is offered to the web browser when an HTTPS-based connection to WebAdmin is established. For being unable to check the certificate's validity, the browser will display a security warning. Once you have accepted the certificate, the initial login page is displayed.

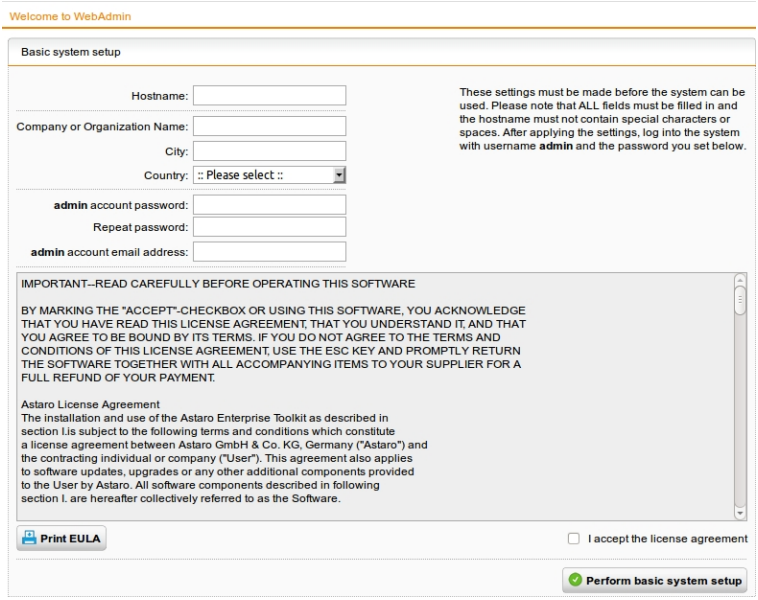

Figure 1 WebAdmin: Initial Login Page

2. **Fill out the Basic System Setup form.**
   Enter accurate information of your company in the text boxes presented here. In addition, specify a password and valid email address for the administrator account. If you accept the license agreement, click the *Perform Basic System Setup* button to continue logging in. While performing the basic system setup, a number of certificates and certificate authorities are being created:

   - **WebAdmin CA:** The CA with which the WebAdmin certificate was signed (see *Management* > *WebAdmin Settings* > *HTTPS Certificate*).
   - **VPN Signing CA:** The CA with which digital certificates are signed that are used for VPN connections (see *Site-to-site VPN* > *Certificate Management* > *Certificate Authority*).
   - **WebAdmin Certificate:** The digital certificate of WebAdmin (see *Site-to-site VPN* > *Certificate Management* > *Certificates*).
   - **Local X.509 Certificate:** The digital certificate of Sophos UTM that is used for VPN connections (see *Site-to-Site VPN* > *Certificate Management* > *Certificates*).

The login page appears. (With some browsers it may, however, happen that you are presented another security warning because the certificate has changed according to your entered values.)

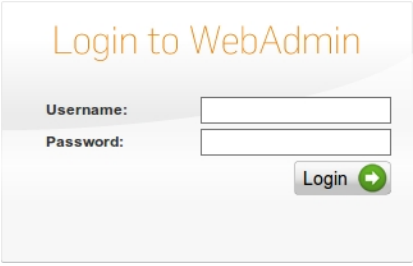

Figure 2 WebAdmin: Regular Login Page

3. **Log into WebAdmin.**
   Type `admin` in the *Username* field and enter the password you have specified on the previous screen.

   A configuration wizard is presented to you which will guide you through the initial configuration process.

   Continue: If you want to use the wizard, select this option and then click *Next*. Follow the steps to configure the basic settings of Sophos UTM.

   Restore a backup: If you have a backup file, you can decide to restore this backup file instead. Select this option and then click *Next*. How to continue is described in section *Backup Restoration*.

   Alternatively, you can safely click *Cancel* (at any time during the wizard's steps) and thereby exit the wizard, for example if you want to configure Sophos UTM directly in WebAdmin. You can also click *Finish* at any time to save your settings done so far and exit the wizard.

4. **Install your license.**
   Click the Folder icon to upload your purchased license (a text file). Click *Next* to install the license. In case you did not purchase a license, click *Next* to use the built-in 30-day trial license with all features enabled that is shipped with Sophos UTM.

   Note – If the selected license does not contain a certain subscription, the respective page will be disabled during the further procedure.

5. **Configure the internal network interface.**
   Check the presented settings for the internal network interface (*eth0*). The settings for this interface are based on the information you provided during the installation of the software. Additionally, you can set Sophos UTM to act as DHCP server on the internal interface by selecting the checkbox.

   Note – If you change the IP address of the internal interface, you must connect to WebAdmin again using the new IP address after finishing the wizard.

6. **Select the uplink type for the external interface.**
   Select the connection type of your uplink/Internet connection the external network card is going to use. The type of interface and its configuration depend on what kind of connection to the Internet you are going to use. Click *Next*.

   In case Sophos UTM has no uplink or you do not want to configure it right now, select the *Setup Internet connection later* checkbox. If you configure an Internet uplink, IP masquerading will automatically be configured for connections from the internal network to the Internet.

   If you select *Standard Ethernet interface with static IP address*, specifying a *Default gateway* is optional. If you leave the text box blank, your default gateway setting of the installation routine will persist. You can skip each of the following steps by clicking *Next*. You can make and change those skipped settings later in WebAdmin.

   Note – If your license does not allow one of the following features, the concerning feature will not be displayed.

7. **Make your basic firewall settings.**
   You can now select what types of services you want to allow on the Internet. Click *Next* to confirm your settings.
8. **Make your advanced threat protection settings.**
   You can now make settings regarding intrusion prevention and command&control/botnet detection for several operation systems and databases. Click *Next* to confirm your settings.
9. **Make your web protection settings.**

You can now select whether the web traffic should be scanned for viruses and spyware. Additionally, you can select to block webpages that belong to certain categories. Click *Next* to confirm your settings.

10. **Make your email protection settings.**
    You can now select the first checkbox to enable the POP3 proxy. You can also select the second checkbox to enable UTM as inbound SMTP relay: Enter the IP address of your internal mail server and add SMTP domains to route. Click *Next* to confirm your settings.

11. **Make your wireless protection settings.**
    You can now select the checkbox to enable wireless protection. In the box, select or add the interfaces that are allowed to connect your wireless access points to your system. Click the Folder icon to add an interface or click the Plus icon to create a new interface. Enter the other wireless network parameters. Click *Next* to confirm your settings.

12. **Make your advanced threat adaptive learning settings.**
    You can now select if you want to send anonymous data to the Sophos research team. This data is used to improve future versions and to improve and enlarge the network visibility and application control library.

13. **Confirm your settings.**
    A summary of your settings is displayed. Click *Finish* to confirm them or *Back* to change them. However, you can also change them in WebAdmin later.

    After clicking *Finish* your settings are saved and you are redirected to the Dashboard of WebAdmin, providing you with the most important system status information of the Sophos UTM unit.

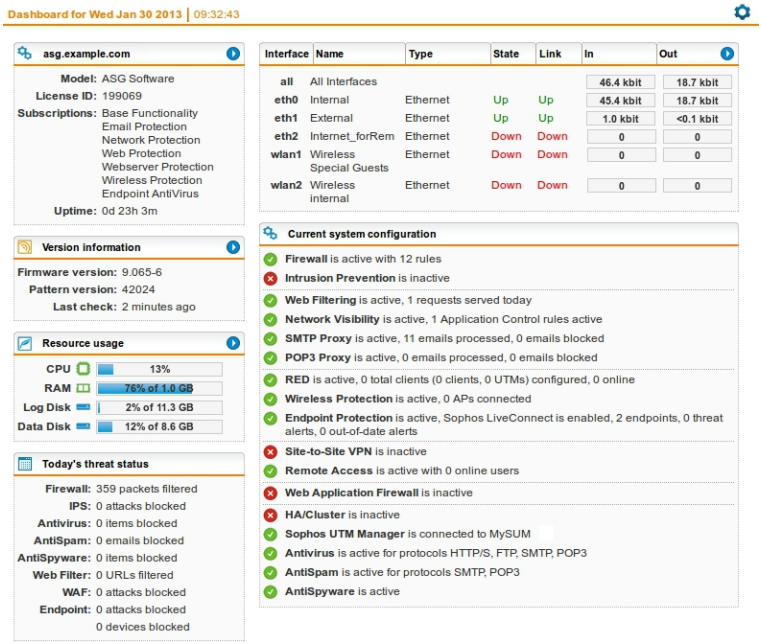

Figure 3 WebAdmin: Dashboard

If you encounter any problems while completing these steps, please contact the support department of your Sophos UTM supplier. For more information, you might also want to visit the following websites:

- Sophos UTM Support Forum
- Sophos Knowledgebase

1.5 Backup Restoration

The WebAdmin configuration wizard (see section *Basic Configuration*) allows you to restore an existing backup file instead of going through the basic configuration process. Do the following:

1. **Select *Restore existing backup file* in the configuration wizard.**
   Select *Restore existing backup file* in the configuration wizard and click *Next*.

   You are directed to the upload page.

2. **Upload the backup**.
   Click the Folder icon, select the backup file you want to restore, and click *Start Upload*.
3. **Restore the backup**.
   Click *Finish* to restore the backup.

Important Note – You will not be able to use the configuration wizard afterwards.

As soon as the backup has been restored successfully you will be redirected to the login page.

2 WebAdmin

WebAdmin is the web-based administrative interface that allows you to configure every aspect of Sophos UTM. WebAdmin consists of a menu and pages, many of which have multiple tabs. The menu on the left of the screen organizes the features of Sophos UTM in a logical manner. When you select a menu item, such as *Network Protection*, it expands to reveal a submenu and the associated page opens. Note that for some menu items no page is associated. Then, the page of the previously selected menu or submenu item keeps being displayed. You have to select one of the submenu items, which opens the associated page at its first tab.

On the first start of the WebAdmin the *Setup Wizard* appears unique. Follow the instructions to set up the most important settings.

The procedures in this documentation direct you to a page by specifying the menu item, sub-menu item, and the tab, for example: "On the *Interfaces & Routing* > *Interfaces* > *Hardware* tab, configure ..."

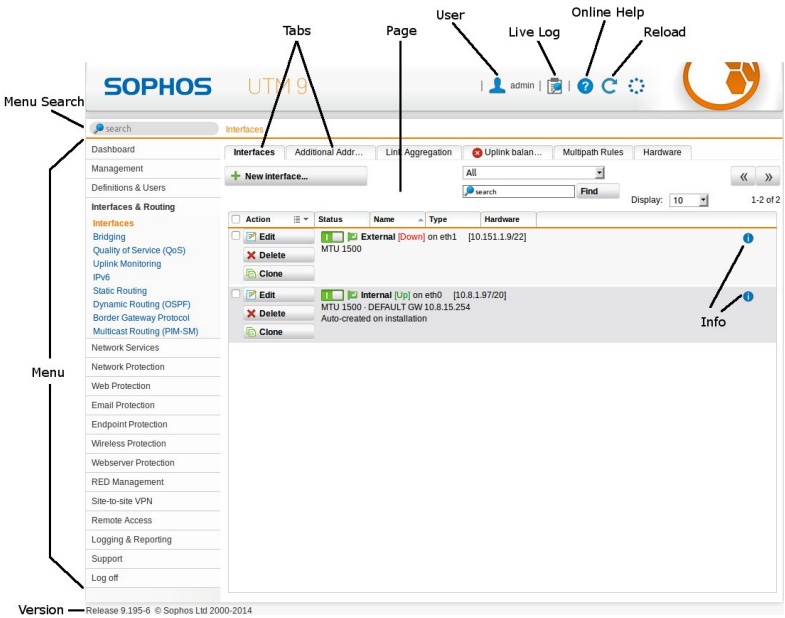

Figure 4 WebAdmin: Overview

2.1 WebAdmin Menu

The WebAdmin menu provides access to all configuration options of Sophos UTM, that is, there is no need for using a command line interface to configure specific parameters.

- **Dashboard:** The Dashboard graphically displays a snapshot of the current operating status of the Sophos UTM unit.
- **Management:** Configure basic system and WebAdmin settings as well as all settings that concern the configuration of the Sophos UTM unit.
- **Definitions & Users:** Configure network, service, and time period definitions as well as user accounts, user groups, and external authentication services for use with the Sophos UTM unit.
- **Interfaces & Routing:** Configure system facilities such as network interfaces as well as routing options, among other things.
- **Network Services:** Configure network services such as DNS and DHCP, among other things.
- **Network Protection:** Configure basic network protection features such as firewall rules, voice over IP, or intrusion prevention settings.
- **Web Protection:** Configure the Web Filter and application control of Sophos UTM unit as well as the FTP proxy.
- **Email Protection:** Configure the SMTP and POP3 proxies of the Sophos UTM unit as well as email encryption.
- **Endpoint Protection:** Configure and manage the protection of endpoint devices in your network.
- **Wireless Protection:** Configure wireless access points for the gateway.
- **Webserver Protection:** Protect your webservers from attacks like cross-site scripting and SQL injection.
- **RED Management:** Configure your remote Ethernet device (RED) appliances.
- **Site-to-site VPN:** Configure site-to-site Virtual Private Networks.
- **Remote Access:** Configure remote access VPN connections to the Sophos UTM unit.

- **Logging & Reporting:** View log messages and statistics about the utilization of the Sophos UTM unit and configure settings for logging and reporting.
- **Support:** Access to the support tools available at the Sophos UTM unit.
- **Log Off:** Log out of the user interface.

Searching the Menu

Above the menu a search box is located. It lets you search the menu for keywords in order to easily find menus concerning a certain subject. The search function matches the name of menus but additionally allows for hidden indexed aliases and keywords.

As soon as you start typing into the search box, the menu automatically reduces to relevant menu entries only. You can leave the search box at any time and click the menu entry matching your prospect. The reduced menu stays intact, displaying the search results, until you click the reset button next to it.

Tip – You can set focus on the search box via the keyboard shortcut `CTRL+Y`.

2.2 Button Bar

The buttons in the upper right corner of WebAdmin provide access to the following features:

- **Username/IP:** Shows the currently logged in user and the IP address from which WebAdmin is accessed. If other users are currently logged in, their data will be shown, too.
- **Open Live Log:** Clicking this button opens the live log that is associated with the WebAdmin menu or tab you are currently on. To see a different live log without having to change the menu or tab, hover over the Live Log button. After some seconds a list of all available live logs opens where you can select a live log to display. Your selection is memorized as long as you stay on the same WebAdmin menu or tab.

  Tip – You can also open live logs via the *Open Live Log* buttons provided on multiple WebAdmin pages.

- **Online Help:** Every menu, submenu, and tab has an online help screen that provides context-sensitive information and procedures related to the controls of the current

WebAdmin page.

Note – The online help is version-based and updated by means of patterns. If you update to a new firmware version, your online help will also be updated, if available.

- **Reload:** To request the already displayed WebAdmin page again, always click the *Reload* button.

Note – Never use the reload button of the browser, because otherwise you will be logged out of WebAdmin.

2.3 Lists

Many pages in WebAdmin consist of lists. The buttons on the left of each list item enable you to edit, delete, or clone the item (for more information see section *Buttons and Icons*). To add an item to the list, click the *New …* button, where "…" is a placeholder for the object being created (e.g., interface). This opens a dialog box where you can define the properties of the new object.

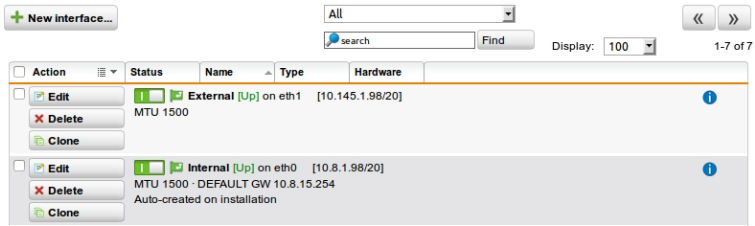

Figure 5 WebAdmin: Example of a List

With the first drop-down list on the top you can filter all items according to their type or group. The second field on the top lets you search for items specifically. Enter a search string and click *Find*.

Lists with more than ten items are split into several chunks, which can be browsed with Forward (>>) and Backward (<<) buttons. With the *Display* drop-down list, you can temporarily change the number of items per page. Additionally, you can change the default setting for all lists on the *Management* > *WebAdmin Settings* > *User Preferences* tab.

The header of a list provides some functionality. Normally, clicking a header field sorts the list for that object field of that name, e.g. clicking the field *Name* sorts the list by the objects' names. The

Action field in the header contains some batch options you can carry out on previously selected list objects. To select objects, select their checkbox. Note that the selection stays valid across multiple pages, that is, while browsing between pages of a list already selected objects stay selected.

Tip – Clicking on the Info icon will show all configuration options in which the object is used.

2.4 Searching in Lists

A filter field helps you to quickly reduce the number of items displayed in a list. This makes it much easier to find the object(s) you were looking for.

Important Facts

- A search in a list typically scans several fields for the search expression. A search in `Users & Groups` for example considers the username, the real name, the comment, and the first email address. Generally speaking, the search considers all texts which you can see in the list, excluding details displayed via the Info icon.
- The list search is case-insensitive. That means it makes no difference whether you enter upper- or lower-case letters. The search result will contain matches both with upper-case and lower-case letters. Searching explicitly for upper-case or lower-case letters is not possible.
- The list search is based on Perl regular expression syntax (although case-insensitive). Typical search expressions known from e.g. text editors like * and ? as simple wildcard characters or the AND and OR operators *do not* work in list search.

Examples

The following list is a small selection of useful search strings:

Simple string: Matches all words that contain the given string. For example, "inter" matches "Internet", "interface", and "printer".

Beginning of a word: Mark the search expression with a `\b` at the beginning. For example, `\binter` matches "Internet" and "interface" but not "printer".

End of a word: Mark the search expression with a `\b` at the end. For example, `http\b` matches "http" but not "https".

Beginning of an entry: Mark the search expression with a `^` at the beginning. For example, `^inter` matches "Internet Uplink" but not "Uplink Interfaces".

IP addresses: Searching for IP addresses, you need to escape dots with a backslash. For example, `192\.168` matches "192.168".
To search more generally for IP addresses use `\d` which matches any digit. `\d+` matches multiple digits in a row. For example, `\d+\.\d+\.\d+\.\d+` matches any IPv4 address.

Note – It makes sense to rather use an easy, fail-safe search expression which will lead to more matches than to rack your brains for a supposedly more perfect one which can easily lead to unexpected results and wrong conclusions.

You can find a detailed description of regular expressions and their usage in Sophos UTM in the Sophos Knowledgebase.

2.5 Dialog Boxes

Dialog boxes are special windows which are used by WebAdmin to prompt you for entering specific information. The example shows a dialog box for creating a new static route in the *Interfaces & Routing* > *Static Routing* menu.

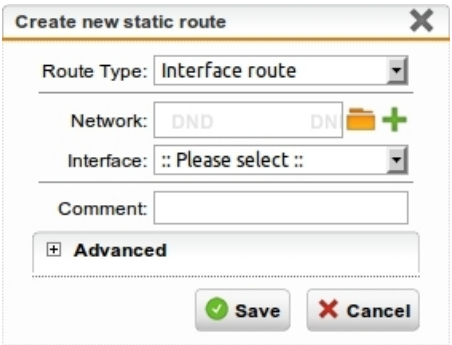

Figure 6 WebAdmin: Example of a Dialog Box

Each dialog box can consist of various widgets such as text boxes, checkboxes, and so on. In addition, many dialog boxes offer a drag-and-drop functionality, which is indicated by a special

background reading *DND*. Whenever you encounter such a box, you can drag an object into the box. To open the object list from where to drag the objects, click the Folder icon that is located right next to the text box. Depending on the configuration option, this opens the list of available networks, interfaces, users/groups, or services. Clicking the green Plus icon opens a dialog window letting you create a new definition. Some widgets that are not necessary for a certain configuration are grayed out. In some cases, however, they can still be edited, but having no effect.

Note – You may have noticed the presence of both *Save* and *Apply* buttons in WebAdmin. The *Save* button is used in the context of creating or editing objects in WebAdmin such as static routes or network definitions. It is always accompanied by a *Cancel* button. The *Apply* button, on the other hand, serves to confirm your settings in the backend, thus promptly activating them.

2.6 Buttons and Icons

WebAdmin has some buttons and functional icons whose usage is described here.

Buttons	Meaning
View	Shows a dialog box with detailed information on the object.
Edit	Opens a dialog box to edit properties of the object.
Delete	Deletes the object. If an object is still in use somewhere, there will be a warning. Not all objects can be deleted if they are in use.
Clone	Opens a dialog box for creating an object with identical settings/properties. Helps you to create similar objects without having to type all identical settings over and over again.

Functional Icons	Meaning
	**Info:** Shows all configurations where the object is in use.
	**Details:** Links to another WebAdmin page with more information about the topic.
	**Toggle switch:** Enables or disables a function. Green when enabled, gray when disabled, and amber when configuration is required before enabling.

Functional Icons	Meaning
	Folder: Has two different functions: (1) Opens an object list (see section below) on the left side where you can choose appropriate objects from. (2) Opens a dialog window to upload a file.
	**Plus:** Opens a dialog window to add a new object of the required type.
	Action: Opens a drop-down menu with actions. The actions depend on the location of the icon: (1) Icon in list header: the actions, e.g., *Enable*, *Disable*, *Delete*, apply to the selected list objects. (2) Icon in text box: with the actions *Import* and *Export* you can import or export text, and with *Empty* you delete the entire content. There is also a filter field which helps you to drill down a list to relevant elements. Note that the filter is case-sensitive.
	**Empty:** Removes an object from the current configuration when located in front of the object. Removes all objects from a box when located in the *Actions* menu. Objects are however never deleted.
	**Import:** Opens a dialog window to import text with more than one item or line. Enhances adding multiple items without having to type them individually, e.g. a large blacklist to the URL blacklist. Copy the text from anywhere and enter it using `CTRL+V`.
	**Export:** Opens a dialog window to export all existing items. You can select a delimiter to separate the items, which can either be new line, colon, or comma. To export the items as text, mark the whole text in the *Exported Text* field and press `CTRL+C` to copy it. You can then paste it into all common applications using `CTRL+V`, for example a text editor.
	**Sort:** Using these two arrows, you can sort list elements by moving an element down or up, respectively.
	**Forward/Backward:** Depending on the location you can navigate through the pages of a long list, or move back and forth along the history of changes and settings.
	**PDF:** Saves the current view of data in a PDF file and then opens a dialog window to download the created file.
	**CSV:** Saves the current view of data in a CSV (comma-separated values) file and then opens a dialog window to download the created file.

2.7 Object Lists

An object list is a drag-and-drop list which is temporarily displayed on the left side of WebAdmin, covering the main menu.

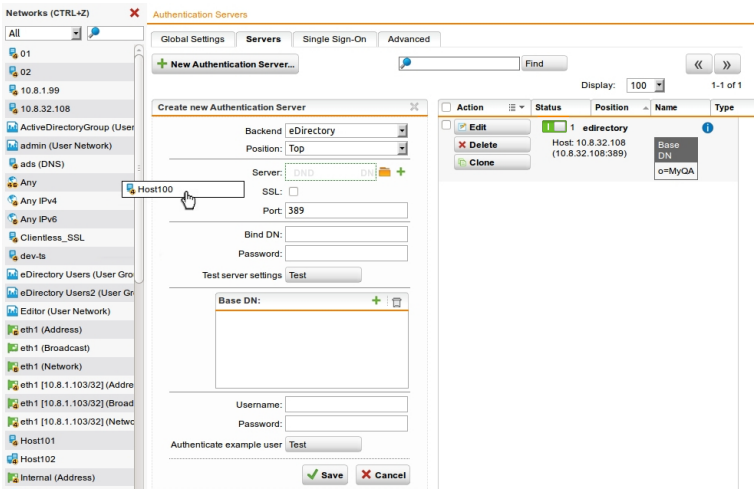

Figure 7 WebAdmin: Dragging an Object From the Object List *Networks*

An object list is opened automatically when you click the Folder icon (see section above), or you can open it manually via a keyboard shortcut (see *Management* > *WebAdmin Settings* > *User Preferences*).

The object list gives you quick access to WebAdmin objects like users/groups, interfaces, networks, and services to be able to select them for configuration purposes. Objects are selected simply by dragging and dropping them onto the current configuration.

According to the different existing object types, there are five different types of object lists. Clicking the Folder icon will always open the type required by the current configuration.

3 Dashboard

The Dashboard graphically displays a snapshot of the current operating status of Sophos UTM.

The Dashboard displays by default when you log in to WebAdmin and shows the following information:

Hint – Clicking the Dashboard Settings icon on the top right opens a dialog window where you can, amongst others, configure which topic sections are displayed.

- **General Information:** Hostname, model, license ID, subscriptions, and uptime of the unit. The display color of a subscription switches to orange 30 days before its expiration date. During the last 7 days and after expiration, a subscription is displayed in red.
- **Version Information:** Information on the currently installed firmware and pattern versions as well as available updates.
- **Resource Usage:** Current system utilization, including the following components:
  - The CPU utilization in percent
  - The RAM utilization in percent. Please note that the total memory displayed is the part that is usable by the operating system. With 32-bit systems, in some cases that does not represent the actual size of the physical memory installed, as part of it is reserved for hardware.
  - The amount of hard disk space consumed by the log partition in percent
  - The amount of hard disk space consumed by the root partition in percent
  - The status of the UPS (uninterruptible power supply) module (if available)
- **Today's Threat Status:** A counter for the most relevant security threats detected since midnight:
  - The total of dropped and rejected data packets for which logging is enabled
  - The total of blocked intrusion attempts
  - The total of blocked viruses (all proxies)
  - The total of blocked spam messages (SMTP/POP3)
  - The total of blocked spyware (all proxies)

- The total of blocked URLs (HTTP/S)
- The total of blocked webserver attacks (WAF)

- **Interfaces:** Name and status of configured network interface cards. In addition, information on the average bit rate of the last 75 seconds for both incoming and outgoing traffic is shown. The values presented are obtained from bit rate averages based on samples that were taken at intervals of 15 seconds. Clicking a traffic value of an interface opens a Flow Monitor in a new window. The Flow Monitor displays the traffic of the last ten minutes and refreshes automatically at short intervals. For more information on the Flow Monitor see chapter *Flow Monitor*.
- **Advanced Threat Protection:** Status of Advanced Threat Protection. The display shows if Advanced Threat Protection is enabled and it shows a counter of infected hosts.
- **Current System Configuration:** Enabled/disabled representation of the most relevant security features. Clicking one of the entries opens the WebAdmin page with the respective settings:
  - **Firewall:** Information about the total of active firewall rules.
  - **Intrusion Prevention:** The intrusion prevention system (IPS) recognizes attacks by means of a signature-based IPS rule set.
  - **Web Filtering:** An application-level gateway for the HTTP/S protocol, featuring a rich set of web filtering techniques for the networks that are allowed to use its services.
  - **Network Visibility:** Sophos' layer 7 application control allows to categorize and control network traffic.
  - **SMTP Proxy:** An application-level gateway for messages sent via the *Simple Mail Transfer Protocol* (SMTP).
  - **POP3 Proxy:** An application-level gateway for messages sent via the *Post Office Protocol 3* (POP3).
  - **RED:** Configuration of Remote Ethernet Device (RED) appliances for branch office security.
  - **Wireless Protection:** Configuration of wireless networks and access points.
  - **Endpoint Protection:** Management of endpoint devices in your network. Displays the number of connected endpoints and alerts.
  - **Site-to-Site VPN:** Configuration of site-to-site VPN scenarios.
  - **Remote Access:** Configuration of road warrior VPN scenarios.

- **Web Application Firewall:** An application-level gateway to protect your web-servers from attacks like cross-site scripting and SQL injection.
- **HA/Cluster:** High availability (HA) failover and clustering, that is, the distribution of processing-intensive tasks such as content filtering, virus scanning, intrusion detection, or decryption equally among multiple cluster nodes.
- **Sophos UTM Manager:** Management of your Sophos UTM appliance via the central management tool Sophos UTM Manager (SUM).
- **Antivirus:** Protection of your network from web traffic that carries harmful and dangerous content such as viruses, worms, or other malware.
- **Antispam:** Detection of unsolicited spam emails and identification of spam transmissions from known or suspected spam purveyors.
- **Antispyware:** Protection from spyware infections by means of two different virus scanning engines with constantly updated signature databases and spyware filtering techniques that protects both inbound and outbound traffic.

3.1 Dashboard Settings

You can modify several settings concerning the Dashboard. Click the Dashboard Settings icon on the top right of the Dashboard to open the *Edit Dashboard Settings* dialog window.

Refresh dashboard: By default, the Dashboard is updated at intervals of five seconds. You can configure the refresh rate from *Never* to *60 seconds*.

Left Column – Right Column: The Dashboard is divided into different topic sections providing information on the respective topic. With the two boxes *Left Column* and *Right Column* you can arrange those topic sections and add or remove them from display. Those settings will then be reflected by the Dashboard. Use the Sort icons to sort the topic sections of a column. To add or remove a particular topic section from display, select or unselect its checkbox.

The topic sections displayed by default are described in the Dashboard chapter. There are some additional topic sections which can be displayed and which are described here:

- **Web Protection: Top Apps:** Overview of the most used applications. In this section, hovering the cursor on an application displays one or two icons with additional functionality:
  - Click the *Block* icon to block the respective application from now on. This will create a rule on the *Application Control Rules* page. This option is unavailable for

applications relevant to the flawless operation of Sophos UTM. WebAdmin traffic, for example, cannot be blocked as this might lead to shutting yourself out of WebAdmin. Unclassified traffic cannot be blocked, either.

- Click the *Shape* icon to enable traffic shaping of the respective application. A dialog window opens where you are asked to define the rule settings. Click *Save* when you are done. This will create a rule both on the *Traffic Selectors* and on the *Bandwidth Pools* page.
  Traffic shaping is not available when viewing the *All Interfaces* Flow Monitor as shaping works interface-based.

- **Web Protection: Top Sites by Time:** Overview of the most visited domains according to time.
- **Web Protection: Top Sites by Traffic:** Overview of the most visited domains according to traffic.
- **Logging:** Status of the log partition of your Sophos UTM unit, including information about the disk space left and fillup rate.
- **News Feed:** News about Sophos and its products.
- **Chart: Concurrent Connections:** Daily statistics and histogram of the total of concurrent connections.
- **Chart: Log Partition Status:** Four-week statistics and histogram of the log partition usage.
- **Chart: CPU Usage:** Daily statistics and histogram of the current processor usage in percent.
- **Chart: Memory/Swap Usage:** Daily statistics and histogram of the memory and swap usage in percent.
- **Chart: Partition Usage:** Daily statistics and histogram of the usage of selected partitions in percent.

Enable autogrouping on Dashboard: Select this option to display the information on the Dashboard compactly. This option only affects the selected *Web Protection* items in the left column and the selected *Chart* items in the right column. If selected, the respective information elements will be displayed as overlaying tabs on the Dashboard. If unselected, the information elements are displayed side by side.

Click *Save* to save your settings.

3.2 Flow Monitor

The Flow Monitor of Sophos UTM is an application which gives quick access to information on network traffic currently passing the interfaces of UTM. It can be easily accessed via the Dashboard by clicking one of the interfaces at the top right. By clicking *All Interfaces* the Flow Monitor displays the traffic accumulated on all active interfaces. By clicking a single interface, the Flow Monitor displays the traffic of this interface only.

Note – The Flow Monitor opens in a new browser window. As pop-up blockers are likely to block this window it is advisable to deactivate pop-up blockers for WebAdmin.

The Flow Monitor provides two views, a chart and a table, which are described in the next sections. It refreshes every five seconds. You can click the *Pause* button to stop refreshing. After clicking *Continue* to start refreshing again, the Flow Monitor updates to the current traffic information.

Tabular View

The Flow Monitor table provides information on network traffic for the past five seconds:

#: Traffic is ranked based on its current bandwidth usage.

Application: Protocol or name of the network traffic if available. Unclassified traffic is a type of traffic unknown to the system. Clicking an application opens a window which provides information on the server, the port used, bandwidth usage per server connection, and total traffic.

Clients: Number of client connections using the application. Clicking a client opens a window which provides information on the client's IP address, bandwidth usage per client connection, and total traffic. Note that with unclassified traffic the number of clients in the table may be higher than the clients displayed in the additional information window. This is due to the fact that the term "unclassified" comprises more than one application. So, there might be only one client in the information window but three clients in the table, the latter actually being the connections of the single client to three different, unclassified applications.

Bandwidth Usage Now: The bandwidth usage during the last five seconds. Clicking a bandwidth opens a window which provides information on the download and upload rate of the application connection.

Total Traffic: The total of network traffic produced during the "lifetime" of a connection. Example 1: A download started some time in the past and still going on: the whole traffic produced during the time from the beginning of the download will be displayed. Example 2: Several clients using facebook: as long as one client keeps the connection open, the traffic produced by all clients so far adds up to the total traffic displayed.
Clicking a total traffic opens a window which provides information on the overall download and upload rate of the application connection.

Actions: Depending on the application type, there are actions available (except for unclassified traffic).

- Blocking: Click the *Block* button to block the respective application from now on. This will create a rule on the *Application Control Rules* page. This option is unavailable for applications relevant to the flawless operation of Sophos UTM. WebAdmin traffic, for example, cannot be blocked as this might lead to shutting yourself out of WebAdmin. Unclassified traffic cannot be blocked, either.
- Traffic shaping: Click the *Shape* button to enable traffic shaping of the respective application. A dialog window opens where you are asked to define the rule settings. Click *Save* when you are done. This will create a rule both on the *Traffic Selectors* and on the *Bandwidth Pools* page.
  Traffic shaping is not available when viewing the *All Interfaces* Flow Monitor as shaping works interface-based.
- Download throttling: Click the *Throttle* button to enable download throttling for the respective application. A dialog window opens where you are asked to define the rule settings. Click *Save* when you are done. This will create a rule both on the *Traffic Selectors* and on the *Download Throttling* page. Download throttling is not available when viewing the *All Interfaces* Flow Monitor as throttling works interface-based.

Chart View

The Flow Monitor chart displays the network traffic for the past ten minutes. The horizontal axis reflects time, the vertical axis reflects the amount of traffic while dynamically adapting the scale to the throughput.

At the bottom of the chart view a legend is located which refers to the type of traffic passing an interface. Each type of traffic has a different color so that it can be easily distinguished in the chart.

Note – The Flow Monitor displays much more differentiated information on traffic if Network Visibility is enabled (see chapter *Web Protection* > *Application Control* > *Network Visibility*).

When hovering the mouse cursor on a chart a big dot will appear, which gives detailed information of this part of the chart. The dot is clung to the line of the chart. As you move the mouse cursor the dot follows. In case a chart has several lines, the dot switches between them according to where you move the mouse cursor. Additionally, the dot changes its color depending on which line its information refer to, which is especially useful with lines running close to each other. The dot provides information on type and size of the traffic at the respective point of time.

4 Management

This chapter describes how to configure basic system settings as well as the settings of the web-based administrative interface of Sophos UTM, *WebAdmin*, among others. The *Overview* page shows statistics of the last WebAdmin sessions including possible changes. Click the *Show* button in the *Changelog* column to view the changes in detail.

In the *State* column, the end times of previous WebAdmin sessions are listed.

Note – You can end a WebAdmin session by clicking the *Log off* menu. If you close the browser without clicking the *Log off* menu, the session times out after the time span defined on the *Management* > *WebAdmin Settings* > *Advanced* tab.

The following topics are included in this chapter:

4.1 System Settings

The tabs under *System Settings* allow you to configure basic settings of your UTM such as hostname, date, and time.

4.1.1 Organizational

Enter the name and location of your organization and an email address to reach the person or group technically responsible for the operation of your Sophos UTM. Note that this data is also used in certificates for IPsec, email encryption and WebAdmin.

4.1.2 Hostname

Enter the hostname of your UTM as a *fully qualified domain name* (FQDN) into this field, for example `utm.example.com`. A hostname may contain alphanumeric characters, dots, and hyphens. At the end of the hostname there must be a special designator such as `com`, `org`, or `de`. The hostname will be used in notification messages to identify UTM. It will also appear in status messages sent by the Web Filter. Note that the hostname does not need to be registered in the DNS zone for your domain.

4.1.3 Time and Date

On your UTM, date and time should always be set correctly. This is needed both for getting correct information from the logging and reporting systems and to assure interoperability with other computers on the Internet.

Usually, you do not need to set the time and date manually. By default, automatic synchronization with public Internet time servers is enabled (see section *Synchronize Time with Internet Server* below).

In the rare case that you need to disable synchronization with time servers, you can change the time and date manually. However, when doing so, pay attention to the following caveats:

- Never change the system time from standard time to daylight saving time or vice versa. This change is always automatically covered by your time zone settings even if automatic synchronization with time servers is disabled.
- Never change date or time manually while synchronization with time servers is enabled, because automatic synchronization would typically undo your change right away. In case you must set the date or time manually, remember to first remove all servers from the *NTP Servers* box in the *Synchronize Time with Internet Server* section below and click *Apply*.

- After manually changing the system time, wait until you see the green confirmation message, stating that the change was successful. Then reboot the system (*Management > Shutdown/Restart*). This is highly recommended as many services rely on the fact that time is changing continuously, not abruptly. Jumps in time therefore might lead to malfunction of various services. This advice holds universally true for all kind of computer systems.
- In rare cases, changing the system time might terminate your WebAdmin session. In case this happens, log in again, check whether the time is now correctly set and restart the system afterwards.

If you operate multiple interconnected UTMs that span several time zones, select the same time zone for all devices, for example UTC (Coordinated Universal Time)—this will make log messages much easier to compare.

Note that when you manually change the system time, you will encounter several side-effects, even when having properly restarted the system:

- **Turning the clock forward**
  - Time-based reports will contain no data for the skipped hour. In most graphs, this time span will appear as a straight line in the amount of the latest recorded value.
  - Accounting reports will contain values of 0 for all variables during this time.
- **Turning the clock backward**
  - There is already log data for the corresponding time span in time-based reports.
  - Most diagrams will display the values recorded during this period as compressed.
  - The elapsed time since the last pattern check (as displayed on the Dashboard) shows the value "never", even though the last check was in fact only a few minutes ago.
  - Automatically created certificates on UTM may become invalid because the beginning of their validity periods would be in the future.
  - Accounting reports will retain the values recorded from the future time. Once the time of the reset is reached again, the accounting data will be written again as normal.

Because of these drawbacks the system time should only be set once when setting up the system with only small adjustments being made thereafter. This especially holds true if accounting and reporting data needs to be processed further and accuracy of the data is important.

Set Date And Time

To configure the system time manually, select date and time from the respective drop-down lists. Click *Apply* to save your settings.

Set Time Zone

To change the system's time zone, select an area or a time zone from the drop-down list. Click *Apply* to save your settings.

Changing the time zone does not change the system time, but only how the time is represented in output, for example in logging and reporting data. Even if it does not disrupt services, we highly recommend to reboot afterwards to make sure that all services use the new time setting.

Synchronize Time With Internet Server

To synchronize the system time using a timeserver, select one or more NTP servers. Click *Apply* after you have finished the configuration.

NTP servers: The *NTP Server Pool* is selected by default. This network definition is linked to the big virtual cluster of public timeservers of the *pool.ntp.org* project. In case your Internet service provider operates NTP servers for customers and you have access to these servers, it is recommended to remove the *NTP Server Pool* and use your provider's servers instead. When choosing your own or your provider's servers, using more than one server is useful to improve precision and reliability. The usage of three independent servers is almost always sufficient. Adding more than three servers rarely results in additional improvements, while increasing the total server load. Using both *NTP Server Pool* and your own or your provider's servers is not recommended because it will usually neither improve precision nor reliability.

Tip – If you want client computers to be able to connect to these NTP servers, add them to the allowed networks on the *Network Services > NTP* page.

Test Configured Servers: Click this button if you want to test whether a connection to the selected NTP server(s) can be established from your device and whether it returns usable time data. This will measure the time offset between your system and the servers. Offsets should generally be well below one second if your system is configured correctly and has been operating in a stable state for some time.

Right after enabling NTP or adding other servers, it is normal to see larger offsets. To avoid large time jumps, NTP will then slowly skew the system time, such that eventually, it will become correct without any jumping. In that situation, please be patient. In particular, in this case, do *not*

restart the system. Rather, return to check about an hour later. If the offsets decrease, all is working as it should.

4.1.4 Shell Access

Secure Shell (SSH) is a command-line access mode primarily used to gain remote shell access to UTM. It is typically used for low-level maintenance or troubleshooting. To access this shell you need an SSH client, which usually comes with most Linux distributions.

Allowed Networks

Use the *Allowed networks* control to restrict access to this feature to certain networks only. Networks listed here will be able to connect to the SSH service.

Authentication

In this section you can define an authentication method for SSH access and the strictness of access. The following authentication methods are available:

- Password (default)
- Public key
- Password and public key

To use *Public Key Authentication* you need to upload the respective public key(s) into the field *Authorized keys for loginuser* for each user allowed to authenticate via their public key(s).

Allow root login: You can allow SSH access for the root user. This option is disabled by default as it leads to a higher security risk. When this option is enabled, the root user is able to login via their public key. Upload the public key(s) for the root user into the field *Authorized keys for root*.

Click *Apply* to save your settings.

Shell User Passwords

Enter passwords for the default shell accounts `root` and `loginuser`. To change the password for one out of these two accounts only, just leave both input boxes for the other account blank.

Note – To enable SSH shell access, passwords must be set initially. In addition, you can only specify passwords that adhere to the password complexity settings as configured on the *Defin-*

itions & Users > *Authentication Services* > *Advanced* tab. That is, if you have enabled complex passwords, shell user passwords must meet the same requirements.

SSH Daemon Listen Port

This option lets you change the TCP port used for SSH. By default, this is the standard SSH port `22`. To change the port, enter an appropriate value in the range from `1024` to `65535` in the *Port number* box and click *Apply*.

4.1.5 Scan Settings

Antivirus Engine Preferences

Select the antivirus engine which will be used in all single scan configurations throughout WebAdmin. In dual scan configurations, both antivirus engines will be used. Note that dual scan is not available with BasicGuard subscription. Click *Apply* to save your settings.

Advanced Threat Protection Options

Select the Send suspicious content to SophosLabs for analysis option to help improve protection. SophosLabs features a cloud-based sandbox where the behavior of suspected malware can be automatically observed and analysed. This helps ensure speedy delivery of protection updates directly to your UTM. Disabling this functionality may increase defense response time.

All submissions are sent over a secure channel and are handled according to the SophosLabs Information Security Policy.

4.1.6 Reset Configuration or Passwords

The options on the *Reset Configuration or Passwords* tab let you delete the passwords of the shell users. In addition, you can execute a factory reset, and you can reset the UTM's system ID.

Reset System Passwords

Executing the *Reset System Passwords Now* function will reset the passwords of the following users:

- root (shell user)
- loginuser (shell user)

- admin (predefined administrator account)

In addition, to halt the system, select the *Shutdown system afterwards* option.

Security Note – The next person connecting to the WebAdmin will be presented an *Admin Password Setup* dialog window. Thus, after resetting the passwords, you should usually quickly log out, reload the page in your browser, and set a new admin password.

Besides, shell access will not be possible anymore until you set new shell passwords on the *Management > System Settings >* *Shell Access* tab.

Factory Reset

The *Run Factory Reset Now* function resets the device back to the factory default configuration. The following data will be deleted:

- System configuration
- Web Filter cache
- Logs and reporting data
- Databases
- Update packages
- Licenses
- Passwords
- High availability status

However, the version number of Sophos UTM Software will remain the same, that is, all firmware and pattern updates that have been installed will be retained.

Note – Sophos UTM will shut down once a factory reset has been initiated.

UTM ID Reset

With the *Reset UTM ID Now* function you reset the system ID of the UTM to a new, random value. This is for example relevant when you use endpoint protection. Every UTM using endpoint protection identifies itself on Sophos LiveConnect with its unique system ID. When you for example clone a virtual UTM using endpoint protection and want the clone to use it too, you need to reset the cloned UTM's system ID so that it can afterwards identify with the new system ID. During the reset, if turned on, endpoint protection will be turned off.

Note – Endpoints are connected to their UTM using the UTM system ID. If you reset the UTM system ID and there is no other UTM listening on the old UTM ID, their endpoints will need to be reinstalled.

Note – If a UTM is connected to Sophos UTM Manager, and you reset its UTM system ID, the UTM will connect as a new device. If necessary, you can merge the two devices.

4.2 WebAdmin Settings

The tabs under *Management* > *WebAdmin Settings* allow you to configure basic WebAdmin settings such as access control, the TCP port, user preferences, and the WebAdmin language, among other things.

4.2.1 General

On the *WebAdmin Settings* > *General* tab you can configure the WebAdmin language and basic access settings.

WebAdmin Language

Select the language of WebAdmin. The selected language will also be used for some WebAdmin output, e.g., email notifications or the executive report. Note that this setting is global and applies to all users. Click *Apply* to save your settings.

After changing the language, it might be necessary to empty your browser cache to make sure that all texts are displayed in the correct language.

WebAdmin Access Configuration

Here you can configure which users and/or networks should have access to WebAdmin.

Allowed administrators: Sophos UTM can be administered by multiple administrators simultaneously. In the *Allowed administrators* box you can specify which users or groups should have unlimited read and write access to the WebAdmin interface. By default, this is the group of *SuperAdmins*. How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.

Allowed networks: The *Allowed networks* box lets you define the networks that should be able to connect to the WebAdmin interface. For the sake of a smooth installation of UTM, the

default is `Any`. This means that the WebAdmin interface can be accessed from everywhere. Change this setting to your internal network(s) as soon as possible. The most secure solution, however, would be to limit the access to only one administrator PC through HTTPS. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Log access traffic: If you want to log all WebAdmin access activities in the firewall log, select the *Log access traffic* checkbox.

4.2.2 Access Control

On the *WebAdmin Settings > Access Control* tab you can create WebAdmin roles for specific users. This allows for a fine-grained definition of the rights a WebAdmin user can have.

There are two user roles predefined:

Auditor: Users having this role can view logging and reporting data.

Readonly: Users having this role can view everything in WebAdmin without being able to edit, create, or delete anything.

To assign users or groups one of these roles, click the *Edit* button and add the respective user (s) or group(s) to the *Members* box.

You can create further roles, according to your security policies. Do the following:

1. **On the *Access Control* tab, click *New Role*.**
   The *Create Role* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this definition.

   Members: Add or select users or groups who are to have this role. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

   Grant read-only access (optional): Select this checkbox to grant read-only access to all areas of WebAdmin to the given members.

   Rights: This box contains different rights levels for the different functions of WebAdmin: auditor and manager. A manager has full administration rights for the respective function (s), whereas an auditor has only viewing rights. You can choose one or more rights by selecting the respective checkbox in front of a right.
   Example: You could give the user Jon Doe manager rights for Email Protection and

additionally select the checkbox *Grant read-only access*. He would then be able to change settings in the Email Protection section and view all other areas of WebAdmin without being able to change anything there.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   Your settings will be saved.

To either edit or delete a role, click the corresponding buttons. Note that the *Auditor* and *Readonly* roles cannot be deleted.

4.2.3 HTTPS Certificate

On the *Management* > *WebAdmin Settings* > *HTTPS Certificate* tab you can import the WebAdmin CA certificate into your browser, regenerate the WebAdmin certificate, or choose a signed certificate to use for WebAdmin and User Portal.

During the initial setup of the WebAdmin access you have automatically created a local CA certificate on UTM. The public key of this CA certificate can be installed into your browser to get rid of the security warnings when accessing the WebAdmin interface.

To import the CA certificate, proceed as follows:

1. **On the *HTTPS Certificate* tab, click *Import CA Certificate*.**
   The public key of the CA certificate will be exported.

   You can either save it to disk or install it into your browser.

2. **Install the certificate** (optional).
   The browser will open a dialog box letting you choose to install the certificate immediately.

Note – Due to different system times and time zones the certificate might not be valid directly after its creation. In this case, most browsers will report that the certificate has expired, which is not correct. However, the certificate will automatically become valid after a maximum of 24 hours and will stay valid for 27 years.

Re-generate WebAdmin Certificate

The WebAdmin certificate refers to the hostname you have specified during the initial login. If the hostname has been changed in the meantime, the browser will display a security warning. To avoid this, you can create a certificate taking the new hostname into account. For that purpose, enter the hostname as desired and click *Apply*. Note that due to the certificate change, to

be able to continue working in WebAdmin, you probably need to reload the page via your web browser, accept the new certificate, and log back into WebAdmin.

Choose WebAdmin/User Portal Certificate

If you do not want to import the CA certificate but instead use your own signed certificate for WebAdmin and User Portal, you can select it here. However, for the certificate to be selectable from the drop-down list, you need to upload it first on the *Remote Access* > *Certificate Management* > *Certificates* tab in PKCS#12 format, containing the certificate, its CA and its private key. To use the uploaded certificate, select it from the *Certificates* drop-down list and click *Apply*.

4.2.4 User Preferences

On the *Management* > *WebAdmin Settings* > *User Preferences* tab you can configure some user preferences such as global shortcuts and items per page for the currently logged in user.

WebAdmin Shortcuts Configuration

Here you can configure keyboard shortcuts to open and close the drag-and-drop object lists used in many configurations (for more information see *WebAdmin* > *Object Lists*) or to set the cursor focus on the menu search box (see also *WebAdmin* > *WebAdmin Menu*). Use the drop-down list to select a different modifier key and the text box to enter a different character. You can also turn off the keyboard shortcut by selecting *Off* from the drop-down list.

If you want to return to the default settings, click the *Reset to Defaults* button. Click *Apply* to save your settings.

Table Pager Options

Here you can globally define the pagination of tables for WebAdmin, i.e. how many items are displayed per page. Click the drop-down list and select a value. Click *Apply* to save your settings.

WebAdmin Browser Title Customization

Here you can change the label which is displayed on the WebAdmin browser window or tab. You can enter plain text and/or use the following variables:

- %h: hostname
- %u: username
- %i: remote IP address

The default setting is `WebAdmin - User %u - Device %h` which translates for example into *WebAdmin - User admin - Device my_gateway.example.com*. Click *Apply* to save your settings.

4.2.5 Advanced

WebAdmin Idle Timeout

Log Out After: In this field you can specify the period of time (in seconds) how long a WebAdmin session can remain idle before the administrator is forced to log in again. By default, the idle timeout is set to 1,800 seconds. The range is from 60 to 86,400 seconds.

Log Out on Dashboard: By default, when you have opened the *Dashboard* page of WebAdmin, the auto logout function is enabled. You can, however, select this option to disable the auto logout function for Dashboard only.

WebAdmin TCP Port

By default, port `4444` is used as WebAdmin TCP port. In the *TCP Port* box you can enter either `443` or any value between `1024` and `65535`. However, certain ports are reserved for other services. In particular, you can never use port `10443`, and you cannot use the same port you are using for the User Portal or for SSL remote access. Note that you must add the port number to the IP address (separated by a colon) in the browser's address bar when accessing WebAdmin, for example `https://192.168.0.1:4444`

Terms of Use

Your company policies might demand that users accept terms of use when they want to access WebAdmin. Select the checkbox *Display "Terms of Use" After Login* to enforce that users must accept the terms of use each time they log into WebAdmin. Users will then be presented the terms of use after having logged in. If they do not accept them they will be logged out again.

You can change the terms of use text according to your needs. Click *Apply* to save your settings.

Sophos Adaptive Learning

You can help improving Sophos UTM by allowing it to transfer anonymous general information of your current configuration as well as information about detected viruses, or anonymous application fingerprints to Sophos. That kind of information cannot and will not be tracked back to you. No user-specific information is collected, i.e., no user or object names, no comments, or other personalized information. However, URLs for which a virus was found will be transmitted if web filter antivirus scanning is enabled.

The information is encrypted and transmitted to Sophos using SSL. Once delivered, the data is stored in an aggregated form and made available to Sophos' software architects for making educated design decisions and thus improve future versions of Sophos UTM.

Send anonymous telematry data: If enabled, the UTM gathers the following information:

- Configuration and usage data: The system will send the following data to Sophos' servers once a week.
  - Hardware and license information (not the owner), for example:

    ```
    processor Intel(R) Core(TM)2 Duo CPU E8200 @ 2.66GHz
    memory 512MiB System Memory
    eth0 network 82545EM Gigabit Ethernet Controller
    id: UTM
    version: 9.000000
    type: virtual
    license: standard
    mode: standalone
    active_ips: 2
    system_id: 58174596-276f-39b8-854b-ffa1886e3c6c
    ```

    The system ID identifies your UTM only in the way that information of your system is not accidentally collected twice, e.g. after a re-installation.
  - Features in use (only whether they are turned on or off), for example:

    ```
    main->backup->status: 1
    main->ha->status: off
    ```
  - Amount of configured objects, for example:

    ```
    objects->interface->ethernet: 2
    objects->http->profile: 5
    ```
  - CPU, memory and swap usage values in percent over the last seven days
- Virus data: The system writes the following data into a file that will be uploaded automatically to Sophos' servers every 15 minutes.
  - Information about viruses found by web protection, for example threat name, MIME type, URL of the request, or file size.
- Intrusion prevention data: The IPS log will be checked every minute for new alerts. If there is a new alert, the following data will be sent instantly to Sophos:

- Information about the alert, for example snort rule identifier and timestamp.
- Hardware and license information (not the owner), for example CPU total and CPU usage, memory total and memory usage, SWAP total and SWAP usage, system ID, engine version and pattern version.

  The data is sent every 24 hours.

- Advanced Threat Protection data: The system generates and uploads advanced threat protection data every 30 minutes.
  - Gathered information: system ID, timestamp, Sophos threat name, source IP, destination host, detection component, detection detail, number of threats, rule identifier.

Send anonymous application accuracy telemetry data: You can help to improve the recognition and classification abilities of network visibility and application control by participating in the Sophos UTM AppAccuracy Program. If enabled, the system will collect data in form of anonymous application fingerprints and will send that to Sophos' research team. There the fingerprints will be used to identify unclassified applications and to improve and enlarge the network visibility and application control library.

4.3 Licensing

The availability of certain features on Sophos UTM is defined by licenses and subscriptions, i.e. the licenses and subscriptions you have purchased with your UTM enable you to use certain features and others not.

4.3.1 How to Obtain a License

Sophos UTM ships with a 30-day trial license with all features enabled. After expiration, you must install a valid license to further operate Sophos UTM. All licenses (including free home use licenses) are created in the MyUTM Portal.

Once you have received the activation keys by email after purchasing a UTM license, you must use these keys in order to create your license or upgrade an existing license. To activate a license, you have to log in to the MyUTM Portal and visit the license management page. At the top of the page is a form where you can cut and paste the activation key from the email into this field. For more information see the MyUTM User Guide.

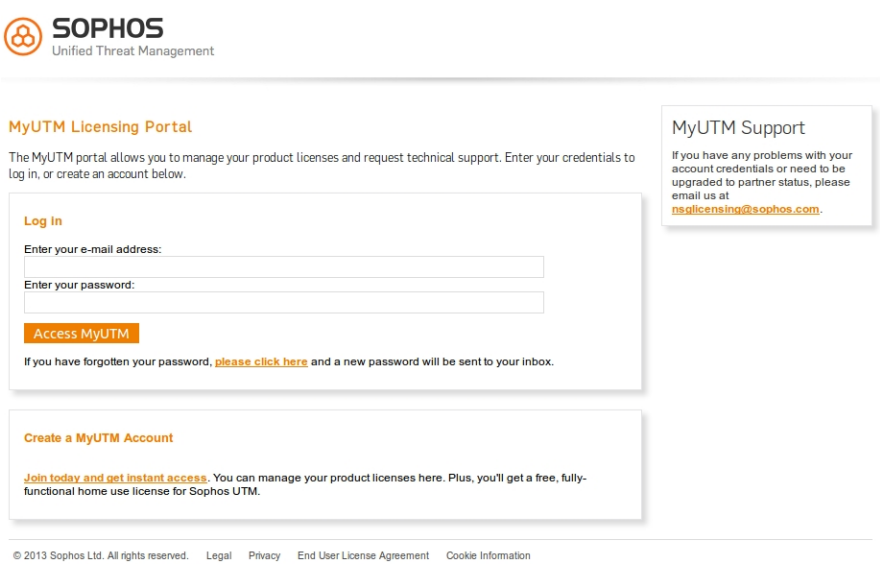

Figure 8 MyUTM Portal

Another form appears asking you to fill in information about the reseller you purchased the license from as well as your own details. The portal tries to pre-fill as much of this form as possible. Also, Sophos collects the UTM hardware serial number on this form if appropriate. After submitting this form, your license is created, and you are forwarded to the license detail page to download the license file.

To actually use the license, you must download the license file to your hard drive and then log in to your WebAdmin installation. In WebAdmin, navigate to the *Management > Licensing > Installation* tab and use the upload function to find the license text file on your hard drive. Upload the license file, and WebAdmin will process it to activate any subscriptions and other settings that the license outlines.

Note – The activation key you received by email cannot be imported into WebAdmin. This key is only used to activate the license. Only the license file can be imported to UTM.

4.3.2 Licensing Model

The modular licensing model of Sophos is very flexible. First, there is a base license, providing basic functions for free (see table below). Second, there are six additional subscriptions:

- Network Protection
- Web Protection
- Email Protection
- Endpoint Protection
- Wireless Protection
- Webserver Protection

Those can be purchased separately or in combination according to your needs. The FullGuard license contains all subscriptions. Each of the subscriptions enables certain features of the product. The table below gives you an overview which features are enabled with which subscription.

Feature	Base License	Network	Web	Email	Endpoint	Wireless	Webserver
Management (Backup, Notifications, SNMP, SUM, ...)	✔						
Local Authentication (Users, Groups)	✔						
Basic Networking (Static Routing, DHCP, DNS, Auto QoS, NTP, ...)	✔						
Firewall/NAT (DNAT, SNAT, ...)	✔						

Feature	Base License	Network	Web	Email	Endpoint	Wireless	Webserver
PPTP & L2TP Remote Access	✔						
Local Logging, standard executive reports	✔						
Intrusion Prevention (Patterns, DoS, Flood, Portscan ...)		✔					
IPsec & SSL Site-to-site VPN, IPsec & SSL Remote Access		✔					
Advanced Networking (Link Aggregation, link balancing, Policy Routing, OSPF, Multicast, custom QoS, Server Load Balancing, Generic Proxy ...)		✔	(✔)	(✔)			
User Portal		✔	✔	✔			
High Availability		✔	✔	✔			

Feature	Base License	Network	Web	Email	Endpoint	Wireless	Webserver
Remote Auth (AD, eDir, RADIUS, ...)		✔	✔	✔			
Remote Logging, advanced executive reports (archiving, configuration)		✔	✔	✔			
Basic Web Filtering & FTP Proxy			✔				
Web & FTP malware filtering			✔				
Application Control			✔				
Basic SMTP Proxy, Quarantine Report, Mail Manager				✔			
SMTP & POP3 malware filtering				✔			
Endpoint Protection, Antivirus					✔		
Endpoint Protection, Device Control					✔		

Feature	Base License	Network	Web	Email	Endpoint	Wireless	Webserver
Wireless Protection						✔	
Webserver Protection							✔

There is also a BasicGuard subscription, available for UTM appliance model 100, which offers its own subset of the above mentioned features (for more information visit the product webpage).

UTMs can also be managed and licensed by Sophos UTM Manager (SUM). In this case, the SUM provides the MSP (Managed Service Provider) license to the UTM, and the *Installation* tab is disabled. Subscriptions can only be enabled by your SUM service provider.

For more detailed information on subscriptions and their feature set please refer to your certified UTM Partner or the Sophos UTM webpage.

Missing subscriptions result in disabled tabs in WebAdmin. Above the tabs a licensing warning message is displayed.

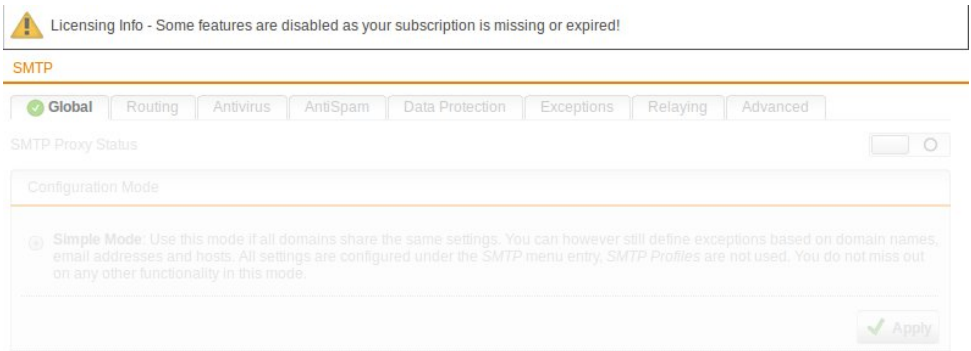

Figure 9 Licensing: Subscription Warning Message

Up2Dates

Each subscription enables full automatic update support, i.e. you will be automatically informed about new firmware updates. Also, firmware and pattern updates can be downloaded (and installed) automatically.

A base license without any subscriptions supports only limited automatic updates: solely pattern updates such as online help updates and the like will continue to be downloaded and installed automatically. You will, however, not be informed about available firmware updates, and the firmware updates have to be downloaded manually. Announcements for new firmware updates can be found in the Sophos UTM Up2Date Blog.

Support and Maintenance

The base license comes with *Web Support*. You can use the Sophos UTM Support Forum and the Sophos Knowledgebase.

As soon as you purchase one of the subscriptions you will be automatically upgraded to *Standard Support*, where you can additionally open a support case in MyUTM Portal or contact your certified UTM Partner.

There is also the possibility to purchase a *Premium Support* subscription, which offers 24/7 support with a UTM Engineer being your contact person.

4.3.3 Overview

The *Licensing* > *Overview* tab provides detailed information about your license and is divided into multiple areas:

- **Base License:** Shows basic license parameters such as ID, registration date, or type.
- **Network Protection, Email Protection, Web Protection, Webserver Protection, Wireless Protection, Endpoint AntiVirus, BasicGuard:** These sections show information for subscriptions, such as whether they have been purchased and are therefore enabled, their expiration date, and a short description of the features they provide.

  Note – When using MSP licensing, no expirations will be displayed, as licenses are managed by Sophos UTM Manager (SUM). Traditional keys and subscriptions are replaced with the SUM MSP system. For information about the managing SUM, see *Central Management* > *Sophos UTM Manager*.

- **Support Services:** Shows the support level plus the date until it is valid.

4.3.4 Installation

On the *Management* > *Licensing* > *Installation* tab you can upload and install a new license.

Note – When using MSP licensing, the tab is disabled, as licenses are managed by Sophos UTM Manager (SUM). New licenses can be installed by your SUM service provider. For information about the managing SUM, see *Central Management* > *Sophos UTM Manager*.

To install a license, proceed as follows:

1. **Open the *Upload File* dialog window.**
   Click the Folder icon next to the *License file* box.

   The *Upload File* dialog window opens.
2. **Select the license file.**
   Browse to the directory where your license file resides.

   Select the license file you want to upload.
3. **Click *Start Upload*.**
   Your license file will be uploaded.
4. **Click *Apply*.**
   Your license will be installed. Note that the new license will automatically replace any other license already installed.

   The installation of the license will take approximately 60 seconds.

4.3.5 Active IP Addresses

The free Sophos UTM Manager license allows for unlimited IP addresses.

If you do not have a license allowing unlimited users (IP addresses), this tab displays information on IP addresses covered by your license. IP addresses that exceed the scope of your license are listed separately. If the limit is exceeded you will receive an email notification at regular intervals.

Note – IP addresses not seen for a period of seven days will automatically be removed from the license counter.

4.4 Up2Date

The *Management* > *Up2Date* menu allows the configuration of the update service of Sophos UTM. Regularly installed updates keep your UTM up-to-date with the latest bug-fixes, product improvements, and virus patterns. Each update is digitally signed by Sophos—any unsigned or forged update will be rejected.

There are two types of updates available:

- **Firmware updates:** A firmware update contains bug-fixes and feature enhancements for Sophos UTM Software.
- **Pattern updates:** A pattern update keeps the antivirus, antispam, intrusion prevention definitions as well as the online help up-to-date.

In order to download Up2Date packages, UTM opens a TCP connection to the update servers on port `443`—allowing this connection without any adjustment to be made by the administrator. However, if there is another firewall in between, you must explicitly allow the communication via the port `443` TCP to the update servers.

4.4.1 Overview

The *Management* > *Up2Date* > *Overview* tab provides a quick overview whether your system is up-to-date. From here, you can install new firmware and pattern updates.

Up2Date Progress

This section is only visible when you have triggered an installation process. Click the button *Watch Up2Date Progress in New Window* to monitor the update progress. If your browser does not suppress pop-up windows, a new window showing the update progress will be opened. Otherwise you will have to explicitly allow the pop-up window.

Note – A backup will be sent to the standard backup email recipients before an installation process is started.

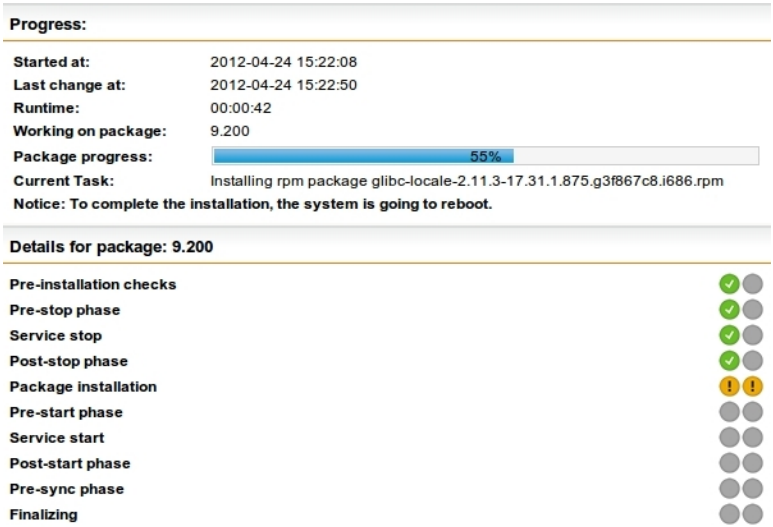

Figure 10 Up2Date: Progress Window

Firmware

The *Firmware* section shows the currently installed firmware version. If an update package is available, a button *Update to Latest Version Now* is displayed. Additionally, you will see a message in the *Available Firmware Up2Dates* section. You can directly download and install the most recent update from here. Once you have clicked *Update To Latest Version Now*, you can watch the update progress in new a window. For this, click the *Reload* button of WebAdmin.

Available Firmware Up2Dates

If you have selected *Manual* on the *Configuration* tab, you can see a *Check for Up2Date Packages Now* button in this section, which you can use to download firmware Up2Date packages manually. If there are more than one Up2Dates available, you can select which one you are going to install. You can use the *Update to Latest Version Now* button in the *Firmware* section if you want to install the most recent version directly.
There is a *Schedule* button available for each Up2Date with which you can define a specific date and time where an update is to be installed automatically. To cancel a scheduled installation, click *Cancel*.

A note on "implicit" installations: There can be a constellation, where you schedule an Up2Date package which requires an older Up2Date package to be installed first. This Up2Date package

will be automatically scheduled for installation before the actual Up2Date package. However, you can define a specific time for this package, too, but you cannot prevent its installation.

Pattern

The *Pattern* section shows the current version of the installed patterns. If you have selected *Manual* on the *Configuration* tab, you can see a *Update Patterns Now* button. Use this button to download and install new patterns if available.

Note – The current pattern version does not need to be identical with the latest available pattern version in order for the UTM unit to be working correctly. A deviation between the current and the latest available pattern version might occur when new patterns are available, which, however, do not apply to the unit you are using. What patterns are downloaded is dependent on your settings and hardware configuration. For example, if you do not use the intrusion prevention feature of Sophos UTM, newly available IPS patterns will not be installed, thus increasing the divergence between the currently installed and the latest available pattern version.

4.4.2 Configuration

By default, new update packages are automatically downloaded to UTM.

Firmware Download Interval

This option is set to 15 minutes by default, that is Sophos UTM checks every 15 minutes for available firmware updates. Sophos UTM will automatically download (but not install) available firmware update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to *Monthly* or you can disable automatic firmware download by selecting *Manual* from the drop-down list. If you select *Manual* you will find a *Check for Up2Date Packages Now* button on the *Overview* tab.

Pattern Download/Installation Interval

This option is set to 15 minutes by default, that is Sophos UTM checks every 15 minutes for available pattern updates. Sophos UTM will automatically download and install available pattern update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to *Monthly* or you can disable automatic pattern download and installation by selecting *Manual* from the drop-down list. If you select *Manual* you will find a *Update Patterns Now* button on the *Overview* tab.

4.4.3 Advanced

The *Management* > *Up2Date* > *Advanced* tab lets you configure further Up2Date options such as selecting a parent proxy or Up2Date cache for your UTM.

Note – Update packages can be downloaded from Sophos UTM FTP server.

Manual Up2Date Package Upload: If your UTM does not have direct access to the Internet or an Up2Date cache to download new update packages directly, you can upload the update package manually. To do so, proceed as follows:

1. **Open the *Upload File* dialog window.**
   Click the Folder icon next to the *Up2Date file* box.

   The *Upload File* dialog window opens.
2. **Select the update package.**
   Click *Browse* in the *Upload File* dialog window and select the update package you want to upload.
3. **Click *Start Upload*.**
   The update package will be uploaded to UTM.
4. **Click *Apply*.**
   Your settings will be saved.

Parent Proxy

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

Use a parent proxy: Select the checkbox to enable parent proxy use. Select or add the host and enter the port of the proxy. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

Proxy requires authentication: If the parent proxy requires authentication, enter username and password here.

If a parent proxy is configured, Sophos UTM fetches both firmware and pattern Up2Dates from it.

4.5 Backup/Restore

The backup restoring function allows you to save the UTM settings to a file on a local disk. This backup file allows you to install a known good configuration on a new or misconfigured system.

Be sure to make a backup after every system change. This will ensure that the most current settings are always available. In addition, keep your backups in a safe place, as it also contains security-relevant data such as certificates and cryptographic keys. After generating a backup, you should always check it for readability. It is also a good idea to use an external program to generate MD5 checksums, for this will allow you to check the integrity of the backup later on.

4.5.1 Backup/Restore

On the *Management* > *Backup/Restore* > *Backup/Restore* tab you can create backups, import backups, as well as restore, download, send, and delete existing backups.

Available Backups

This section is only visible if at least one backup has been created before, either by the automatic backup function or manually (see section *Create Backup*).

All backups are listed giving date and time of their creation, their UTM version number, the user who created it, and the comment.

You can decide whether to download, restore, delete, or send a backup.

- **Download:** Opens a dialog window where you can decide to download the file encrypted (provide password) or unencrypted. Click *Download Backup*. You are prompted to select a location in the file system for the downloaded backup to reside.
    - **Encrypt before downloading:** Before downloading or sending it, you have the option to encrypt the backup. Encryption is realized with Blowfish cipher in CBC mode. Provide a password (second time for verification). You will be asked for this password when importing the backup. The file extension for encrypted backups is `ebf`, for unencrypted backups `abf`.

> **Note –** A backup does include administrator passwords, the high availability passphrase if configured, as well as all RSA keys and X.509 certificates. Since this information is confidential, it is good practice to enable encryption.

- **Restore:** Replaces the current system settings by the settings stored in a backup. You will have to log in again afterwards. If the selected backup contains all data you can log in directly. If the selected backup does not contain all data (see section *Create Backup*) you will have to enter the necessary data during the login procedure. If only the host data has been removed in the selected backup you can add an additional administrative email address if you want. It will be used where no recipient is given and as additional address where multiple recipients are possible.
    - Restoring backups from USB flash drive: You can also restore unencrypted backup files (file extension `abf`) from a FAT formatted USB flash drive such as a simple USB stick. To restore a backup from a USB flash drive, copy the backup file to the USB flash drive and plug the device into Sophos UTM prior to boot up. If several backup files are stored on the device, the lexicographically first file will be used (numbers precede letters). For example, suppose the backup files `gateway_backup_2012-04-17.abf` and `2011-03-20_gateway_backup.abf` are both stored on the USB flash drive. During the boot up, the second file will be used because it begins with a number, although it is much older than the other one.

      In addition, a lock file is created after the successful recovery of a backup, preventing the installation of the same backup over and over again while the USB flash drive is still being plugged in. However, if you want to install a previous backup once again, you must first reboot with no USB flash drive plugged in. This will delete all lock files. When you now boot with the USB flash drive plugged in again, the same backup can be installed.
- **Delete:** Deletes a backup from the list. Using the Delete icon on the bottom of the list, you can delete all selected backups. To select backups, click the checkboxes to the left of the backups or use the checkbox on the bottom to select all backups.
- **Send:** In a dialog window you can specify the email recipients. By default, the address (es) provided on the *Automatic Backups* tab are selected. Then decide if you want to send the file encrypted (provide password) or unencrypted. Click *Send Now* to send the backup.
    - **Encrypt before sending:** See *Encrypt before downloading* above.

Create Backup

Backups are not only useful to restore your system after an (unwanted) change or failure. Moreover, they can be used as templates to set up systems that should have a similar configuration so that those systems are already pre-configured in some way which can save you a lot of time. For that, you can strip certain information from a backup before it is created, e.g. hostname, certificates, etc.

To create a backup with the current system state, proceed as follows:

1. **In the *Create Backup* section, enter a comment** (optional).
   The comment will be displayed along with the backup in the backup list.
2. **Make the following settings** (optional):

   Remove unique site data: Select this option to create the backup without host-specific data. This includes hostname, system ID, SNMP data, HA data, license, shell user passwords, and anonymization passwords as well as all certificates, public and private keys, fingerprints and secrets of Email Protection, Web Protection, Client Authentication, IPsec, SSL VPN, RED, WebAdmin, Web Application Firewall, and proxies.
   Such backups are a convenient means to set up multiple similar systems. There are some things to consider though: 1) After restoring you are presented the basic system setup. 2) Only the first interface is configured, the primary IP address being the one that has been configured during installation. All other interfaces will be disabled and set to IP address 0.0.0.0.

   Caution – Although most of the host-specific data is being removed, such a backup template still contains confidential information, such as user passwords. Therefore it is good practice to always encrypt it.

   Remove administrative mail addresses: Select this option to additionally remove the administrator email addresses used in various parts of UTM, e.g. postmaster addresses in Email Protection, notifications, etc. This option is especially useful for IT partners who set up Sophos UTM devices at customers' sites.
3. **Click *Create Backup Now.***
   The backup appears in the list of available backups.

   If a backup is created with one or both of the options selected, the backup entry contains a respective additional comment.

Import Backup

To import a backup, click the Folder icon and select a backup file to upload, then click *Start Upload*. When importing an encrypted backup file, you must provide the correct passphrase prior to importing the backup. Note that the backup will not instantly be restored. Instead, it will be added to the *Available Backups* list.

4.5.2 Automatic Backups

On the *Management* > *Backup/Restore* > *Automatic Backup* tab you can configure several options dealing with the automatic generation of backups. To have backups created automatically, proceed as follows:

1. **Enable automatic backups on the *Automatic Backups* tab.**
   Click the toggle switch.

   The toggle switch turns green and the *Options* and *Send Backups by Email* areas become editable.

2. **Select the interval.**
   Automatic backups can be created at various intervals.

   You can choose between daily, weekly, and monthly.

3. **Specify the maximum number of backups to be stored.**
   Automatically created backups are stored up to the number you enter here. Once the maximum has been reached, the oldest automatic backups will be deleted.

   Note that this applies to automatically created backups only. Backups created manually and backups created automatically before a system update will not be deleted.

4. **Click *Apply*.**
   Your settings will be saved.

To save you the work of backing up your UTM manually, the backup feature supports emailing the backup file to a list of defined email addresses.

Recipients: Automatically generated backups will be sent to users contained in the *Recipients* box. Multiple addresses can be added. By default, the first administrator's email address is used.

Encrypt email backups: In addition, you have the option to encrypt the backup (Triple DES encryption).

Password: Once you have selected the *Encrypt email backups* option, provide a password (second time for verification). You will be prompted for this password when importing the backup.

Automatically created backups will appear in the *Available Backups* list on the *Backup/Restore* tab, marked with the `System` flag indicating the *Creator*. From there, they can be restored, downloaded, or deleted as any backup you have created by yourself.

4.6 User Portal

The User Portal of Sophos UTM is a special browser-based application on the unit providing personalized email and remote access services to authorized users. It can be accessed by browsing to the URL of Sophos UTM, for example, `https://192.168.2.100` (note the HTTPS protocol and the missing port number `4444` you would normally enter for accessing the WebAdmin interface).

Among other things, the User Portal contains the email quarantine, which holds messages that are infected by malicious software, contain suspicious attachments, are identified as spam, or contain certain expressions you have explicitly declared forbidden.

On the login page, users can select a language from the drop-down list located on the right side of the header bar.

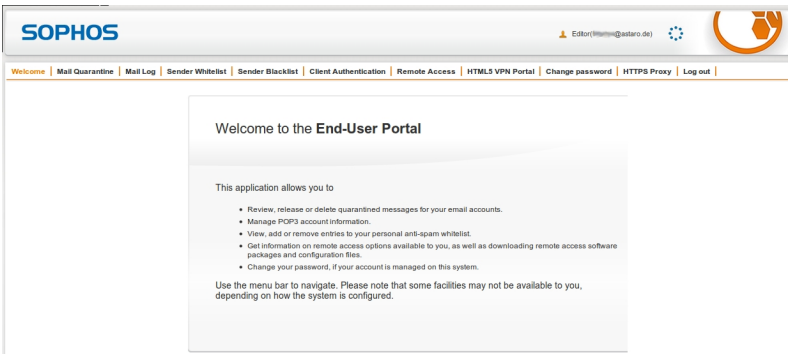

Figure 11 User Portal: Welcome Page

On the User Portal, users have access to the following services:

- **SMTP Quarantine:** Users can view and release messages held in quarantine. Which types of messages they are allowed to release can be determined on the *Email*

Protection > *Quarantine Report* > *Advanced* tab. (The tab is called *Mail Quarantine* when POP3 is disabled.)

- **SMTP Log:** Here, users can view the SMTP log of their mail traffic. (The tab is called *Mail Log* when POP3 is disabled.)
- **POP3 Quarantine:** Users can view and release messages held in quarantine. Which types of messages they are allowed to release can be determined on the *Email Protection* > *Quarantine Report* > *Advanced* tab. (The tab is called *Mail Quarantine* when SMTP is disabled.)
- **POP3 Accounts:** Users can enter their credentials of POP3 accounts they use. Only those spam emails will appear in the User Portal for which POP3 account credentials are given. A user for whom POP3 account credentials are stored will receive an individual Quarantine Report for each email address. Note that allowed POP3 servers must be specified on the *Email Protection* > *POP3* > *Advanced* tab.
- **Sender Whitelist:** Here, senders can be whitelisted, thus messages from them are not regarded as spam. However, emails with viruses or unscannable emails will still be quarantined. Whitelisted senders can be specified by either entering valid email addresses (e.g., `jdoe@example.com`) or all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`).
- **Sender Blacklist:** Here, users can blacklist email senders, e.g. `phishing@hotmail.com`, or whole domains, e.g. `*@hotmail.com`. The blacklist is applied to both SMTP and POP3 email, if these are in use on the system. Blacklisted senders can be specified by clicking the Plus icon, entering the address and clicking the Tick icon to save it. SPX
- **Hotspots:** Here, users can find and manage access data for hotspots. The tab is only available if at least one hotspot has been enabled for the specific user. For hotspots of the type password-of-the-day, the current password is available and can be changed. For hotspots of the type voucher, vouchers can be generated, printed, exported, and deleted. A list of generated vouchers shows information on their usage. For more information see *Wireless Protection* > *Hotspots*.
- **Client Authentication:** Here, users can download the setup file of Sophos Authentication Agent (SAA). The SAA can be used as authentication mode for the Web Filter. The *Client Authentication* tab is only available if Client Authentication is enabled. For more information see *Definitions & Users* > *Client Authentication*.
- **OTP Token:** Here, users find one or more QR codes and the respective detail information for configuring the UTM's one-time password service on their mobile devices. For

more information see *Definitions & Users* > *Authentication Services* > *One-time Password*.

- **Remote Access:** Users can download remote access client software and configuration files provided for them. However, the *Remote Access* tab is only available if at least one remote access mode has been enabled for the specific user.
- **HTML5 VPN Portal:** Here, users can open VPN connections to predefined hosts using predefined services. The tab is only available if at least one VPN connection has been enabled for the specific user. For more information see *Remote Access* > *HTML5 VPN Portal*.
- **Change Password:** Users can change the password for accessing the User Portal.
- **HTTPS Proxy:** Users can import the HTTP/S Proxy CA certificate to get rid of error messages when visiting secure websites. After clicking *Import Proxy CA Certificate*, users will be prompted by their browser to trust the CA for different purposes. For more information see *Web Protection* > *Filtering Options* > *HTTPS CAs*.
- **Log out:** Click here to log out of the User Portal. This is only necessary when you have selected *Remember My Login* at login (which creates a cookie) and you want to explicitly logout and have this cookie deleted. Otherwise, there is no need to use the *Log out* link—closing the browser tab or window is sufficient.

4.6.1 Global

On the *Management* > *User Portal* > *Global* tab you can enable the User Portal. Additionally you can specify which networks and which users should be granted access to the User Portal.

To enable User Portal access, proceed as follows:

1. **Enable the User Portal.**
   Click the toggle switch.

   The toggle switch turns amber and the *End-User Portal Options* area becomes editable.
2. **Select the allowed networks.**
   Add or select the networks that should be allowed to access the User Portal. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.
3. **Select the allowed users.**

Select the users or user groups or add new users that should be able to access the User Portal. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

If you do not want to grant access to all users, unselect the *Allow all users* checkbox and select the users and user groups individually.

4. **Click *Apply*.**
   Your settings will be saved.

4.6.2 Advanced

On the *Advanced* tab you can configure an alternative hostname and port number for the User Portal as well as language and security options.

Language

During login, the User Portal fetches the language settings of the web browser and loads the respective locales to display the portal in the same language as the browser defaults. For browser language settings that are not available for the User Portal, you can select here which language will be the fallback language. Users have additionally the option to select a language on the User Portal login page.

Security

The User Portal uses cookies to track sessions. Persistent cookies permit to return after having closed a session without having to log in again. They can always be deleted from user-side, however, by using the *Log Out* button of the User Portal.

Disable Portal Items

For the features listed here a menu item is displayed in the User Portal when the respective feature has been enabled in WebAdmin. However, here you can define menu items that should *not* be displayed in the User Portal. To do so, select the respective option(s) and click *Apply*.

Network Settings

Hostname: By default, this is UTM's hostname as given on the *Management > System Settings > Hostname* tab. However, if you want to grant access to the User Portal for users gaining access over the Internet, it might be necessary to enter an alternative hostname here that can be publicly resolved.

Listen Address: Default value is *Any*. When using the web application firewall you need to give a specific interface address for the service to listen for User Portal connections. This is necessary for the User Portal connection handler and the web application firewall to be able to differentiate between the incoming SSL connections.

Port: By default, port `443` for HTTPS is selected. You can change the port to any value in the range from `1024` to `65535`. Note that you cannot select either `10443` or the *WebAdmin TCP Port*, which is configured on the *Management* > *WebAdmin Settings* > *Advanced* tab. Independent of the defined port, the User Portal can always be accessed via HTTPS only.

Welcome Message

You can customize the welcome message of the User Portal. Simple HTML markup and hyperlinks are allowed.

Note – Changing the welcome message is not possible when using a home use license.

4.7 Notifications

Sophos UTM comes with a notification feature that informs you immediately about all sorts of security-relevant events occurring on UTM, either by email or SNMP trap. All events that might possibly be of interest to an administrator are represented by various error, warning, and information codes. What notifications are sent depends on the selection you have configured on the *Notifications* tab.

4.7.1 Global

On the *Management* > *Notifications* > *Global* tab you can configure the sender address (i.e., the *From* address) to be taken for notification emails sent by UTM. By default, this is `do-not-reply@fw-notify.net`. If you want to change this address, it is advisable to enter an email address of your domain, as some mail servers might be configured to check whether a given sender address really exists.

In addition, you can specify the recipients of UTM notifications. By default, this is the administrator's email address you had entered during the initial setup.

Limit Notifications: Some security-relevant events such as detected intrusion attempts will create a lot of notifications, which may quickly clog the notification recipients' email inboxes. For this reason, Sophos UTM has sensible default values to limit the number of notifications sent per

hour. If you disable this option, every security-relevant event will create a notification, provided the event is configured so as to send a notification on the *Management* > *Notifications* > *Notifications* tab.

Device Specific Text

Here you can enter a description of Sophos UTM, e.g. its location, which will be displayed in the notifications sent.

4.7.2 Notifications

Notifications are divided into three categories:

- **CRIT:** Messages informing about critical events that might render UTM inoperable.
- **WARN:** Warnings about potential problems that need your attention, for example, exceeding thresholds.
- **INFO:** Merely informational messages such as the restart of a system component, for example.

You can select whether you want to send the notification as email or SNMP trap.

4.7.3 Advanced

In case your UTM cannot send emails directly, you can configure a smarthost to send the emails. Proceed as follows:

1. **Enable *External SMTP* on the *Management* > *Notifications* > *Advanced* tab.**
   Click the toggle switch.
2. **Enter your smarthost**.
   You can use drag-and-drop. The port is preset to the default SMTP port `25`.
   - **Use TLS:** Select this checkbox if you want to enforce TLS when sending notifications. Note that notifications will not be sent if the smarthost does not support TLS.
3. **Specify the authentication settings.**
   If the smarthost requires authentication, check the *Authentication* checkbox and enter the corresponding username and password.
4. **Click *Apply*.**
   Your settings will be saved.

4.8 Customization

The tabs under *Management* > *Customization* allow you to customize and localize email notifications and status messages created by Sophos UTM, making it possible to adapt those messages to both your policy and your corporate identity.

In addition, you can edit and upload custom web templates to further change the way that users receive block messages and other notifications.

Note – Customization is not possible when using a home use license.

4.8.1 Global

On the *Management* > *Customization* > *Global* tab you can customize global display options for the system messages presented to users. Note that UTF-8/Unicode is supported.

The example below shows the customizable global options (*Company Logo* and *Custom Company Text*), along with an example of a "Content Block" message, which is configured on the *Management* > *Customization* > *Web Messages* page.

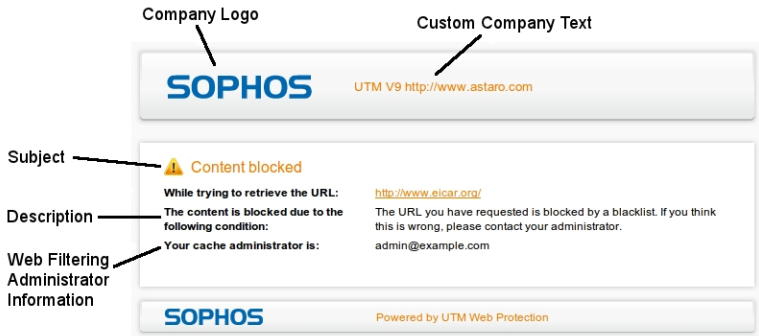

Figure 12 Customization: Example Blocked Page and Its Customizable Parts

Company Logo

You can upload your own logo/banner (in `png` format only), which is used in the following contexts:

- Web messages
- POP3 blocked messages
- Quarantine release status messages (which will appear in the Quarantine Report after a spam email has been released from the quarantine or whitelisted.)
- Quarantine Report

Some of the messages displayed to users have been optimized for the default logo (195 x 73 pixels with a transparent background). For the best-looking results, use an image that has the same attributes.

To upload a logo:

1. **Open the *Upload file* dialog window.**
   Click the Folder icon next to the *Upload new logo* box.

   The *Upload file* dialog window opens.

2. **Select the logo.**
   Browse to the location where the logo that you want to upload resides.

   Once you have selected the logo, click *Start Upload*.

3. **Click *Apply*.**
   The logo will be uploaded, replacing the file that is already installed.

Custom Company Text

Customize the message that will be displayed beneath the company logo whenever a website was blocked by the virus scanner or the content filter of Sophos UTM. For example, you might want to enter the administrator's contact data here.

4.8.2 Web Messages

Customize the text for web filtering messages displayed by Sophos UTM. Some messages are displayed when users are restricted from downloading files that are too large, are of a certain type, or contain a virus. Other messages are displayed when users attempt to access restricted websites or applications, while users are downloading files, or when users are required to authenticate with the UTM. You can translate messages into other languages or, for example, modify the messages to show customer support contact information.

Note – The text entered in the fields of the *Web Messages* tab can be referenced in custom web templates. For more information, see *Web Templates*.

The following messages are configurable:

Content Block

- **Surf Protection:** This message is displayed when a user attempts to access a webpage whose URL matches a category that is configured to be blocked or the site's reputation falls below the specified threshold. For more information, see *Web Protection* > *Web Filtering*.
- **Blacklist:** This message is displayed when a user attempts to retrieve a webpage that matches a blacklisted URL. To blacklist URLs, see *Web Protection* > *Web Filtering* > *Policies* > *Website Filtering*.
- **MIME Type:** This message is displayed when a user requests a file that is a blocked MIME type. For more about specifying MIME types, see *Web Protection* > *Web Filtering* > *Policies* > *Downloads*.
- **File Extension:** This message is displayed when a user requests a blocked file extension. For more about specifying file extensions, see *Web Protection* > *Web Filtering* > *Policies* > *Downloads*.
- **File Size:** This message is displayed when a user requests a file that exceeds the file size limit. To configure download size limits, see *Web Protection* > *Web Filtering* > *Policies* > *Downloads*.
- **Application Control:** This message is displayed when a user attempts to use a type of network traffic that is configured to be blocked by Application Control. For more information on Application Control, see *Web Protection* > *Application Control*.
- **Virus Detected:** This message is displayed when a file is blocked due to a virus infection. For more information on configuring virus protection, see *Web Protection* > *Web Filtering* > *Policies* > *Antivirus*.

Download/Scan

- **Download in Progress:** This message is displayed while a file is being downloaded. See *Download Manager*.
- **Virus Scan in Progress:** This message is displayed while the UTM scans files for malicious content. See *Download Manager*.

- **Download Complete:** This message is displayed after a file has been fully downloaded, scanned, and determined safe. See *Download Manager*.

Authentication

- **Transparent Mode Authentication:** This option only applies if you use Web Filtering in Transparent Mode, and you have selected the "Browser" authentication mode. For more information, see *Web Protection > Web Filter Profiles > Proxy Profiles*. The text is displayed on the authentication page, where users must log in before using the Web Filter. If the *Terms of Use* field is filled in, a disclaimer is displayed on the authentication page. If this field is empty (as it is by default), a disclaimer is not displayed.
- **Bypass Content Block:** This message is displayed when a page is blocked by Surf Protection and the option to bypass blocking option is enabled (see *Web Protection > Filtering Options > Bypass Users*). If the *Terms of Use* field is filled in, a disclaimer is displayed on the authentication page. If this field is empty (as it is by default), a disclaimer is not displayed.

Error

- **Server Error:** This message is displayed if an error occurs while processing the user's request.

Administrator Information: Here you can enter information about the administrator managing the Web Filter, including the administrator's email address.

4.8.2.1 Modifying a Web Message

To modify a Content Block, Download/Scan, Authentication, or Error message:

1. **Select the message.**
   From the *Page* drop-down list, select the end user message that you want to edit.

   The *Subject* and *Description* for that message are displayed.
2. **Modify the Subject and/or Description.**
   Modify the default text as necessary.
3. **Click *Apply*.**
   The text changes are saved.

4.8.2.2 Download Manager

If the Web Filter is enabled, the web browser will display the following download pages while downloading content greater than 1 MB in size that is neither text nor an image. The download

page will not be displayed when video or audio streams are requested or more than 50 % of the file has been downloaded within five seconds.

The information provided on the download pages can be customized on the *Web Messages* tab.

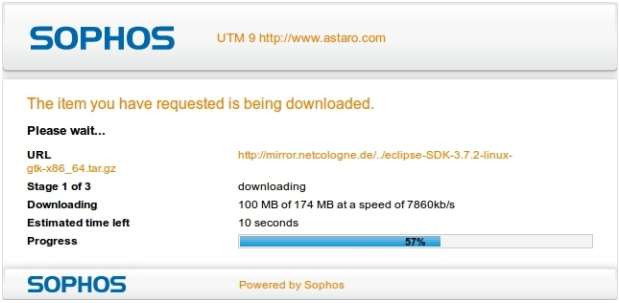

Figure 13 Customization: HTTP Download Page Step 1 of 3: Downloading File

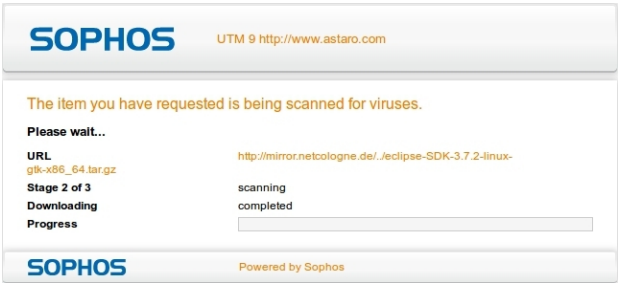

Figure 14 Customization: HTTP Download Page Step 2 of 3: Virus Scanning

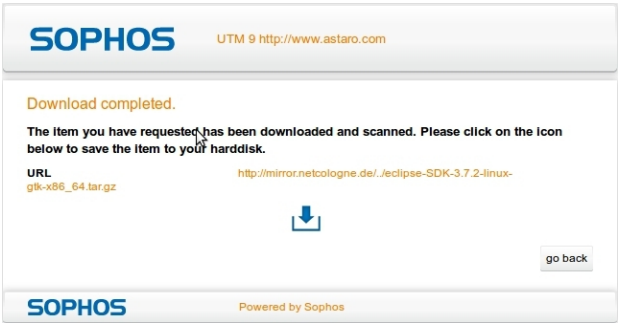

Figure 15 Customization: HTTP Download Page Step 3 of 3: File Download Completed

4.8.3 Web Templates

To customize both the appearance and content of messages that are displayed to users, you can upload HTML files to Sophos UTM. As a guide, Sophos provides several sample templates.These templates show you how to use variables that can dynamically insert information that is relevant for individual user messages. For example, if a file is blocked because it contains a virus, you can include a variable that inserts the name of the virus that was blocked.

4.8.3.1 Customizing Web Templates

Caution – Customizing Sophos UTM notifications is an advanced topic. Only those with sufficient knowledge of HTML and JavaScript should attempt these tasks.

You can upload custom versions of Sophos UTM notifications, including block messages, status messages, error messages, and authentication prompts. The four sample templates contain working examples of variables as well as several sample images. Either use the sample templates as a basis for your custom messages and notifications or upload your own HTML files. Valid variables are described in Using Variables in UTM Web Templates in the Sophos Knowledgebase.

If you want to use the text from a message configured on the *Web Messages* tab, you can insert the appropriate variable in your custom template. For more information, see *Web Messages*.

To download the sample templates and images, click the link below, and save the .zip file:

http://www.astaro.com/lists/Web_Templates.zip

4.8.3.2 Uploading Custom Web Templates and Images

Once you have edited and saved your custom template, you are ready to upload it to the UTM.

To upload a web template or image:

1. **Open the *Upload file* dialog window.**
   Click the Folder icon next to the name of the type of template that you want to upload, or click the Folder icon next to *Images* if you want to upload an image.

   Note – The supported file types are `.png`, `.jpg`, `.jpeg`, and `.gif`.

The *Upload file* dialog window opens.

2. **Select the template or image.**
   Browse to the location of the template or image that you want to upload.

   Once you have selected the template or image, click *Start Upload*.

   The *Upload file* dialog window closes.

3. **Click *Apply*.**
   The template or image will be uploaded.

4.8.4 Email Messages

Customize the text that is displayed in user messages generated by the SMTP/POP3 proxies of Sophos UTM. You can translate these messages into other languages or modify them to show customer support contact information, for example. The following messages can be customized:

Quarantine

Email released from quarantine: This message is shown when an email was successfully released from the quarantine.

Error on releasing email from quarantine: This message is shown when an error occurred while releasing an email from the quarantine.

POP3

POP3 message blocked: This message is sent to the recipient when a POP3 email message was blocked.

Figure 16 Customization: POP3 Proxy Blocked Message

4.9 SNMP

The *Simple Network Management Protocol* (SNMP) is used by network management systems to monitor network-attached devices such as routers, servers, and switches. SNMP allows the administrator to make quick queries about the condition of each monitored network device. You can configure Sophos UTM to reply to SNMP queries or to send SNMP traps to SNMP management tools. The former is achieved with so-called *management information bases* (MIBs). An MIB specifies what information can be queried for which network device. Sophos UTM supports SNMP version 2 and 3 and the following MIBs:

- **DISMAN-EVENT-MIB:** Event Management Information Base
- **HOST-RESOURCES-MIB:** Host Resources Management Information Base
- **IF-MIB:** Interfaces Group Management Information Base
- **IP-FORWARD-MIB:** IP Forwarding Table Management Information Base
- **IP-MIB:** Management Information Base for the *Internet Protocol* (IP)
- **NOTIFICATION-LOG-MIB:** Notification Log Management Information Base
- **RFC1213-MIB:** Management Information Base for Network Management of TCP/IP-based Internet: MIB II
- **SNMPv2-MIB:** Management Information Base for the *Simple Network Management Protocol* (SNMP)
- **TCP-MIB:** Management Information Base for the *Transmission Control Protocol* (TCP)
- **UDP-MIB:** Management Information Base for the *User Datagram Protocol* (UDP)

In order to get Sophos UTM system information, an SNMP manager must be used that has at least the RFC1213-MIB (MIB II) compiled into it.

4.9.1 Query

On the *Management* > *SNMP* > *Query* page you can enable the usage of SNMP queries.

To configure SNMP queries, proceed as follows:

1. **Enable *SNMP Queries*.**
   Click the toggle switch.

The sections *SNMP Version* and *SNMP Access Control* become editable.

2. **Select the SNMP version.**
   In the *SNMP Version* section, select a version from the drop-down list. SNMP version 3 requires authentication.
3. **Select allowed networks.**
   Networks listed in the *Allowed Networks* box are able to query the SNMP agent running on Sophos UTM. Note that the access is always read-only.
   - **Community String:** When using version 2, enter a community string. An SNMP community string acts as a password that is used to protect access to the SNMP agent. By default, the SNMP community string is "public", but you can change it to any setting that best suits your needs.

     Note – Allowed characters for the community string are: (a-z), (A-Z), (0-9), (+), (_), (@), (.), (-), (blank).

   - **Username/Password:** When using version 3, authentication is required. Enter a username and password (second time for verification) to enable the remote administrator to send queries. The password must have at least eight characters. SNMP v3 uses SHA for authentication and AES for encryption. Note that username and password are used for both of them.
4. **Click *Apply*.**
   Your settings will be saved.

Furthermore, you can enter additional information about UTM.

Device Information

The *Device Information* text boxes can be used to specify additional information about UTM such as its name, location, and administrator. This information can be read by SNMP management tools to help identify UTM.

Note – All SNMP traffic (protocol version 2) between UTM and the *Allowed Networks* is not encrypted and can be read during the transfer over public networks.

Astaro Notifier MIB

This section allows you to download the Astaro MIB which contains the definitions of the Sophos UTM notification SNMP traps. For historical reasons the MIB uses the Astaro Private Enterprise

Code (SNMPv2-SMI::enterprises.astaro).

4.9.2 Traps

In the *Traps* tab you can define an SNMP trap server to which notifications of relevant events occurring on UTM can be sent as SNMP traps. Note that special SNMP monitoring software is needed to display those traps.

The messages that are sent as SNMP traps contain so-called object identifiers (OID), for example, `.1.3.6.1.4.1.9789`, which belong to the private enterprise numbers issued by IANA. Note that `.1.3.6.1.4.1` is the `iso.org.dod.internet.private.enterprise` prefix, while `9789` is Astaro's *Private Enterprise Number*. The OID for notification events is `1500`, to which are appended the OIDs of the type of the notification and the corresponding error code (`000-999`). The following notification types are available:

- `DEBUG = 0`
- `INFO = 1`
- `WARN = 2`
- `CRIT = 3`

Example: The notification "INFO-302: New firmware Up2Date installed" will use the OID `.1.3.6.1.4.1.9789.1500.1.302` and has the following string assigned:

```
[<HOST>][INFO][302]
```

Note that `<HOST>` is a placeholder representing the hostname of the system and that only type and error code from the notification's subject field are transmitted.

To select an SNMP trap server, proceed as follows:

1. **Click *New SNMP Trap Sink*.**
   The *Create New SNMP Trap Sink* dialog box opens.
2. **Make the following settings:**
   Host: The host definition of the SNMP trap server.

   Community: An SNMP community string acts as a password that is used to protect access to querying SNMP messages. By default, the SNMP community string is set to "public". Change it to the string that is configured on the remote SNMP trap server.

Note – Allowed characters for the community string are: (a-z), (A-Z), (0-9), (+), (_), (@), (.), (-), (blank).

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new SNMP trap server will be listed on the *Traps* tab.

4.10 Central Management

The pages of the *Central Management* menu let you configure interfaces to management tools that can be used to monitor or remotely administer the gateway.

4.10.1 Sophos UTM Manager

Sophos UTM Manager (SUM) is Sophos' central management product. You can connect several UTM appliances to a SUM where they centrally can be monitored, configured and maintained. SUM 4.2 supports configuring UTM 9.2 only. Other UTM versions will appear in SUM as well and can be monitored. If for example a UTM 9.2 connects with a SUM 4.1 it falls into legacy mode. Then backups and up2date installations are still allowed.

On this tab, you can configure the connection of your UTM to one or two SUMs.

Note – When using MSP licensing, disabling SUM, changing the SUM host, or modifying the rights of the SUM administrator can only be done by Sophos UTM Manager (SUM).

To prepare Sophos UTM to be monitored by a SUM server, proceed as follows:

1. **On the *Sophos UTM Manager* tab, enable SUM.**
   Click the toggle switch.

   The toggle switch turns amber and the *SUM Settings* area becomes editable.

2. **Specify the *SUM host*.**
   Select or add the SUM server UTM should connect to. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   - **Authentication** (optional): If the SUM server requires authentication, select this option and enter the same password (shared secret) as configured on the SUM

server.

- **Use SUM server as Up2Date cache** (optional): Up2Date packages can be fetched from a cache located on the SUM server. If you want to use this functionality for your gateway, select the option *Use SUM server as Up2Date cache*. Please ensure that on your managing SUM server the Up2Date cache functionality is enabled accordingly. Note that usage of the Up2Date cache functionality is mutually exclusive with using a parent proxy configuration for Up2Dates.

3. **Define the rights of the SUM administrator.**
On SUM, the administrator responsible for this UTM can only administer those areas of your UTM which are explicitly allowed to be administered here. The rights listed here correspond to the SUM Gateway Manager main menu and administrative options.

   Administration: If selected, the administrator can use all features located in the *Maintenance* and *Management* menus. He can, for example, view the inventory, create and restore backups, and schedule actions like firmware updates.

   Reporting: If selected, the administrator can use all features located in the *Reporting* menu. He can, for example, request reports from UTM.

   Monitoring: If selected, UTM will be displayed on the *Monitoring* pages and the administrator can use all associated features.

   Configuration: If selected, the administrator can use all features located in the *Configuration* menu. He can, for example, deploy objects (networks, hosts, VPNs) to UTM.

   Note – Please refer to the Sophos UTM Manager Administration Guide for detailed information.

4. **Click *Apply*.**
Your settings will be saved.

   UTM will now try to establish a connection to Sophos UTM Manager. Once the connection between both systems is established, the connection status will turn green. Then UTM can be monitored and administered by the SUM server selected here. You will be able to see the current connection status and health in the *SUM Health* section. Reloading the page will update this data. Please use the *Open Live Log* button and read carefully the messages from the message board to be able to diagnose connection problems should they occur.

Settings for a Second SUM

In this section, you can optionally add a second SUM. This is useful in case for example you do the configuration by yourself (first SUM server) but want your machines still to be monitored by a third party, e.g. your MSSP (second SUM server). The settings are almost identical to the first SUM's settings, except that the *Configuration* option is missing because they are limited to the first SUM.

Note – The communication between the gateway and SUM takes place on port `4433`, whereas the Sophos UTM Manager can be accessed through a browser via the HTTPS protocol on port `4444` for the WebAdmin and on port `4422` for the Gateway Manager interface.

SUM Health

You will be able to see the current connection status and health in the section called *SUM Health*. Reloading the page will update this data.

SUM Objects

This area is disabled (grayed-out) unless there are objects that have been created via a SUM and if this SUM is now disconnected from the Sophos UTM. SUM-created objects can be network definitions, remote host definitions, IPsec VPN tunnels, etc.

The button *Cleanup Objects* can be pressed to release any objects that were created by the SUM the device has formerly been managed with. These objects are normally locked and can only be viewed on the local device. After pressing the button, the objects become fully accessible and can be reused or deleted by a local administrator.

Note – In case former SUM-created objects are cleaned up, they cannot be re-transformed when reconnecting to that same SUM. This means that if the remote SUM still hosts object definitions for a device which later re-establishes a connection to it, those objects will be deployed to the device again—although local copies will then already exist.

Live Log

You can use the live log to monitor the connection between your Sophos UTM and the SUM. Click the *Open Live Log* button to open the live log in a new window.

4.11 High Availability

The main cause for an Internet security system to fail is because of a hardware failure. The ability of any system to continue providing services after a failure is called failover. Sophos UTM provides high availability (HA) failover, allowing you to set up a hot standby system in case the primary system fails (active-passive). Alternatively, you can use Sophos UTM to set up a cluster, which operates by distributing dedicated network traffic to a collection of nodes (active-active) similar to conventional load-balancing approaches in order to get optimal resource utilization and decrease computing time.

The concepts *high availability* and *cluster* as implemented in Sophos UTM are closely related. For a high availability system can be considered a two-node cluster, which is the minimum requirement to provide redundancy.

Each node within the cluster can assume one of the following roles:

- **Master:** The primary system in a hot standby/cluster setup. Within a cluster, the master is responsible for synchronizing and distributing of data.
- **Slave:** The standby system in a hot standby/cluster setup which takes over operations if the master fails.
- **Worker:** A simple cluster node, responsible for data processing only.

All nodes monitor themselves by means of a so-called heart-beat signal, a periodically sent multicast UDP packet used to check if the other nodes are still alive. If any node fails to send this packet due to a technical error, the node will be declared *dead*. Depending on the role the failed node had assumed, the configuration of the setup changes as follows:

- If the master node fails, the slave will take its place and the worker node with the highest ID will become slave.
- If the slave node fails, the worker node with the highest ID will become slave.
- If a worker node fails, you may notice a performance decrease due to the lost processing power. However, the failover capability is not impaired.

Reporting

All reporting data is consolidated on the master node and is synchronized to the other cluster nodes at intervals of five minutes. In case of a takeover, you will therefore lose not more than

five minutes of reporting data. However, there is a distinction in the data collection process. The graphs displayed in the *Logging & Reporting > Hardware* tabs only represent the data of the node currently being master. On the other hand, accounting information such as shown on the *Logging & Reporting > Network Usage* page represents data that was collected by all nodes involved. For example, today's CPU usage histogram shows the current processor utilization of the master node. In the case of a takeover, this would then be the data of the slave node. However, information about top accounting services, for example, is a collection of data from all nodes that were involved in the distributed processing of traffic that has passed the unit.

Notes

- The *Address Resolution Protocol* (ARP) is only used by the actual master. That is to say, slave and worker nodes do not send or reply to ARP requests.
- In case of a failover event, the unit that takes over operations performs an ARP announcement (also known as *gratuitous ARP*), which is usually an ARP request intended to update the ARP caches of other hosts which receive the request. Gratuitous ARP is utilized to announce that the IP of the master was moved to the slave.
- All interfaces configured on the master must have a physical link, that is, the port must be properly connected to any network device.

4.11.1 Hardware and Software Requirements

The following hardware and software requirements must be met to provide HA failover or cluster functionality:

- Valid license with the high availability option enabled (for the stand-by unit you only need an additional base license).
- Two UTM units with identical software versions and hardware or two UTM appliances of the same model.
- Heartbeat-capable Ethernet network cards. Check the HCL to figure out which network cards are supported. The HCL is available at the Sophos Knowledgebase (use "HCL" as search term).
- Ethernet crossover cable (for connecting master and slave in a hot standby system). UTM appliance models 320, 425, and 525, whose dedicated HA interface is a Gigabit auto-MDX device, can be connected through a standard IEEE 802.3 Ethernet cable as

the Ethernet port will automatically exchange send/receive pairs.

- Network switch (for connecting cluster nodes).

4.11.2 Status

The *Management* > *High Availability* > *Status* tab lists all devices involved in a hot standby system or cluster and provides the following information:

- **ID:** The device's node ID. In a hot standby system, the node ID is either `1` (master) or `2` (slave).
  The node ID in a cluster can range from 1-10, as a cluster can have up to a maximum of 10 nodes.
- **Role:** Each node within the cluster can assume one of the following roles:
  - MASTER: The primary system in a hot standby/cluster setup. It is responsible for synchronizing and distributing of data within a cluster.
  - SLAVE: The standby system in a hot standby/cluster setup which takes over operations if the master fails.
  - WORKER: A simple cluster node, responsible for data processing only.
- **Device Name:** The name of the device.
- **Status:** The state of the device concerning its HA status; can be one of the following:
  - ACTIVE: The node is fully operational. In case of a hot standby (active-passive) setup, this is the status of the active node.
  - READY: The node is fully operational. In case of a hot standby (active-passive) setup, this is the status of the passive node.
  - UNLINKED: One ore more interface links are down.
  - UP2DATE: An Up2Date is in progress.
  - UP2DATE-FAILED: An Up2Date has failed.
  - DEAD: The node is not reachable.
  - SYNCING: Data Synchronization is in progress. This status is displayed when a takeover process is going on. The initial synchronizing time is at least 5 minutes. It can, however, be lengthened by all synchronizing-related programs. While a SLAVE is synchronizing and in state *SYNCING*, there is no graceful takeover, e.g. due to link failure on master node.

- **Version:** Version number of Sophos UTM Software installed on the system.
- **Last Status Change:** The time when the last status change occurred.

Reboot/Shutdown: With these buttons, a device can be manually rebooted or shut down.

Remove Node: Use this button to remove a dead cluster node via WebAdmin. All node-specific data like mail quarantine and spool is then taken over by the master.

Click the button *Open HA Live Log* in the upper right corner to open the high availability live log in a separate window.

4.11.3 System Status

The *Management* > *High Availability* > *System Status* tab lists all devices involved in a hot standby system or cluster and provides information about the resource usage of each device:

- The CPU utilization in percent
- The RAM utilization in percent
- The swap utilization in percent
- The amount of hard disk space consumed by the log partition in percent
- The amount of hard disk space consumed by the root partition in percent
- The status of the UPS (uninterruptible power supply) module (if available)

4.11.4 Configuration

The high availability functionality of Sophos UTM covers four basic settings:

- Off
- Automatic Configuration
- Hot Standby (Active-Passive)
- Cluster (Active-Active)

Automatic Configuration: Sophos UTM features a plug-and-play configuration option for UTM appliances that allows the setup of a hot standby system/cluster without requiring reconfiguration or manual installation of devices to be added to the cluster. Simply connect the dedicated HA interfaces (`eth3`) of your UTM appliances with one another, select *Automatic Configuration* for all devices, and you are done.

Note – For *Automatic Configuration* to work, all UTM appliances must be of the same model. For example, you can only use two UTM 320 appliances to set up a HA system; one UTM 220 unit on the one hand and one UTM 320 unit on the other hand cannot be combined.

If you connect two UTM appliances through this dedicated interface, all devices will recognize each other and configure themselves automatically as an HA system—the device with the longer uptime becoming master. If the unlikely case should occur that the uptime is identical, the decision which device is becoming master will be made based on the MAC address.

Using UTM Software, the *Automatic Configuration* option is to be used on dedicated slave systems to automatically join a master or already configured hot standby system/cluster. For that reason, *Automatic Configuration* can be considered a transition mode rather than a high availability operation mode in its own right. For the high availability operation mode will change to *Hot Standby* or *Cluster* as soon as a device with *Automatic Configuration* selected joins a hot standby system or cluster, respectively. The prerequisite, however, for this feature to work is that the option *Enable Automatic Configuration of New Devices* is enabled on the master system. This function will make sure that those devices will automatically be added to the hot standby system/cluster whose high availability operation mode is set to *Automatic Configuration*.

Hot Standby (active-passive): Sophos UTM features a hot standby high availability concept consisting of two nodes, which is the minimum required to provide redundancy. One of the major improvements introduced in Sophos UTM Software 9 is that the latency for a takeover could be reduced to less than two seconds. In addition to firewall connection synchronization, the gateway also provides IPsec tunnel synchronization. This means that road warriors as well as remote VPN gateways do not need to re-establish IPsec tunnels after the takeover. Also, objects residing in the quarantine are also synchronized and are still available after a takeover.

Cluster (active-active): (Not available with BasicGuard subscription.) To cope with the rising demand of processing large volumes of Internet traffic in real time, Sophos UTM features a clustering functionality that can be employed to distribute processing-intensive tasks such as content filtering, virus scanning, intrusion prevention, or decryption equally among multiple cluster nodes. Without the need of a dedicated hardware-based load balancer, the overall performance of the gateway can be increased considerably.

Note – When configuring a cluster, make sure you have configured the master node first before connecting the remaining units to the switch.

Setting up the master, slaves, or workers is pretty similar. Proceed as follows:

1. **Select a high availability operation mode.**
   By default, high availability is turned off. The following modes are available:
   - Automatic Configuration
   - Hot Standby (active-passive)
   - Cluster (active-active)

   Note – If you want to change the high availability operation mode, you must always set the mode back to *Off* before you can change it to either *Automatic Configuration*, *Hot Standby*, or *Cluster*.

   Note – If the license/subscription has expired or is non-existent, the operation mode changing is limited to *Off* and the current operation mode.

   Depending on your selection, one or more options will be displayed.

2. **Make the following settings:**
   Sync NIC: Select the network interface card through which master and slave systems will communicate. If link aggregation is active you can select here a link aggregation interface, too.

   Note – Only those interfaces are displayed that have not been configured yet. It is possible to change the synchronization interface in a running configuration. Note that afterwards all nodes are going to reboot.

   The following options can only be configured if you either select *Hot Standby* or *Cluster* as operation mode:

   Device Name: Enter a descriptive name for this device.

   Device Node ID: Select the node ID of the device. In a case of a failure of the primary system, the node with the highest ID will become master.

   Encryption Key: The passphrase with which the communication between master and slave is encrypted (enter the passphrase twice for verification). Maximum key length is 16 characters.

3. **Click *Apply*.**
   The high-availability failover is now active on the device.

The gateway in hot standby mode will be updated at regular intervals over the data transfer connection. Should the active primary system encounter an error, the secondary will immediately and automatically change to normal mode and take over the primary system's functions.

Note – When you deactivate a hot standby system/cluster, the slave and worker nodes will perform a factory reset and shut down.

More information (especially use cases) can be found in the *HA/Cluster Guide*, which is available at the Sophos Knowledgebase.

Advanced

This section allows you to make some advanced settings.

Enable Automatic Configuration of New Devices: If you have configured a hot standby system/cluster manually, this option will make sure that those devices will automatically be added to the hot standby system/cluster whose high-availability operation mode is set to *Automatic configuration*. However, this option is of no effect on slave systems, so you can leave it enabled, which is the default setting.

Keep Node(s) Reserved During Up2Date: If selected, during an update to a new system version, half of the HA/Cluster nodes will keep the current system version. When the new version is stable, you can update the remaining nodes on the *Management > High Availability > Status* page. In case the new version leads to a failure of all updated nodes, the remaining nodes will build a new HA/Cluster with the old version. You can then install the old version on the failed nodes or wait for the next update.

If *Keep Node(s) Reserved During Up2Date* is enabled, reserved nodes will not be synchronized anymore after an update, because synchronization is restricted to nodes having the same system version. Instead, the state of the reserved nodes will be preserved. So, if for whatever reason you decide to reactivate the reserved nodes, configuration changes or reporting data coming up in the time span between update start and reactivation will be lost.

Preferred Master: Here you can define a designated master node by selecting a node from the drop-down list. In case of a failover, the selected node will not stay in Slave mode after the link recovers but instead will switch back to Master mode.

Backup Interface: To prevent that both master and slave become master at the same time (master-master situations), for example, because of a failure of the HA synchronization interface or an unplugged network cable, a backup heartbeat interface can be selected. This additional heartbeat interface can be any of the configured and active Ethernet interfaces. If a backup interface is selected, an additional heartbeat signal is sent via this interface in one direction from the master to the slave to make sure that the master-slave configuration stays intact. If the master-slave connection is disabled and the backup interface becomes involved, the administrator will receive a notification informing that one of the cluster nodes is dead. However, this option is of no effect on slave systems, so you can leave it unconfigured.

Note – In case of a failure of the HA synchronization interface, no configuration is synchronized anymore. The backup interface only prevents master-master situations.

4.12 Shutdown and Restart

On this tab you can manually shut down or restart Sophos UTM.

Shutdown: This action allows you to shut down the system and to stop all services in a proper manner. For systems without a monitor or LCD display, the end of the shutdown process is signaled by an endless series of beeps at intervals of one second.

To shut down Sophos UTM, proceed as follows:

1. **Click *Shutdown (Halt) the System Now.***
2. **Confirm the warning message.**
   When asked "Really shut down the system?", click *OK*.

   The system is going down for halt.

Depending on your hardware and configuration, this process may take several minutes to complete. Only after the system has completely shut down you should turn off the power. If you turn off the power without the system being shut down properly, the system will check the consistency of its file system during the next booting, meaning that the boot-up process will take much longer than usual. In the worst case, data may have been lost.

The system will beep five times in a row to indicate a successful system start.

Restart: This action will shut down the system completely and reboot. Depending on your hardware and configuration, a complete restart can take several minutes.

To restart Sophos UTM, proceed as follows:

1. **Click *Restart (Reboot) the System Now*.**
2. **Confirm the warning message.**
   When asked "Really restart the system?", click *OK*.

   The system is going down for halt and reboot.

5 Definitions & Users

This chapter describes how to configure network, service, and time period definitions used throughout Sophos UTM. The *Definitions Overview* page in WebAdmin shows the number of network definitions according to type as well as the numbers of service definitions according to protocol type.

The pages of the *Definitions & Users* menu allow you to define networks and services that can be used in all other configuration menus in one central place. This allows you to work with the names you define rather than struggling with IP addresses, ports, and network masks. Another benefit of definitions is that you can group individual networks and services together and configure them all at once. If, for example, you assign certain settings to these groups at a later time, these settings will apply to all networks and services contained therein.

Additionally, this chapter describes how to configure user accounts, user groups, and external authentication servers of Sophos UTM as well as authentication for client PCs.

The following topics are included in this chapter:

5.1 Network Definitions

The *Definitions & Users* > *Network Definitions* menu lets you create hosts, networks, and network groups as well as MAC address definitions. The definitions created here can be used in many other WebAdmin configurations.

5.1.1 Network Definitions

The *Definitions & Users* > *Network Definitions* > *Network Definitions* tab is the central place for defining hosts, networks, and network groups on UTM. The definitions created here can be

used on many other WebAdmin configuration menus.

Opening the tab, by default, all network definitions are displayed. Using the drop-down list on top of the list, you can choose to display network definitions with certain properties.

Tip – When you click on the Info icon of a network definition in the *Network Definitions* list, you can see all configuration options in which the network definition is used.

The network table also contains static networks, which were automatically created by the system and which can neither be edited nor deleted:

- **Internal (Address):** A definition of this type will be added for each network interface. It contains the current IP address of the interface. Its name consists of the interface name with "(Address)" appended to it.
- **Internal (Broadcast):** A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 broadcast address of the interface. Its name consists of the interface name with "(Broadcast)" appended to it.
- **Internal (Network):** A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 network of the interface. Its name consists of the interface name with "(Network)" appended to it.
- **Any (IPv4/IPv6):** A network definition (for IPv4 and IPv6 each, if IPv6 is enabled) bound to the interface which serves as default gateway. Making use of it in your configuration should make the configuration process easier. With uplink balancing enabled, the definition *Internet* is bound to *Uplink Interfaces*.

  Note – IPv6 entries are only visible if it is activated in *Interfaces & Routing* > *IPv6*.

Note – User network objects authenticated via client authentication will always be shown as unresolved due to performance reasons.

To create a network definition, proceed as follows:

1. **On the *Network Definitions* tab, click *New Network Definition*.**
   The *Create New Network Definition* dialog box opens.
2. **Make the following settings:**
   (Note that further parameters of the network definition will be displayed depending on the selected definition type.)

Name: Enter a descriptive name for this definition.

Type: Select the network definition type. The following types are available:

- **Host:** A single IP address. Provide the following information:
  - **IPv4 Address/IPv6 Address:** The IP address of the host (note that you cannot enter the IP address of a configured interface).
  - **DHCP Settings** (optional): In this section you can create static mappings between hosts and IP address. For that purpose, you need a configured DHCP server (see *Network Services > DHCP > Servers*).

    Note – To avoid an IP address clash between regularly assigned addresses from the DHCP pool and those statically mapped make sure that the latter are not in the scope of the DHCP pool. For example, a static mapping of `192.168.0.200` could result in two systems receiving the same IP address if the DHCP pool is `192.168.0.100` – `192.168.0.210`.

    IPv4 DHCP: Select the IPv4 DHCP server to be used for static mapping.

    MAC Addresses: Enter the MAC addresses of the hosts' network interface cards. The MAC addresses are usually specified in a format consisting of six groups of two hexadecimal digits, separated by colons or hyphens (e.g., `00:04:76:16:EA:62`).

    IPv6 DHCP: Select the IPv6 DHCP server to be used for static mapping.

    DHCP Unique IDs: Enter the DUIDs of the hosts. With e.g. Windows operating systems, the DUID can be found in the Windows Registry: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters`

    Please note that you have to enter the groups of two hexadecimal digits separated by colons (e.g., `00:01:00:01:13:30:65:56:00:50:56:b2:07:51`).
  - **DNS Settings** (optional): If you do not want to set up your own DNS server but need static DNS mappings for a few hosts of your network, you can enter these mappings in this section of the respective hosts. Note that this only scales for a limited number of hosts and is by no means intended as a

replacement of a fully operable DNS server.
Hostname: Enter the fully qualified domain name (FQDN) of the host.

Reverse DNS: Select the checkbox to enable the mapping of the host's IP address to its name. Note that although several names can map to the same IP address, one IP address can only ever map to one name.

Additional Hostnames: Click the Plus icon to add additional hostnames for the host.

- **DNS Host:** A DNS hostname, dynamically resolved by the system to produce an IP address. DNS hosts are useful when working with dynamic IP endpoints. The system will re-resolve these definitions periodically according to the TTL (Time To Live) values and update the definition with the new IP address (if any). Provide the following information:
  - **Hostname:** The hostname you want to resolve.
- **DNS Group:** Similar to DNS host, but can cope with multiple RRs (Resource Records) in DNS for a single hostname. It is useful for defining firewall rules and exceptions in transparent proxies.
- **Network:** A standard IP network, consisting of a network address and a netmask. Provide the following information:
  - **IPv4 Address/IPv6 Address:** The network address of the network (note that you cannot enter the IP address of a configured interface).
  - **Netmask:** The bit mask used to tell how many bits in an octet(s) identify the subnetwork, and how many bits provide room for host addresses.
- **Range:** Select to define a whole IPv4 address range. Provide the following information:
  - **IPv4 From:** First IPv4 address of the range.
  - **IPv4 To:** Last IPv4 address of the range.
  - **IPv6 From:** First IPv6 address of the range.
  - **IPv6 To:** Last IPv6 address of the range.
- **Multicast Group:** A network that comprises a defined multicast network range.
  - **IPv4 Address:** The network address of the multicast network, which must be in the range `224.0.0.0` to `239.255.255.255`.
  - **Netmask:** The bit mask used to tell how many bits in an octet(s) identify the subnetwork, and how many bits provide room for host addresses.

- **Network Group:** A container that includes a list of other network definitions. You can use them to bundle networks and hosts for better readability of your configuration. Once you have selected *Network group*, the *Members* box appears where you can add the group members.
- **Availability Group:** A group of hosts and/or DNS hosts sorted by priority. Alive status of all hosts is checked with ICMP pings at an interval of 60 seconds, by default. The host with the highest priority and an alive status is used in configuration. Once you have selected *Availability Group*, the *Members* box appears where you can add the group members.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
The options displayed depend on the selected *Type* above.

Interface (optional): You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.

Monitoring Type (only with type *Availability group*): Select the service protocol for the alive status checks. Select either *TCP* (TCP connection establishment), *UDP* (UDP connection establishment), *Ping* (ICMP Ping), *HTTP Host* (HTTP requests), or *HTTPS Hosts* (HTTPS requests) for monitoring. When using *UDP* a ping request will be sent initially which, if successful, is followed by a UDP packet with a payload of 0. If ping does not succeed or the ICMP port is unreachable, the host is regarded as down.

Port (only with monitoring type *TCP* or *UDP*): Number of the port the request will be sent to.

URL (optional, only with monitoring types *HTTP Host* or *HTTPS Host*): URL to be requested. You can use other ports than the default ports 80 or 443 by adding the port information to the URL, e.g., `http://example.domain:8080/index.html`. If no URL is entered, the root directory will be requested.

Interval: Enter a time interval in seconds at which the hosts are checked.

Timeout: Enter a maximum time span in seconds for the hosts to send a response. If a host does not respond during this time, it will be regarded as dead.

Always Resolved: This option is selected by default, so that if all hosts are unavailable, the group will resolve to the host which was last available. Otherwise the group will be set to *unresolved* if all hosts are dead.

4. **Click *Save*.**
   The new definition appears on the network definition list.

To either edit or delete a network definition, click the corresponding buttons.

5.1.2 MAC Address Definitions

The *Definitions & Users > Network Definitions > MAC Address Definitions* tab is the central place for defining MAC address definitions, i.e., lists of MAC addresses. A MAC address definition can be used like a network definition. Additionally it can be used to further restrict a rule based on hosts/IP addresses to only match devices which have one of the defined MAC addresses.

Tip – When you click on the Info icon of a MAC address definition, you can see all configuration options in which the definition is used.

To create a MAC address definition, proceed as follows:

1. **On the *MAC Address Definitions* tab, click *New MAC Address List*.**
   The *Create MAC Address List* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this definition.

   MAC Addresses: Click the Plus icon to enter individual MAC addresses subsequently or use the Action icon to import a list of MAC addresses via copy and paste. The MAC addresses are usually specified in a format consisting of six groups of two hexadecimal digits, separated by colons or hyphens (e.g., `00:04:76:16:EA:62`).

   Hosts: Add or select the hosts whose MAC addresses you want to add to the MAC address definition. The MAC addresses defined in the *DHCP Settings* section of the host definition will be added to the MAC address list. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Note – The number of addresses per address definition is limited for the following uses: To restrict access to a wireless network, the maximum is 200. To restrict access to a RED appliance, the maximum is 200 for RED 10 and 400 for RED 50.

   Note – You can either enter MAC addresses or hosts or both.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new definition appears on the *MAC Address Definition* list.

To either edit or delete a MAC address definition, click the corresponding buttons.

5.2 Service Definitions

On the *Definitions & Users* > *Service Definitions* page you can centrally define and manage services and service groups. Services are definitions of certain types of network traffic and combine information about a protocol such as TCP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic accepted or denied by UTM.

Tip – When you click on the Info icon of a service definition in the *Service Definitions* list, you can see all configuration options in which the service definition is used.

To create a service definition, proceed as follows:

1. **On the *Service Definitions* page, click *New Service Definition*.**
   The *Create New Service Definition* dialog box opens.
2. **Make the following settings:**
   (Note that further parameters of the service definition will be displayed depending on the selected definition type.)

   Name: Enter a descriptive name for this definition.

   Type of Definition: Select the service type. The following types are available:

   - **TCP:** Transmission Control Protocol (TCP) connections use port numbers ranging from `0` to `65535`. Lost packets can be recognized through TCP and be requested again. In a TCP connection, the receiver notifies the sender when a data packet was successfully received (connection related protocol). TCP sessions begin with a three way handshake and connections are closed at the end of the session. Provide the following information:
     - **Destination Port:** Enter the destination port either as single port number (e.g., `80`) or as a range (e.g., `1024:64000`), using a colon as delimiter.

- **Source Port:** Enter the source port either as single port number (e.g., `80`) or as a range (e.g., `1024:64000`), using a colon as delimiter.

- **UDP:** The *User Datagram Protocol* (UDP) uses port numbers between `0` and `65535` and is a stateless protocol. Because it does not keep state, UDP is faster than TCP, especially when sending small amounts of data. This statelessness, however, also means that UDP cannot recognize when packets are lost or dropped. The receiving computer does not signal the sender when receiving a data packet. When you have selected *UDP*, the same configuration options can be edited as for TCP.
- **TCP/UDP:** A combination of TCP and UDP appropriate for application protocols that use both sub protocols such as DNS. When you have selected *TCP/UDP*, the same configuration options can be edited as for TCP or UDP.
- **ICMP/ICMPv6:** The *Internet Control Message Protocol* (ICMP) is chiefly used to send error messages, indicating, for example, that a requested service is not available or that a host or router could not be reached. Once you have opted for *ICMP* or *ICMPv6*, select the ICMP code/type. Note that IPv4 firewall rules do not work with ICMPv6 and IPv6 firewall rules do not work with ICMP.
- **IP:** The *Internet Protocol* (IP) is a network and transport protocol used for exchanging data over the Internet. Once you have selected *IP*, provide the number of the protocol to be encapsulated within IP, for example `121` (representing the SMP protocol).
- **ESP:** The *Encapsulating Security Payload* (ESP) is a part of the IPsec tunneling protocol suite that provides encryption services for tunneled data via VPN. Once you have selected ESP or AH, provide the *Security Parameters Index* (SPI), which identifies the security parameters in combination with the IP address. You can either enter a value between 256 and 4,294,967,296 or keep the default setting given as the range from 256 to 4,294,967,296 (using a colon as delimiter), especially when using automatic IPsec key exchange. Note that the numbers 1-255 are reserved by the *Internet Assigned Numbers Authority* (IANA).
- **AH:** The *Authentication Header* (AH) is a part of the IPsec tunneling protocol suite and sits between the IP header and datagram payload to maintain information integrity, but not secrecy.
- **Group:** A container that includes a list of other service definitions. You can use them to bundle service definitions for better readability of your configuration. Once

you have selected *Group*, the *Members* box opens where you can add group members (i.e., other service definitions).

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new definition appears on the *Service Definitions* list.

To either edit or delete a definition, click the corresponding buttons.

Note – The type of definition cannot be changed afterwards. If you want to change the type of definition, you must delete the service definition and create a new one with the desired settings.

5.3 Time Period Definitions

On the *Definitions & Users* > *Time Period Definitions* page you can define single or recurring time slots that can in turn be used to limit for example firewall rules or content filter profile assignments to specific time ranges.

Tip – When you click on the Info icon of a time period definition in the *Time Period Definitions* list, you can see all configuration options in which the time period definition is used.

To create a time period definition, proceed as follows:

1. **On the *Time Period Definitions* tab, click *New Time Period Definition*.**
   The *Create New Time Period Definition* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this time period definition.

   Type: Select the time period definition type. The following types are available:

   - **Recurring Event:** These events will be repeated periodically. You can select the start time, the end time, and the weekdays on which the time period definition should be applied. If the time span extends into the next day, the selected weekdays refer to the start time. Start and stop dates cannot be selected for this type.

- **Single Event:** These events will only take place once. You can both select a start date/time and an end date/time. As these definitions do not recur, the option *Weekdays* cannot be selected for this type.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new time period definition appears on the *Time Period Definitions* list.

To either edit or delete a time period definition, click the corresponding buttons.

5.4 Users & Groups

The *Definitions & Users > Users & Groups* menu lets you create users and groups for WebAdmin access as well as for remote access, User Portal access, email usage etc.

5.4.1 Users

On the *Definitions & Users > Users & Groups > Users* tab you can add user accounts to UTM. In its factory default configuration, Sophos UTM has one administrator called *admin*.

Tip – When you click on the Info icon of a user definition in the *Users* list, you can see all configuration options in which the user definition is used.

When you specify an email address in the *New User* dialog box, an X.509 certificate for this user will be generated simultaneously while creating the user definition, using the email address as the certificate's VPNID. On the other hand, if no email address is specified, a certificate will be created with the user's *Distinguished Name* (DN) as VPN ID. That way, if a user is authenticated by means of a backend group such as eDirectory, a certificate will be created even if no email address is set in the corresponding backend user object.

Because the VPN ID of each certificate must be unique, each user definition must have a different and unique email address. Creating a user definition with an email address already present in the system will fail. The certificates can be used for various remote access methods supported by Sophos UTM with the exception of PPTP, L2TP over IPsec using PSK, and native IPsec using RSA or PSK.

To add a user account, proceed as follows:

1. **On the *Users* tab, click *New User*.**
   The *Create New User* dialog box opens.

2. **Make the following settings:**
   Username: Enter a descriptive name for this user (e.g. jdoe). Note that for using remote access via PPTP or L2TP over IPsec, the username may only contain ASCII printable characters[1].

   Real name: Enter the user's real name (e.g. John Doe).

   Email address: Enter the user's primary email address.

   Additional email addresses (optional): Enter additional email addresses of this user. Spam emails sent to any of these addresses will be listed in an individual Quarantine Report for each email address, which is sent to the primary email address specified above.

   Authentication: Select the authentication method. The following methods are available:

   - **Local:** Select to authenticate the user locally on UTM.
   - **Remote:** Select to authenticate the user using one of the external authentication methods supported by Sophos UTM. For more information, see *Definitions & Users > Authentication Services*.
   - **None:** Select to prevent the user from authentication completely. This is useful, for example, to disable a user temporarily without the need to delete the user definition altogether.

   Password: Enter a user password (second time for verification). Only available if you selected *Local* as authentication method. Note that Basic User Authentication does not support umlauts. Note that for using remote access via PPTP or L2TP over IPsec, the password may only contain ASCII printable characters[2].

   Backend sync: Some basic settings of the user definition such as the real name or the user's email address can be updated automatically by synchronizing the data with external backend authentication servers (only available if you selected *Remote* as authentication method). Note that the option will automatically be set according to the *Enable*

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters
[2] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

Backend Sync on Login option on the *Authentication Services* > *Advanced* tab, if the user is selected for prefetching.

Note – Currently, only data with Active Directory and eDirectory servers can be synchronized.

X.509 certificate: Once the user definition has been created, you can assign an X.509 certificate for this user when editing the user definition. By default, this is the certificate that was automatically generated upon creating the user definition. However, you can also assign a third-party certificate, which you can upload on the *Remote Access* > *Certificate Management* > *Certificates* tab.

Use static remote access IP (optional): Select if you want to assign a static IP address for a user gaining remote access instead of assigning a dynamic IP address from an IP address pool. For IPsec users behind a NAT router, for example, it is mandatory to use a static remote access IP address.

Note – The static remote access IP can only be used for remote access through PPTP, L2TP, and IPsec. It cannot be used, however, for remote access through SSL.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Users can create and maintain their own email whitelist and blacklist (see chapter User Portal). You can view those lists here and, if necessary, modify them.
4. **Click *Save*.**
   The new user account appears on the *Users* list.

If you want to make this user a regular administrator having access to the web-based administrative interface WebAdmin, add the user to the group of *SuperAdmins*, which is configured on the *Definitions & Users* > *Users & Groups* > *Groups* tab in WebAdmin.

Note – If you have deleted a user object and want to create a user object with the same name, make sure you have also deleted the certificate associated with this user on the *Remote Access* > *Certificate Management* > *Certificates* tab. Otherwise you will get an error message stating that an item with that name already exists.

You can download remote access certificates and/or configurations of users for whom some sort of remote access has been enabled. For that, select the checkbox in front of the respective users and select the desired option from the *Actions* drop-down list in the list header. Remote access users can also download those files themselves when they are allowed to use the User Portal.

5.4.2 Groups

On the *Definitions & Users* > *Users & Groups* > *Groups* page you can add user groups to UTM. In its factory default configuration, Sophos UTM has one user group called *SuperAdmins*. If you want to assign administrative privileges to users, that is, granting access to WebAdmin, add them to the group of *SuperAdmins*; this group should not be deleted.

Tip – When you click on a group definition in the *Groups* list, you can see all configuration options in which the group definition is used.

To add a user group, proceed as follows:

1. **On the *Groups* tab, click *New Group*.**
   The *Create New Group* dialog box opens.
2. **Make the following settings:**
   Group name: Enter a descriptive name for this group. Note that this name does not need to correspond to the names of your backend groups.

   Group type: Select the type of the group. You can choose between a group of static members and two group types promoting dynamic membership.

   - **Static members:** Select the local users who shall become member of this group.
   - **IPsec X509 DN mask:** Users are dynamically added to an IPsec X509 DN group definition if they have successfully logged in to the gateway through an IPsec connection and if specific parameters of their distinguished names match the values specified in the *DN Mask* box.
   - **Backend membership:** Users are dynamically added to a group definition if they have been successfully authenticated by one of the supported authentication mechanisms. To proceed, select the appropriate backend authentication type:
     - **Active Directory:** An Active Directory user group of UTM provides group memberships to members of Active Directory server user groups configured on a Windows network. For more information, see *Definitions &*

Users > Authentication Services > Servers.

- **eDirectory:** An eDirectory user group of UTM provides group memberships to members of eDirectory user groups configured on an eDirectory network. For more information, see *Definitions & Users > Authentication Services > Servers*.
- **RADIUS:** Users are automatically added to a RADIUS backend group when they have been successfully authenticated using the RADIUS authentication method.
- **TACACS+:** Users are automatically added to a TACACS+ backend group when they have been successfully authenticated using the TACACS+ authentication method.
- **LDAP:** Users are automatically added to an LDAP backend group when they have been successfully authenticated using the LDAP authentication method.

Limit to backend group(s) membership (optional; only with backend groups *Active Directory* or *eDirectory*): For all X.500-based directory services you can restrict the membership to various groups present on your backend server if you do not want all users of the selected backend server to be included in this group definition. The group(s) you enter here once selected this option must match a *Common Name* as configured on your backend server. Note that if you select this option for an Active Directory backend, you can omit the `CN=` prefix. If you select this option for an eDirectory backend, you can use the eDirectory browser that lets you conveniently select the eDirectory groups that should be included in this group definition. However, if you do not use the eDirectory browser, make sure to include the `CN=` prefix when entering eDirectory containers.

Check an LDAP attribute (optional; only with backend group *LDAP*): If you do not want all users of the selected backend LDAP server to be included in this group definition, you can select this checkbox to restrict the membership to those users matching a certain LDAP attribute present on your backend server. This attribute is then used as an LDAP search filter. For example, you could enter `groupMembership` as attribute with `CN=Sales,O=Example` as its value. That way you could include all users belonging to the sales department of your company into the group definition.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new user group appears on the *Groups* list.

To either edit or delete a group, click the corresponding buttons.

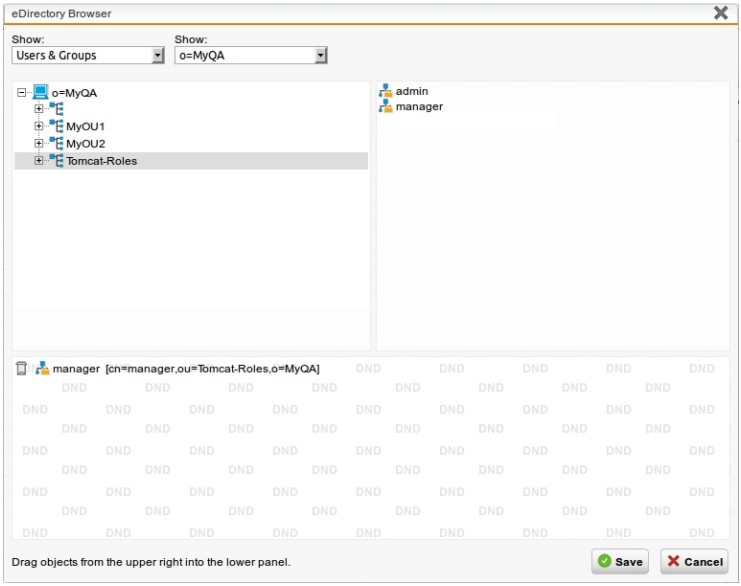

Figure 17 Groups: eDirectory Browser of Sophos UTM

5.5 Client Authentication

Sophos provides an authentication client for Windows and Mac OS so that users directly authenticate at the UTM. This gives you user-based control on web surfing and network traffic by, for example, creating firewall rules based on user networks or group networks. Additionally, wherever possible, IP addresses, hostnames, and the like are replaced by usernames to provide a better readability of reporting data and objects.

Note – In WebAdmin, user network objects authenticated via client authentication will always be shown as unresolved due to performance reasons.

Users who want or should use Client Authentication need to install the Sophos Authentication Agent (SAA) on their client PC or Mac OS computer. The SAA can be downloaded either via

this WebAdmin page or via the User Portal. Note that only users who are within the user group of the Client Authentication configuration will find a download link on their User Portal page.

To configure Client Authentication, do the following:

1. **On the *Client Authentication* tab, enable Client Authentication.**
   Click the toggle switch.

   The toggle switch turns green and the *Client Authentication Options* area becomes editable.

2. **Select the allowed networks.**
   Add or select the networks that should use Client Authentication. Note that those networks need to be directly connected to the UTM for Client Authentication to work. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

3. **Select the allowed users and groups.**
   Select single users or groups or add new users into the *Allowed Users and Groups* box. This can be also your already existing authentication group, e.g. an Active Directory user group. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

4. **Click *Apply*.**
   Your settings will be saved.

   Client Authentication is now available for the selected networks.

Client Authentication Program

When Client Authentication is enabled, you can download the Sophos Authentication Agent (SAA) here. You can either distribute the SAA manually or have your users download the client from the User Portal.

Download EXE: Downloads the Client Authentication program including the CA certificate for direct installation on client PCs. This is the same file as can be downloaded from the User Portal.

Download MSI: Downloads the Client Authentication MSI package. This package is designed for automatic package installation via domain controller (DC) and does not contain the CA certificate.

Download DMG: Downloads the Client Authentication Mac OS X disk image. This image is designed for installation on client computers having an OS X operating system.

Download CA: Downloads the CA certificate that has to be rolled out in addition to the MSI package.

The SAA can be used as authentication mode for the Web Filter. For more information see chapter *Web Protection* > *Web Filtering* > *Global*.

5.6 Authentication Services

On the *Definitions & Users* > *Authentication Services* page databases and backend servers of external user authentication services like Single Sign-On or One-time Password can be managed. External user authentication allows you to validate user accounts against existing user databases or directory services on other servers of your network. Authentication services currently supported are:

- Novell's eDirectory
- Microsoft's Active Directory
- RADIUS
- TACACS+
- LDAP

5.6.1 Global Settings

The *Definitions & Users* > *Authentication Services* > *Global Settings* tab lets you configure basic authentication options. The following options are available:

Create users automatically: When this option is selected, Sophos UTM will automatically create a user object whenever an unknown user of a configured backend group successfully authenticates against one of the various authentication services supported by Sophos UTM. For example, if you configure a RADIUS backend group and you add this group as a member to one of the roles defined on the *Management* > *WebAdmin Settings* > *Access Control* tab, Sophos UTM will automatically create a user definition for a RADIUS user who has successfully logged in to WebAdmin.

- **Automatic User Creation for Facilities:** Automatic user creation can be enabled or disabled for specific services. Users are only created for enabled services. This option is not available—and automatic user creation is disabled for all facilities—when the *Create*

users automatically option is not selected.

Note – This feature does not work for Active Directory *Single Sign-On* (SSO).

Those user objects are also needed to grant access to the User Portal of Sophos UTM. In addition, for all user objects created automatically an X.509 certificate will be generated. Note, however, that automatic user creation will fail in case of an email address conflict, for the user definition to be created automatically must not have configured an email address that is already present on the system. All email addresses must be unique within the system because they are used as identifiers for X.509 certificates.

Important Note – Authentication (i.e., the action of determining who a user is) and authorization (i.e., the action of determining what a user is allowed to do) for a user whose user object was created automatically are always done on the remote backend server/directory service. Therefore, automatically created user objects in Sophos UTM are useless if the corresponding backend server is not available or if the user object has been deleted on the remote site.

Note also that except for Active Directory *Single Sign-On* (SSO) Sophos UTM caches user authentication data it has retrieved from a remote authentication server for 300 seconds. For this reason, changes made to the remote user settings will only take effect after the cache has expired.

Authentication Cache

Every time Sophos UTM gets a user request, e.g., `http`, from a yet unknown user and authentication is required, the Sophos User Authentication (SUA) writes an entry to the authentication cache. Over time, in environments with frequently changing users it can be reasonable to empty the cache from time to time. Also, if you want to force an immediate new authentication for all users. Use the button *Flush Authentication Cache* to empty the authentication cache.
An authentication is valid for 300 seconds. During this time, other authentication requests by the same user are looked up directly in the cache. This technique takes load off backend authentication services like eDirectory.

Note – Flushing the cache does not affect users that are remotely logged on.

Live Log

Open Live Log: Click the button to see the log of the *Sophos User Authentication* (SUA) in a new window.

5.6.2 Servers

On the *Definitions & Users > Authentication Services > Servers* tab, you can create one or more authentication servers, such as eDirectory, Active Directory, LDAP, RADIUS, and TACACS+.

5.6.2.1 eDirectory

Novell eDirectory is an X.500 compatible directory service for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object-oriented database that represents all the assets in an organization in a logical tree. Those assets can include people, servers, workstations, applications, printers, services, groups, and so on.

To configure eDirectory authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Create New Authentication Server* opens.
2. **Make the following settings:**
   Backend: Select *eDirectory* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   Server: Select or add an eDirectory server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   SSL: Select this option to enable SSL data transfer. The *Port* will then change from `389` (LDAP) to `636` (ldaps = LDAP over SSL).

   Port: Enter the port of the eDirectory server. By default, this is port `389`.

   Bind DN: The *Distinguished Name* (DN) of the user to bind to the server with. This user is needed if anonymous queries to the eDirectory server are not allowed. Note that the user must have sufficient privileges to obtain all relevant user object information from the eDirectory server in order to authenticate users. eDirectory users, groups, and

containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., `CN=administrator,DC=intranet,DC=example,DC=com`).

Password: Enter the password of the bind user.

Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., `O=Example,OU=RnD`). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click *Save*.**
   The server will be displayed in the *Servers* list.

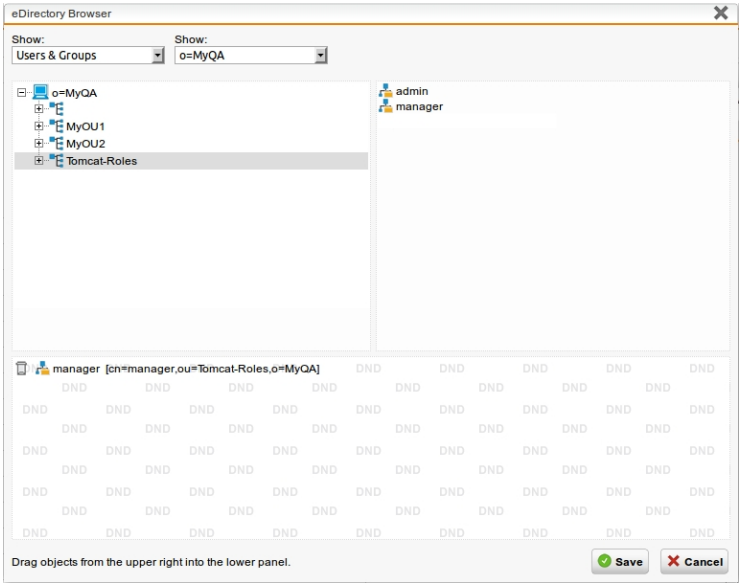

Figure 18 Groups: eDirectory Browser of Sophos UTM

5.6.2.2 Active Directory

Active Directory (AD) is Microsoft's implementation of a directory service and is a central component of Windows 2000/2003 servers. It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides a means of centrally organizing, managing, and controlling access to these resources.

The Active Directory authentication method allows you to register Sophos UTM at a Windows domain, thus creating an object for Sophos UTM on the primary *domain controller* (DC). UTM is then able to query user and group information from the domain.

Note – UTM supports Active Directory 2003 and newer.

To configure Active Directory authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Create New Authentication Server* opens.

2. **Make the following settings:**
   Backend: Select *Active Directory* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   Server: Select or add an Active Directory server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   SSL: Select this option to enable SSL data transfer. The *Port* will then change from `389` (LDAP) to `636` (ldaps = LDAP over SSL).

   Port: Enter the port of the Active Directory server. By default, this is port `389`.

   Bind DN: The full *Distinguished Name* (DN) of the user to bind to the server in LDAP notation. This user is needed if anonymous queries to the Active Directory server are not allowed. The bind user must have sufficient privileges to obtain all relevant user object information from the Active Directory server in order to authenticate users; a requirement usually met by the administrator of the domain.

   Each DN consists of one or more *Relative Distinguished Names* (RDN) constructed from some attributes of the Active Directory user object and includes its username, the node where it resides, and the top-level DN of the server, all specified in LDAP notation and separated by commas.

   - The username must be the name of the user who is able to access the directory and is to be specified by the `CN` designator (e.g., `CN=user`). While using a popular account with domain permissions, such as "admin" is possible, it is highly recommended for best practices that the user not have admin rights, as it is sufficient for them to have read permission on all objects of the subtree starting at the given base DN.
   - The information of the node where the user object resides must include all subnodes between the root node and the user object and is usually comprised of so-called *organizational units* and *common name* components. Organizational units (indicated by the combined folder/book icon in the Microsoft Management Console) are to be specified by the `OU` designator. Note that the order of the nodes is from the lowest to the highest node, that is, the more specific elements come first (e.g., `OU=Management_US,OU=Management`). On the other hand, default Active Directory containers (indicated by a simple Folder icon) such as the pre-defined *Users* node are to be specified using the `CN` designator (e.g., `CN=Users`).

- The top-level DN of the server can consist of several domain components, each specified by the `DC` designator. Note that the domain components are given in the same order as the domain name (for example, if the domain name is `example.com`, the DN part would be `DC=example,DC=com`).

An example bind user DN for a user named `administrator` whose object is stored in the `Users` container in a domain called `example.com` would look like this: `CN=administrator,CN=Users,DC=example,DC=com`

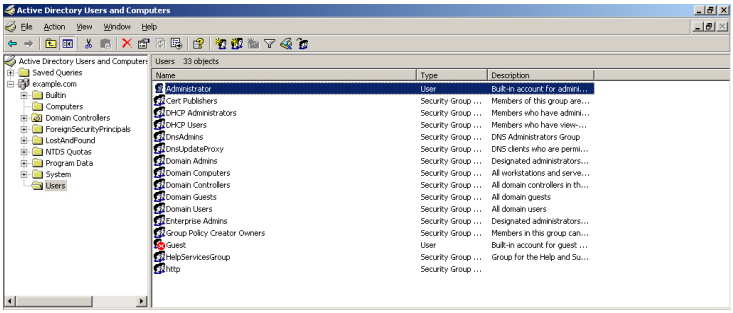

Figure 19 Authentication: Microsoft Management Console

Now, suppose you create an organizational unit called *Management* with the subnode *Management_US* and move the administrator user object into it, the DN of the administrator would change to: `CN=administrator,OU=Management_US,OU=Management,DC=example,DC=com`

Password: Enter the password of the bind user.

Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., `O=Example,OU=RnD`). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click *Save*.**
   The server will be displayed in the *Servers* list.

User Principal Name

Sometimes users should be required to use the User Principal Name notation 'user@domain' when entering their credentials, for example when using Exchange servers in combination with Active Directory servers.

- Clone a desired server to start a new server
- Change *Backend* to *LDAP*
- Change *User Attribute* to >
- Enter *userPrincipalname* into *Custom* field.

If not present already, this will set up a 'LDAP Users' group which you will have to use instead of the 'Active Directory Users' group.

Note – The format 'domain\user' is not supported. Use the format 'user@domain' instead.

5.6.2.3 LDAP

LDAP, an abbreviation for *Lightweight Directory Access Protocol*, is a networking protocol for querying and modifying directory services based on the X.500 standard. Sophos UTM uses the LDAP protocol to authenticate users for several of its services, allowing or denying access based on attributes or group memberships configured on the LDAP server.

To configure LDAP authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Create New Authentication Server* opens.
2. **Make the following settings:**
   Backend: Select *LDAP* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

Server: Select or add an LDAP server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

SSL: Select this option to enable SSL data transfer. The *Port* will then change from `389` (LDAP) to `636` (ldaps = LDAP over SSL).

Port: Enter the port of the LDAP server. By default, this is port `389`.

Bind DN: The *Distinguished Name* (DN) of the user to bind to the server with. This user is mandatory. For security reasons, anonymous queries to the LDAP server are not supported. Note that the user must have sufficient privileges to obtain all relevant user object information from the LDAP server in order to authenticate users. LDAP users, groups, and containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., `CN=administrator,DC=intranet,DC=example,DC=com`).

Password: Enter the password of the bind user.

Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

User attribute: Select the user attribute that is to be used as the filter for searching the LDAP directory. The user attribute contains the actual login name each user is prompted for, for example by remote access services. The following user attributes can be selected:

- CN (Common Name)
- SN (Surname)
- UID (User ID)

If usernames in your LDAP directory are not stored in any of these forms, select *<<Custom>>* from the list and enter your custom attribute into the *Custom* field below. Note that this attribute must be configured on your LDAP directory.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., `O=Example,OU=RnD`). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click *Save*.**
   The server will be displayed in the *Servers* list.

5.6.2.4 RADIUS

RADIUS, the acronym of *Remote Authentication Dial In User Service* is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server.

The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on UTM allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. Whereas passwords are encrypted using the RADIUS secret, the username is transmitted in plain text.

To configure RADIUS authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Create New Authentication Server* opens.

2. **Make the following settings:**
   Backend: Select *RADIUS* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   Server: Select or add a RADIUS server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Port: Enter the port of the RADIUS server. By default, this is port `1812`.

   Shared Secret: The shared secret is a text string that serves as a password between a RADIUS client and a RADIUS server. Enter the shared secret.

Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

NAS identifier: Select the appropriate NAS identifier from the list. For more information see the Note and the table below.

Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click *Save*.**
   The server will be displayed in the *Servers* list.

Note – Each user authentication service of Sophos UTM such as PPTP or L2TP querying the RADIUS server sends a different identifier (NAS identifier) to the RADIUS server. For example, the PPTP service sends the NAS identifier `pptp` to the RADIUS server when trying to authenticate this user.That way, the various services can be differentiated on the RADIUS server, which is useful for authorization purposes, that is, the granting of specific types of service to a user. Below you can find the list of user authentication services and their corresponding NAS identifier.

User Authentication Service	NAS Identifier
SSL VPN	`ssl`
PPTP	`pptp`
IPsec	`ipsec`
L2TP over IPsec	`l2tp`
SMTP proxy	`smtp`
User Portal	`portal`
WebAdmin	`webadmin`

User Authentication Service	NAS Identifier
SOCKS proxy	`socks`
Web Filter	`http`
Authentication Client	`agent`
Wireless Access Points	NAS ID is the wireless network name.

Table 1: RADIUS NAS Identifiers

5.6.2.5 TACACS+

TACACS+ (the acronym of *Terminal Access Controller Access Control System*) is a proprietary protocol by Cisco Systems, Inc. and provides detailed accounting information and administrative control over authentication and authorization processes. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates these operations. Another difference is that TACACS+ utilizes the TCP protocol (port `49`) while RADIUS uses the UDP protocol.

To configure TACACS+ authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Create New Authentication Server* opens.

2. **Make the following settings:**
   Backend: Select *TACACS+* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   Server: Select or add a TACACS+ server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Port: Enter the port of the TACACS+ server. By default, this is port `49`.

   Key: Enter the authentication and encryption key for all TACACS+ communication between Sophos UTM and the TACACS+ server. The value for the key to be entered here should match the one configured on the TACACS+ server. Enter the key (second time for verification).

Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click *Save*.**
   The server will be displayed in the *Servers* list.

5.6.3 Single Sign-On

On the *Definitions & Users* > *Authentication Services* > *Single Sign-On* tab you can configure single sign-on functionality for Active Directory and/or eDirectory.

Active Directory Single Sign-On (SSO)

Note that the Active Directory SSO facility is currently only used with the Web Filter to provide single sign-on with browsers that support NTLMv2 or Kerberos authentication.

To activate the single sign-on functionality, UTM must join the Active Directory domain. In order for the domain joining to work, the following prerequisites must be met:

- The time zone on the gateway and the domain controller (DC) must be the same.
- There MUST NOT be a time difference of more than five minutes between the gateway clock and the DC clock.
- The UTM hostname must exist in the ADDNS system.
- UTM must use the AD DNS as forwarder, or must have a DNS request route for the AD domain which points to the AD DNS server.

To configure Active Directory SSO, do the following:

1. **Create an Active Directory server on the *Servers* tab.**
2. **Make the following settings:**
   Domain: Name of the domain (for example `intranet.mycompany.com`). UTM searches all DCs retrievable via DNS.

Admin username: User with administrative privileges who is allowed to add computers to that domain (usually "Administrator").

Password: The password of the admin user.

3. **Click *Apply*.**
   Your settings will be saved.

Note on Kerberos authentication support: In order for opportunistic SSO Kerberos support to work, the clients MUST use the FQDN hostname of UTM in their proxy settings—using the IP address will not work. NTLMv2 mode is not affected by this requirement, and will automatically be used if it is not met, or if the browser does not support Kerberos authentication.

eDirectory Single Sign-On (SSO)

Here, you can configure SSO for eDirectory. If you have configured *eDirectory SSO* as authentication method in *Web Protection* > *Web Filtering*, the eDirectory server selected here will be used.

To configure eDirectory SSO, do the following:

1. **Create an eDirectory server on the *Servers* tab.**
2. **Make the following settings:**
   Server: eDirectory server for which you want to enable SSO.

   Sync interval: Time (in seconds) between two synchronization events between UTM and eDirectory server.
3. **Click *Apply*.**
   Your settings will be saved.

5.6.4 One-time Password

On the *Definitions & Users* > *Authentication Services* > *One-time Password* tab you can configure the one-time password (OTP) service, and you can monitor or edit the tokens of the one-time password users. One-time passwords are a method to improve security for password-based authentication. The user-specific password, which is sometimes too weak, will be amended with a one-time password that is valid for only one login. Thus, even if an attacker gets hold of it, he will not be able to log in with it.

One-time passwords generally change consistently, in regular intervals, being calculated automatically by a specific algorithm. Soon after a new password is calculated, the old password

expires automatically. To calculate one-time passwords, the user needs to have either a mobile device with an appropriate software, or a special hardware or security token. Hardware tokens are ready to use from the start. On the mobile device, the end user needs to install Google Authenticator or a similar software and deploy the configuration, which is available in the User Portal as a QR code, on the start page or on the *OTP Token* page (see *User Portal* page). Having done that, the device calculates one-time passwords in token-specific intervals. It is important that date and time are correct on the mobile device as the time stamp is used for one-time password generation.

Note – To authenticate on the facilities where the one-time password is required, the user has to enter his user-specific UTM password, directly followed by the one-time password.

The administrator can also generate one-time passwords, also known as passcodes, manually. In this case, you have to ensure that these not time-limited one-time passwords are safely transmitted to the end user. This process, however, should only be considered as a temporary solution, for example when a user temporarily has no access to his or her password calculating device.

Note: Once an OTP token is created an information icon appears on the right side for each token. You can view the QR code and its details by clicking on the information icon.

Enabling and Configuring One-time Password Service

To configure the one-time password service, do the following:

1. **In the *OTP Settings* section, make the following settings:**
   All users must use one-time passwords: By default, this checkbox is enabled and all users have to use one-time passwords. If only specific users should use one-time passwords, disable the checkbox and select or add users or groups to the box.

   Auto-create OTP tokens for users: If selected, a QR code for configuring the mobile device software will be presented to the authorized users the next time they log in to the User Portal. For this to work, make sure that the users have access to the User Portal (see *Management > User Portal* pages). When a user logs in to the User Portal, the respective token will appear in the *OTP Tokens* list. Enabling this feature is recommended when you are using soft tokens on mobile devices. If your users only use hardware tokens you should instead disable the checkbox and add or import the tokens before enabling the OTP feature.

Enable OTP for facilities: Here you select the UTM facilities that should be accessed with one-time passwords by the selected users. When you select the *Auto-create OTP tokens for users* checkbox, the User Portal needs to be enabled for security reasons: As the User Portal gives access to the OTP tokens, it should have no weaker protection itself. To activate OTP for secure shell access, you have to additionally enable shell access usage for the respective tokens (see Adding or Editing OTP Tokens Manually). The corresponding users then have to log in as *loginuser* with the loginuser password, appended by the one-time password.

Caution – Especially when selecting WebAdmin or Shell Access for OTP usage, you have to ensure that the selected users have access to the one-time password tokens. Otherwise you may log them out permanently.

Default token timestep: To synchronize one-time password generation on the mobile device and on the UTM, the timestep has to be identical on both sides. Some hardware tokens use 60 seconds. Google Authenticator for example uses a timestep of 30 seconds which is the default value here. If the timestep does not match, authentication fails. The value entered here is used automatically for each new OTP token.

2. **Click *Apply*.**
   Your settings will be saved.

3. **If you use hardware tokens, import or add them into the *OTP Tokens* section.**
   Use the data received from the hardware token vendor to generate a CSV separated file, using semicolons, in UTF-8 encoding. The file has to contain three columns with the following content: secret, timestep, and comment. The secret, a unique, device-specific string, is mandatory, and should have a hexadecimal format and a length of 128 bit. The other columns may be empty. If timestep is empty, the default token timestep defined in the *OTP Settings* section is used.

   Click the Import icon on the top right of the list. Then paste the CSV separated data into the text box and click *Save*.

   After the import you can modify the entries using the Edit icon. Additionally, you can always add single entries by clicking the Plus icon (see Adding or Editing OTP Tokens Manually).

4. **Enable the one-time password service.**
   Click the toggle switch on top of the page. The toggle switch turns green.

If *Auto-create OTP tokens for users* is enabled, as soon as one of the users specified for one-time password authentication logs in to the User Portal for the first time, the UTM auto-creates the OTP token entry if it was not generated up front. Additionally, the Reset icon of the entry is enabled.

Using the toggle switch of an entry you can disable it, for example in case the user lost his hardware token. Using the appropriate icon, you can delete an entry, for example if a hardware token is broken. Be aware that in both cases, if the *Auto-create OTP tokens for users* option is enabled, the user can still re-authenticate because he has access to the token secret. In the *OTP Tokens* list, a new entry will be displayed.

The Reset icon serves to set a token to a 'never-used' state, i.e., the user is presented the QR code again when logging in to the User Portal.

On the top right of the *OTP Tokens* list, a search box and navigation icons are available to navigate through and to filter the list.

Adding or Editing OTP Tokens Manually

You can add or edit OTP tokens.

Tip – Usually you would not add single OTP tokens but either import them—in case of hardware tokens—or, using mobile devices, automatically generate them, using the *Auto-create OTP tokens for users* option.

1. **Open the dialog to add or edit the OTP token.**
   To add an OTP token, click the green Plus icon on the top right of the *OTP Tokens* list.

   To edit an OTP token, click the Edit icon in front of the respective entry in the *OTP Tokens* list.

2. **Make the following settings:**
   User: Select or add the user to whom the token should be assigned.

   Secret: This is the shared secret of the user's hardware token or soft token. A hardware token has an unchangeable secret, given by the hardware producer. The soft token is created randomly by the UTM, when *Auto-create OTP tokens for users* is enabled. The secret should have a hexadecimal format and a length of 128 bit.

   Comment (optional): Add a description or other information. This text will be displayed with the QR code in the User Portal. If you define different tokens for one person, e.g., a

hardware token and a soft token for the mobile phone, it is useful to enter some explanation here as the user will be displayed all QR codes side by side.

3. **Optionally, make the following advanced settings:**
   Use custom token timestep: If you need another timestep for a token than the default token timestep defined in the *OTP Settings* section, enable this checkbox and enter the value. The timestep defined here has to correspond with the timestep of the user's password generation device, otherwise authentication fails.

   Hide token information in User Portal: If enabled, the token will not be displayed in the User Portal. This can be useful for hardware tokens, where no configuration is needed, or for example when the soft tokens should not be configured by the end-user, but centrally, by the administrator.

   Token can be used for shell access: If enabled, the token can be used for command-line access to the UTM. For this to work, shell access has to be enabled in the *OTP Settings* section, and shell access with password authentication has to be enabled for the UTM in general (see *Management* > *System Settings* > *Shell Access*).
   OTP tokens with permission for shell access have a Command Shell icon on the right. For one-time password shell access, the user then has to log in as *loginuser* with the loginuser password, appended by the one-time password.

   Additional codes (only when editing an OTP token): You can add one-time passwords manually for a token. Either click the green Plus icon to enter one one-time password at a time, or use the *Generate* button to generate 10 one-time passwords at once. You can also import or export the one-time passwords using the Action icon. These one-time passwords are not time-limited. A one-time password will be deleted automatically when the user logged in with it. OTP tokens with additional one-time passwords have a Plus icon on the right. Hovering the cursor on it shows the list of one-time passwords.

4. **Click *Save*.**
   Your settings will be saved.

5.6.5 Advanced

Block Password Guessing

This function can be used to prevent password guessing. After a configurable number of failed login attempts (default: 3), the IP address trying to gain access to one of the facilities will be blocked for a configurable amount of time (default: 600 seconds).

Drop packets from blocked hosts: If enabled, all packets coming from blocked hosts will be dropped for the specified time. This option serves to avoid DoS attacks.

Facilities: The check will be performed for the selected facilities.

Never block networks: Networks listed in this box are exempt from this check.

Local Authentication Passwords

Using this option, you can force the use of strong passwords for administrators or locally registered users having administrative privileges. You can configure password complexity to adhere to the following security requirements:

- Minimum password length, default is eight characters
- Require at least one lowercase character
- Require at least one uppercase character
- Require at least one numeral
- Require at least one non-alphanumeric character

To enable the selected password properties select the *Require complex passwords* checkbox and click *Apply*.

Active Directory Group Membership Synchronization

Use this option to enable background syncing of AD group membership information.

The UTM can periodically synchronize group membership information and cache it locally to reduce traffic to the Active Directory server. When this option is enabled, group membership information will be synchronized with the configured Active Directory Single Sign-On server.

Click *Synchronize Now* to immediately synchronize group membership information.

Prefetch Directory Users

Users from eDirectory or Active Directory can be synchronized with UTM. This will pre-create user objects on UTM such that these user objects already exist, when the user logs in. The synchronization process can run weekly or daily.

To enable prefetching, make the following settings:

Server: The drop-down list contains servers that have been created on the *Servers* tab. Select a server for which you want to enable prefetching.

Prefetch interval: Select an interval to prefetch users. To run the synchronization weekly, select the day of the week when synchronization should start. To run the synchronization daily, select *Daily*.

Prefetch time: Select a time to prefetch users.

Groups: To specify which groups should be pre-created, enter the groups here. You can use the integrated LDAP browser to select these groups.

Enable Backend Sync on Login (optional): With every prefetch event, the *Backend sync* option of the involved users (*Users & Groups > Users* tab) will be set to the value defined here. If the option is enabled, the users' *Backend sync* option will be enabled, if the option is disabled, the users' *Backend sync* option will be disabled.

Click *Apply* to save your settings.

Prefetch Now: Click this button to start prefetching immediately.

Open Prefetch Live Log: Click this button to open the prefetch live log.

6 Interfaces & Routing

This chapter describes how to configure interfaces and network-specific settings in Sophos UTM. The *Network Statistics* page in WebAdmin provides an overview of today's top ten accounting services, top source hosts, and concurrent connections. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective reporting section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- Interfaces
- Bridging
- Quality of Service (QoS)
- Uplink Monitoring
- IPv6
- Static Routing
- Dynamic Routing (OSPF)
- Border Gateway Protocol
- Multicast Routing (PIM-SM)

6.1 Interfaces

A gateway requires at least two network interface cards to connect an internal LAN to an external one (e.g., the Internet) in a secure fashion. In the following examples, the network card `eth0` is always the interface connected to the internal network. Network card `eth1` is the interface connected to the external network (for example, to the Internet). These interfaces are also called the trusted and untrusted interfaces, respectively.

Network cards are automatically recognized during the installation. With the Software Appliance, if new network cards are added later, a new installation will be necessary. To reinstall the system, simply make a backup of your configuration, install the software, and restore your backup.

The gateway must be the only point of contact between internal and external networks. All data must pass through UTM. We strongly recommend against connecting both internal and

external interfaces to one hub or switch, except if the switch is configured as a VLAN switch. There might be wrong ARP resolutions (Address Resolution Protocol), also known as "ARP clash", which cannot be administered by all operating systems (for example, such as those from Microsoft). Therefore, one physical network segment has to be used for each gateway network interface.

The *Interfaces* menu allows you to configure and manage all network cards installed on UTM and also all interfaces with the external network (Internet) and interfaces to the internal networks (LAN, DMZ).

Note – While planning your network topology and configuring UTM, take care to note which interface is connected to which network. In most configurations, the network interface with SysID `eth1` is chosen as the connection to the external network. In order to install the high availability (HA) failover, the selected network cards on both systems must have the same SysID. Installing the HA failover is described in more detail on page *Management* > *High Availability*.

The following sections explain how to manage and configure different interface types on the tabs *Interfaces*, *Additional Addresses*, *Link Aggregation*, *Uplink Balancing*, *Multipath Rules*, and *Hardware*.

6.1.1 Interfaces

On the *Interfaces* tab you can configure network cards and virtual interfaces. The list shows the already defined interfaces with their symbolic name, hardware device, and current addresses. The interface status is also displayed. By clicking the toggle switch, you can activate and deactivate interfaces. Please note that interface groups do not have a toggle switch.

Tip – When you click the Info icon of an interface definition in the *Interfaces* list, you can see all configuration options in which the interface definition is used.

Newly added interfaces may show up as *Down* while they are in the process of being set up. You can select to edit and delete interfaces by clicking the respective buttons.

6.1.1.1 Automatic Interface Network Definitions

Each interface on your UTM has a symbolic name and a hardware device assigned to it. The symbolic name is used when you reference an interface in other configuration settings. For

each interface, a matching set of network definitions is automatically created by UTM:

- A definition containing the current IP address of the interface, its name consisting of the interface name and the *(Address)* suffix.
- A definition containing the network attached to the interface, its name consisting of the interface name and the *(Network)* suffix. This definition is not created for *Point-to-Point* (PPP) type interfaces.
- A definition containing the broadcast address of the interface, its name consisting of the interface name and the *(Broadcast)* suffix. This definition is not created for *Point-to-Point* (PPP) type interfaces.

When the interface uses a dynamic address allocation scheme (such as DHCP or remote assignment), these definitions are automatically updated. All settings referring to these definitions, for example firewall and NAT rules, will also automatically be updated with the changed addresses.

One interface with the symbolic name *Internal* is already predefined. It is the management interface and will typically be used as the "internal" UTM interface. If you want to rename it, you should do so right after the installation.

6.1.1.2 Interface Types

The following list shows which interface types can be added to UTM, and what type of hardware is needed to support them:

Group: You can organize your interfaces in groups. In appropriate configurations, you can then select a single interface group instead of multiple interfaces individually.

3G/UMTS: This is an interface based on a USB modem stick. The stick needs to be plugged in and UTM needs to be rebooted before interface creation.

DSL (PPPoA/PPTP): PPP over ATM. A DSL PPPoA device lets you attach your gateway to *PPP-over-ATM* compatible DSL lines. These devices use the PPTP protocol to tunnel IP packets. They require a dedicated Ethernet connection (they cannot co-exist with other interfaces on the same hardware). You must attach a DSL modem to the interfaces network segment. The network parameters for these device types can be assigned by the remote station (typically, your ISP). In addition, you need to enter username and password for your ISP account. You also need to enter the IP address of your modem. This address is usually hardwired in the modem and cannot be changed. To communicate with the modem, you have to enter a NIC IP address and netmask. The modem's IP address must be inside the network defined by these parameters. The *Ping Address* must be a host on the other side of the PPTP link that responds

to ICMP ping requests. You can try to use the DNS server of your ISP. If this address cannot be pinged, the connection is assumed to be dead, and will be reinitiated.

DSL (PPPoE): PPP over Ethernet. A DSL PPPoE device lets you attach your gateway to *PPP-over-Ethernet* compatible DSL lines. These devices require a dedicated Ethernet connection (they cannot co-exist with other interfaces on the same hardware). You must attach a DSL modem to the interfaces network segment. The network parameters for these device types can be assigned by the remote station (typically, your ISP). In addition, you need to enter username and password for your ISP account.

Ethernet DHCP: This is a standard Ethernet interface with DHCP.

Ethernet Static: This is a normal Ethernet interface, with 10, 100, or 1000 Mbit/s bandwidth.

Ethernet VLAN: VLAN (Virtual LAN) is a method to have multiple layer-2 separated network segments on a single hardware interface. Every segment is identified by a "tag", which is just an integer number. When you add a VLAN interface, you will create a "hardware" device that can be used to add additional interfaces (aliases), too. PPPoE and PPPoA devices cannot be run over VLAN virtual hardware.

Modem (PPP): This type of interface lets you connect UTM to the Internet through a PPP modem. For the configuration you need a serial interface and an external modem on the UTM. And you also need the DSL access data including username and password. You will get these data from your (ISP).

About Flexible Slots

Certain types of Sophos hardware appliances allow to easily change interface hardware by providing so-called slots where slot modules can be inserted and switched flexibly. If such hardware is being used, WebAdmin displays the slot information along with the hardware interfaces. This looks for example like *eth1 [A6] Intel Corporation 82576 Gigabit Network Connection*, where the slot information is provided in the square brackets, *A6* being the 6th port in slot A. Currently, up to three slots are possible, labeled A-C with up to eight ports each. Onboard interface cards will be labeled *[MGMT1]* and *[MGMT2]*.

Slot information is provided in the following places of WebAdmin:

- *Interfaces & Routing* > *Interfaces* > *Interfaces*
- *Interfaces & Routing* > *Interfaces* > *Hardware*
- Throughout WebAdmin in *Hardware* drop-down lists and lists where hardware interface information is displayed

For up-to-date information on which appliance types come with flexible slots, please refer to the Sophos UTM webpage.

6.1.1.3 Group

You can combine two or more interfaces to a group. Groups can ease your configuration tasks. When creating multipath rules, you need to configure a group if you want to balance traffic over a defined group of uplink interfaces only instead of using all uplink interfaces.

To configure a *Group* interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *Group* from the drop-down list.

   Interfaces: Add the interfaces to be grouped.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The group is added to the interface list. Groups do not have a status.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.4 3G/UMTS

Sophos UTM supports network connections via 3G/UMTS USB sticks.

To configure a 3G/UMTS interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *3G/UMTS* from the drop-down list.

Hardware: Select a USB modem stick from the drop-down list. Note that you need to reboot after you plugged the USB stick in.

Network: Select the mobile network type, which is either *GSM/W-CDMA*, *CDMA*, or *LTE*.

IPv4/IPv6 default GW (optional): Select this option if you want to use the default gateway of your provider.

PIN (optional): Enter the PIN of the SIM card if a PIN is configured.

APN Autoselect: (optional): By default, the APN (Access Point Name) used is retrieved from the USB modem stick. If you unselect the checkbox, enter APN information into the *APN* field.

Username/Password (optional): If required, enter a username and password for the mobile network.

Dial String (optional): If your provider uses a different dial string, enter it here. Default is `*99#`.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
Init String: Enter the string to initialize the USB modem stick. Remember that it might become necessary to adjust the init string to the USB modem stick. In this case, the init string can be gathered from the associated USB modem stick manual. If you do not have the required documentation available, keep the default setting *ATZ*.

Reset String: Enter the reset string for the USB modem stick. Keep in mind that it might be necessary to adjust the reset string to the USB modem stick. In this case you can gather it from the associated USB modem stick manual. If you do not have the required documentation available, keep the default setting *ATZ*.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).By default, an MTU of 1500 bytes is set for the *3G/UMTS* interface type.

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.5 Ethernet Static

To configure a network card for a static Ethernet connection to an internal or external network, you must configure the network card with an IP address and netmask.

To configure a static Ethernet interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *Ethernet Static* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

Tip – For an external connection (e.g., to the Internet) choose the network card with SysID eth1. Please note that one network card cannot be used as both an *Ethernet Static* interface and a *PPP over Ethernet (PPPoE DSL)* or *PPTP over Ethernet (PPPoA DSL)* connection simultaneously.

IPv4/IPv6 address: Enter the IP address of the interface.

Netmask: Select a network mask (IPv4) and/or enter an IPv6 network mask.

IPv4/IPv6 default GW (optional): Select this option if you want to use a statically defined default gateway.

Default GW IP (optional): Enter the IP address of the default gateway.

Note – You can configure an interface to have an IPv4 and an IPv6 address simultaneously.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).By default, an MTU of 1500 bytes is set for the *Ethernet Static* interface type.

Proxy ARP: To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off).
This option is available on broadcast-type interfaces. When you switch it on, UTM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes

are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.6 Ethernet VLAN

In order to connect UTM to the virtual LANs, the system requires a network card with a tag-capable driver. A tag is a 4-byte header attached to packets as part of the Ethernet header. The tag contains the number of the VLAN that the packet should be sent to: the VLAN number is a 12-bit number, allowing up to 4095 virtual LANs. In WebAdmin this number is referred to as the *VLAN tag*.

Note – Sophos maintains a list of supported tag-capable network interface cards. The *Hardware Compatibility List (HCL)* is available at the Sophos Knowledgebase. Use "HCL" as search term to locate the corresponding page.

To configure an Ethernet VLAN interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *Ethernet VLAN* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

   VLAN Tag: Enter the VLAN tag to use for this interface.

   IPv4/IPv6 address: Enter the IP address of the interface.

   Netmask: Select a network mask (IPv4) and/or enter an IPv6 network mask.

   IPv4/IPv6 default GW (optional): Select this option if you want to use a statically defined default gateway.

   Default GW IP (optional): Enter the IP address of the default gateway.

   Note – You can configure an interface to have an IPv4 and an IPv6 address simultaneously.

   Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the *Ethernet VLAN* interface type.

   Proxy ARP: To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off).
   This option is available on broadcast-type interfaces. When you switch it on, UTM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

   Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes

are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.7 Ethernet DHCP

To configure an *Ethernet DHCP* interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *Ethernet DHCP* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

> **Tip –** For an external connection (e.g., to the Internet) choose the network card with SysID `eth1`. Please note that one network card cannot be used as both a *Ethernet DHCP* and a *PPP over Ethernet* (PPPoE-DSL) or *PPTP over Ethernet* (PPPoA-DSL) connection simultaneously.

IPv4/IPv6 default GW (optional): Select this option if you want to use the default gateway of your provider.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Hostname: If your ISP requires to receive the hostname of your system, enter it here.

   MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the *Ethernet DHCP* interface type.

   Proxy ARP: To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off).
   This option is available on broadcast-type interfaces. When you switch it on, UTM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

   Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

   Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

5. **Enable the interface.**
   Click the toggle switch to activate the interface.

The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.8 DSL (PPPoE)

The configuration will require the DSL connection information, including username and password, provided by your ISP. VDSL is also supported by this interface type.

Note – Once the DSL connection is activated, the UTM will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time.

To configure a DSL (PPPoE) interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *DSL (PPPoE)* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

   VDSL: Select this checkbox if and only if your connection is a VDSL connection. The *MTU* changes to `1476`.

   Static PPPoE IP (optional): Select the checkbox if you have a static IP address assigned by your ISP, and enter the IP address and corresponding netmask into the appearing textboxes.

   - **IPv4/IPv6 Address:** Enter the IP address of the interface.
   - **Netmask:** Select a netmask from the drop-down list and/or enter an IPv6 netmask.

Note – You can configure an interface to have an IPv4 and an IPv6 address simultaneously.

IPv4/IPv6 Default GW (optional): Select this option if you want to use the default gateway of your provider.

Username: Enter the username, provided by your ISP.

Password: Enter the password, provided by your ISP.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1492 bytes is set for the *DSL (PPPoE)* interface type.

   VLAN tag (only if *VDSL* is enabled): Enter the VLAN tag to be added to the PPPoE packets. For the correct tag, refer to your VDSL provider. Default is 7, which is currently used for the PPPoE connection of the Deutsche Telekom.

   Daily reconnect: Define at what time you want the connection to close and reopen. You can select either *Never* or pick a specific time.

   Reconnect delay: Here you can change the reconnect delay. By default, it is set to *5 Seconds*. If your ISP demands a longer delay you can set it to *One Minute* or *Fifteen Minutes*.

   Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

   Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Multilink: If enabled, you can bundle multiple PPP connections. A multilink PPP connection only works if your ISP supports Multilink PPP.

Multilink slaves: Select the interfaces you want to bundle with the hardware selected above to one multilink.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.9 DSL (PPPoA/PPTP)

To configure a connection using the *PPP over ATM Protocol* (PPPoA), you will need an unused Ethernet interface on the UTM as well as an external ADSL modem with an Ethernet port. The connection to the Internet proceeds through two separate connections. Between the UTM and the ADSL modem, a connection using the *PPTP over Ethernet Protocol* is established. The ADSL modem is, in turn, connected to the ISP using the *PPP over ATM Dialing Protocol*.

The configuration will require the DSL connection information, including username and password, provided by your Internet Service Provider (ISP).

Note – Once the DSL connection is activated, the UTM will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time.

To configure a DSL (PPPoA/PPTP) interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *DSL (PPPoA/PPTP)* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

   IPv4/IPv6 default GW (optional): Select this option if you want to use the default gateway of your provider.

   Username: Enter the username, provided by your ISP.

   Password: Enter the password, provided by your ISP.

   Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Modem IP: Enter the IP address of your ADSL modem here. This address will usually be provided by your ISP or the modem hardware and cannot be changed. Example: `10.0.0.138` (with AonSpeed).

   NIC address: Enter the IP address of the network card on the UTM which is attached to the modem here. This address must be in the same subnet as the modem. Example: `10.0.0.140` (with AonSpeed).

   NIC netmask: Enter the network mask to use here.
   Example: `255.255.255.0` (with AonSpeed).

   Ping address (optional): Enter the IP address of a host on the Internet that responds to ICMP ping requests. In order to test the connection between the UTM and the external network, you have to enter an IP address of a host on the other side of the PPTP link. You can try to use the DNS server of your ISP. The UTM will send ping requests to this host: if no answer is received, the connection will be broken.

   MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1492 bytes is set for the *DSL (PPPoA)* interface type.

Daily reconnect: Define at what time you want the connection to close and reopen. You can select either *Never* or pick a specific time.

Reconnect delay: Here you can change the reconnect delay. By default, it is set to *5 Seconds*. If your ISP demands a longer delay you can set it to *One Minute* or *Fifteen Minutes*.

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.10 Modem (PPP)

For the configuration you need a serial interface and an external PPP modem on the UTM. And you also need the DSL access data including username and password. You will get these data from your Internet Service Provider (ISP).

To configure a *Modem (PPP)* interface, proceed as follows:

On the *Interfaces* tab, click *New Interface*.

1. The *Create New Interface* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for the interface.

   Type: Select *Modem (PPP)* from the drop-down list.

   Hardware: Select an interface from the drop-down list.

   IPv4/IPv6 default GW (optional): Select this option if you want to use the default gateway of your provider.

   Username: Enter the username, provided by your ISP.

   Password: Enter the password, provided by your ISP.

   Dial String: Enter the phone number. Example: `5551230`

   Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Line Speed: Set the speed in bits per seconds for the connection between the UTM and the modem. Common values are 57,600 Bits/s and 115,200 Bits/s.

   Flow Control: Select the method to control the data flow.
   If the data is transferred via the serial connection it might happen that the system cannot process incoming data fast enough. To ensure that no data is lost, this method of controlling the data flow becomes necessary. With the serial connection two methods are available:

   - *Hardware* signals
   - *Software* signals

   Since in a PPP connection all eight bits are used for the data transfer line and the transferred data contains the bytes of the command signs *Control S* and *Control Q*, we recommend keeping the default setting *Hardware* and using a serial connection cable.

   Init String: Enter the string to initialize the modem. Remember that it might become necessary to adjust the init string to the modem. In this case, the init string can be gathered from the associated modem manual. If you do not have the required documentation available, keep the default setting *ATZ*.

   Reset String: Enter the reset string for the modem. Keep in mind that it might be necessary to adjust the reset string to the modem. In this case you can gather it from the associated modem manual. If you do not have the required documentation available, keep the default setting *ATZ*.

MTU: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface).By default, an MTU of 1492 bytes is set for the *Modem (PPP)* interface type.

Asymmetric (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.2 Additional Addresses

One network card can be configured with additional IP addresses (also called *aliases*). This function allows you to manage multiple logical networks on one physical network card. It can also be used to assign further addresses to a UTM running NAT (Network Address Translation).

To configure additional addresses on standard Ethernet interfaces, proceed as follows:

1. **On the *Additional Addresses* tab, click *New Additional Address*.**
   The *Create New Additional Address* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the new additional address.

   On Interface: Select an interface from the drop-down list to which the address is to be assigned.

   IPv4/IPv6 Address: Enter the additional IP address of the interface.

   Netmask: Select a netmask from the drop-down list and/or enter an IPv6 netmask.

   Note – You can configure an interface to have an IPv4 and an IPv6 address simultaneously.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
4. **Enable the additional address.**
   Click the toggle switch to activate the additional address.

   The additional address is now enabled (toggle switch is green). The additional address might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the additional address is fully operable.

To either edit or delete an additional address, click the corresponding buttons.

6.1.3 Link Aggregation

Link aggregation, which is also known as "port trunking" or "NIC bonding", allows you to aggregate multiple Ethernet network ports into one virtual interface. The aggregated ports appear as a single IP address to your system. Link aggregation is useful to increase the link speed beyond the speed of any one single NIC or to provide basic failover and fault tolerance by redundancy in the event any port or switch fails. All traffic that was being routed over the failed port or switch is automatically re-routed to use one of the remaining ports or switches. This failover is completely transparent to the system using the connection.

Note – In a high-availability environment, Ethernet connections can even be on different HA units.

You can define up to four different link aggregation groups. A group can consist of one or multiple interfaces.

To create a link aggregation group (LAG), proceed as follows:

1. **For each LAG, select the interfaces you want to add.**
   A group can consist of a configured interface and/or one or more unconfigured interfaces.

   To use a configured interface, select it from the *Convert Interface* drop-down list. To use unconfigured interfaces, select the respective checkbox(es).

2. **Enable the LAG.**
   Activate a group by clicking the button *Enable this group*.

   Once the link aggregation group has been configured, a new LAG interface (e.g., `lag0`) becomes available for selection if you are going to create an interface definition on the *Interfaces* tab. On top of the bonding interface you can create one of the following:

   - Ethernet Static
   - Ethernet VLAN
   - Ethernet DHCP
   - Alias interfaces

To disable a LAG, clear the checkboxes of the interfaces that make up the LAG, click *Update this Group*, and confirm the warning message. The status of the LAG interface is shown on the *Support > Advanced > Interfaces Table* tab.

6.1.4 Uplink Balancing

With the uplink balancing function you can combine more than one Internet uplink, either for having backup uplinks available or for using load balancing among multiple uplinks. Combining up to 32 different uplinks is supported. Note that with BasicGuard subscription, only two uplinks can be combined.

Uplink balancing is automatically enabled when you assign a default gateway to an interface in addition to an already existing interface with a default gateway. All interfaces possessing a

default gateway will be added to the *Active interfaces* box and uplink balancing automatically organizes the balancing between those interfaces from then on. Any other interface with a default gateway will automatically be added, too.

On the *Multipath Rules* tab you can define specific rules for the traffic to be balanced.

To manually set up uplink balancing, proceed as follows:

1. **Enable uplink balancing.**
   Click the toggle switch.

   The toggle switch turns amber and the *Uplink Balancing* area becomes editable.

2. **Select active interfaces.**
   Add one or more interfaces by clicking the Folder icon and dragging interfaces from the object list. With multiple interfaces, traffic coming from clients is balanced by source, i.e., all traffic coming from one source uses the same interface, whereas traffic from another source can be sent to another interface. If one of the interfaces is unavailable, traffic will be taken over by the remaining interface(s).

   Note – Initially, when uplink balancing has been enabled automatically, the *Active interfaces* list already contains all interfaces having a default gateway. If you remove an interface from the list, the *Default gateway* checkbox of the interface will automatically be unselected. Thus, every interface having a default gateway has to be either on this list or on the *Standby interfaces* box below. However, you can add interfaces without default gateway and enter the default gateway address later on.

   Note – The sequence of the interfaces is important: In configurations where only one interface can be used, and for packets sent from the UTM itself, by default the first available active interface is used. You can change the interface sequence by clicking the Sort icons in the box.

   Using the Edit Scheduler icon on the box header, you can set individual balancing behavior and interface persistence of the active interfaces:

   Weight: Weight can be set from 0 to 100 and specifies how much traffic is processed by an interface relative to all other interfaces. A weighted round robin algorithm is used for this, a higher value meaning that more traffic is routed to the respective interface. The values are evaluated relative to each other so they need not add up to 100. Instead, you can have a configuration for example, where interface 1 has value 100, interface 2 has value

50 and interface 3 has value 0. Here, interface 2 gets only half the traffic of interface 1, whereas interface 3 only comes into action when none of the other interfaces is available. A value of zero means that always another interface with a higher value is chosen if available.

Persistence: Interface persistence is a technique which ensures that traffic having specific attributes is always routed over the same uplink interface. Persistence has a default timeout of one hour.

3. **Select standby interfaces** (optional).
Here, you can optionally add failover interfaces that should only come into action if all active interfaces become unavailable. In this case, the first available standby interface in the given order will be used. You can change the interface sequence by clicking the Sort icons in the box.

4. **Change monitoring settings** (optional).
By default, *Automatic monitoring* is enabled to detect possible interface failures. This means that the health of all uplink interfaces is monitored by having them contact a specific host on the Internet at an interval of 15 seconds. By default, the monitoring host is the third ping-allowing hop on the route to one of the root DNS servers. However, you can define the hosts for monitoring the server pool yourself. For these hosts you can select another service instead of ping, and modify the monitoring interval and timeout.

   If the monitoring hosts do not send a response anymore, the respective interface is regarded as dead and not used anymore for distribution. On the Dashboard, in the *Link* column of the interface, *Error* will be displayed.

   Note – Automatically, the same monitoring settings are used for both uplink monitoring (*Uplink Monitoring > Advanced*) and uplink balancing (*Interfaces > Uplink Balancing*).

   To define hosts for monitoring the server pool yourself, proceed as follows:

   1. **Unselect the *Automatic monitoring* checkbox.**
   The *Monitoring hosts* box becomes editable.

   2. **Add monitoring hosts.**
   Select or add one or more hosts that you want to use for monitoring instead of random hosts. If an interface is monitored by more than one host, it will only be regarded as dead if all monitoring hosts do not respond in the defined time span. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Note – If a selected host is bound to an interface, it will only be used to monitor this interface. If a host is not bound to an interface, it will be used to monitor all interfaces. Interfaces not covered by the selected hosts will be monitored by automatic monitoring.

Click the Monitoring Settings icon in the box header to set the monitoring details:

Monitoring type: Select the service protocol for the monitor checks. Select either *TCP* (TCP connection establishment), *UDP* (UDP connection establishment), *Ping* (ICMP Ping), *HTTP Host* (HTTP requests), or *HTTPS Host* (HTTPS requests) for monitoring. When using *UDP* a ping request will be sent initially which, if successful, is followed by a UDP packet with a payload of 0. If ping does not succeed or the ICMP port is unreachable, the connection is regarded as down.

Port (only with monitoring types *TCP* and *UDP*): Port number the request will be sent to.

URL (optional, only with monitoring types *HTTP/S Host*): URL to be requested. You can use other ports than the default ports 80 or 443 by adding the port information to the URL, e.g., `http://example.domain:8080/index.html`. If no URL is entered, the root directory will be requested.

Interval: Enter a time interval in seconds at which the hosts are checked.

Timeout: Enter a maximum time span in seconds for the monitoring hosts to send a response. If all monitoring hosts of an interface do not respond during this time, the interface will be regarded as dead.

3. **Click *Apply*.**
   Your settings will be saved.

A new virtual network interface named *Uplink Interfaces* is automatically created and now available for use by other functions of the Sophos UTM, e.g. IPsec rules. The virtual network interface *Uplink Interfaces* comprises all uplink interfaces added to the interface list.
Additionally, a new network group named *Uplink Primary Addresses* is automatically created and now available for use by other functions of the Sophos UTM, e.g. firewall rules. It refers to the primary addresses of all *Uplink Interfaces*.

In case of an interface failure, open VPN tunnels can be automatically re-established over the next available interface provided DynDNS is used or the remote server accepts the IP

addresses of all uplink interfaces. As a prerequisite, the IPsec rule must use the *Uplink Interfaces* as *Local interface*.

6.1.5 Multipath Rules

On the *Interfaces & Routing* > *Interfaces* > *Multipath Rules* tab you can set rules for uplink balancing. The rules are applied to the active interfaces on the *Uplink Balancing* tab when there is more than one interface to balance traffic between. Without multipath rules, all services are balanced by source, i.e., all traffic coming from one source uses the same interface, whereas traffic from another source can be sent to another interface. Multipath rules allow you to change this default interface persistence.

Note – Multipath rules can be set up for the service types TCP, UDP, or IP.

To create a multipath rule, proceed as follows:

1. **On the *Multipath Rules* tab, click *New Multipath Rule*.**
   The *Create New Multipath Rule* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the multipath rule.

   Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore. Place the more specific rules at the top of the list to make sure that more vague rules match last.

   Source: Select or add a source IP address or network to match.

   Service: Select or add the network service to match.

   Destination: Select or add a destination IP address or network to match.

   Tip – How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Itf. persistence: *Interface persistence* is a technique which ensures that traffic having specific attributes is always routed over the same uplink interface. Persistence has a default timeout of one hour, however you can change this timeout on the *Uplink Balancing* tab. You can decide what should be the basis for persistence:

- **By connection:** (default) Balancing is based on the connection, i.e., all traffic belonging to a particular connection uses the same interface, whereas traffic of another connection can be sent to another interface.
- **By source:** Balancing is based on the source IP address, i.e., all traffic coming from one source uses the same interface, whereas traffic from another source can be sent to another interface.

  Note – Basically, persistence by source cannot work when using a proxy because the original source information is lost. The HTTP proxy however is an exception: Traffic generated by the HTTP proxy will match against the original client source IP address and thus complies with interface persistence rules *By source*, too.

- **By destination:** Balancing is based on the destination IP address, i.e., all traffic going to one destination uses the same interface, whereas traffic to another destination can be sent to another interface.
- **By source/destination:** Balancing is based on the source/destination IP address combination, i.e., all traffic coming from a specific source A and going to a specific destination B uses the same interface. Traffic with another combination can be sent to another interface. Also, please notice the note above.
- **By interface:** Select an interface from the *Bind Interface* drop-down list. All traffic applying to the rule will be routed over this interface. In case of an interface failure and if no subsequent rules match, the connection falls back to default behavior.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Balanced to (not with persistence by interface): Add an interface group to the field. All traffic applying to the rule will be balanced over the interfaces of this group. By default, *Uplink Interfaces* is selected, so connections are balanced over all uplink interfaces.

   Skip rule on interface error: If selected, in case of an interface failure, the next matching multipath rule will be used for the traffic. If unselected, no other multipath rule will be used for the defined traffic in case of an interface failure. This for example makes sense when you want to ensure that SMTP traffic is only sent from a specific static IP address to prevent your emails from being classified as spam by the recipients due to an invalid sender IP address.

4. **Click *Save*.**
   The new multipath rule is added to the *Multipath Rules* list.
5. **Enable the multipath rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a rule, click the corresponding buttons.

6.1.6 Hardware

The *Interfaces & Routing* > *Interfaces* > *Hardware* tab lists all configured interfaces showing information such as the Ethernet mode of operation or the MAC address. On UTM hardware devices, for each interface, auto negotiation can be enabled or disabled.

Auto Negotiation: Usually, the Ethernet mode of operation (1000BASE-T full-duplex, 100BASE-T full-duplex, 100BASE-T half-duplex, 10BASE-T full-duplex, 10BASE-T half-duplex, and so on) between two network devices is automatically negotiated by choosing the best possible mode of operation supported by both devices, where higher speed (e.g. 1000 Mbit/sec) is preferred over lower speed (e.g. 100 Mbit/sec), and full duplex is preferred over half duplex at the same speed.

Caution – For proper 1000 Mbit/sec operation, auto negotiation is always required and mandatory by IEEE Std 802.3ab. Thus, be careful to never switch *Auto Negotiation* off for any interface with *Link mode 1000BASE-T*. The timing of your network link may fail, causing service degradation or failure. For 100 Mbit/sec and 10 Mbit/sec operation, auto negotiation is optional, but still recommended for use whenever possible.

Auto negotiation is enabled by default. In the rare case that you need to switch it off, click the *Edit* button of the corresponding interface card and change the setting in the appearing dialog box *Edit NIC Parameters* via the drop-down list *Link Mode*. Note that the drop-down list is only available with UTM hardware devices. Click *Save* to save your changes.

Caution – Be careful when disabling auto negotiation, as this might lead to mismatches, resulting in a significant performance decrease or even disconnect. If the respective network interface card is your interface to WebAdmin you may lose access to WebAdmin!

In case one of your interfaces lost its network link due to manipulation of auto negotiation or speed settings, just changing the settings back will typically not bring the interface back to normal operation: Changing auto negotiation or speed settings on disconnected interfaces is not reliable. Therefore first switch on auto negotiation and then reboot UTM to bring back normal operation.

HA Link Monitoring: If high availability is enabled, all configured interfaces are monitored for link status. In case of a link failure, a takeover is triggered. If a configured interface is not always connected (e.g. management interface) please disable HA link monitoring for the corresponding interface. Otherwise all HA nodes will stay in status UNLINKED. To disable HA link monitoring click the *Edit* button of the corresponding interface card and change the setting in the appearing dialog box *Edit NIC Parameters*. Click *Save* to save your changes.

Set Virtual MAC: Sometimes it is useful to be able to change the MAC address of a device. For example, there are some ISPs where the modem must be reset when the device connected to it changes and by that the MAC address of that device. By setting the MAC address to the value of the former device, a reset of the modem can be avoided.

UTM, however, does not overwrite the original MAC address of the device but instead sets a virtual MAC address. To do so, click the *Edit* button of the corresponding interface card. In the appearing dialog box *Edit NIC Parameters*, select the checkbox *Set Virtual MAC* and enter a valid MAC address. Click *Save* to save your changes.

To restore the original MAC address, click the *Edit* button of the corresponding interface card. In the appearing dialog box *Edit NIC Parameters*, unselect the checkbox *Set Virtual MAC*. Click *Save* to save your changes.

6.2 Bridging

Bridging is a packet forwarding technique primarily used in Ethernet networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on broadcasting to locate unknown devices.

Through bridging, several Ethernet networks or segments can be connected to each other. The data packets are forwarded through bridging tables, which assign the MAC addresses to a bridge port. The resulting bridge will transparently pass traffic across the bridge interfaces.

Note – Such traffic must explicitly be allowed by means of appropriate firewall rules.

Note – Most virtual hosts do not permit MAC address changes or promiscuous mode by default on their virtual interfaces. For bridging to work on virtual hosts, make sure that on the virtual host MAC address validation is disabled and promiscuous mode is allowed.

6.2.1 Status

To configure a bridge, proceed as follows:

1. **Enable bridging on the *Status* tab.**
   On the *Interfaces & Routing* > *Bridging* > *Status* tab, click the toggle switch.

   The toggle switch turns amber and the *Bridge Configuration* area becomes editable.

2. **Select the bridging mode.**
   You can choose between two bridging modes:

   - **Bridge all NICs:** Select this option to have all available Ethernet network interface cards joined to a bridge. Specifying a *Convert Interface* is mandatory with this mode. All interfaces except for the converted interface will be deleted.
   - **Bridge Selected NICs:** You can select individual NICs that should form the bridge. This requires that there are unused network interface cards available. Select one or more of them to form the bridge. It is also possible to specify a *Convert Interface* that will be copied to the new bridge.

   Note – For link aggregation you can bridge two LAG interfaces, for example, by using one of those two as a *Convert Interface*.

3. **Select the interface that should be converted to a bridge.**
   Only an already configured interface can be selected. The bridge will inherit the address settings of that interface, as well as alias addresses and VLAN settings.

4. **Click *Create Bridge*.**
   The network interfaces are being combined and the bridge is being activated (toggle switch shows green).

To cancel the configuration, click the amber colored toggle switch.

Once the bridge has been configured, the converted interface appears as a bridge device with SysID `br0` on the *Interfaces & Routing* > *Interfaces* tab. All interfaces that are members of the

remove an interface from the bridge, clear its checkbox and click *Update Bridge*.

To remove the bridge, proceed as follows:

1. **On the *Status* tab, click the toggle switch.**
   The toggle switch turns amber.
2. **Click *Confirm Removal of Bridge*.**
   The toggle switch turns gray. The bridge has been successfully removed.

6.2.2 Advanced

On the *Interfaces & Routing* > *Bridging* > *Advanced* tab, the following bridging options can be configured:

Allow ARP broadcasts: This function allows you to configure whether global ARP broadcasts should be forwarded by the bridge. If enabled, the bridge will allow broadcasts to the MAC destination address `FF:FF:FF:FF:FF:FF`. This, however, could be used by an alleged attacker to gather various information about the network cards employed within the respective network segment or even the security product itself. Therefore, the default setting is not to let such broadcasts pass the bridge.

Spanning Tree Protocol: Enabling this option will activate the Spanning Tree Protocol (STP). This network protocol detects and prevents bridge loops.

Caution – Be aware that the Spanning Tree Protocol is known to provide no security, therefore attackers may be able to alter the bridge topology.

Ageing Timeout: The amount of time in seconds after which an inactive MAC address will be deleted. The default time is 300 seconds.

Allow IPv6 Pass Through: Enabling this option will allow IPv6 traffic to pass the bridge without any inspection.

Virtual MAC Address: Here you can enter a static MAC address for the bridge. By default (and as long as the entry is 00:00:00:00:00:00), the bridge uses the lowest MAC address of all member interfaces.

Forwarded EtherTypes: By default, a bridge configured on the Sophos UTM only forwards IP packets. If you want additional protocols to be forwarded, you have to add their EtherType to this box. The types have to be entered as four-digit hexadecimal numbers. Popular examples are AppleTalk (type 809B), Novell (type 8138), or PPPoE (types 8863 and 8864). A typical use

case would be a bridge between your RED interfaces which should forward additional protocols between the connected networks.

6.3 Quality of Service (QoS)

Generally speaking, *Quality of Service* (QoS) refers to control mechanisms to provide better service to selected network traffic, and to provide priority in terms of guaranteed bandwidths in particular. In Sophos UTM, priority traffic is configured on the *Quality of Service (QoS)* tabs, where you can reserve guaranteed bandwidths for certain types of outbound network traffic passing between two points in the network, whereas shaping of inbound traffic is optimized internally by various techniques such as *Stochastic Fairness Queuing* (SFQ) or *Random Early Detection* (RED).

6.3.1 Status

The *Quality of Service (QoS)* > *Status* tab lists the interfaces for which QoS can be configured. By default, QoS is disabled for each interface.

To configure QoS for an interface, proceed as follows:

1. **Click the *Edit* button of the respective interface.**
   The *Edit Interface* dialog box opens.
2. **Make the following settings:**
   Downlink kbit/sec/Uplink kbit/sec: Enter the uplink and downlink bandwidth (in Kbit/s) provided by your ISP. For example, for a 5 Mbit/s Internet connection for both uplink and downlink, enter `5120`).

   If you have a fluctuating bandwidth, enter the lowest value that is guaranteed by your ISP. For example, if you have a 5 Mbit/s Internet connection for both uplink and downlink with a variation of 0.8 Mbit/s, enter 4300 Kbit/s. Note that if the available bandwidth becomes temporarily higher than the configured lowest guaranteed value, the gateway can make a projection taking the new bandwidth into account, so that the percentage bandwidth for the priority traffic will be increased as well; unfortunately, this does not work vice versa.

   Limit Uplink: Selecting this option tells the QoS function to use the configured downlink and uplink bandwidth as the calculation base for prioritizing traffic that passes this inter-

face. The *Limit Uplink* option is selected by default and should be used for the following interface types:

- Ethernet Static interface (with a router sitting in between the gateway and the Internet—the bandwidth provided by the router is known)
- Ethernet VLAN interface (with a router sitting in between the gateway and the Internet—the bandwidth provided by the router is known)
- DSL (PPPoE)
- DSL (PPPoA)
- Modem (PPP)

Clear the *Limit Uplink* checkbox for these interfaces whose traffic shaping calculation base can be determined by the maximum speed of the interface. However, this only applies to the following interface types:

- Ethernet Static interface (directly connected to the Internet)
- Ethernet VLAN interface (directly connected to the Internet)
- Ethernet DHCP

For interfaces with no specific uplink limit given, the QoS function shapes the entire traffic proportionally. For example, if you have configured 512 Kbit/s for VoIP traffic on a Ethernet DHCP interface and the available bandwidth has decreased by half, then 256 Kbit/s would be used for this traffic (note that proportional shaping works in both directions in contrast to interfaces that rely on a fix maximum limit).

Download Equalizer: If enabled, *Stochastic Fairness Queuing* (SFQ) and *Random Early Detection* (RED) queuing algorithms will avoid network congestion. In case the configured downlink speed is reached, packets from the most downlink consuming stream will be dropped.

Upload Optimizer: If enabled, this option will automatically prioritize outgoing TCP connection establishments (TCP packets with *SYN* flag set), acknowledgment packets of TCP connections (TCP packets with *ACK* flag set and a packet length between 40 and 60 bytes) and DNS lookups (UDP packets on port `53`).

3. **Click *Save*.**
   Your settings will be saved.
4. **Enable QoS for the interface.**
   Click the toggle switch of the interface. The toggle switch turns green.

6.3.2 Traffic Selectors

A traffic selector can be regarded as a QoS definition which describes certain types of network traffic to be handled by QoS. These definitions later get used inside the bandwidth pool definition. There you can define how this traffic gets handled by QoS, like limiting the overall bandwidth or guarantee a certain amount of minimum bandwidth.

To create a traffic selector, proceed as follows:

1. **On the *Traffic Selector* tab, click *New Traffic Selector*.**
   The *Create New Traffic Selector* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this traffic selector.

   Selector type: You can define the following types:

   - **Traffic selector:** Using a traffic selector, traffic will be shaped based on a single service or a service group.
   - **Application selector:** Using an application selector, traffic will be shaped based on applications, i.e. which traffic belongs to which application, independent from the port or service used.
   - **Group:** You can group different service and application selectors into one traffic selector rule. To define a group, there must be some already defined single selectors.

   Source: Add or select the source network for which you want to enable QoS.

   Service: Only with *Traffic selector*. Add or select the network service for which you want to enable QoS. You can select among various predefined services and service groups. For example, select VoIP protocols (SIP and H.323) if you want to reserve a fixed bandwidth for VoIP connections.

   Destination: Add or select the destination network for which you want to enable QoS.

   Tip – How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Control by: Only with *Application selector*. Select whether to shape traffic based on its application type or by a dynamic filter based on categories.

- **Applications:** The traffic is shaped application-based. Select one or more applications in the box *Control these applications*.
- **Dynamic filter:** The traffic is shaped category-based. Select one or more categories in the box *Control these categories*.

Control these applications/categories: Only with *Application selector*. Click the Folder icon to select applications/categories. A dialog window opens, which is described in detail in the next section.

Productivity: Only with *Dynamic filter*. Reflects the productivity score you have chosen.

Risk: Only with *Dynamic filter*. Reflects the risk score you have chosen.

Note – Some applications cannot be shaped. This is necessary to ensure a flawless operation of Sophos UTM. Such applications miss a checkbox in the application table of the *Select Application* dialog window, e.g. *WebAdmin*, *Teredo* and *SixXs* (for IPv6 traffic), *Portal* (for User Portal traffic), and some more. When using dynamic filters, shaping of those applications is also prevented automatically.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**

TOS/DSCP (only with selector type *Traffic Selector*): In special cases it can be useful to distinguish traffic to be handled by QoS not only by its source, destination, and service but additionally based on its TOS or DSCP flags in the IP header.

- **Off:** With this default option all traffic matching the source, service and destination selected above will be handled by QoS.
- **TOS bits:** Select this option if you want to restrict the traffic handled by QoS to IP packets with specific TOS bits (Type of Service) settings. You can choose between the following settings:
  - Normal service
  - Minimize monetary cost
  - Maximize reliability
  - Maximize throughput
  - Minimize delay

- **DSCP bits:** Select this option if you want to restrict the traffic handled by QoS to IP packets with specific DSCP bits (Differentiated Services Code Point) settings. You can either specify a single *DSCP Value* (an integer in the range from 0-63) or select a predefined value from the *DSCP Class* list (e.g., *BE default dscp (000000)*).

Amount of data sent/received: Select the checkbox if you want the traffic selector to match based on the amount of bytes transferred by a connection so far. With this feature you can e.g. limit the bandwidth of large HTTP uploads without constraining regular HTTP traffic.

- **Sent/Received:** From the drop-down list, select *More than* to define the traffic selector only for connections which exceed a certain amount of traffic. Select *Less than* to define it for connections with less traffic so far.
- **kByte:** Enter the threshold for the amount of traffic.

Helper: Some services use dynamic port ranges for data transmission. For each connection, the ports to be used are negotiated between the endpoints via a control channel. The UTM uses a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used. To include the traffic sent through the dynamic ports in the traffic selector, select *Any* in the *Service* box above, and select the respective service from the *Helper* drop-down list.

4. **Click *Save*.**
   The new selector appears on the *Traffic Selectors* list.

If you defined many traffic selectors, you can combine multiple selectors inside a single traffic selector group, to make the configuration more convenient.

This traffic selector or traffic selector group can now be used in each bandwidth pool. These pools can be defined on the *Bandwidth Pools* tab.

The Select Application or Category Dialog Window

When creating application control rules you need to choose applications or application categories from a dialog window called *Select one or more applications/categories to control*.

The table in the lower part of the dialog window displays the applications you can choose from or which belong to a defined category. By default, all applications are displayed.

The upper part of the dialog window provides three configuration options to limit the number of applications in the table:

- **Category:** Applications are grouped by category. This list contains all available categories. By default, all categories are selected, which means that the table below displays all applications available. If you want to limit the displayed applications to certain categories, click into the category list and select only one or more categories relevant to you.
- **Productivity:** Applications are also classified by their productivity impact which means how much they influence productivity. Example: Salesforce, a typical business software, has the score 5 which means its usage adds to productivity. On the contrary, Farmville, an online game, has the score 1 which means its usage is counterproductive. The network service DNS has the score 3 which means its productivity impact is neutral.
- **Risk:** Applications are also classified by the risk they carry when used with regard to malware, virus infections, or attacks. A higher number means a higher risk.

Tip – Each application has an Info icon which, when clicked, displays a description of the respective application. You can search the table by using the filter field in the table header.

Now, depending on the type of control you selected in the *Create New Traffic Selector* dialog box, do the following:

- Control by dynamic filter: Select the categories from the *Category* box and click *Apply* to adopt the selected categories to your rule.
- Control by application: From the table, select the applications you want to control by clicking the checkbox in front. Click *Apply* to adopt the selected applications to your rule.

After clicking *Apply*, the dialog window closes and you can continue to edit the settings of your traffic selector rule.

6.3.3 Bandwidth Pools

On the *Quality of Service (QoS)* > *Bandwidth Pools* tab you can define and manage bandwidth pools for bandwidth management. With a bandwidth pool, you reserve a guaranteed bandwidth for a specific outgoing traffic type, optionally limited by a maximum bandwidth limit.

To create a bandwidth pool, proceed as follows:

1. **On the *Bandwidth Pools* tab, select an interface.**
   From the *Bound to interface* drop-down list, select the interface for which you want to create a bandwidth pool.

2. **Click *New Bandwidth Pool*.**
   The *Create New Bandwidth Pool* dialog box opens.

3. **Make the following settings:**
   Name: Enter a descriptive name for this bandwidth pool.

   Position: The position number, defining the priority of the bandwidth pool. Lower numbers have higher priority. Bandwidth pools are matched in ascending order. Once a bandwidth pool has matched, bandwidth pools with a higher number will not be evaluated anymore. Place the more specific pools at the top of the list to make sure that more vague pools match last. For example, if you have configured a traffic selector for web traffic (HTTP) in general and for web traffic to a particular host, place the bandwidth pool that uses the latter traffic selector on top of the bandwidth pool list, that is, select position 1 for it.

   Bandwidth: Enter the uplink bandwidth (in Kbit) you want to reserve for this bandwidth pool. For example, if you want to reserve 1 Mbit/s for a particular type of traffic, enter `1024`.

   Note – You can only assign up to 90 % of the entire available bandwidth to a bandwidth pool. The gateway always reserves 10 % of the bandwidth for so-called unshaped traffic. To stay with the example above, if your uplink Internet connection is 5 Mbit/s and you want to assign as much bandwidth as possible to VoIP traffic, you can at most enter a value of 4608 Kbit/s.

   Specify upper bandwidth limit: The value you entered in the *Bandwidth* field above represents the guaranteed bandwidth to be reserved for a specific kind of traffic. However, a bandwidth pool usually allocates more bandwidth for its traffic if available. If you want a particular traffic not to consume more than a certain amount of your bandwidth, select this option to restrict the allocation of bandwidth to be used by this bandwidth pool to an upper limit.

   Traffic selectors: Select the traffic selectors you want to use for this bandwidth pool.

   Comment (optional): Add a description or other information.

4. **Click *Save*.**
   The new bandwidth pool appears on the *Bandwidth Pools* list.

5. **Enable the rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a bandwidth pool, click the corresponding buttons.

6.3.4 Download Throttling

On the *Quality of Service (QoS)* > *Download Throttling* tab you can define and manage rules to throttle incoming traffic. If packets are coming in faster than the configured threshold, excess packets will be dropped immediately without being listed in the firewall rules log file. As a result of TCP congestion avoidance mechanisms, affected senders should reduce their sending rates in response to the dropped packets.

To create a download throttling rule, proceed as follows:

1. **On the *Download Throttling* tab, select an interface.**
   From the *Bound to interface* drop-down list, select the interface for which you want to create a download throttling rule.
2. **Click *New Download Throttling Rule*.**
   The *Create New Download Throttling Rule* dialog box opens.
3. **Make the following settings:**
   Name: Enter a descriptive name for this download throttling rule.

   Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore. Place the more specific rules at the top of the list to make sure that more vague rules match last.

   Limit (kbit/s): The upper limit (in Kbit) for the specified traffic. For example, if you want to limit the rate to 1 Mbit/s for a particular type of traffic, enter 1024.

   Limit: Combination of traffic source and destination where the above defined limit should apply:

   - **shared:** The limit is equally distributed between all existing connections. I.e., the overall download rate of the traffic defined by this rule is limited to the specified value.
   - **each source address:** The limit applies to each particular source address.

- **each destination address:** The limit applies to each particular destination address.
- **each source/destination:** The limit applies to each particular pair of source or destination address.

Traffic selectors: Select the traffic selectors for which you want to throttle the download rates. The defined limit will be divided between the selected traffic selectors.

Comment (optional): Add a description or other information.

4. **Click *Save*.**
   The new download throttling rule appears on the *Download Throttling* list.
5. **Enable the rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a rule, click the corresponding buttons.

6.3.5 Advanced

Keep classification after encapsulation

Select this checkbox if you want to make sure that after encapsulation a packet will still match the traffic selector of the original service if no other traffic selector matches.

The assignment of an encapsulated IP packet to a traffic selector works as follows:

1. The original IP packet is compared with the existing traffic selectors in the given order. The packet is assigned to the first matching traffic selector (e.g., Internal -> HTTP -> Any).
2. The IP packet gets encapsulated, and the service changes (e.g., to IPsec).
3. The encapsulated packet is compared with the existing traffic selectors in the given order. The packet is assigned to the first matching traffic selector (e.g., Internal -> IPsec -> Any).
4. If no traffic selector matches, the assignment depends on the *Keep classification after encapsulation* option:
   - If the option is selected, the encapsulated packet will be assigned to the traffic selector found in step 1.

- If the option is not selected, the encapsulated packet will not be assigned to any traffic selector and therefore cannot be part of a bandwidth pool.

Explicit Congestion Notification support

ECN (Explicit Congestion Notification) is an extension to the Internet Protocol and allows end-to-end notifications of network congestion without dropping packets. ECN only works if both endpoints of a connection successfully negotiate to use it. Selecting this checkbox, the UTM will send the information that it is willing to use ECN. If the other endpoint agrees, they will exchange ECN information. Note that the underlying network and involved routers must support ECN as well.

6.4 Uplink Monitoring

The menu *Interfaces & Routing* > *Uplink Monitoring* gives you the possibility to monitor your uplink connection and to define certain actions which will be automatically applied in case the connection status changes.

For example, you can automatically turn on a backup VPN tunnel using another link, or disable an alias IP address so that it will trigger a monitoring service.

6.4.1 Global

On the *Uplink Monitoring* > *Global* tab you can enable or disable uplink monitoring.

To enable uplink monitoring, click the toggle switch.
The toggle switch turns green.

If uplink monitoring is enabled, the *Uplink Status* section shows all current uplink interfaces and their statuses:

- *ONLINE:* The uplink connection is established and functional.
- *OFFLINE:* According to the monitoring, the uplink connection is defective.
- *DOWN:* Either the uplink interface is disabled administratively, or—in case of a dynamic interface—the remote PPP or DHCP server is not reachable.
- *STANDBY:* The interface is defined as a standby interface on the *Interfaces* > *Uplink Balancing* tab, and it is currently not in use.

Note – If uplink balancing is enabled, the uplinks will always be monitored, even if uplink monitoring is disabled. Therefore, even if uplink monitoring is disabled, the uplink interfaces are displayed on this page when uplink balancing is enabled. In this case, the monitoring settings can be modified on the *Interfaces* > *Uplink Balancing* tab.

6.4.2 Actions

On the *Interfaces & Routing* > *Uplink Monitoring* > *Actions* tab you can define actions that will be automatically applied in case the uplink connection status changes. For example, you might want to disable an additional address, when your uplink connection is down.

To create a new action, do the following:

1. **On the *Actions* tab, click *New Action*.**
   The dialog box *Create New Action If Uplink Goes Offline* opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the action.

   Type: Select the connection type for which you want to define an action.

   - **IPsec tunnel:** Select this option from the drop-down list if you want to define an action for an IPsec tunnel.
   - **Additional address:** Select this option from the drop-down list if you want to define an action for an additional address.

   IPsec tunnel: (Only available with Type *IPsec Tunnel*.) If there are any IPsec tunnels defined, you can select one of them here. For more information on IPsec tunnels see chapter *Remote Access* > *IPsec*.

   Add. address: (Only available with Type *Additional Address*.) If there are any additional addresses defined, you can select one of them here. For more information on additional addresses see chapter *Interfaces & Routing* > *Interfaces* > *Additional Addresses*.

   Action: You can either select *Enable* or *Disable* here, which means that, in case of an uplink interruption, the above selected IPsec tunnel or additional address is going to be enabled or disabled.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The action will be saved and applied in case the uplink connection is interrupted.

To either edit or delete an action, click the corresponding buttons.

6.4.3 Advanced

On the *Uplink Monitoring* > *Advanced* tab you can disable automatic monitoring of the uplink connection and define one or more hosts instead which are used for monitoring.

By default, *Automatic monitoring* is enabled to detect possible interface failures. This means that the health of all uplink interfaces is monitored by having them contact a specific host on the Internet at an interval of 15 seconds. By default, the monitoring host is the third ping-allowing hop on the route to one of the root DNS servers. However, you can define the hosts for monitoring the server pool yourself. For these hosts you can select another service instead of ping, and modify the monitoring interval and timeout.

The monitoring hosts will then be contacted in certain periods and if none of them is reachable, the uplink connection is regarded as down. Subsequently, the actions defined on the *Actions* tab will be carried out.

Note – Automatically, the same monitoring settings are used for both uplink monitoring (*Uplink Monitoring* > *Advanced*) and uplink balancing (*Interfaces* > *Uplink Balancing*).

To use your own hosts for monitoring, do the following:

1. **Unselect the *Automatic monitoring* checkbox.**
   The *Monitoring hosts* box becomes editable.
2. **Add monitoring hosts.**
   Select or add one or more hosts that you want to use for monitoring instead of random hosts. If an interface is monitored by more than one host, it will only be regarded as dead if all monitoring hosts do not respond in the defined time span. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Note – If a selected host is bound to an interface, it will only be used to monitor this interface. If a host is not bound to an interface, it will be used to monitor all interfaces. Interfaces not covered by the selected hosts will be monitored by automatic monitoring.

   Click the Monitoring Settings icon in the box header to set the monitoring details:

Monitoring type: Select the service protocol for the monitor checks. Select either *TCP* (TCP connection establishment), *UDP* (UDP connection establishment), *Ping* (ICMP Ping), *HTTP Host* (HTTP requests), or *HTTPS Host* (HTTPS requests) for monitoring. When using *UDP* a ping request will be sent initially which, if successful, is followed by a UDP packet with a payload of 0. If ping does not succeed or the ICMP port is unreachable, the connection is regarded as down.

Port (only with monitoring types *TCP* and *UDP*): Port number the request will be sent to.

URL (optional, only with monitoring types *HTTP/S Host*): URL to be requested. You can use other ports than the default ports 80 or 443 by adding the port information to the URL, e.g., `http://example.domain:8080/index.html`. If no URL is entered, the root directory will be requested.

Interval: Enter a time interval in seconds at which the hosts are checked.

Timeout: Enter a maximum time span in seconds for the monitoring hosts to send a response. If all monitoring hosts of an interface do not respond during this time, the interface will be regarded as dead.

3. **Click *Apply*.**
   Your settings will be saved.

6.5 IPv6

Starting with version 8, Sophos UTM supports IPv6, the successor of IPv4.

The following functions of UTM fully or partly support IPv6.

- Access to WebAdmin and User Portal
- SSH
- NTP
- SNMP
- SLAAC (Stateless Address Autoconfiguration) and DHCPv6 client support for all dynamic interface types
- DNS
- DHCP server
- BGP

- OSPF
- IPS
- Firewall
- NAT
- ICMP
- Server Load Balancing
- Web Filter
- Web Application Firewall
- SMTP
- IPsec (Site-to-site only)
- Syslog server

6.5.1 Global

On the *IPv6* > *Global* tab you can enable IPv6 support for Sophos UTM. Moreover, if enabled, IPv6 information is provided here, e.g., status information or prefix delegation information.

IPv6 support is disabled by default. To enable IPv6, do the following:

1. **On the *Global* tab, enable IPv6.**
   Click the toggle switch.

   The toggle switch turns green. If IPv6 has never been enabled or configured before, the *Connectivity* area displays the string *None*.

As soon as IPv6 is enabled, you will find several network and other object definitions referring explicitly to IPv6 around WebAdmin. You can generally use them as you are used to from IPv4 objects.

Note – If IPv6 is enabled, the icons of network objects and the like bear an additional mark that tells you whether the respective object is an IPv6 object or IPv4 object or both.

6.5.2 Prefix Advertisements

On the *IPv6* > *Prefix Advertisements* tab you can configure your Sophos UTM to assign clients an IPv6 address prefix which in turn enables them to pick an IPv6 address by themselves. Prefix

advertisement (or router advertisement) is an IPv6 feature where routers (or in this case the UTM) behave like a DHCP server in IPv4, in a way. However, the routers do not assign IPs directly to clients. Instead, clients in an IPv6 network assign themselves a so-called link-local address for the primary communication with the router. The router then tells the client the prefix for its network segment. Subsequently, the clients generate an IP address consisting of the prefix and their MAC address.

To create a new prefix, do the following:

1. **On the *Prefix Advertisements* tab, click *New Prefix*.**
   The dialog box *Create New Prefix* opens.
2. **Make the following settings:**
   Interface: Select an interface that has an IPv6 address with a 64 bit netmask configured.

   DNS server 1/2 (optional): The IPv6 addresses of the DNS servers.

   Domain (optional): Enter the domain name that will be transmitted to the clients (e.g., `intranet.example.com`).

   Valid lifetime: The time the prefix is to be valid. Default is 30 days.

   Preferred lifetime: The time after which another prefix, whose preferred lifetime has not yet expired, is to be selected by the client. Default is 7 days.

   Other config (optional): This option is selected by default. It ensures that a given DNS server and domain name are additionally announced via DHCPv6 for the given prefix. This is useful since, at the moment, there are too few clients which are able to fetch the DNS information from the prefix advertisement (RFC 5006/ RFC 6106). Note that this DHCPv6 configuration is hidden and therefore not visible or editable via the DHCP configuration menu.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new prefix configuration appears on the *Prefix Advertisements* list.

6.5.3 Renumbering

On the *IPv6 > Renumbering* tab you can allow automatic renumbering of IPv6 addresses managed by the UTM in case of a prefix change. Additionally, you can renumber IPv6 addresses manually.

The following IPv6 addresses will be modified:

- Hosts, networks, and range definitions
- Primary and secondary interface addresses
- DHCPv6 server ranges and mappings
- DNS mappings

An IPv6 prefix provided via tunnel brokerage will not be renumbered.

Automatic IPv6 Renumbering

By default, IPv6 addresses managed by your UTM are automatically renumbered in the event that the IPv6 prefix changes. Prefix changes are initiated by your ISP via DHCPv6 prefix delegation. To deactivate renumbering, unselect the checkbox and click *Apply*.

Manual IPv6 Renumbering

You can renumber particular IPv6 addresses managed by the UTM manually. This can be useful if you change your ISP, and your new provider assigns a new IPv6 prefix statically to you instead of automatically via DHCPv6.

1. **Specify the current prefix of the IPv6 addresses to be renumbered.**
   Enter the prefix into the *Old prefix* field.
2. **Specify the new prefix.**
   Enter the prefix into the *New prefix* field.
3. **Click *Apply*.**

   All IPv6 addresses with the defined current prefix will be renumbered using the new prefix.

6.5.4 6to4

On the *IPv6* > *6to4* tab you can configure your Sophos UTM to automatically tunnel IPv6 addresses over an existing IPv4 network. With 6to4, every IPv4 address has a `/48` prefix from the IPv6 network to which it is mapped. The resulting IPv6 address consists of the prefix `2002` and the IPv4 address in hexadecimal notation.

Note – You can either have *6to4* enabled or *Tunnel Broker*.

To enable IP address tunneling for a certain interface, do the following:

1. **On the *6to4* tab, enable 6to4.**
   Click the toggle switch.

   The toggle switch turns amber and the *6to4* area and the *Advanced* area become editable.

2. **Select an interface.**
   Select an interface from the *Interface* drop-down list which has a public IPv6 address configured.

3. **Click *Apply*.**
   Your settings will be saved. The interface status is displayed on the *Global* tab.

Advanced

You can change the *Server Address* to use a different 6to4 relay server.

Click *Apply* to save your settings.

6.5.5 Tunnel Broker

On the *IPv6* > *Tunnel Broker* tab you can enable the use of a tunnel broker. Tunnel brokerage is a service offered by some ISPs which allows you to access the Internet using an IPv6 address.

Note – You can either have *6to4* enabled or *Tunnel Broker*.

Sophos UTM supports the following tunnel brokers:

- Teredo (only anonymous)
- Freenet6 (by GoGo6) (anonymous or with user account)
- SixXS (user account necessary)

To use a tunnel broker, do the following:

1. **On the *Tunnel Broker* tab, enable the use of tunnel broker.**
   Click the toggle switch.

   The toggle switch turns green and the *Tunnel Broker* area and the *Advanced* area become editable. The tunnel broker is immediately active using anonymous authentication at Teredo. The connection status is displayed on the *Global* tab.

Tunnel Broker

You can change the default tunnel broker settings.

Authentication: Select an authentication method from the drop-down list.

- **Anonymous:** Using this method you do not need a user account at the respective broker. The IP address assigned will be, however, temporary.
- **User:** You need to register at the respective broker to get a user account.

Broker: You can select another broker from the drop-down list.

Username (only available with *User*): Provide your username for the respective broker.

Password (only available with *User*): Provide your password for the username.

Click *Apply* to save your settings.

Advanced

Here you can provide another server address for your selected tunnel broker.

Click *Apply* to save your settings.

6.6 Static Routing

Every computer connected to a network uses a routing table to determine the path along which an outbound data packet must be sent to reach its destination. For example, the routing table contains the information whether the destination address is on the local network or if the data packet must be forwarded to a router. If a router is involved, the table contains information about which router is to be used for which network.

Two types of routes can be added to the routing table of Sophos UTM: standard static routes and policy routes. With static routes, the routing target is exclusively determined by the packet's destination address. With policy routes, however, it is possible to make routing decisions based on the source interface, source address, service, or destination address.

Note – You do not need to set additional routes for networks attached to UTM's interfaces, as well as default routes. The system inserts these routes automatically.

6.6.1 Standard Static Routes

The system automatically inserts routing entries into the routing table for networks that are directly connected to the system. Manual entries are necessary in those cases where there is an additional router which is to be accessed via a specific network. Routes for networks, that are

not directly connected and that are inserted to the routing table via a command or a configuration file, are called static routes.

To add a standard static route, proceed as follows:

1. **On the *Standard Static Routes* tab click *New Static Route.***
   The *Create New Static Route* dialog box opens.
2. **Make the following settings:**
   Route type: The following route types are available:
   - **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
   - **Gateway route:** Packets are sent to a particular host (gateway).
   - **Blackhole route:** Packets are discarded silently. This is useful in connection with OSPF or other dynamic adaptive routing protocols to avoid routing loops, route flapping, and the like.

   Network: Select the destination networks of data packets UTM must intercept.

   Interface: Select the interface through which the data packets will leave UTM (only available if you selected *Interface Route* as route type).

   Gateway: Select the gateway/router to which UTM will forward data packets (only available if you selected *Gateway Route* as route type).

   Comment (optional): Add a description or other information.
3. **Optionally, make the following advanced setting:**
   Metric: Enter a metric value which can be an integer from 0 to 4294967295 with a default of 5. The metric value is used to distinguish and prioritize routes to the same destination. A lower metric value is preferred over a higher metric value. IPsec routes automatically have the metric 0.
4. **Click *Save*.**
   The new route appears on the *Standard Static Route* list.
5. **Enable the route.**
   Click the toggle switch to activate the route.

To either edit or delete a route, click the corresponding buttons.

6.6.2 Policy Routes

When a router receives a data packet, it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria. Policy-based routing allows for forwarding or routing of data packets according to your own policies.

To add a policy route, proceed as follows:

1. **On the *Policy Routes* tab click *New Policy Route*.**
   The *Create New Policy Route* dialog box opens.

2. **Make the following settings:**
   Position: The position number, defining the priority of the policy route. Lower numbers have higher priority. Routes are matched in ascending order. Once a route has matched, routes with a higher number will not be evaluated anymore.

   Route type: The following route types are available:

   - **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
   - **Gateway route:** Packets are sent to a particular host (gateway).

   Source interface: The interface on which the data packet to be routed has arrived. The *Any* setting applies to all interfaces.

   Source network: The source network of the data packets to be routed. The *Any* setting applies to all networks.

   Service: The service definition that matches the data packet to be routed. The drop-down list contains all predefined services as well as the services you have defined yourself. These services allow you to specify precisely which kind of traffic should be processed. The *Any* setting matches any combination of protocols and source and destination ports.

   Destination network: The destination network of the data packets to be routed. The *Any* setting applies to all networks.

Target interface: The interface for the data packets to be sent to (only available if you selected *Interface Route* as route type).

Gateway: Select the gateway/router to which the gateway will forward data packets (only available if you selected *Gateway Route* as route type).

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new route appears on the *Policy Routes* list.
4. **Enable the route.**
   Click the toggle switch to activate the route.

To either edit or delete a route, click the corresponding buttons.

6.7 Dynamic Routing (OSPF)

The *Open Shortest Path First* (OSPF) protocol is a link-state hierarchical routing protocol primarily used within larger autonomous system networks. Sophos UTM supports OSPF version 2. Compared to other routing protocols, OSPF uses cost as its routing metric. The cost of an OSPF-enabled interface is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. Therefore, a higher bandwidth indicates a lower cost. For example, there is more overhead (higher cost) and time delays involved in crossing a 56 Kbit/s serial line than crossing a 10 Mbit/s Ethernet line.

The OSPF specification does not specify how the cost of an attached network should be computed—this is left to the vendor. Therefore you are free to define your own computation formula. However, if your OSPF network is adjacent to other networks that have cost already defined, you are advised to apply the same computation base.

By default, the cost of an interface is calculated based on the bandwidth. Cisco, for example, computes the cost by dividing 10^8 through the bandwidth of the interface in bits per second. Using this formula, it will cost $10^8/10000000 = 10$ to cross a 10 Mbit/s Ethernet line, whereas it will cost $10^8/1544000 = 64$ to cross a 1.544 Mbit/s line (T1) (note that the cost is rounded down to the nearest integer).

6.7.1 Global

On the *Interfaces & Routing* > *Dynamic Routing (OSPF)* > *Global* tab you can make the basic settings for OSPF. Before you can enable the OSPF function, you must have at least one OSPF area configured (on the *Area* tab).

Caution – Configuring the OSPF function of Sophos UTM requires a technically adept and experienced administrator who is familiar with the OSPF protocol. The descriptions of configuration options given here are by far not sufficient to provide a comprehensive understanding of the OSPF protocol. You are thus advised to use this feature with caution, as a misconfiguration may render your network inoperable.

To configure OSPF, proceed as follows:

1. **On the *Area* tab, create at least one OSPF area.**
2. **On the *Global* tab, enable OSPF.**
   Click the toggle switch.

   The toggle switch turns amber and the *Router* area becomes editable.
3. **Enter the router ID.**
   Enter a unique router ID to identify the Sophos UTM device to other OSPF routers.
4. **Click *Apply*.**
   Your settings will be saved.

To disable OSPF click the toggle switch.

6.7.2 Area

An OSPF network is divided into areas. These are logical groupings of routers whose information may be summarized towards the rest of the network. Areas are identified by a 32-bit ID in dot-decimal notation similar to the notation of IP addresses.

Altogether, there are six types of OSPF areas:

- **Backbone:** The area with ID 0 (or `0.0.0.0`) is reserved for the OSPF network backbone, which forms the core of an OSPF network—all other areas are connected to it.

- **Normal:** A normal or regular area has a unique ID ranging from 1 (or `0.0.0.1`) to 4,294,967,295 (or `255.255.255.255`). Normal areas handle external routes by flooding them bi-directionally across the *Area Border Router* (ABR). Note that external routes are defined as routes which were distributed in OSPF from another routing protocol.
- **Stub:** Typically, a stub area does not have direct connections to any external networks. Injecting external routes into a stub area is unnecessary because all traffic to external networks must be routed through an *Area Border Router* (ABR). Therefore, a stub area substitutes a default route for external routes to send traffic to external networks.
- **Stub No-Summary:** A *Stub No-Summary* or *totally stubby area* is similar to a stub area, however this area does not allow so-called summary routes, that is, it restricts type 3 summary link state advertisements (LSAs) from flowing into the area.
- **NSSA:** A not-so-stubby area (NSSA) is a type of stub area that in contrast to stub areas can support external connections. Note that NSSAs do not support virtual links.
- **NSSA No-Summary:** A *NSSA No-Summary* is similar to a NSSA, however this area does not allow so-called summary routes, that is, it restricts type 3 summary link state advertisements (LSAs) from flowing into the area.

To create an OSPF area, proceed as follows:

1. **On the *Area* tab, click *New OSPF Area*.**
   The *Create New OSPF Area* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the area.

   Area ID: Enter the ID of the area in dot-decimal notation (e.g., `0.0.0.1` for a normal area or `0.0.0.0` for the backbone area).

   Area Type: Select an area type (see description above) to specify the characteristics of the network that will be assigned to the area in question.

   Auth-Type: Select the authentication type used for all OSPF packets sent and received through the interfaces in the area. The following authentication types are available:

   - **MD5:** Select to enable MD5 authentication. MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value.
   - **Plain-Text:** Select to enable plain-text authentication. The password is transmitted in clear text over the network.
   - **Off:** Select to disable authentication.

Connect Via Interface: Select an OSPF-enabled interface. Note that to specify an OSPF-enabled interface here it must have been created on the *Interfaces* tab first.

Connect Virtual Links: All areas in an OSPF *autonomous system* (AS) must be physically connected to the backbone area (area 0). In some cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. In the *Connect Virtual Links* box, enter the router ID associated with the virtual link neighbor in decimal dot notation (e.g., `10.0.0.8`).

Cost: The cost of sending or receiving a data packet in this area. Valid values for cost are in the range from 1 to 65535.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new area definition appears on the *Area* tab.

To either edit or delete an OSPF area, click the corresponding buttons.

Open Live Log: The OSPF live log logs all activities on the OSPF interface. Click the button to open the live log in a new window.

6.7.3 Interfaces

On the *Interfaces & Routing* > *Dynamic Routing (OSPF)* > *Interfaces* tab you can create interface definitions to be used within an OSPF area. Each definition contains various parameters that are specific for OSPF-enabled interfaces.

To create an OSPF interface definition, proceed as follows:

1. **On the *Interfaces* tab, click *New OSPF Interface*.**
   The *Create New OSPF Interface* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this interface.

   Interface: Select the interface to associate with this OSPF interface definition.

   Auth-Type: Select the authentication type used for all OSPF packets sent and received through this interface. The following authentication types are available:

   - **MD5:** Select to enable MD5 authentication. MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function with a 128-bit hash value.

- **Plain-Text:** Select to enable plain-text authentication. The password is transmitted in clear text over the network.
- **Off:** Select to disable authentication.

Message Digest: Select the message digest (MD) to specify that MD5 authentication is used for this OSPF interface. Note that to select a message digest here it must have been created on the *Message Digests* tab first.

Cost: The cost of sending a data packet on this interface. Valid values for cost are in the range from 1 to 65535.

Advanced Options (optional): Selecting the *Advanced Options* checkbox will reveal further configuration options:

- **Hello Interval:** Specify the period of time (in seconds) that Sophos UTM waits between sending *Hello* packets through this interface. The default value is ten seconds.
- **Retransmit Interval:** Specify the period of time (in seconds) between link state advertisement (LSA) retransmissions for the interface when an acknowledgment for the LSA is not received. The default value is five seconds.
- **Dead Interval:** Specify the period of time (in seconds) Sophos UTM waits to receive a *Hello* data packet through the interface. The default value is 40 seconds. By convention, the *Dead Interval* value is four times greater than the value for the *Hello Interval*.
- **Priority:** Specify the router priority, which is an 8-bit number ranging from 1 to 255 primarily used in determining the designated router (DR) for the particular network. The default value is 1.
- **Transmit Delay:** Specify the estimated period of time (in seconds) it takes to transmit a link state update packet on the interface. The range is from 1 to 65535 seconds; the default value is 1.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The OSPF interface definition appears on the *Interfaces* tab.

To either edit or delete an OSPF interface, click the corresponding buttons.

Open Live Log: The OSPF live log logs all activities on the OSPF interface. Click the button to open the live log in a new window.

6.7.4 Message Digests

On the *Interfaces & Routing* > *Dynamic Routing (OSPF)* > *Message Digests* tab so-called message digest keys can be generated. Message digest keys are needed to enable MD5 authentication with OSPF. MD5 authentication uses the password to generate a message digest, which is a 128-bit checksum of the data packet and password. The message digest is sent with the data packet along with a key ID associated with the password.

Note – The receiving routers must be configured with an identical message digest key.

To create a message digest key, proceed as follows:

1. **On the *Message Digest* tab, click *New Message Digest Key*.**
   The *Create New Message Digest Key* dialog box opens.
2. **Make the following settings:**
   ID: Enter the key identifier for this message digest key; the range is from 1 to 255.

   MD5-key: Enter the associated password, which must be a string of up to 16 alphanumeric characters.
3. **Click *Save*.**
   The new key appears on the *Message Digests* list.

To either edit or delete a digest key, click the corresponding buttons.

6.7.5 Debug

The *Interfaces & Routing* > *Dynamic Routing (OSPF)* > *Debug* tab shows detailed information about relevant OSPF parameters in a separate browser window. The following information is available:

- **Show IP OSPF Neighbor:** Used to display OSPF neighbor information on a per-interface basis.
- **Show IP OSPF Routes:** Used to display the current state of the routing table.
- **Show IP OSPF Interface:** Used to display OSPF-related interface information.
- **Show IP OSPF Database:** Used to display lists of information related to the OSPF database for a specific router.

- **Show IP OSPF Border-Routers:** Used to display the internal OSPF routing table entries to an *Area Border Router* (ABR) and *Autonomous System Boundary Router* (ASBR).

6.7.6 Advanced

On the *Interfaces & Routing* > *Dynamic Routing (OSPF)* > *Advanced* tab further OSPF-related configuration options are located concerning the injection (redistribution) of routing information from a domain other than OSPF into the OSPF domain.

Note – Policy routes cannot be redistributed.

Redistribute connected: Select if you want to redistribute routes of directly connected networks; the default metric (cost) value is 10.

Redistribute static: Select if you want to redistribute static routes.

Note – IPsec tunnels must have *Strict Routing* disabled to be redistributed (see chapter Connections).

Redistribute IPsec: Select if you want to redistribute the IPsec routes; the *bind to interface* option should be disabled.

Redistribute SSL VPN: Select if you want to redistribute SSL VPN; the default metric (cost) value is 10.

Redistribute BGP: Select if you want to redistribute BGP routes; the default metric (cost) value is 10.

Announce default route: Select if you want to redistribute a default route into the OSPF domain.

Note – A default route will be advertised into the OSPF domain regardless of whether it has a route to `0.0.0.0/0`.

Interface link detection: Select if routes on interfaces should only be announced if an interface link is detected.

6.8 Border Gateway Protocol

The Border Gateway Protocol (BGP) is a routing protocol used mainly by Internet Service Providers (ISP) to enable communication between multiple autonomous systems (AS), that is between multiple ISPs, thus being the backbone of the Internet. An autonomous system is a collection of connected IP networks controlled by one or more ISPs and connected via an internal routing protocol (e.g. IGP). BGP is described as path vector protocol and, in contrast to IGP, makes routing decisions based on path, network policies, and/or rulesets. For this reason it can be regarded as a reachability protocol rather than a routing protocol.

Each ISP (or other network provider) must have an officially registered Autonomous System Number (ASN) to identify themselves on the network. Although an ISP may support multiple autonomous systems internally, to the Internet only the routing protocol is relevant. ASN with a number of the range 64512-65534 are private and can only be used internally.

BGP uses TCP as the transport protocol, on port 179.

When BGP is used between routers of a single AS it's called interior BGP (iBGP); when it is used between routers of different AS it is called exterior BGP (eBGP).

A strength of eBGP is that it prevents routing loops, that is an IP packet never passes an AS twice. This is accomplished in the following way: An eBGP router maintains a complete list of all AS an IP packet needs to pass to reach a certain network segment. When sending, it shares that information with neighbor eBGP routers which in turn update their routing list if necessary. When an eBGP router finds that it is already on such an UPDATE list it does not add itself again.

6.8.1 Global

On the *Border Gateway Protocol* > *Global* page, you can enable and disable BGP for the UTM.

1. **To be able to enable BGP, create at least one neighbor on the *Neighbor* page.**
2. **On the *Global* page, enable BGP.**
   Click the toggle switch. The toggle switch turns amber and the *BGP System* section becomes editable.
3. **Make the following settings:**
   AS Number: Enter the Autonomous System Number (ASN) of your system.

Router ID: Enter an IPv4 address as router ID which is sent to neighbors during session initialization.

Networks: Add or select the networks that should be announced to the neighbors by the system. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

4. **Click *Apply*.**

   The toggle switch turns green and BGP becomes active. After a short time, the *BGP Summary* section displays status information.

6.8.2 Systems

On the *Border Gateway Protocol > Systems* page you can create an environment with multiple autonomous systems.

Note – This page is only accessible if you enable the use of multiple AS on the *Advanced* page.

To create a new BGP system, do the following:

1. **On the *Systems* page, click *New BGP System*.**
   The *Create a new BGP System* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the system.

   ASN: Enter the Autonomous System Number (ASN) of your system.

   Router ID: Enter an IPv4 address as router ID which is sent to neighbors during session initialization.

   Neighbor: Select the checkboxes of those neighbors who belong to the AS of this system. Note that you need to create the neighbors beforehand on the *Neighbor* page.

   Networks: Add or select the networks that should be announced by the system. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Install Routes: This option is enabled by default and should only be disabled if you want a BGP router to know the routes but not to actively take part in the BGP routing process. If

there are multiple AS systems where this option is selected, filter lists must be created to ensure that there are no duplicate networks. Otherwise the routing behavior for identical networks is undefined.

3. **Click *Save*.**
   The system appears on the *Systems* list.

6.8.3 Neighbor

On the *Border Gateway Protocol > Neighbor* page, you can create one or more BGP neighbor routers. A neighbor router (or peer router) builds the connection between multiple autonomous systems (AS) or within a single AS. During the first communication, two neighbors exchange their BGP routing tables. After that they send each other updates about changes in the routing table. Keepalive packets are sent to ensure that the connection is up. In case of errors, notifications packets are sent.

Policy routing in BGP differentiates between inbound and outbound policies. This is why defined route maps and filter lists can be applied separately for inbound or outbound traffic.

You need to create at least one neighbor router to be able to enable BGP on the *Global* page.

To create a new BGP neighbor, do the following:

1. **On the *Neighbor* page, click *New BGP Neighbor*.**
   The *Create a new BGP neighbor* dialog box opens.

2. **Make the following settings:**
   Name: Enter the name of the BGP neighbor router.

   Host: Add or select the host definition of the neighbor. The defined IP address must be reachable from the UTM. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Remote ASN: Enter the Autonomous System Number (ASN) of the neighbor.

   Authentication: If the neighbor requires authentication, select *TCP MD5 Signature* from the drop-down list and enter the password which must correspond to the password the neighbor has set.

3. **Make the following advanced settings, if required:**
   Route in/out: If you have defined a route map, you can select it here. With *In* or *Out* you define whether to apply the route map to ingoing or outgoing announcements.

Filter in/out: If you have defined a filter list, you can select it here. With *In* or *Out* you define whether to apply the filter to ingoing or outgoing announcements.

Next-Hop-Self: In an iBGP network, when a router announces an external eBGP network internally, iBGP routers with no direct external connection will not know how to route packets to that network. Selecting this option, the eBGP router announces itself as next hop to reach the external network.

Multihop: In some cases, a Cisco router can run eBGP with a third-party router that does not allow direct connection of the two external peers. To achieve the connection, you can use eBGP multihop. The eBGP multihop allows a neighbor connection between two external peers that do not have direct connection. The multihop is only for eBGP and not for iBGP.

Soft-Reconfiguration: Enabled by default. This option enables storing updates sent by the neighbor.

Default Originate: Sends the default route 0.0.0.0 to the neighbor. The neighbor uses this route only if he needs to reach a network that is not in his routing table.

Weight: Cisco-specific option. Sets a generic weight for all routes learned from this neighbor. You can enter a value between 0 and 65535. The route with the highest weight is preferred to reach a particular network. The weight given here overrides route map weight.

4. **Click *Save*.**
   The neighbor appears on the *Neighbor* list.

6.8.4 Route Map

In BGP, route-map is a command to set conditions for redistributing routes and to enable policy routing. On the *Border Gateway Protocol* > *Route Map* page, you can create route maps for particular networks, setting metric, weight, and/or preference values.

The best path algorithm, which decides which route to take, works as follows:

1. Weight is checked.*
2. Local preference is checked.*
3. Local route is checked.
4. AS path length is checked.

5. Origin is checked.
6. Metric is checked.*

This is only a short description. Since the calculation of the best path is very complex, please refer to pertinent documentation for detailed information which is available on the Internet.

The items followed by an asterisk (*) can be directly configured.

To create a BGP route map, do the following:

1. **On the *Route Map* page, click *New BGP Route Map*.**
   The *Create a new BGP Route Map* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the route map.

   Match By: Select whether the route map should match the IP address of a particular router or a whole AS.

   - **IP Address:** In the *Networks* box, add or select hosts or networks the filter should apply to. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.
   - **AS Number:** In the *AS Regex* box, use BGP regular expressions to define AS numbers the filter should apply to. Example: `_100_` matches any route going through AS100.

   Networks: Add or select networks and/or hosts the route map should apply to. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Metric: By default, a router dynamically learns route metrics. However, you can set your own metric value which can be an integer from 0 to 4294967295. A lower metric value is preferred over a higher metric value.

   Weight: Weight is used to select a best path. It is specified for a specific router and it is not propagated. When multiple routes to the same destination exist, routes with a higher weight value are preferred. Weight is based on the first matched AS path and can be an integer from 0 to 4294967295.

   Note – If a neighbor has been given a weight, it overrides the route map weight if the route to a specified network matches.

Preference: You can set a preference value for the AS path which is sent only to all routers in the local AS. Preference (or local preference) tells the routers in an AS which path has to be preferred to reach a certain network outside the AS. It can be an integer from 0 to 4294967295 and the default is 100.

AS Prepend: AS path prepending is used if preference settings for some reason do not suffice to avoid a certain route, for example a backup route which should only be taken in case the main route is unavailable. It allows you to extend the AS path attribute by repeating your own AS number, e.g. `65002 65002 65002`. This influences the BGP route selection since the shortest AS path is preferred. Note that route maps with AS prepend set need to be selected in the *Route Out* field of a neighbor to work as intended.

3. **Click *Save*.**
   The route map appears on the *Route Map* list.

You can now use the route map on a neighbor definition.

6.8.5 Filter List

On the *Border Gateway Protocol* > *Filter List* page you can create filter lists used to regulate traffic between networks based on IP address or AS number.

To create a filter list, do the following:

1. **On the *Filter List* page, click *New BGP Filter List*.**
   The *Create a new BGP Filter List* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for the filter list.

   Filter By: Select whether the filter should match the IP address of a particular router or a whole AS.

   - **IP Address:** In the *Networks* box, add or select hosts or networks the filter should apply to. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.
   - **AS Number:** In the *AS Regex* box, use BGP regular expressions to define AS numbers the filter should apply to. Example: `_100_` matches any route going through AS100.

Networks: Add or select networks and/or hosts that should be denied or permitted information on certain networks. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Action: From the drop-down list, select an action that should be taken if a filter matches. You can either deny or permit traffic.

- **Deny:** If you deny a network for a particular neighbor via the *Filter In* field on the *Neighbor* page, the UTM will ignore announcements for that network. If you do the same via the *Filter Out* field, the UTM will not send announcements to that neighbor for that network.
- **Permit:** If you permit a network for a particular neighbor via the *Filter In* field on the *Neighbor* page, the UTM will receive announcements for that network only. If you do the same via the *Filter Out* field, the UTM will send announcements to that neighbor for that network only, but not for any other network you might have defined on the *Global* or *Systems* page.

3. **Click *Save*.**
   The filter list appears on the *Filter List* list.

You can now use the filter list on a neighbor definition.

6.8.6 Advanced

On the *Border Gateway Protocol > Advanced* page you can make some additional settings for BGP and you can access BGP debug information windows.

Allow Multiple Autonomous Systems

Allow multiple AS: Select this checkbox if you want to configure multiple AS. This will enable the *Systems* page, where you can then add multiple AS. At the same time, the *BGP System* section on the *Global* page will be disabled, and the *Global* page will display information for all AS.

Strict IP Address Match

Strict IP address match: Select this checkbox to strictly match IP addresses. Example: 10.0.0.0/8 will only match 10.0.0.0/8, but not 10.0.1.0/24.

Multiple Path Routing

Normally only one route path is used, even if there are multiple routes with the same cost. If selected, up to eight equal routes can be used at the same time. This allows load balancing

between multiple interfaces.

BGP Debug

This section provides access to three debug information windows. Click a button to open a window. The name of a button corresponds to the BGP command you would normally invoke on the command line. The window will then display the result of that command in form of a command line output.

Show IP BGP Neighbor: Displays information on the neighbors of the UTM. Check that the link state for each neighbor is *Established*.

Show IP BGP Unicast: Displays the current BGP routing table which gives the preferred paths. This is especially useful to get an overview of your metric, weight, and preference settings and their impact.

Show IP BGP Summary: Displays the status of all BGP connections. This information is also displayed in the *BGP Summary* section on the *Global* page.

6.9 Multicast Routing (PIM-SM)

The menu *Interfaces & Routing > Multicast Routing (PIM-SM)* enables you to configure *Protocol Independent Multicast Sparse Mode* (PIM-SM) for use on your network. PIM is a protocol to dynamically route multicast packets in networks. Multicast is a technique to deliver packets that are to be received by more than one client efficiently using as little traffic as possible. Normally, packets for more than one client are simply copied and sent to every client individually, multiplying the consumed bandwidth by the number of users. Thus servers which have a lot of clients requesting the same packets at the same time, like e.g. servers for streaming content, need a lot of bandwidth.

Multicast, in contrast, saves bandwidth by sending packets only once over each link of the network. To achieve this, multicast includes adequately configured routers in the decision when to create copies on the way from the server (sender) to the client (receiver). The routers use PIM-SM to keep track of active multicast receiver(s) and use this information to configure routing.

A rough scheme of PIM-SM communication is as follows: A sender starts transmitting its multicast data. The multicast router for the sender registers via PIM-SM with the RP router which in turn sends a join message to the sender's router. Multicast packets now flow from the sender to the RP router. A receiver registers itself via an IGMP broadcast for this multicast group at its

local PIM-SM router. This router sends a join request for the receiver towards the RP router, which then in turn forwards multicast traffic to the receiver.

Multicast has its own IP address range which is `224.0.0.0/4`.

6.9.1 Global

On the *Multicast Routing (PIM-SM)* > *Global* tab you can enable and disable PIM. The *Routing Daemon Settings* area displays the status of interfaces and routers involved.

Before you can enable PIM you need to define at least two interfaces to serve as PIM interfaces on the *Interfaces* tab and one router on the *RP Routers* tab.

To enable PIM-SM, do the following:

1. **On the *Global* tab enable PIM-SM.**
   Click the toggle switch.

   The toggle switch turns amber and the *Routing Daemon Settings* area becomes editable.

2. **Make the following settings:**
   Active PIM-SM Interfaces: Select at least two interfaces to use for PIM-SM. Interfaces can be configured on the *Interfaces* tab.

   Active PIM-SM RP Routers: Select at least one RP router to use for PIM-SM. RP routers can be defined on the *RP Routers* tab.

3. **Click *Apply*.**
   Your settings will be saved. PIM-SM communication is now active in your network.

To cancel the configuration, click the amber colored toggle switch. To disable PIM-SM click the green toggle switch.

Live Log

Click the *Open Live Log* button to open the PIM live log in a new window.

6.9.2 Interfaces

On the *Multicast Routing (PIM-SM)* > *Interfaces* tab you can define over which interfaces of Sophos UTM multicast communication should take place.

To create a new PIM-SM interface, do the following:

1. **On the *Interfaces* tab, click *New PIM-SM Interface*.**
   The dialog box *Create a New PIM-SM Interface* opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for PIM-SM interface.

   Interface: Select an interface that is to accept PIM and IGMP network traffic.

   DR priority (optional): Enter a number that defines the designated router (DR) priority for the interface. The router with the highest priority honors IGMP requests if more than one PIM-SM routers are present on the same network segment. Numbers from 0 to 2^{32} are possible. If you do not provide a priority, 0 is used by default.

   IGMP: Select the version of the *Internet Group Management Protocol* that is to be supported. IGMP is used by recipients to establish multicast group memberships.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new PIM-SM interface is added to the interfaces list.

To either edit or delete a PIM-SM interface, click the corresponding buttons.

6.9.3 RP Routers

In order to be able to use multicast on your network you need to configure one or more rendezvous point routers (RP routers). An RP router accepts registrations both from multicast receivers and senders. An RP router is a regular PIM-SM router that is chosen to be the RP router for certain multicast groups as well. All PIM-SM routers must agree on which router is to be the RP router.

To create an RP router, do the following:

1. **On the *RP Routers* tab, click *New Rendezvous Point Router*.**
   The dialog box *Create a New RP Router* opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the RP router.

   Host: Create (or select) the host that should act as rendezvous point router.

   Priority: Enter a number that defines the priority of the RP router. Join messages are sent to the RP router with the lowest priority. Numbers from 0 to 255 are possible. If you do not provide a priority, 0 is used by default.

Multicast Group Prefixes: Enter the multicast group the RP router is responsible for. You can define group prefixes like `224.1.1.0/24` if the RP is responsible for more than one multicast group. The multicast group (prefix) must be within the multicast address range which is `224.0.0.0/4`.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new RP router is added to the routers list.

To either edit or delete an RP router, click the corresponding buttons.

6.9.4 Routes

You need to set up a continuous communication route between receivers and sender(s). If recipient, sender and/or RP router are not within the same network segment, you will need to create a route to enable communication between them.

To create a PIM-SM route, do the following:

1. **On the *Routes* tab, click *New PIM-SM route*.**
   The dialog box *Create a New PIM-SM Route* opens.
2. **Make the following settings:**
   Route type: The following route types are available:
   - **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.
   - **Gateway route:** Packets are sent to a particular host (gateway).

   Network: Select the destination address range where the PIM traffic is to be routed to.

   Gateway: Select the gateway/router to which the gateway will forward data packets (only available if you selected *Gateway Route* as route type).

   Interface: Select the interface to which the gateway will forward data packets (only available if you selected *Interface Route* as route type).

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new PIM-SM route is added to the routes list.

To either edit or delete a PIM-SM route, click the corresponding buttons.

6.9.5 Advanced

On the *Interfaces & Routing > Multicast Routing (PIM-SM) > Advanced* tab you can configure some advanced settings for PIM.

Shortest Path Tree Settings

In some networks the PIM communication route between sender, RP, and recipient is not the shortest network path possible. The option *Enable Switch to Shortest Path Tree* allows to move an existing communication between sender and recipient to the shortest path available, omitting the RP as moderator, when a certain traffic threshold is reached.

Auto Firewall Settings

With this option enabled, the system will automatically create all necessary firewall rules needed to forward multicast traffic for the specified multicast groups.

Debug Settings

Select the option *Enable Debug Mode* to see additional debugging information in the PIM-SM routing daemon log.

7 Network Services

This chapter describes how to configure several network services of Sophos UTM for your network.

The following topics are included in this chapter:

7.1 DNS

The tabs of the *Network Services > DNS* menu contain miscellaneous configuration options, all related to the *Domain Name System* (DNS), a system primarily used to translate domain names (computer hostnames) to IP addresses.

7.1.1 Global

Allowed Networks

You can specify the networks that are to be allowed to use UTM as a recursive DNS resolver. Typically, you will select your internal networks here.

Caution – It is extremely important not to select an *Any* network object, because this introduces a serious security risk and opens your appliance up to abuse from the Internet.

Note – If you already run an internal DNS server, for example as part of Active Directory, you should leave this box empty.

DNSSEC

The Domain Name System Security Extensions (DNSSEC) is a set of extensions to DNS to enhance security. It works by digitally signing DNS lookup records using public-key cryptography. If unselected, the UTM accepts all DNS records. If selected, the UTM validates incom-

ing DNS requests with regard to DNSSEC signing. Only correctly signed records will be accepted from signed zones.

Note – If selected, DNS records might be rejected by DNSSEC-incapable forwarders that are manually installed or assigned by ISP. In this case, on the *Forwarders* tab, remove the DNS forwarders from the box and/or disable the *Use forwarders assigned by ISP* checkbox.

Flush Resolver Cache

The DNS proxy uses a cache for its records. Each record has an expiration date (TTL, time-to-live) at which it will be deleted, which is normally one day. However, you can empty the cache manually e.g. if you want recent changes in DNS records to take effect immediately, not having to wait for the TTL to expire. To empty the cache, click *Flush Resolver Cache Now*.

7.1.2 Forwarders

On the *Network Services* > *DNS* > *Forwarders* tab you can specify so-called DNS forwarders. A DNS forwarder is a *Domain Name System* (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network. If possible, add a DNS forwarder to your configuration. This should be a host "near" your site, preferably one provided by your Internet provider. It will be used as a "parent" cache. This will speed up DNS requests considerably. If you do not specify a forwarding name server, the root DNS servers will be queried for zone information first, taking a longer time to complete requests.

To create a DNS forwarder, proceed as follows:

1. **Select a DNS forwarder.**
   Select or add a DNS forwarder. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Use Forwarders Assigned By ISP (optional): Select the *Use Forwarders Assigned by ISP* checkbox to forward DNS queries to the DNS servers of your ISP. When this box is checked, all forwarders automatically assigned by your ISP will be listed in the line below the box.

2. **Click *Apply*.**
   Your settings will be saved.

7.1.3 Request Routing

Suppose you run your own internal DNS server, this server could be used as an alternate server to resolve DNS queries for a domain you do not want to be resolved by DNS forwarders. On the *Network Services > DNS > Request Routing* tab you can define routes to your own DNS servers.

To create a DNS request route, proceed as follows:

1. **On the *Request Routing* tab, click *New DNS Request Route*.**
   The *Create New DNS Request Route* dialog box opens.
2. **Make the following settings:**
   Domain: Enter the domain for which you want to use an alternate DNS server.

   Target servers: Select or add one or more DNS servers to use for resolving the domain entered above. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new route appears on the *DNS Request Route* list and is immediately active.

To either edit or delete a DNS request route, click the corresponding buttons.

7.1.4 Static Entries

If you do not want to set up your own DNS server but need a static DNS mapping for a few hosts of your network, you can enter these mappings.

Starting with UTM version 9.1, this feature has moved to the *Definitions & Users > Network Definitions* tab. DNS mappings are now defined along with the involved hosts.

When you click the *Static Entries* button, the *Definitions & Users > Network Definitions* tab opens. Automatically, only hosts with static entry are displayed. Use the drop-down list on top of the list to change the filter settings.

7.1.5 DynDNS

Dynamic DNS, or DynDNS for short, is a domain name service which allows static Internet domain names to be assigned to a computer with a varying IP address. You can sign up for the

DynDNS service at the website of the respective DynDNS service provider to get a DNS alias that will automatically be updated when your uplink IP address changes. Once you have registered to this service, you will receive a hostname, username, and password, which are necessary for the configuration.

To configure DynDNS, proceed as follows:

1. **On the *DynDNS* tab, click *New DynDNS*.**
   The *Create New DynDNS* dialog box opens.
2. **Make the following settings:**
   Type: The following DynDNS services are available:
   - **DNSdynamic:** Official website: www.dnsdynamic.org
   - **DNS Park:** Official website: www.dnspark.com
   - **DtDNS:** Official website: www.dtdns.com
   - **DynDNS:** Standard DNS service of the service provider Dynamic Network Services Inc. (Dyn). Official website: www.dyndns.com
   - **DynDNS custom:** Custom DNS service of the service provider Dynamic Network Services Inc. (Dyn) (www.dyndns.com). Custom DNS is designed primarily to work with domains owned or registered by yourself.
   - **easyDNS:** Official website: www.easydns.com
   - **FreeDNS:** Official website: freedns.afraid.org
   - **Namecheap:** Official website: www.namecheap.com
   - **No-IP.com:** Official website: www.noip.com
   - **OpenDNS IP update:** Official website: www.opendns.com
   - **selfHOST:** Official website: www.selfhost.de
   - **STRATO AG:** Official website: www.strato.de
   - **zoneedit:** Official website: www.zoneedit.com

   Note – In the *Server* field the URL is displayed to which the UTM sends the IP changes.

   Assign (not with type *FreeDNS*): Define the IP address the DynDNS name is to be associated with. Selecting *IP of Local Interface* is useful when the interface in question has a public IP address. Typically, you will use this option for your DSL uplink. When you select

First public IP on the default route no interface needs to be specified. Instead, your UTM will send a WWW request to a public DynDNS server which in return will respond with the public IP you are currently using. This is useful when your UTM does not have a public IP address but is located inside a private network, connected to the Internet via a masquerading router.

Note – FreeDNS always uses the first public IP address on the default route.

Interface (not with type *FreeDNS*, only with *IP of local interface*): Select the interface for which you want to use the DynDNS service, most likely this will be your external interface connected to the Internet.

Hostname (not with type *Open DNS IP update*):Enter the domain name you received from your DynDNS service provider (e.g., `example.dyndns.org`). Note that you need not adhere to a particular syntax for the hostname to be entered here. What you must enter here exclusively depends on what your DynDNS service provider requires. Apart from that, you can also use your DynDNS hostname as the gateway's main hostname, which, however, is not mandatory.

Label (only with type *Open DNS IP update*): Enter the label given to the network. Please refer to the OpenDNS Knowledgebase for further information.

Aliases (optional, only with some types): Use this box to enter additional hostnames which should point to the same IP address as the main hostname above (e.g., `mail.example.com, example.com`).

MX (optional, only with type *DNS Park*, *DynDNS*, or *easyDNS*): Mail exchangers are used for directing mail to specific servers other than the one a hostname points to. MX records serve a specific purpose: they let you specify the host (server) to which mail for a specific domain should be sent. For example, if you enter `mail.example.com` as Mail Exchanger, mail addressed to `user@example.com` would be delivered to the host `mail.example.com`.

MX priority (optional, only with type *DNS Park*): Enter a positive integer number indicating whether the specified mail server should be preferred for delivery of mail to the domain. Servers with lower numbers are preferred over servers with higher numbers. You can usually leave the field blank because DNS Park uses a default value of 5 which is appropriate for almost all purposes. For technical details about mail exchanger priorities, see RFC 5321.

Backup MX (optional, only with type *DynDNS* or *easyDNS*): Select this checkbox only if the hostname named in the *Hostname* text box is to serve as main mail exchanger. Then the hostname from the *MX* text box will only be advertised as a backup mail exchanger.

Wildcard (optional, only with type *DynDNS* or *easyDNS*): Select this option if you want subdomains to point to the same IP address as your registered domain. Using this option an asterisk (*) will be added to your domain serving as a wildcard (e.g., `*.example.dyndns.org`), thus making sure that, for example, `www.example.dyndns.org` will point to the same address as `example.dyndns.org`.

Username: Enter the username you received from the DynDNS service provider.

Password: Enter the password you received from the DynDNS service provider.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new DynDNS appears on the *DynDNS* list. The service is still disabled (toggle switch is gray).
4. **Enable DynDNS.**
   Click the toggle switch to enable the DynDNS service.

   The service is now enabled (toggle switch is green).

To either edit or delete a DynDNS, click the corresponding buttons.

You can use multiple DynDNS objects at the same time. When all settings for two hostnames are identical, it is recommended to use the *Aliases* option—instead of creating two distinct objects.

7.2 DHCP

The *Dynamic Host Configuration Protocol* (DHCP) automatically distributes addresses from a defined IP address pool to client computers. It is designed to simplify network configuration on large networks, and to prevent address conflicts. DHCP distributes IP addresses, default gateway information, and DNS configuration information to its clients.

In addition to simplifying the configuration of client computers and allowing mobile computers to move painlessly between networks, DHCP helps to localize and troubleshoot IP address-related problems, as these are mostly issues with the configuration of the DHCP server itself. It also allows for a more effective use of address space, especially when not all computers are

active at the same time, as addresses can be distributed as needed and reused when unneeded.

7.2.1 Servers

The tab *Network Services > DHCP > Server* allows to configure a DHCP server. Sophos UTM provides the DHCP service for the connected network as well as for other networks. The DHCP server can be used to assign basic network parameters to your clients. You can run the DHCP service on multiple interfaces, with each interface and each network to be provided having its own configuration set.

Note – On the *Options* tab you can define additional or different DHCP options to be sent to the clients. A DHCP option defined on the *Options* tab overwrites a setting made on the *Servers* tab if its scope is not set to be global. For example, defining DHCP options for selected hosts only, you can assign them a DNS server or lease time different from what is defined for the DHCP server.

To configure a DHCP server, proceed as follows:

1. **On the *Servers* tab, click *New DHCP Server*.**
   The *Create New DHCP Server* dialog box opens.
2. **Make the following settings:**
   Interface: The interface from which the IP addresses should be assigned to the clients. You can only select an already configured interface.

   Address type: This option is only available when IPv6 is globally enabled. Select the IP version of the DHCP server.

   Range start/end: The IP range to be used as an address pool on that interface. By default, the configured address area of the network card will appear in the text boxes. If the clients are in the same network, the range must be inside the network attached to the interface. If the clients are in another network, the range must be inside the network where the relayed DHCP requests are forwarded from.

   Note – The bigger a defined DHCP IP range, the more memory the UTM will reserve. Please make sure to reduce the DHCP range size to the values you need. The maximum allowed range is a /9 network.

DNS server 1/2: The IP addresses of the DNS servers.

Default gateway (only with IPv4): The IP address of the default gateway.

Note – Both wireless access points and RED appliances need the default gateway to be within the same subnet as the interface they are connected to.

Domain (optional): Enter the domain name that will be transmitted to the clients (e.g., `intranet.example.com`).

Lease time (only with IPv4): The DHCP client automatically tries to renew its lease. If the lease is not renewed during its lease time, the IP address lease expires. Here you can define this time interval in seconds. The default is 86,400 seconds (one day). The minimum is 600 seconds (10 minutes) and the maximum is 2,592,000 seconds (one month).

Valid lifetime (only with IPv6): The DHCP client automatically tries to renew its lease. If the lease is not renewed during its valid lifetime, the IP address lease status becomes invalid, the address is removed from the interface, and it may be assigned somewhere else. You can select an interval between five minutes and infinity, however the valid lifetime must be equal or greater than the preferred lifetime.

Preferred lifetime (only with IPv6): The DHCP client automatically tries to renew its lease. If the lease is not renewed during its preferred lifetime, the IP address lease status becomes deprecated, i.e., it is still valid but will not be used for new connections. You can select an interval between 5 minutes and infinity.

3. **Optionally, make the following advanced settings:**

   WINS node type (only with IPv4): *Windows Internet Naming Service* (WINS) is Microsoft's implementation of *NetBIOS Name Server* (NBNS) on Windows, a name server and service for NetBIOS computer names. A WINS server acts as a database that matches computer names with IP addresses, thus allowing computers using NetBIOS to take advantage of the TCP/IP network. The following WINS node types are available:

   - **Do not set:** The WINS node type is not set and will be chosen by the client.
   - **B-node (no WINS):** B-node systems use broadcasts only.
   - **P-node (WINS only):** P-node systems use only point-to-point name queries to a Windows name server (WINS).

- **M-node (Broadcast, then WINS):** M-node systems broadcast first, then query the name server.
- **H-node (WINS, then Broadcast):** H-node systems query the name server first, then broadcast.

WINS server: Depending on your WINS node type selection, this text box appears. Enter the IP address of the WINS server.

Clients with static mappings only (optional): Select this option to have the DHCP server assign IP addresses only to clients that have a static DHCP mapping (see *Definition & Users > Network Definitions > Network Definitions*).

Enable HTTP proxy auto configuration: Select this option if you want to provide a PAC file for automatic proxy configuration of browsers. For more information see chapter *Web Protection > Filtering Options > Misc*, section *Proxy Auto Configuration*.

Note – HTTP proxy auto configuration is currently not supported with IPv6 by Microsoft Windows.

Clients via DHCP relay agent: If selected, the DHCP server assigns IP addresses to clients which are not in the network of the attached interface. In this case, the address range defined above has to be inside the network where relayed DHCP requests are forwarded from, and not within the network of the attached interface.

Netmask: Select the netmask of the network where relayed DHCP requests are forwarded from.

Comment (optional): Add a description or other information.

4. **Click *Save*.**
   The new DHCP server definition appears on the DHCP server list and is immediately active.

To either edit or delete a DHCP server definition, click the corresponding buttons.

7.2.2 Relay

The *Network Services > DHCP > Relay* tab allows you to configure a DHCP relay. The DHCP service is provided by a separate DHCP server and the UTM works as a relay. The DHCP relay can be used to forward DHCP requests and responses across network segments. You need to

specify the DHCP server and a list of interfaces between which DHCP traffic shall be forwarded.

To configure a DHCP relay, proceed as follows:

1. **On the *Relay* tab, enable *DHCP Relay*.**
   Click the toggle switch.

   The toggle switch turns amber and the *DHCP Relay Configuration* area becomes editable.
2. **Select the DHCP server.**
3. **Add the interfaces involved.**
   Add the interface to the DHCP server as well as all interfaces to the clients' network(s) between which DHCP requests and responses should be forwarded.
4. **Click *Apply*.**
   Your settings will be saved.

To cancel the configuration, click the amber colored toggle switch.

7.2.3 Static Mappings

You can create static mappings between client and IP address for some or all clients. Starting with UTM version 9.1, this feature has moved to the *Definitions & Users > Network Definitions* tab. DHCP mappings are now defined along with the involved hosts.

When you click the *Static Mappings* button, the *Definitions & Users > Network Definitions* tab opens. Automatically, only hosts with static mapping are displayed. Use the drop-down list on top of the list to change the filter settings.

7.2.4 IPv4 Lease Table

Using DHCP, a client no longer owns an IP address, but rather *leases* it from the DHCP server, which gives permission for a client to use the address for a period of time.

The lease table on the *Network Services > DHCP > IPv4 Lease Table* tab shows the current leases issued by the DHCP server, including information about the start date and the date when the lease will expire.

Add Static Mapping to New Host Definition

You can use an existing lease as template for a static MAC/IP mapping with a host to be defined. Do the following:

1. **For the desired lease, click the button *Make Static* in the *Make static* column.**
   The dialog window *Make Static* opens.
2. **Make the following settings:**
   Action: Select *Create a new host*.

   Name: Enter a descriptive name for the new host.

   DHCP server: Select the DHCP server to be used for static mapping. The corresponding DHCP range is displayed below the drop-down list.

   IPv4 address: Change the IP address to an address outside the DHCP pool range.

   Note – When converting a lease to a static mapping you should change the IP address so that it is no longer inside the scope of the DHCP pool. However, if you change the IP address, the address used by the client will not change immediately, but only when it tries to renew its lease for the next time.

   DNS hostname: If you provide a DNS hostname, it will be used as static DNS entry of the host.

   Reverse DNS: Select the checkbox to enable the mapping of the host's IP address to its name. Note that although several names can map to the same IP address, one IP address can only ever map to one name.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   Your settings will be saved.

You can find the new host with the static mapping on the *Definitions & Users* > *Network Definitions* tab.

Add Static Mapping to Existing Host Definition

You can use an existing lease as template for a new static MAC/IP mapping with an existing host definition. Do the following:

1. **For the desired lease, click the *Make Static* button in the *Make Static* column.**
   The dialog window *Make Static* opens.
2. **Make the following settings:**
   Action: Select *Use an existing host*.

   Host: Add the host by clicking the Folder icon.
3. **Click *Save*.**
   Your settings will be saved.

You can find the host with the static mapping on the *Definitions & Users* > *Network Definitions* tab.

7.2.5 IPv6 Lease Table

Using DHCP, a client no longer owns an IP address, but rather *leases* it from the DHCP server, which gives permission for a client to use the address for a period of time.

The lease table on the *Network Services* > *DHCP* > *IPv6 Lease Table* tab shows the current leases issued by the DHCP server, including information about the start date and the date when the lease will expire.

Note – Leases that have been granted via prefix advertisements are not shown in the table.

Add Static Mapping to New Host Definition

You can use an existing lease as template for a static MAC/IP mapping with a host to be defined. Do the following:

1. **For the desired lease, click the button *Make Static*.**
   The dialog window *Make Static* opens.
2. **Make the following settings:**
   Action: Select *Create a new host*.

   Name: Enter a descriptive name for the new host.

   DHCP server: Select the DHCP server to be used for static mapping. The corresponding DHCP range is displayed below the drop-down list.

   IPv6 address: Change the IP address to an address outside the DHCP pool range.

Note – When converting a lease to a static mapping you should change the IP address so that it is no longer inside the scope of the DHCP pool. However, if you change the IP address, the address used by the client will not change immediately, but only when it tries to renew its lease for the next time.

DNS hostname: If you provide a DNS hostname, it will be used as static DNS entry of the host.

Reverse DNS: Select the checkbox to enable the mapping of the host's IP address to its name. Note that although several names can map to the same IP address, one IP address can only ever map to one name.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   Your settings will be saved.

Add Static Mapping to Existing Host Definition

You can use an existing lease as template for a new static MAC/IP mapping with an existing host definition. Do the following:

1. **For the desired lease, click the *Make Static* button in the *Make Static* column.**
   The dialog window *Make Static* opens.
2. **Make the following settings:**
   Action: Select *Use an existing host*.

   Host: Add the host by clicking the Folder icon.
3. **Click *Save*.**
   Your settings will be saved.

You can find the host with the static mapping on the *Definitions & Users > Network Definitions* tab.

7.2.6 Options

The *Network Services > DHCP > Options* tab allows to configure DHCP options. DHCP options are additional configuration parameters provided by a DHCP server to DHCP clients.

Example: For some VoIP phones, to provide them with the necessary information from your DHCP servers you have to create and activate three additional DHCP options on this page:

- *filename*: Name of the boot file.
- *next-server*: Name of the TFTP server which provides the boot file.
- *4 (time-servers)*: IP address of the time server.

DHCP options can have different scopes: They can e.g. be provided to selected hosts only, or from selected servers only, or even globally. For this reason it is possible to define different parameters for the same host. Some DHCP options are already defined on the *DHCP > Servers* tab, e.g., DNS server (option 6). In case of conflicting parameter values, the parameters are provided to the client according to the following priority:

1. DHCP option with scope *Host*
2. DHCP option with scope *MAC prefix*
3. DHCP option with scope *Vendor ID*
4. DHCP option with scope *Server*
5. DHCP server parameter (*DHCP > Servers* tab)
6. DHCP option with scope *Global*

Note – With the DHCP request, a DHCP client submits the information which DHCP options it can deal with. As a result the DHCP server only provides the DHCP options the client understands, no matter which options are defined here.

To create a DHCP option, proceed as follows:

1. **Click *New DHCP Option*.**
   The *Create New DHCP Option* dialog box opens.
2. **Make the following settings:**
   Address type (only if IPv6 is enabled): Select the IP version which you create the DHCP option for.

   Code: Select the code of the DHCP option you want to create.

   Note – With the entry *filename* you can specify a file to be loaded into the DHCP client to be executed there. With *next-server* you define the boot server. The numbered DHCP option codes are defined in RFC 2132 and others.

   Name: Enter a descriptive name for this option.

Type: Only available if you selected a code with the comment *(unknown)*. Select the data type of the option. The data types *IP Address*, *Text* and *Hex* are available. Depending on the selected data type enter the appropriate data in the corresponding field below:

Address: Add or select the host or network group with the IP address(es) to be submitted with this DHCP option to the DHCP client. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Text: Enter the text to be submitted with this DHCP option to the DHCP client.

Hex: Enter the hexadecimal value to be submitted with this DHCP option to the DHCP client. Please note that you have to enter the groups of two hexadecimal digits separated by colons (e.g., `00:04:76:16:EA:62`).

Scope: Define on which condition the DHCP option should be sent.

- **Global:** The DHCP option will be sent by all defined DHCP servers to all DHCP clients.
- **Server:** In the *Server* box, select the DHCP servers which should send the DHCP option. The box displays all DHCP servers defined on the *DHCP Servers* tab.
- **Host:** In the *Host* box, add or select the hosts which should be provided the DHCP option. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.
- **MAC prefix:** Enter a MAC prefix. All DHCP clients with a matching MAC address will be provided the DHCP option.
- **Vendor ID:** Enter a vendor ID or the prefix of a vendor ID. All DHCP clients which match this string will be provided the DHCP option.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new DHCP option appears on the *DHCP Options* list and is immediately active.

To either edit or delete a DHCP option, click the corresponding buttons.

7.3 NTP

The menu *Network Services* > *NTP* allows you to configure an NTP server for the connected networks. The *Network Time Protocol* (NTP) is a protocol used for synchronizing the clocks of computer systems over IP networks. Instead of just synchronizing the time of Sophos UTM, which can be configured on the *Management* > *System Settings* > *Time and Date* tab, you can explicitly allow certain networks to use this service as well.

To enable the use of NTP time synchronization for specific networks, proceed as follows:

1. **Enable the NTP server.**
   Click the toggle switch.
2. **Select *Allowed networks*.**
   Add or select the networks that should be allowed to access the NTP server. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.
3. **Click *Apply*.**
   Your settings will be saved.

8 Network Protection

This chapter describes how to configure basic network protection features of Sophos UTM. The *Network Protection Statistics* page in WebAdmin shows an overview of intrusion prevention events and dropped data packets for both source and destination hosts. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective reporting section of WebAdmin, where you can find more statistical information.

Note – You can directly add a *Network/Host Exception* or a *Threat Exception* by clicking the **Plus** icon in the *Advanced Threat Protection: Recent Events* list.

The following topics are included in this chapter:

8.1 Firewall

The menu *Network Protection* > *Firewall* allows you to define and manage firewall rules of the gateway. Generally speaking, the firewall is the central part of the gateway which functions in a networked environment to prevent some communications forbidden by the security policy. The default security policy of Sophos UTM states that all network traffic is to be blocked and logged, except for automatically generated rule sets that are necessary for other software components of the gateway to work. However, those auto-generated rule sets are not shown on the *Firewall* > *Rules* tab. This policy requires you to define explicitly which data traffic is allowed to pass the gateway.

8.1.1 Rules

On the *Network Protection* > *Firewall* > *Rules* tab you can manage the firewall rule set. Opening the tab, by default, user-created firewall rules are displayed only. Using the drop-down list on top of the list, you can choose to display automatic firewall rules instead, or both types of rules combined. Automatic firewall rules are displayed with a distinct background color. Automatic firewall rules are generated by UTM based on a selected *Automatic firewall rules* checkbox in one of your configurations, e.g., when creating IPsec or SSL connections.

All newly defined firewall rules are disabled by default once added to the rules table. Automatic firewall rules and enabled user-created firewall rules are applied in the given order until the first rule matches. Automatic firewall rules are always on top of the list. The processing order of the user-created firewall rules is determined by the position number, so if you change the order of the rules by their position numbers, the processing order changes as well.

Caution – Once a firewall rule matched, all other rules are ignored. For that reason, the sequence of rules is very important. Never place a rule such as *Any (Source) – Any (Service) – Any (Destination) – Allow (Action)* at the top of the rule table, as this will allow each packet to traverse the gateway in both directions, ignoring all other rules that may follow.

To create a firewall rule, proceed as follows:

1. **On the *Rules* tab, click *New Rule*.**
   The *Create New Rule* dialog box opens.
2. **Make the following settings:**
   Group: The *Group* option is useful to group rules logically. With the drop-down list on top of the list you can filter the rules by their group. Grouping is only used for display purposes, it does not affect rule matching. To create a new group select the << *New group* >> entry and enter a descriptive name in the *Name* field.

   Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore.

   Sources: Add or select source network definitions, describing from which host(s) or networks the packets are originating.

Tip – How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Services: Add or select service definitions, describing the protocol(s) and, in case of TCP or UDP, the source and destination port(s) of the packets.

Destinations: Add or select destination network definitions, describing the target host (s) or network(s) of the packets.

Note – When you select more than one source, service and/or destination, the rule applies to every possible source-service-destination combination. A rule with e.g. two sources, two services and two destinations equates to eight single rules, from each source to each destination using both services.

Action: The action that describes what to do with traffic that matches the rule. The following actions can be selected:

- **Allow:** The connection is allowed and traffic is forwarded.
- **Drop:** Packets matching a rule with this action will be silently dropped.
- **Reject:** Connection requests matching rules with this action will be actively rejected. The sender will be informed via an ICMP message.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
Time period: By default, no time period definition is selected, meaning that the rule is always valid. If you select a time period definition, the rule will only be valid at the time specified by the time period definition. For more information, see *Time Period Definitions*.

Log traffic: If you select this option, logging is enabled and packets matching the rule are logged in the firewall log.

Source MAC addresses: Select a MAC address list definition, describing from which MAC addresses the packets are originating. If selected, packets only match the rule if their source MAC address is listed in this definition. Note that you cannot use a MAC address list in combination with the source *Any*. MAC address list definitions are defined on the *Definitions & Users > Network Definitions > MAC Address Definitions* tab.

4. **Click *Save*.**
   The new rule appears on the *Rules* list.
5. **Enable the firewall rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a rule, click the corresponding buttons.

Open Live Log: This will open a pop-up window containing a real-time log of filtered packets, whose regularly updating display shows recent network activity. The background color indicates which action has been applied:

- Red: The packet was dropped.
- Yellow: The packet was rejected.
- Green: The packet was allowed.
- Gray: The action could not be determined.

The live log also contains information about which firewall rule caused a packet to be rejected. Such information is essential for rule debugging.
Using the search function, you can filter the firewall log for specific entries. The search function even allows to negate expressions by typing a dash in front of the expression, e.g. `-WebAdmin` which will successively hide all lines containing this expression.

Selecting the *Autoscroll* checkbox will automatically scroll down the window's scrollbar to always show the most recent results.

Below are some basic hints for configuring the firewall:

- **Dropped Broadcasts:** By default, all broadcasts are dropped, which in addition will not be logged (for more information, see Advanced). This is useful for networks with many computers utilizing NetBIOS (for example, Microsoft Windows operating systems), because broadcasts will rapidly clutter up your firewall log file. To define a broadcast drop rule manually, group the definitions of the broadcast addresses of all attached networks, add another "global_broadcast" definition of `255.255.255.255/255.255.255.255`, then add a rule to drop all traffic to these addresses on top of your firewall configuration. On broadcast-heavy networks, this also has the benefit of increasing the system performance.

- **Rejecting IDENT Traffic:** If you do not want to use the IDENT reverse proxy, you can actively reject traffic to port `113` (IDENT) of your internal networks. This may prevent longer timeouts on services that use IDENT, such as FTP, IRC, and SMTP.

  Note – If you use masquerading, IDENT requests for masqueraded networks will arrive on the masquerading interface.

- Since NAT will change the addresses of network packets, it has implications on the firewall functionality.
  - DNAT is applied *before* the firewall. This means that the firewall will "see" the already translated packets. You must take this into account when adding rules for DNAT related services.
  - SNAT and Masquerading is applied *after* the firewall. This means that the firewall still "sees" the untranslated packets with the original source addresses.

The control panels in the table header can be used to filter firewall rules for specific criteria to rearrange rules for better readability. If you have defined groups you can select a group from the drop-down menu and thus see all rules that belong to this group. Using the search field you can look for a keyword or just a string to see the rules related to it. The search comprises a rule's source, destination, service, group name, and comment.

8.1.2 Country Blocking

On the *Network Protection* > *Firewall* > *Country Blocking* tab you can enable blocking of traffic coming from or going to a certain country or location. You can either block single countries/locations or whole continents. The blocking is based on the GeoIP information of the host's IP address.

To enable country blocking, proceed as follows:

1. **Enable country blocking.**
   Click the toggle switch.

   The toggle switch turns amber and the *Countries* section becomes editable.

2. **Select the locations to block.**
   Via the drop-down lists in front of the location names, specify the blocking status for the respective location:

- **All:** All traffic coming from or going to this location is blocked.
- **From:** Traffic coming from this location is blocked.
- **To:** Traffic going to this location is blocked.
- **Off:** Traffic from as well as to this location is allowed.

Tip – You can easily select an identical blocking status for all locations of a region. To do so, select the desired blocking status in the drop-down list in front of the respective region name.

3. **Click *Apply*.**
   Your settings will be saved. Traffic from and/or to selected locations will be blocked now according to your settings. Note that you can define exceptions for the blocked locations on the *Country Blocking Exceptions* tab.

Tip – Each section of this page can be collapsed and expanded by clicking the Collapse icon on the right of the section header.

8.1.3 Country Blocking Exceptions

On the *Network Protection > Firewall > Country Blocking Exceptions* tab you can define exceptions for countries that are blocked on the *Country Blocking* tab. Exceptions can be made for traffic between a blocked country/location and specific hosts or networks, taking into account the direction and the service of the traffic.

To create a country blocking exception, proceed as follows:

1. **Click *New Exception List*.**
   The *Create Exception* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the exception.

   Comment (optional): Add a description or other information.

   Skip blocking of these:

   - **Region:** Using this drop-down list, you can narrow down the countries displayed in the *Countries* box.

- **Countries:** Select the checkboxes in front of the locations or countries you want to make the exception for. To select all countries at once, enable the *Select all* checkbox.

  Note – To select all IP addresses, including those that are not associated with any country, for example internal IP addresses, deselect all checkboxes using the *Deselect all* checkbox.

For all requests: Select the condition under which the country blocking should be skipped. You can choose between outgoing and incoming traffic, referring to the hosts/networks to be selected in the box below.

- **Hosts/networks:** Add or select the hosts/networks that should be allowed to send traffic to or receive traffic from the selected countries—depending on the entry selected in the drop-down list above. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Using these services: Optionally, add the services that should be allowed between the selected hosts/networks and the selected countries/locations. If no service is selected, all services are allowed.

3. **Click *Save*.**
   The new country blocking exception appears on the *Country Blocking Exception* list.

To either edit or delete an exception, click the corresponding buttons.

8.1.4 ICMP

On the *Network Protection > Firewall > ICMP* tab you can configure the settings for the *Internet Control Message Protocol* (ICMP). ICMP is used to exchange connection-related status information between hosts. ICMP is important for testing network connectivity or troubleshooting network problems.

Allowing any ICMP traffic on this tab will override ICMP settings being made in the firewall. If you only want to allow ICMP for certain hosts or networks, you should use the *Firewall > Rules* tab instead.

Global ICMP Settings

The following global ICMP options are available:

- **Allow ICMP on gateway:** This option enables the gateway to respond to ICMP packets of any kind.
- **Allow ICMP through gateway:** This option enables the forwarding of ICMP packets through the gateway if the packets originate from an internal network, i.e., a network without default gateway.
- **Log ICMP redirects:** ICMP redirects are sent from one router to another to find a better route for a packet's destination. Routers then change their routing tables and forward the packet to the same destination via the supposedly better route. If you select this option, all ICMP redirects received by the gateway will be logged in the firewall log.

Note – If enabled, the ICMP settings apply to all ICMP packets, including ping and traceroute—if sent via ICMP—, even if the corresponding ping and traceroute settings are disabled.

Ping Settings

The program *ping* is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP *echo request* packets to the target host and listening for ICMP *echo response* replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

The following ping options are available:

- **Gateway is ping visible:** The gateway responds to ICMP *echo request* packets. This feature is enabled by default.
- **Ping from Gateway:** You can use the ping command on the gateway. This feature is enabled by default.
- **Gateway forwards pings:** The gateway forwards ICMP *echo request* and *echo response* packets originating from an internal network, i.e., a network without default gateway.

Note – If enabled, the ping settings also allow traceroute ICMP packets, even if the corresponding traceroute settings are disabled.

Traceroute Settings

The program *traceroute* is a computer network tool used to determine the route taken by packets across an IP network. It lists the IP addresses of the routers that were involved in transporting the packet. If the packet's route cannot be determined within a certain time frame,

traceroute will report an asterisk (*) instead of the IP address. After a certain number of failures, the check will end. An interruption of the check can have many causes, but most likely it is caused by a firewall along the network path that blocks traceroute packets.

The following traceroute options are available:

- **Gateway is traceroute visible:** The gateway responds to traceroute packets.
- **Gateway forwards traceroute:** The gateway forwards traceroute packets originating from an internal network, i.e., a network without default gateway.

Note – In addition, the UDP ports for UNIX traceroute applications are opened, too.

Note – If enabled, the traceroute settings also allow ping packets, even if the corresponding ping settings are disabled.

8.1.5 Advanced

The *Network Protection* > *Firewall* > *Advanced* tab contains advanced settings for the firewall and the NAT rules.

Connection Tracking Helpers

So-called connection tracking helpers enable protocols that use multiple network connections to work with firewall or NAT rules. All connections handled by the firewall are tracked by the *conntrack* kernel module, a process better known as *connection tracking*. Some protocols such as FTP and IRC require several ports to be opened, and hence require special connection tracking helpers supporting them to operate correctly. These helpers are special kernel modules that help identify additional connections by marking them as being related to the initial connection, usually by reading the related addresses out of the data stream.

For example, for FTP connections to work properly, the FTP conntrack helper must be selected. This is due to the specifics of the FTP protocol, which first establishes a single connection that is called the FTP control connection. When commands are issued through this connection, other ports are opened to carry the rest of the data (e.g., downloads or uploads) related to that specific command. The problem is that the gateway will not know about these extra ports, since they were negotiated dynamically. Therefore, the gateway will be unable to know that it should let the server connect to the client over these specific ports (active FTP connections) or to let clients on the Internet connect to the FTP server (passive FTP connections).

This is where the FTP conntrack helper becomes effective. This special helper is added to the connection tracking module and will scan the control connection (usually on port 21) for specific information. When it runs into the correct information, it will add that specific information to a list of expected connections as being related to the control connection. This in return enables the gateway to track both the initial FTP connection as well as all related connections properly.

Connection tracking helpers are available for the following protocols:

- FTP
- IRC (for DCC)
- PPTP
- TFTP

Note – The PPTP helper module needs to be loaded if you want to offer PPTP VPN services on the gateway. Otherwise PPTP sessions cannot be established. The reason for this is that PPTP first establishes a TCP port 1723 connection before switching to *Generic Routing Encapsulation* (GRE) communication, which is a separate IP protocol. If the PPTP helper module is not loaded, all GRE packets will be blocked by the gateway. Alternatively, if you do not want to use the PPTP helper module, you can manually add firewall rules allowing GRE packets for incoming and outgoing traffic.

Protocol Handling

Enable TCP window scaling: The TCP receive window (RWin) size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host. For more efficient use of high bandwidth networks, a larger TCP window size may be used. However, the TCP window size field controls the flow of data and is limited to 2 bytes, or a window size of 65535 bytes. Since the size field cannot be expanded, a scaling factor is used. TCP window scaling is a kernel option of the TCP/IP stack and can be used to increase the maximum window size from 65535 bytes to 1 Gigabyte. Window scaling is enabled by default. However, since some network devices such as routers, load balancers, gateways, and so on still do not fully support window scaling, depending on your environment it might be necessary to turn it off.

Use strict TCP session handling: By default, the system can "pick up" existing TCP connections that are not currently handled in the connection tracking table due to a network facility reset. This means that interactive sessions such as SSH and Telnet will not quit when a network interface is temporarily unavailable. Once this option is enabled, a new three-way handshake

will always be necessary to re-establish such sessions. Additionally, this option does not allow the TCP connection methods simultaneous open or TCP split handshakes. It is generally recommended to leave this option turned off.

Validate packet length: If enabled, the firewall will check the data packets for minimal length if the ICMP, TCP, or UDP protocol is used. If the data packets are smaller than the minimal values, they will be blocked and a record will be written to the firewall log.

Spoof protection: By default, spoof protection is disabled. You can choose between the following settings:

- **Normal:** The gateway will drop and log packets which either have the same source IP address as the interface itself or which arrive on an interface which has a source IP of a network assigned to another of its interfaces.
- **Strict:** The gateway will also drop and log all packets which have a destination IP for an interface but arriving on an interface other than assigned, that is, if it arrives on an interface for which it is not destined. For example, those packets will be dropped that were sent from an external network to the IP address of the internal interface which is supposed to accept packets from the internal network only.

Logging Options

Log FTP data connections: The UTM will log the FTP data connections of (file and directory listings). The log records are marked by the string "FTP data".

Log unique DNS requests: The UTM will log all outgoing requests to DNS servers as well as their outcome. The log records are marked by the string "DNS request".

Log dropped broadcasts: By default, the firewall drops all broadcasts, which in addition will not be logged. However, if you need broadcasts to be logged in the firewall log, for example, for audit purposes, select this option.

8.2 NAT

The menu *Network Protection* > *NAT* allows you to define and manage NAT rules of the gateway. *Network Address Translation* (NAT) is the process of rewriting the source and/or destination addresses of IP packets as they pass through a router or gateway. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address. When a client sends an IP packet to the router, NAT translates the sending address to a different, public IP address before forwarding the packet to the Internet.

When a response packet is received, NAT translates the public address into the original address and forwards it to the client. Depending on system resources, NAT can handle arbitrarily large internal networks.

8.2.1 Masquerading

Masquerading is a special case of *Source Network Address Translation* (SNAT) and allows you to masquerade an internal network (typically, your LAN with private address space) behind a single, official IP address on a network interface (typically, your external interface connected to the Internet). SNAT is more generic as it allows to map multiple source addresses to several destination addresses.

Note – The source address is only translated if the packet leaves the gateway system via the specified interface. Note further that the new source address is always the current IP address of that interface (meaning that this address can be dynamic).

To create a masquerading rule, proceed as follows:

1. **On the *Masquerading* tab, click *New Masquerading Rule*.**
   The *Create New Masquerading Rule* dialog box opens.
2. **Make the following settings:**
   Network: Select the (internal) network you want to masquerade.

   Interface: Select the (external) interface that is connected to the Internet.

   Use Address: If the interface you selected has more than one IP address assigned (see *Interfaces & Routing* > *Interfaces* > *Additional Addresses*), you can define here which IP address is to be used for masquerading.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new masquerading rule appears on the *Masquerading* rule list.
4. **Enable the masquerading rule.**
   Click the toggle switch to activate the masquerading rule.

To either edit or delete a rule, click the corresponding buttons.

Note – You need to allow traffic from the internal network to the Internet in the firewall if you want your clients to access external servers.

IPsec packets are never affected by masquerading rules. To translate the source address of IPsec packets create an SNAT or Full NAT rule.

8.2.2 NAT

Destination Network Address Translation (DNAT) and *Source Network Address Translation* (SNAT) are both special cases of NAT. With SNAT, the IP address of the computer which initiated the connection is rewritten, while with its counterpart DNAT, the destination addresses of data packets are rewritten. DNAT is especially useful when an internal network uses private IP addresses, but an administrator wants to make some services available to the outside.

This is best demonstrated with an example. Suppose your internal network uses the address space `192.168.0.0/255.255.255.0` and a webserver running at IP address `192.168.0.20` port `80` should be available to Internet-based clients. Because the `192.168.` address space is private, the Internet-based clients cannot send packets directly to the webserver. It is, however, possible for them to communicate with the external (public) address of the UTM. DNAT can, in this case, take packets addressed to port `80` of the system's address and forward them to the internal webserver.

Note – *PPTP VPN Access* is incompatible with DNAT.

In contrast to masquerading, which always maps to the primary network interface address, SNAT maps the source address to the address specified in the SNAT rule.

1:1 NAT is a special case of DNAT or SNAT. In this case all addresses of an entire network are being translated one-to-one into the addresses of another network having the same netmask. So the first address of the original network will be translated into the first address of the other network, the second into the second and so on. A 1:1 NAT rule can be applied to either the source or the destination address.

Note – By default, port `443` (HTTPS) is used for the User Portal. If you plan to forward port `443` to an internal server, you need to change the TCP port of the User Portal to another value (e.g., `1443`) on the *Management > User Portal > Advanced* tab.

Because DNAT is done before firewalling, you must ensure that appropriate firewall rules are defined. For more information, see *Network Protection* > *Firewall* > *Rules*.

To define a NAT rule, proceed as follows:

1. **On the *NAT* tab, click *New NAT Rule.***
   The *Create New NAT Rule* dialog box opens.
2. **Make the following settings:**
   Group: The *Group* option is useful to group rules logically. With the drop-down list on top of the list you can filter the rules by their group. Grouping is only used for display purposes, it does not affect rule matching. To create a new group select the << *New group* >> entry and enter a descriptive name in the *Name* field.

   Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore.

   Rule type: Select the network address translation mode. Depending on your selection, various options will be displayed. The following modes are available:

   - **SNAT (source):** Maps the source address of defined IP packets to one new source address. The service can be changed, too.
   - **DNAT (destination):** Maps the destination address of defined IP packets to one new destination address. The service can be changed, too.
   - **1:1 NAT (whole networks):** Maps IP addresses of a network to another network one-to-one. The rule applies either for the source or for the destination address of the defined IP packets.
   - **Full NAT (source + destination):** Maps both the source address and the destination address of defined IP packets to one new source and one new destination address. The source service and the target service can be changed, too.
   - **No NAT:** This option can be regarded as a kind of exception rule. For example, if you have a NAT rule for a defined network you can create a *No NAT* rule for certain hosts inside this network. Those hosts will then be exempted from NAT.

   Matching Condition: Add or select the source and destination network/host and the service for which you want to translate addresses. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

- **For traffic from:** The original source address of the packets. This can be either a single host or an entire network, or, except for the *1:1 NAT* rule type, a network range.
- **Using service:** The original service type of the packets (consisting of source and destination ports as well as a protocol type).

  Note – A traffic service can only be translated when the corresponding addresses are translated as well. In addition, a service can only be translated to another service when the two services use the same protocol.

- **Going to:** The original destination address of the packets. This can be either a single host or an entire network. With *SNAT* and *No NAT*, it can also be a network range.

Action: Add or select the source and/or destination and/or the service type into which you want to translate the original IP packet data. The displayed parameters depend on the selected *Rule type*. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

- **Change the source to** (only with *SNAT* or *Full NAT* mode): Select the source host, that is, the new source address of the packets.
- **Change the destination to** (only with *DNAT* or *Full NAT* mode): Select the destination host, that is, the new destination address of the packets.
- **And the service to** (only with *DNAT*, *SNAT* or *Full NAT* mode): Select the new service of the packets. Depending on the selected *Rule type* this can be the source and/or destination service.
- **1:1 NAT mode** (only with *1:1 NAT* mode): Select one of the following modes:
  - **Map destination:** Changes the destination address.
  - **Map source:** Changes the source address.

  Note – You need to add an entire network into the field *For traffic from* when you want to map the source, or into the field *Going to* when you want to map the destination.

- **Map to** (only with *1:1 NAT* mode): Select the network you want to translate the original IP addresses into. Please note that the original network and the translated network must have the same netmask.

Automatic firewall rule (optional): Select this option to automatically generate firewall rules to allow the corresponding traffic passing through the firewall.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Rule applies to IPsec packets (only with *SNAT* or *Full NAT* mode): Select this option if you want to apply the rule to traffic which is going to be processed by IPsec. By default this option is not selected, thus IPsec traffic is excluded from source network address translation.

   Log initial packets (optional): Select this option if you want to write the initializing packet of a communication to the firewall log. Whenever the NAT rule is used, you will then find a message in the firewall log saying "Connection using NAT". This option works for stateful as well as stateless protocols.

4. **Click *Save*.**
   The new rule appears on the *NAT* list.

5. **Enable the NAT rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

To either edit or delete a rule, click the corresponding buttons.

8.3 Advanced Threat Protection

On the menu *Network Protection* > *Advanced Threat Protection* you can enable and configure the Advanced Threat Protection feature to rapidly detect infected or compromised clients inside your network, and raise an alert or drop the respective traffic. Advanced Threat Protection aims at typical challenges in current corporate networks: on the one hand management of a mobile workforce with an increasing number of different mobile devices (BYOD), and on the other hand malware evolution and distribution methods getting faster and faster. The Advanced Threat Protection analyzes network traffic, e.g., DNS requests, HTTP requests, or IP packets in general, coming from and going to all networks. It also incorporates Intrusion Prevention and Antivirus data if the respective features are activated. The database used to identify threats is updated constantly by a CnC/Botnet data feed from Sophos Labs through pattern updates.

Based on this data, infected hosts and their communication with command-and-control (CnC) servers can quickly be identified and dealt with.

8.3.1 Global

On the *Advanced Threat Protection* > *Global* tab, you can activate the *Advanced Threat Protection System* of Sophos UTM.

To enable Advanced Threat Protection, proceed as follows:

1. **Enable the Advanced Threat Protection system.**
   Click the toggle switch.

   The toggle switch turns amber and the *Global Settings* area becomes editable.

2. **Make the following settings:**
   Policy: Select the security policy that the Advanced Threat Protection system should use if a threat has been detected.

   - **Drop:** The data packet will be logged and dropped.
   - **Alert:** The data packet will be logged.

   Network/host exceptions: Add or select the source networks or hosts that should be exempt from being scanned for threats by Advanced Threat Protection. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Threat exceptions: Add destination IP addresses or domain names that you want to skip from being scanned for threats by Advanced Threat Protection. This is the place where you would add false positives to prevent them from being detected as threat. Examples: `8.8.8.8` or `google.com`.

   Caution – Be careful with specifying exceptions. By excluding sources or destinations you may expose your network to severe risks.

3. **Click *Apply*.**
   Your settings will be saved.

If enabled, and a threat is detected, it will be listed on the Network Protection page. A notification will be sent to the administrator if enabled on the *Management* > *Notifications* > *Notifications* page. The notification is set by default for drop and alert.

Live Log

The Advanced Threat Protection live log can be used to monitor the detected threats. Click the button to open the live log in a new window.

Note – IPS and Web Proxy threats will not be displayed in the *Live Log*.

8.4 Intrusion Prevention

On the menu *Network Protection* > *Intrusion Prevention* you can define and manage IPS rules of the gateway. The *Intrusion Prevention system* (IPS) recognizes attacks by means of a signature-based IPS rule set. The system analyzes the complete traffic and automatically blocks attacks before they can reach the network. The existing rule set and attack patterns are updated through the pattern updates. New IPS attack pattern signatures are automatically imported to the rule set as IPS rules.

8.4.1 Global

On the *Network Protection* > *Intrusion Prevention* > *Global* tab you can activate the *Intrusion Prevention System* (IPS) of Sophos UTM.

To enable IPS, proceed as follows:

1. **Enable the intrusion prevention system.**
   Click the toggle switch.

   The toggle switch turns amber and the *Global IPS Settings* area becomes editable.

2. **Make the following settings:**
   Local networks: Add or select the networks that should be protected by the intrusion prevention system. If no local network is selected, intrusion prevention will automatically be deactivated and no traffic is monitored. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Policy: Select the security policy that the intrusion prevention system should use if a blocking rule detects an IPS attack signature.

- **Drop silently:** The data packet will be dropped without any further action.
- **Terminate connection:** A terminating data packet (*RST* for TCP and *ICMP Port Unreachable* for UDP connections) will be sent to both communication partners to close the connection.

Note – By default, *Drop silently* is selected. There is usually no need to change this, especially as terminating data packets can be used by an alleged intruder to draw conclusions about the gateway.

3. **Click *Apply*.**
   Your settings will be saved.

Live Log

The intrusion prevention live log can be used to monitor the selected IPS rules. Click the button to open the live log in a new window.

8.4.2 Attack Patterns

The *Network Protection* > *Intrusion Prevention* > *Attack Patterns* tab contains IPS rules grouped according to common attack patterns. Attack patterns have been combined as follows:

- **Operating System Specific Attacks:** Attacks trying to exploit operating system related weaknesses.
- **Attacks Against Servers:** Attacks targeted at all sorts of servers (for example, webservers, mail servers, and so on).
- **Attacks Against Client Software:** Attacks aimed at client software such as web browsers, mutimedia players, and so on.
- **Protocol Anomaly:** Attack patterns look out for network anomalies.
- **Malware:** Software designed to infiltrate or damage a computer system without the owner's informed consent (for example, trojans, DoS communication tools, and the like).

To improve performance, you should clear the checkboxes that do not apply to services or software employed in your local networks. For example, if you do not operate a webserver in your local network, you can cancel the selection for *HTTP Servers*.

For each group, the following settings are available:

Action: By default, each rule in a group has an action associated with it. You can choose between the following actions:

- **Drop:** The default setting. If an alleged attack attempt has been determined, the causing data packets will be dropped.
- **Alert:** Unlike the *Drop* setting, critical data packets are allowed to pass the gateway but will create an alert message in the IPS log.

Note – To change the settings for individual IPS rules, use the *Modified Rules* box on the *Intrusion Prevention > Advanced* tab. A detailed list of IPS rules used in Sophos UTM 9 is available at the UTM website.

Rule Age: By default, IPS patterns are restricted to those dating from the last 12 months. Depending on individual factors like overall patch level, legacy systems, or other security requirements, you can select another time span. Selecting a shorter time span will reduce the number of rules and thus improve performance.

Add extra warnings: When this option is selected, each group will include additional rules increasing the IPS detection rate. Note that these rules are more general and vague than the explicit attack patterns and will therefore likely produce more alerts. For that reason, the default action for these rules is *Alert*, which cannot be configured.

Notify: When this option is selected, a notification is sent to the administrator for every IPS event matching this group. Note that this option only takes effect if you have enabled the notification feature for the intrusion prevention system on the *Management > Notifications > Notifications* tab. In addition, what type of notification (i.e., email or SNMP trap) is to be sent depends on the settings made there. Note further that it might take up to five minutes before changes of the notification settings will become effective.

8.4.3 Anti-DoS/Flooding

On the *Anti-DoS/Flooding* tab you can configure certain options aimed at defending *Denial of Service* (DoS) and *Distributed Denial of Service* (DDoS) attacks.

Generally speaking, DoS and DDoS attacks try to make a computer resource unavailable for legitimate requests. In the simplest case, the attacker overloads the server with useless packets in order to overload its performance. Since a large bandwidth is required for such attacks, more and more attackers start using so-called *SYN flood attacks*, which do not aim at overloading the bandwidth, but at blocking the system resources. For this purpose, they send so-called SYN

packets to the TCP port of the service often with a forged sender address, thus causing the server to spawn a half-open connection by sending back a TCP/SYN-ACK packet, and waiting for an TCP/ACK packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests.

Such attacks, however, can be prevented by limiting the amount of SYN (TCP), UDP, and ICMP packets being sent into your network over a certain period of time.

TCP SYN Flood Protection

To enable SYN (TCP) flood protection, proceed as follows:

1. **On the *Anti-DoS/Flooding* tab, select the checkbox *Use TCP SYN Flood Protection*.**
2. **Make the following settings:**
   Mode: The following modes are available:
   - **Source and destination addresses:** Select this option if you want to drop SYN packets by both their source and destination IP address. First, SYN packets matching the source IP address are restricted to the source packet rate value specified below. Second, if there are still too many requests, they will additionally be filtered according to their destination IP address and restricted to the destination packet rate value specified below. This mode is set as default.
   - **Destination address only:** Select this option if you want to drop SYN packets according to the destination IP address and destination packet rate only.
   - **Source address only:** Select this option if you want to drop SYN packets according to the source IP address and source packet rate only.

   Logging: This option lets you select the log level. The following levels are available:
   - **Off:** Select this log level if you want to turn logging completely off.
   - **Limited:** Select this log level to limit logging to five packets per seconds. This level is set as default.
   - **Everything:** Select this log level if you want verbose logging for all SYN (TCP) connection attempts. Note that SYN (TCP) flood attacks may lead to extensive logging.

Source packet rate: Here you can specify the rate of packets per second that is allowed for source IP addresses.

Destination packet rate: Here you can specify the rate of packets per second that is allowed for destination IP addresses.

Note – It is important to enter reasonable values here, for if you set the rate too high, your webserver, for instance, might fail because it cannot deal with such an amount of SYN (TCP) packets. On the other hand, if you set the rate too low, your gateway might show some unpredictable behavior by blocking regular SYN (TCP) requests. Reasonable settings for every system heavily depend on your hardware. Therefore, replace the default values by numbers that are appropriate for your system.

3. **Click *Apply*.**
   Your settings will be saved.

UDP Flood Protection

UDP Flood Protection detects and blocks UDP packet floods.
The configuration of *UDP Flood Protection* is identical to *TCP SYN Flood Protection*.

ICMP Flood Protection

ICMP Flood Protection detects and blocks ICMP packet floods.
The configuration of *ICMP Flood Protection* is identical to *TCP SYN Flood Protection*.

8.4.4 Anti-Portscan

The *Network Protection > Intrusion Prevention > Anti-Portscan* tab lets you configure general portscan detection options.

Portscans are used by hackers to probe secured systems for available services: In order to intrude into a system or to start a DoS attack, attackers need information on network services. If this information is available, attackers might take advantage of the security deficiencies of these services. Network services using the TCP and UDP Internet protocols can be accessed via special ports and this port assignment is generally known, for example the SMTP service is assigned to the TCP port 25. Ports that are used by the services are referred to as open, since it is possible to establish a connection to them, whereas unused ports are referred to as closed; every attempt to connect with them will fail. Attackers try to find the open ports with the help of a particular software tool, a port scanner. This program tries to connect with several ports on the

destination computer. If it is successful, the tool displays the relevant ports as open and the attackers have the necessary information, showing which network services are available on the destination computer.

Since there are 65535 distinct and usable port numbers for the TCP and UDP Internet protocols, the ports are scanned at very short intervals. If the gateway detects an unusually large number of attempts to connect to services, especially if these attempts come from the same source address, the gateway is most likely being port scanned. If an alleged attacker performs a scan of hosts or services on your network, the portscan detection feature will recognize this. As an option, further portscans from the same source address can be blocked automatically. Please note that the portscan detection is limited to Internet interfaces, i.e. interfaces with a default gateway.

Technically speaking, a portscan is detected when a detection score of 21 points in a time range of 300 ms for one individual source IP address is exceeded. The detection score is calculated as follows:

- Scan of a TCP destination port less than `1024` = 3 points
- Scan of a TCP destination port greater or equal `1024` = 1 point

To enable portscan detection, proceed as follows:

1. **On the *Anti-Portscan* tab, enable *Portscan Detection*.**
   Click the toggle switch.

   The toggle switch turns green and the *Global Settings* area becomes editable.

2. **Make the following settings:**
   Action: The following actions are available:

   - **Log event only:** No measures are taken against the portscan. The event will be logged only.
   - **Drop traffic:** Further packets of the portscan will be silently dropped. A port scanner will report these ports as filtered.
   - **Reject traffic:** Further packets of the portscan will be dropped and an ICMP "destination unreachable/port unreachable" response will be sent to the originator. A port scanner will report these ports as closed.

   Limit logging: Enable this option to limit the amount of log messages. A portscan detection may generate many logs while the portscan is being carried out. For example, each SYN packet that is regarded as belonging to the portscan will generate an entry in the firewall log. Selecting this option will restrict logging to five lines per second.

3. **Click *Apply*.**
   Your settings will be saved.

8.4.5 Exceptions

On the *Network Protection* > *Intrusion Prevention* > *Exceptions* tab you can define source and destination networks that should be excluded from intrusion prevention.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this exception.

   Skip These Checks: Select the security checks that should be skipped:

   - **Intrusion Prevention:** When you select this option, the IPS of Sophos UTM will be disabled.
   - **Portscan Protection:** Selecting this option disables the protection from attacks aimed at searching your network hosts for open ports.
   - **TCP SYN Flood Protection:** Once selected, the protection from TCP SYN flooding attacks will be disabled.
   - **UDP Flood Protection:** Once selected, the protection from UDP flooding attacks will be disabled.
   - **ICMP Flood Protection:** Once selected, the protection from ICMP flooding attacks will be disabled.

   For All Requests: Select at least one condition for which the security checks are to be skipped. You can logically combine several conditions by selecting either *And* or *Or* from the drop-down list in front of a condition. The following conditions can be set:

   - **Coming from These Source Networks:** Select to add source hosts/networks that should be exempt from the security checks of this exception rule. Enter the respective hosts or networks in the *Networks* box that opens after selecting the condition.

- **Using These Services:** Select to add services that should be exempt from the security checks of this exception rule. Add the respective services to the *Services* box that opens after selecting the condition.
- **Going to These Destinations:** Select to add hosts/networks that should be exempt from the security checks of this exception rule. Enter the respective hosts or networks in the *Destinations* box that opens after selecting the condition.

Tip – How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.
4. **Enable the exception.**
   The new exception is disabled by default (toggle switch is gray). Click the toggle switch to enable the exception.

   The exception is now enabled (toggle switch is green).

To either edit or delete an exception, click the corresponding buttons.

Note – If you want to except intrusion prevention for packets with the destination address of the gateway, selecting *Any* in the *Destinations* box will not succeed. You must instead select an interface definition of the gateway that contains the gateway's IP address, for example, *Internal (Address)* if you want to exclude intrusion prevention for the gateway's internal address.

8.4.6 Advanced

Pattern Set Optimization

Activate file-related patterns: By default, patterns against file-based attacks are disabled as protection against those threats is usually covered by the Antivirus engine. This default setting (disabled) provides maximum performance while enabling this option will provide maximum recognition rate. Enabling file-related patterns may be a sensible option where no other virus protection is available, e.g., Web Protection is turned off or no client Antivirus program is installed.

Manual Rule Modification

In this section, you can configure manual modifications to each IPS rule overwriting the default policy, which is taken from the attack pattern groups. Such modifications should be configured by experienced users only.

To create a modified rule, proceed as follows:

1. **In the *Modified rules* box, click the Plus icon.**
   The *Modify Rule* dialog box opens.
2. **Make the following settings:**
   Rule ID: Enter the ID of the rule you want to modify. To look up the rule ID, go to the list of IPS rules at the Sophos website. (In the folder, look for files with *IPS-rules* in their names, available for different UTM versions and pattern versions, and both in HTML and XML format.) In addition, they can either be determined from the IPS log or the IPS report.

   Disable this rule: When you select this option, the rule of the respective ID will be disabled.

   If you do *not* select this option, however, the following two options are available:

   - **Disable notifications:** Selecting this option will not trigger a notification in case the rule in question was applied.
   - **Action:** The action each rule is associated with it. You can choose between the following actions:
     - **Drop:** If an alleged attack attempt has been determined, the causing data packets will be dropped.
     - **Alert:** Unlike the *Drop* setting, critical data packets are allowed to pass the gateway but will create an alert message in the IPS log.
3. **Click *Save*.**
   The rule appears in the *Modified rules* box. Please note that you also need to click *Apply* on the bottom of the page to commit the changes.

Note – If you add a rule ID to the *Modified rules* box and set the action to *Alert*, for example, this modification will only take effect if the group to which the rule belongs is enabled on the *Attack Patterns* tab. If the corresponding attack pattern group is disabled, modifications to individual IPS rules will have no effect.

Performance Tuning

In addition, to increase the performance of the intrusion prevention system and to minimize the amount of false positive alerts, you can limit the scope of IPS rules to only some of your internal servers. For example, suppose you have activated the *HTTP Servers* group on the *Attack Patterns* tab and you have selected a particular HTTP server here. Then, even if the intrusion prevention system recognizes an attack against an HTTP server, the associated action (*Drop* or *Alert*) will only be applied if the IP address of the affected server matches the IP address of the HTTP server selected here.

You can limit the scope of IPS rules for the following server types:

- **HTTP:** All attack pattern groups subsumed under *HTTP Servers*
- **DNS:** Attack pattern group *DNS*
- **SMTP:** Attack pattern groups *Exchange* and *Sendmail*
- **SQL:** All attack pattern groups subsumed under *Database Servers*

8.5 Server Load Balancing

With the server load balancing function you can distribute incoming connections (e.g., SMTP or HTTP traffic) to several servers behind the gateway. Balancing is based on the source IP address with a persistence time of one hour. If the interval between two requests from the same source IP address exceeds that interval, the balancing is redecided. The traffic distribution is based on a simple round-robin algorithm.

All servers from the server pool are monitored either by ICMP ping, TCP connection establishment, or HTTP/S requests. In case of a failure the affected server is not used anymore for distribution, any possible source IP persistence is overruled.

Note – A return code of HTTP/S requests must either be `1xx Informational`, `2xx Success`, `3xx Redirection`, or `4xx Client Error`. All other return codes are taken as failure.

8.5.1 Balancing Rules

On the *Network Protection* > *Server Load Balancing* > *Balancing Rules* tab you can create load balancing rules for Sophos UTM Software. After having created a rule, you can additionally

define weight distribution between servers and set interface persistence.

To create a load balancing rule, proceed as follows:

1. **On the *Balancing Rules* tab, click *New Load Balancing Rule*.**
   The *Create New Load Balancing Rule* dialog box opens.
2. **Make the following settings:**
   Service: The network service you want to balance.

   Virtual server: The original target host of the incoming traffic. Typically, the address will be the same as the gateway's external address.

   Real servers: The hosts that will in turn accept traffic for the service.

   Tip – How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Check type: Select either *TCP* (TCP connection establishment), *UDP* (UDP connection establishment), *Ping* (ICMP Ping), *HTTP Host* (HTTP requests), or *HTTPS Hosts* (HTTPS requests) for service monitoring. When using *UDP* a ping request will be sent initially which, if successful, is followed by a UDP packet with a payload of 0. If ping does not succeed or the ICMP port is unreachable, the server is regarded as down. For *HTTP* and *HTTPS* requests you can enter a *URL*, which can either be with or without hostname, e.g. `index.html` or `http://www.example.com/index.html`.

   Interval: Enter a check interval in seconds. The default is 15 seconds, i.e., every 15 seconds the health status of all real servers is checked.

   Timeout: Enter a maximum time span in seconds for the real servers to send a response. If a real server does not respond during this time, it will be regarded as dead.

   Automatic firewall rules (optional): Select this checkbox to automatically generate firewall rules. These rules allow forwarding traffic from any host to the real servers.

   Shutdown virtual server address (optional): If and only if you use an additional address as virtual server for load balancing (see chapter *Interfaces* > *Additional Addresses*) this checkbox can be enabled. In case all real servers become unavailable that additional address interface will be automatically shut down.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new rule appears on the *Balancing Rules* list.
4. **Enable the load balancing rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a rule, click the corresponding buttons.

Example: Suppose that you have two HTTP servers in your DMZ with the IP addresses `192.168.66.10` and `192.168.66.20`, respectively. Assumed further you want to distribute HTTP traffic arriving on the external interface of your gateway equally to both servers. To set up a load balancing rule, select or create a host definition for each server. You may call them *http_server_1* and *http_server_2*. Then, in the *Create New Load Balancing Rule* dialog box, select *HTTP* as *Service*. In addition, select the external address of the gateway as *Virtual server*. Finally, put the host definitions into the *Real servers* box.

Weight Distribution and Interface Persistence

To distribute weight between the load balancing servers and/or to set interface persistence of them, do the following:

1. **Click the *Edit* button of a load balancing rule.**
   The *Edit Load Balancing Rule* dialog box opens.
2. **Click the Scheduler button on the header of the *Real servers* box.**
   The *Edit Scheduler* dialog window opens.
3. **Make the following settings:**
   Weight: Weight can be set from 0 to 100 and specifies how much traffic is processed by a server relative to all other servers. A weighted round robin algorithm is used for this, a higher value meaning more traffic is routed to the respective server. The values are evaluated relative to each other so they need not add up to 100. Instead, you can have a configuration for example, where server 1 has value 100, server 2 has value 50 and server 3 has value 0. Here, server 2 gets only half the traffic of server 1, whereas server 3 only comes into action when none of the other servers is available. A value of zero means that always another server with a higher value is chosen if available.

   Persistence: Interface persistence is a technique which ensures that subsequent connections from a client are always routed over the same uplink interface. Persistence has

a default timeout of one hour. You can also disable interface persistence for this balancing rule.

4. **Click *Save*.**
   The *Edit Scheduler* dialog window closes and your settings are saved.
5. **Click *Save*.**
   The *Edit Load Balancing Rule* dialog box closes.

8.6 VoIP

Voice over Internet Protocol (VoIP) is the routing of voice conversations over the Internet or through any other IP-based network. Sophos UTM offers support for the most frequently employed protocols used to carry voice signals over the IP network:

- SIP
- H.323

8.6.1 SIP

The *Session Initiation Protocol* (SIP) is a signalization protocol for the setup, modification, and termination of sessions between two or several communication partners. It is primarily used in setting up and tearing down voice or video calls. To use SIP, you first have to register your IP address and URLs at your ISP. SIP uses UDP or TCP on port `5060` to indicate which IP addresses and port numbers are to be used between the endpoints to exchange media data (video or voice). Since opening all ports for all addresses would cause a severe security issue, the gateway is able to handle SIP traffic on an intelligent basis. This is achieved by means of a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy. For that purpose you must specify both a SIP server network and a SIP client network definition in order to create appropriate firewall rules enabling the communication via the SIP protocol.

To enable support for the SIP protocol, proceed as follows:

1. **On the *SIP* tab, enable SIP protocol support.**
   Click the toggle switch.

   The toggle switch turns amber and the *Global SIP Settings* area becomes editable.

2. **Make the following settings:**
   SIP server networks: Here you can add or select the SIP servers (provided by your ISP) the SIP clients should be allowed to connect to; for security reasons, do not select *Any*. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   SIP client networks: Add or select the hosts/networks of the SIP clients that should be allowed to initiate or respond to a SIP communication. A SIP client is an endpoint in the LAN that participates in real-time, two-way communications with another SIP client. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Expectation mode: Select how strict the initializing of communication sessions should be:

   - **Strict:** Incoming calls are only allowed from the ISP's registrar, i.e. the IP address the REGISTER SIP message was sent to. Additionally, the UTM only accepts media (voice or video) data sessions from signaling endpoints, i.e., the devices that exchanged the SIP message. Some providers send the media data from another IP address than the SIP message, which will be rejected by the UTM.
   - **Client/server networks:** Incoming calls are allowed from all clients of the defined SIP server or client networks. Media data is accepted from another sender IP address than the one that sent the SIP message, provided that the address belongs to the defined SIP server or client networks.
   - **Any:** Incoming calls as well as media data are permitted from anywhere.

3. **Click *Apply*.**
   Your settings will be saved.

To cancel the configuration, click the amber colored toggle switch.

8.6.2 H.323

H.323 is an international multimedia communications protocol standard published by the *International Telecommunications Union* (ITU-T) and defines the protocols to provide audio-visual communication sessions on any packet-switched network. H.323 is commonly used in *Voice over IP* (VoIP) and IP-based videoconferencing.

H.323 uses TCP on port `1720` to negotiate which dynamic port range is to be used between the endpoints when setting up a call. Since opening all ports within the dynamic range would cause

a severe security issue, the gateway is able to allow H.323-related traffic on an intelligent basis. This is achieved by means of a special connection tracking helper monitoring the control channel to determine which dynamic ports are being used and then only allowing these ports to pass traffic when the control channel is busy. For that purpose you must specify both an H.323 gatekeeper and a client network definition in order to create appropriate firewall rules enabling the communication via the H.323 protocol.

To enable support for the H.323 protocol, proceed as follows:

1. **On the *H.323* tab, enable H.323 protocol support.**
   Click the toggle switch.

   The toggle switch turns amber and the *Global H.323 Settings* area becomes editable.

2. **Make the following settings:**
   H.323 Gatekeeper: Add or select an H.323 gatekeeper. An H.323 gatekeeper controls all H.323 clients (endpoints such as Microsoft's NetMeeting) in its zone. More specifically, it acts as a monitor of all H.323 calls within its zone on the LAN. Its most important task is to translate between symbolic alias addresses and IP addresses. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   H.323 Client: Here you can add or select the host/network to and from which H.323 connections are initiated. An H.323 client is an endpoint in the LAN that participates in real-time, two-way communications with another H.323 client. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Enable Strict Mode (optional): Select this option to enhance security. However, if you are facing connection problems with your ISP, disable strict mode.

3. **Click *Apply*.**
   Your settings will be saved.

To cancel the configuration, click the amber colored toggle switch.

8.7 Advanced

The tabs of the *Network Protection > Advanced* menu let you configure additional network protection features such as a generic proxy, SOCKS proxy, and IDENT reverse proxy.

8.7.1 Generic Proxy

A generic proxy, also known as a port forwarder, combines both features of DNAT and masquerading, forwarding all incoming traffic for a specific service to an arbitrary server. The difference to standard DNAT, however, is that a generic proxy also replaces the source IP address of a request with the IP address of the interface for outgoing connections. In addition, the destination (target) port number can be changed as well.

To add a generic proxy rule, proceed as follows:

1. **On the *Generic Proxy* tab, click *New Generic Proxy Rule*.**
   The *Create New Generic Proxy Rule* dialog box opens.
2. **Make the following settings:**
   Interface: Select the interface for incoming connections.

   Service: Add or select the service definition of the traffic to be proxied.

   Host: Add or select the target host where the traffic should be forwarded to.

   Service: Add or select the target service of the traffic to be proxied.

   Allowed Networks: Add or select the networks to which port forwarding should be applied.

   > **Tip –** How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new rule appears on the *Generic Proxy* rule list.
4. **Enable the generic proxy rule.**
   The new rule is disabled by default (toggle switch is gray). Click the toggle switch to enable the rule.

   The rule is now enabled (toggle switch is green).

To either edit or delete a rule, click the corresponding buttons.

8.7.2 SOCKS Proxy

SOCKS is a versatile Internet protocol that allows client-server applications to transparently use the services of a network firewall. It is used by many client applications behind a firewall to communicate with hosts on the Internet. Examples are IRC/Instant Messaging clients, FTP clients, and Windows SSH/Telnet clients. Those clients behind a firewall wanting to access exterior servers connect to a SOCKS proxy server instead. This proxy server controls the eligibility of the client to access the external server and passes the request on to the server. Your client application must explicitly support the SOCKS 4 or SOCKS 5 protocol versions.

The default port for SOCKS is `1080`. Almost all clients have implemented this default port setting, so it normally does not have to be configured. The differences between SOCKS and NAT are that SOCKS also allows "bind" requests (listening on a port on behalf of a client—a feature which is supported by very few clients only) and that SOCKS 5 allows user authentication.

When enabling the SOCKS proxy, you must define one or more networks which should have access to the proxy. When you require user authentication, you can also select the users or groups that should be allowed to use the SOCKS proxy.

Note – Without user authentication, the SOCKS proxy can be used with both the SOCKS 4 and SOCKS 5 protocols. When user authentication is selected, only SOCKS 5 will work. If you want the proxy to resolve hostnames in SOCKS 5 mode, you must also activate the DNS proxy, because otherwise DNS resolution will fail.

To configure the SOCKS proxy, proceed as follows:

1. **On the *SOCKS Proxy* tab, enable the SOCKS proxy.**
   Click the toggle switch.

   The toggle switch turns amber and the *SOCKS Proxy Options* area becomes editable.

2. **Make the following settings:**
   Allowed networks: Add or select the networks that should be allowed to use the SOCKS proxy. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Enable user authentication: If you select this option, users must provide a username and password to log in to the SOCKS proxy. Because only SOCKS 5 supports user authentication, SOCKS 4 is automatically disabled.

Allowed users: Select the users or groups or add new users that should be allowed to use the SOCKS proxy. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

3. **Click *Apply*.**
   Your settings will be saved.

8.7.3 IDENT Reverse Proxy

The IDENT protocol is used by remote servers for a simple verification of the identity of accessing clients. Although this protocol is unencrypted and can easily be spoofed, many services still use (and sometimes require) the IDENT protocol.

To configure the IDENT relay, proceed as follows:

1. **On the *IDENT Reverse Proxy* tab, enable the IDENT relay.**
   Click the toggle switch.

   The toggle switch turns green and the *Global Settings* area becomes editable.

2. **Make the following settings:**
   Forward to Internal Hosts (optional): Since IDENT queries are not covered by the gateway's connection tracking, they will get "stuck" if masquerading is used. You can select the *Forward to Internal Hosts* option to pass on IDENT queries to masqueraded hosts behind the gateway. Note that the actual IP connection will not be forwarded. Instead, the gateway will in turn ask the internal client for an IDENT reply and will forward that string to the requesting server. This scheme will work with most "mini-IDENT" servers built into popular IRC and FTP clients.

   Default Response: The gateway offers support for answering IDENT requests when you enable the IDENT relay. The system will always reply with the string entered in the *Default Response* box, regardless of the local service that has initiated the connection.

3. **Click *Apply*.**
   Your settings will be saved.

9 Web Protection

This chapter describes how to configure basic web protection features of Sophos UTM.

The following topics are included in this chapter:

- Web Filtering
- Web Filter Profiles
- Filtering Options
- Policy Test
- Application Control
- FTP

The *Web Protection Statistics* page in WebAdmin provides an overview of the most used applications and application categories, the most surfed domains according to time and traffic as well as the top users surfing. In addition, the top blocked website categories are shown. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective reporting section of WebAdmin, where you can find more statistical information.

Note – You can find detailed information on how the web usage data is collected and how the statistics are calculated on the *Logging & Reporting > Web Protection > Web Usage Reports* page.

In the *Top Applications* section, hovering the cursor on an application displays one or two icons with additional functionality:

- Click the *Block* icon to block the respective application from now on. This will create a rule on the *Application Control Rules* page. This option is unavailable for applications relevant to the flawless operation of Sophos UTM. WebAdmin traffic, for example, cannot be blocked as this might lead to shutting yourself out of WebAdmin. Unclassified traffic cannot be blocked, either.
- Click the *Shape* icon to enable traffic shaping of the respective application. A dialog window opens where you are asked to define the rule settings. Click *Save* when you are done. This will create a rule both on the *Traffic Selectors* and on the *Bandwidth Pools* page.
  Traffic shaping is not available when viewing the *All Interfaces* Flow Monitor as shaping works interface-based.

9.1 Web Filtering

The tabs of the *Web Protection* > *Web Filtering* menu allow you to configure Sophos UTM Software as an HTTP/S caching proxy. In addition to simple caching services, the HTTP/S proxy of Sophos UTM features a rich set of web filtering techniques for the networks that are allowed to use its services. This includes preventing virus and spyware infections by means of two different virus scanning engines with constantly updated signature databases and spyware filtering techniques that protects both inbound and outbound traffic. Moreover, Sophos UTM can control access to various webpages by employing sophisticated website categorization, using the world's largest real-time URL database. Used in conjunction with Sophos Endpoint Software, Sophos UTM can enforce and monitor these same web policies on endpoint machines that are on external networks. To enable *Endpoint Web Control*, see *Endpoint Protection* > *Web Control*.

You can still manage your filter actions on the *Web Filter Profiles* > *Filter Actions* tab. There you can add, modify, clone or delete filter actions. But now you can create, modify, and assign filter actions by launching the *Add/Edit Filter Action* wizard on the *Web Filtering* > *Policies* tab.

9.1.1 Web Filtering Changes

As of the 9.2 release, Sophos UTM includes a new simplified interface for creating and managing your web filtering policies. While the interface has changed considerably, functionality has not changed. All of your existing settings have been preserved and if you make no changes the system will behave in the exact same way.

Previously, complex web policy involved creating web filtering profiles. These consisted of filter actions, created on the *Filter Actions* tab, which were then assigned to users and groups through filter assignments on the *Filter Assignments* tab, and then configured on the *Proxy Profiles* tab. Now, you can configure all aspects of your Web Filtering policy, including your default configuration and advanced filtering profiles from the *Web Filtering* > *Policies* tab.

Note – Take some time to familiarize yourself with the new interface and read the following overview. While it is different than previous releases, it should be much easier to create and maintain complex web policies.

9.1.1.1 Some Key Differences

- Many tabs that were under *Web Protection* > *Web Filtering* have moved to *Web Protection* > *Filtering Options*.
- The new UTM interface describes web filtering rules in terms of policies. A policy is the same as an assigned filter action in previous versions.
- In version 9.1 and prior, the Default Profile had only a single Filter Assignment (called the default assignment). As of 9.2 you can have many Policies within the default profile.
- What was called the fallback action is now called the *Base Policy*. The function is the same. The Base Policy contains the Filter Action that is used if no other policies match.
- Creation of filter actions is now done with a multi-tab dialog, the *Filter Action Wizard*.
- Proxy profiles are now called filter profiles, and can be managed on the *Web Filter Profiles* > *Filter Profiles* tab. The policies associated with a filter profile are displayed on the *Policies* tab of the *Edit Profile* and *Add Profile* dialogues.
- In 9.1 and prior, a single filter assignment could be used in multiple proxy profiles. As of version 9.2, a Policy is specific to a single filter profile.

9.1.1.2 Common Tasks

The following is a brief overview of how you perform common tasks in 9.2 and later compared to the 9.1 interface.

How do I:	**9.1**	**9.2**
Edit the default policy?	Configure the various tabs under *Web Filtering*: ● *Web Filtering* > *Antivirus/Malware* ● *Web Filtering* > *URL Filtering* ● *Web Filtering* > *Advanced*	*Web Filtering* > *Policies*
Create or edit a proxy profile?	*Web Filtering Profiles* > *Proxy Profiles*	*Web Filtering* > *Web Filtering Profiles*

Add or edit an exception to my default policy?	*Web Filtering > Exceptions*	1. *Web Filtering > Policies* 2. Select the *Default content filter action* for the *Base Policy* 3. Under *Website Filtering*, click the green Plus icon next to *Block/Allow these websites*
Assign a filter assignment to a proxy profile?	1. Create a filter action on *Web Filtering Profiles > Filter Actions* 2. Create a filter assignment on *Web Filtering Profiles > Filter Assignments* 3. Edit or add a proxy profile on *Web Filtering Profiles > Proxy Profiles*	1. On *Web Filtering Profiles > Filter Profiles*, click on the name of a *Filter Profile*, or create a profile by clicking the green Plus icon 2. On the *Policies* tab, click the green plus icon to add a policy 3. Select a *Filter Action*, or click the green plus icon to create one.
Create a new Filter Action for my Filter Assignment?	*Web Filtering Profiles > Filter Assignments*	On *Web Filtering > Policies*, when creating or editing a policy, click the green Plus icon next to *Filter Action*.
Modify advanced settings?	*Web Filtering > Advanced*	*Filtering Options > Misc*
Manage trusted HTTPS CAs?	*Web Filtering > HTTPS CAs*	*Filtering Options > HTTPS CAs*

9.1.1.3 Migration

When you upgrade to version 9.2, your previous configuration and settings will all be preserved. However, as the interface has changed considerably, things may not be where you expect them to be. Following are a few things you will notice about your configuration.

Proxy Profiles are now called Filter Profiles. One of the first things you will see is that in any Filter Profile, including the default policy on *Web Filtering > Policies*, is that there are several disabled policies and one or more enabled policies. This may be confusing at first, but the functionality is

the same as in 9.1. These changes make it easier to update your configuration, and to take advantage of the new features in 9.2.

After upgrade, your default policy on *Web Filtering > Policies* and your filter profiles under *Web Filtering Profiles > Filter Profiles* may contain a list of many disabled policies. In 9.1, when you edited a profile, there was a list of *Filter Assignments* with checkboxes that were either checked or unchecked. In 9.2 there is a list of *Policies* that are either enabled or disabled. When you see disabled policies that have been migrated, these are unchecked filter assignments from 9.1.

Because policies are specific to a single filter profile, the migration puts a copy of every filter assignment into each proxy profile. This means you can delete a policy in one profile and it does not affect others. Because most Profiles don't need the migrated disabled policies you can safely delete them.

This is also true in the default filter profile shown in the *Web Filtering > Policies* tab. In 9.1 the default filter assignment is not shown in the UI, but it is there. In 9.2 it has been migrated to a Policy with the name "xxxx". Because the default Proxy Profile can now have multiple Policies, the other Filter Assignments have been migrated in as disabled Policies. Again, these can be deleted if not needed.

Why did we migrate these if we then say they can be deleted? The reason is that you may wish to consolidate or move your settings. For example, in 9.1 you may have created an additional proxy profile so that you could have multiple assignments (which was not possible in the 9.1 default profile). In 9.2 that restriction is removed and it is simpler to put everything in the default Profile. The migration has been done so that you only need to set your Profile's networks correctly and enable the migrated policies. You can then delete the additional filter profiles, simplifying your configuration.

9.1.2 Global

On the *Web Protection > Web Filtering > Global* tab you can make the global settings for the Web Filter.

To configure the Web Filter, proceed as follows:

1. **On the *Global* tab, enable the Web Filter.**
   Click the toggle switch.

   The toggle switch turns green and the *Primary Web Filter Profile* area becomes editable.

2. **Select the allowed networks.**
   Select the networks that should be allowed to use the Web Filter. By default, the Web Filter listens for client requests on TCP port `8080` and allows any client from the networks listed in the *Allowed networks* box to connect.

   Caution – It is extremely important not to select an *Any* network object, because this introduces a serious security risk and opens your appliance up to abuse from the Internet.

3. **Select Scan HTTPS (SSL) traffic options.**
   Select an option for scanning HTTPS (SSL) traffic:
   - *Do not scan*: Do not scan any HTTPS traffic.
   - *URL filtering only*: Do checks based on URL, but do not scan the actual HTTPS traffic.
   - *Decrypt and scan*: Fully decrypt and scan the contents of HTTPS traffic.

4. **Select a mode of operation.**
   Note that when you select an operation mode that requires user authentication, you need to select the users and groups that shall be allowed to use the Web Filter. The following modes of operation are available:

   - **Standard mode:** In standard mode, the Web Filter will listen for client requests on port 8080 by default and will allow any client from the networks listed in *Source networks* box to connect. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.
     Select an authentication mode:
     - **None:** Select to not use any authentication.
     - **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Definitions & Users > Authentication Services > Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

       Note – When defining the Active Directory user group, we highly recommend to add the desired entries to the *Active Directory groups* box by manually entering the plain Active Directory group or user names instead

of the LDAP strings. Example: Instead of an LDAP string `CN=ads_group1,CN=Users,DC=example,DC=com`, just enter the name `ads_group1`.

Note – When using Kerberos, only add groups to the *Active Directory groups* box, as entries for users are not be accepted by the Web Filter.

- **Agent:** Select to use the Sophos Authentication Agent (SAA). Users need to start the agent and authenticate in order to be able to use the Web Filter.
- **Apple OpenDirectory SSO:** Select when you have configured *LDAP* on the *Definitions & Users > Authentication Services > Servers* tab and you are using Apple OpenDirectory. Additionally, you have to upload a MAC OS X Single Sign-On Kerberos keyfile on the *Web Protection > Web Filtering > Advanced* tab for the proxy to work properly. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration. Note that the Safari browser does not support SSO.
- **Basic user authentication:** In this mode, each client must authenticate itself against the proxy before using it. For more information about which authentication methods are supported, see *Definitions & Users > Authentication Services*. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.
- **eDirectory SSO:** Select when you have configured *eDirectory* on the *Definitions & Users > Authentication Services > Servers* tab. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

Note – For eDirectory and Active Directory Single-Sign-On (SSO) modes, the Web Filter caches accessing IP addresses and credentials for up to fifteen minutes, for Apple OpenDirectory SSO it caches only the group information. This is done to reduce the load on the authentication servers. However it also means that changes to users, groups, or the login status of accessing users may take up to fifteen minutes to be reflected by the Web Filter.

- **Transparent mode:** In transparent mode, all connections made by client browser applications on port `80` (port `443`, respectively, if SSL is used) are

intercepted and redirected to the Web Filter without client-side configuration. The client is entirely unaware of the Web Filter server. The advantage of this mode is that no additional administration or client-side configuration is necessary, the disadvantage however is that only HTTP (port 80) requests can be processed. Thus, when you select the transparent mode, the client's proxy settings will become ineffective.

Note – In transparent mode, the Web Filter will strip NTLM authentication headers from HTTP requests. Furthermore, the Web Filter cannot handle FTP requests in this mode. If your clients want to access such services, you must open the port (`21`) in the firewall. Note further that some webservers transmit some data, in particular streaming video and audio, over a port different from port 80. These requests will not be noticed when the Web Filter operates in transparent mode. To support such traffic, you must either use a different mode or enter an explicit firewall rule allowing them.

Full transparent (optional): Select to preserve the client source IP instead of replacing it by the gateway's IP. This is useful if your clients use public IP addresses that should not be disguised by the Web Filter. The option is only meaningful and therefore only available when running in bridged mode.

Select an authentication mode:

- **None:** Select to not use any authentication.
- **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Definitions & Users > Authentication Services > Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

  Note – When defining the Active Directory user group, we highly recommend to add the desired entries to the *Active Directory groups* box by manually entering the plain Active Directory group or user names instead of the LDAP strings. Example: Instead of an LDAP string `CN=ads_group1,CN=Users,DC=example,DC=com`, just enter the name `ads_group1`.

Note – When using Kerberos, only add groups to the *Active Directory groups* box, as entries for users are not be accepted by the Web Filter.

- **Agent:** Select to use the Sophos Authentication Agent (SAA). Users need to start the agent and authenticate in order to be able to use the Web Filter.
- **Browser:** When selected the users will be presented a login dialog window in their browser to authenticate themselves at the Web Filter. This mode allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by users to be able to go on. For more information on the disclaimer, please refer to chapter *Management* > *Customization* > *Web Messages*.

You can select *Block access on authentication failure* for authentication types other than *None*.

Select *Enable Device-specific Authentication* to control authentication by device. Once enabled, you can click the plus icon to add devices and associate authentication modes for those devices.

5. **Click *Apply*.**
   Your settings will be saved.

Important Note – When SSL scanning is enabled in combination with the transparent mode, certain SSL connections are destined to fail, e.g. SSL VPN tunnels. To enable SSL VPN connections, add the respective target host to the *Transparent Mode Skiplist* (see *Web Protection* > *Filtering Options* > *Misc*).
Furthermore, to access hosts with a self-signed certificate you need to create an exception for those hosts, selecting the option *Certificate Trust Check*. The proxy will then not check their certificates.

Live Log

The Web Filtering live log gives you information on web requests. Click the *Open Live Log* button to open the Web Filtering live log in a new window.

9.1.3 Policies

Use the *Web Protection* > *Web Filtering* > *Policies* tab to create and manage web filtering policy assignments. By default, the Base Policy is listed along the bottom of the *Policies* tab. Policies will be enforced top to bottom. If no policy is triggered, the Base Policy will apply.

To create a new policy, proceed as follows:

1. **Click the Plus icon on the upper right.**
   The *Add Policy* dialog is displayed.
2. **Make the following settings:**
   Name: Enter a descriptive name for this policy.

   Users/Groups: Select the users or user groups or add new users to be assigned to the policy. How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.

   Advanced settings: If you select *Apply this policy to requests that have skipped authentication due to an exception,* it will apply this policy to items exempted from authentication on the *Filtering Options* > *Exceptions* page.

   Time event: The policy will be active for the time period you select. Choose *Always* to enable the policy at all times. Time period definitions are managed on the *Definitions & Users* > *Time Period Definitions* tab.

   Filter action: Select an existing filter action or click the Plus icon to create a new one using the Filter Action Wizard. There is a *Default content filter action* that you can edit, or you can create a new one. A filter action defines the types of web protection you want to apply in a policy. Filter actions can also be managed on the *Web Filter Profiles* > *Filter Actions* tab.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new policy appears at the top of the *Policies* list.
4. **Enable the policy.**
   The new policy is disabled by default (toggle switch is gray). Click the toggle switch to enable the policy. The policy is now enabled (toggle switch is green).

- To modify a policy, click on its name.
- To change the order in which policies are executed, move them up or down in the list by clicking the up or down arrow to the right.
- To modify a filter action, click on the filter action name to display the *Edit Filter Action* wizard or switch to the *Web Filter Profiles > Filter Actions* tab.

9.1.3.1 Filter Action Wizard

The *Add/Edit Filter Action* wizard is used to create or edit filter actions for use in your web policies. You can launch this wizard from the *Add Policy* or *Edit Policy* dialogs, or by clicking on the name of an existing filter action on the *Web Filtering > Policies* tab.

You can still manage your filter actions on the *Web Filter Profiles > Filter Actions* tab. There you can add, modify, clone or delete filter actions. But now you can create, modify, and assign filter actions by launching the *Add/Edit Filter Action* wizard on the *Web Filtering > Policies* tab.

9.1.3.2 Categories

Configure default settings for controlling access to certain kinds of websites.

Name: Enter a descriptive name for this filter action.

***Allow/Block* selection:** Decide whether your selection of website categories should be allowed or blocked. The following options are available:

- **Allow content that does not match the criteria below:** Block only the categories you have selected.
- **Block content that does not match the criteria below:** Block all categories except the ones you have selected.

The default option is *Allow*. The list of categories will indicate whether selected categories will be allowed or blocked. For cases where a website matches on more than one category, both must apply. For instance, if you allow Entertainment, but block Games, a site that is categorized as both would be allowed if the *Allow* button were selected and blocked if the *Block* button were selected.

Note – For accessing the categorization database, TCP port `6000` or TCP port `80` needs to be open in upstream firewalls. If you have a parent proxy configured, all requests to the database will be sent through the parent proxy.

Block spyware infection and communication: Selecting this option will detect and block spyware. Activating this feature will also detect and block traffic from installed spyware applications. Note that this option is only available if the first option on the page is set to *Allow*.

Note – The spyware category cannot be assigned to any of the 18 available groups, therefore protection from spyware purveyors can only be enabled by selecting the *Block spyware infection and communication* checkbox.

Categories: Set website categories to *Block*, *Allow*, or *Warn*. Website categories and their associated subcategories can be configured on the *Web Protection > Filtering Options > URL Filtering Categories* tab. If you select the *Warn* action, users browsing to a site in that category will first be presented with a warning page, but they can proceed to the site if they choose.

Uncategorized websites: You can set the default behavior of uncategorized websites to *Block Warn* or *Allow*.

Block websites with a reputation below a threshold of: Websites can be classified as either *Trusted*, *Neutral*, *Unverified*, *Suspicious*, or malicious, the latter not being listed. Unclassified websites are referred to as *Unverified*. You can select which reputation a website requires in order to be allowed access from your network. Websites below the selected threshold will be blocked. Note that this option is only available if the first option on the page is set to *Allow*. For more information on website reputations please refer to http://www.trustedsource.org.

Click *Next* to proceed to the next configuration page, *Save* to save your configuration, or *Cancel* to discard all changes and close the configuration dialog.

9.1.3.3 Websites

Block these websites: If you want to block a specific URL or website, or a subset of webpages of a specific domain, regardless of its category, define it here. This has the effect that websites defined here can be blocked even if they belong to a category you want to allow.

1. **Click the Plus icon to open the *Add whitelist/blacklist object* dialog window.**
2. **Make the following settings:**
   - **Name:** Enter a descriptive name for the regular expression object.
   - **Match URLs based on: Domains:** Enter the domains for which you want to block all or specific webpages. Note that you have to enter the entire domain name, including e.g. `www`. Webpages of the specified domains will be blocked if

one of the regular expressions defined below matches the URL. If no regular expression is given, the entire domain will be blocked.

- **Match URLs based on: Regular Expression:** Enter the regular expressions that you want to prohibit for the defined domains. If no domain is specified above, the regular expressions will be applied to all domains. Note that regular expressions do match the URL as well as search results and parts of similar URLs which may lead to unwanted blocking behavior. To limit the matching of your regular expression so specific domains, select *Perform matching on these domains only* and add domains.

  Cross Reference – For detailed information on using regular expressions for web filtering, see the Sophos Knowledgebase.

  Note – You should define the webpages as precisely as possible. Defining regular expressions without a domain may have a negative impact on performance.

- **Comment** (optional): Add a description or other information.

3. **Click *Save*.**

Allow these websites: If you want to allow a specific URL or website, or a subset of webpages of a specific domain, regardless of its category, define it here. This has the effect that websites defined here can be allow even if they belong to a category you want to block.

1. **Click the Plus icon to open the *Add Regular Expression Object* dialog window.**
2. **Make the following settings:**
   - **Name:** Enter a descriptive name for the regular expression object.
   - **Match URLs based on: Domains:** Enter the domains for which you want to block all or specific webpages. Note that you have to enter the entire domain name, including e.g. `www`. Webpages of the specified domains will be blocked if one of the regular expressions defined below matches the URL. If no regular expression is given, the entire domain will be blocked.
   - **Match URLs based on: Regular Expression:** Enter the regular expressions that you want to prohibit for the defined domains. If no domain is specified above, the regular expressions will be applied to all domains. Note that regular expressions do match the URL as well as search results and parts of similar URLs which

may lead to unwanted blocking behavior. To limit the matching of your regular expression so specific domains, select *Perform matching on these domains only* and add domains.

Cross Reference – For detailed information on using regular expressions for web filtering, see the Sophos Knowledgebase.

Note – You should define the webpages as precisely as possible. Defining regular expressions without a domain may have a negative impact on performance.

- **Comment** (optional): Add a description or other information.

3. **Click *Save*.**

9.1.3.4 Downloads

Configure which file types and MIME types are blocked or warned.

Warned File Extensions: Provide the user with a warning before downloading certain file types by adding to the*Warned file extensions* list. You can add additional file extensions or delete file extensions that are not to be warned. To add a file extension, click the Plus icon in the *Warned file extensions* box and enter the file extension you want to warn, for example `exe` (without a leading dot).

Blocked File Extensions: Filter certain files from web traffic using file extensions in the *Blocked file extensions* list. You can add additional file extensions or delete file extensions that are not to be blocked. To add a file extension, click the Plus icon in the *Blocked file extensions* box and enter the file extension you want to block, for example `exe` (without a leading dot).

Note – Files within archives (e.g. `zip` files) will not be scanned for blocked file types, blocked extensions or blocked MIME types. To protect your network from these within archived files, consider blocking archive file types such as zip, rar, etc.

Warned MIME Types: Filter files from web traffic using MIME types listed in the *Warned MIME types* list. To add a MIME type, click the Plus icon in the *Warned MIME types* box and enter the MIME type. You can use wildcards (*) in the *Warned MIME types* list, such as `audio/*`.

Blocked MIME Types: Filter files from web traffic using MIME types listed in the *Blocked MIME types* list. To add a MIME type, click the Plus icon in the *Blocked MIME types* box and

enter the MIME type. You can use wildcards (*) in the *Blocked MIME types* list, such as `audio/*`.

Block downloads larger than: Specify this option to prevent users from downloading files that exceed the specified size (in MB).

Click *Next* to proceed to the next configuration page, *Save* to save your configuration, or *Cancel* to discard all changes and close the configuration dialog.

9.1.3.5 Antivirus

Antivirus

Use Antivirus scanning: Select the option to have inbound and outbound web traffic scanned for viruses. Sophos UTM features several antivirus engines:

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings* > *Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.
- **Block potentially unwanted applications (PUAs):** PUAs are programs that are not malicious, but may be unsuitable for a business environment. This feature is only available when using the Sophos anti-virus engine. To allow specific PUAs if you enable blocking, add exceptions on *Web Filtering* > *Filtering Options* > *PUAs*.

Do not scan files larger than: Specify the maximum size of files to be scanned by the anti-virus engine(s). Files exceeding this size will be exempt from scanning.

Tip – If you want to prevent files larger than the maximum scanning size from being downloaded, set the *Block downloads larger than* value on the *Downloads* page.

Active Content Removal

In the *Active Content Removal* area you can configure the automatic removal of specific web content such as embedded objects in webpages. You can configure the following settings:

- **Disable JavaScript:** This feature will disable all `<SCRIPT>` tags in HTML pages, resulting in the deactivation of functions that are embedded in or included from HTML pages.

- **Remove embedded objects (ActiveX/Java/Flash):** This feature will remove all `<OBJECT>` tags from HTML pages, stripping off dynamic content including ActiveX, Flash, or Java from incoming HTTP traffic.

Click *Next* to proceed to the next configuration page, *Save* to save your configuration, or *Cancel* to discard all changes and close the configuration dialog.

9.1.3.6 Additional Options

Enforce Website Protection Features

SafeSearch: Certain search providers have a SafeSearch feature that is designed to remove adult content from search results. You can enforce the use of SafeSearch for Google, Bing or Yahoo. When enabled, a provider's SafeSearch will be enforced, and cannot be turned off or bypassed by Web Filter users. To configure this feature, select the provider whose SafeSearch you want to enforce.

YouTube for Schools: If enabled, users trying to open a YouTube video are restricted to YouTube videos either belonging to the sub-section YouTube EDU or uploaded by your school account. To make this work, you have to sign up at the YouTube for Schools program to get a School ID which you need to enter below.

Note – On the Sophos UTM, you have to make sure that the top-level domains `youtube.com` and `ytimg.com` as well as videos in general are not blocked. If you have enabled *YouTube for Schools*, you need to enter the School ID or code supplied by YouTube.

Enforce allowed domains for Google Apps: Google Apps can block users from accessing certain services unless their Google account is a member of the Google Apps domain. Turning this on enforces this feature, and cannot be turned off or bypassed by Web Filter users. To configure this feature, select *Enforce allowed domains for Google Apps*. Then, at the top of the *Domains* box, click the Plus icon or the Action icon to add or import Google Apps domains.

Activity Logging

You can select which activities will be logged:

- **Log accessed pages:** This feature will log information about all pages that have been accessed through the UTM.
- **Log blocked pages:** This feature will log information about pages that have been blocked from being accessed.

Network Configuration

You can configure parent proxies, both globally and profile-based (see *Web Protection > Filtering Options > Parent Proxies*).

Note – With parent proxies enabled, HTTPS requests are *not* possible in Transparent mode when SSL scanning is enabled.

To configure a parent proxy, do the following:

1. **Click the Plus icon at the top of the parent proxies list.**
   The *Add Parent Proxy* dialog box opens.
2. **Make the following settings:**

   Name: Enter a descriptive name for the parent proxy.

   Comment (optional): Add a description or other information.

   Use proxy for these hosts: Add hosts to this box for which the parent proxy is to be used, e.g. `*.wikipedia.org`. Note that you can use pattern matching here. Regular expressions, however, are not allowed. If you leave the box empty, an asterisk (*) is automatically added when clicking *Save*, which matches all hosts. Such a proxy definition can therefore be regarded as a fallback proxy which matches when none of the other proxies, if existent, do.

   Parent proxy: Select or add the network definition of the parent proxy.

   Port: The default port for the connection to the parent proxy is 8080. If your parent proxy requires a different port, you can change it here.

   Proxy requires authentication: If the parent proxy requires authentication, select the checkbox and enter username and password in the appearing textboxes.
3. **Click *Save*.**
   The new parent proxy appears in the *Parent Proxies* list and on the *Web Protection > Filtering Options > Parent Proxies* page.

To edit or delete a parent proxy, click the name of the proxy.

Click *Save* to save your configuration, or *Cancel* to discard all changes and close the configuration dialog.

9.2 Web Filter Profiles

Sophos UTM features a Web Filter designed and optimized for controlling what web content is available on a particular network. It thus prevents persons from viewing content which you may consider objectionable. You can configure the Web Filter to apply globally to selected networks. Alternatively, you can create individual Web Filter Profiles that can be used to enforce various security policies to be applied to different segments of your network. That way you can define different content filtering policies for the various departments within your organization, even with varying user authentication methods.

9.2.1 Filter Profiles

Filter profiles can be used to create various content filtering policies, enabling you to apply different policies to different addresses of your network, so that you can define different policies for various departments within your organization. In addition, each filter profile can have its own user authentication method.

To create a filter profile, proceed as follows:

1. **Click the Plus icon on the upper right.**
   The *Add Profile* wizard opens.
2. **Enter a *Name* and *Comment*.**
3. **Select the allowed networks.**
   Select the networks that should be allowed to use the Web Filter. By default, the Web Filter listens for client requests on TCP port `8080` and allows any client from the networks listed in the *Allowed networks* box to connect.
4. **Select the allowed endpoint groups.**
   If Endpoint Web Control is enabled, select the endpoint groups that should be allowed to use the Web Filter.
5. **HTTPS (SSL) traffic:**

   Choose from the following options for scanning SSL traffic:

   - **Do not scan:** This option is only available in transparent mode. When selected, HTTPS traffic does not go through the proxy and does not get scanned.

- **URL filtering only:** This option performs URL category and reputation checks, but does not scan the contents of HTTPS traffic.
- **Decrypt and scan:** Chose this option to decrypt and perform full checks on HTTPS traffic.

6. **Select a mode of operation.**
   Note that when you select an operation mode that requires user authentication, you need to select the users and groups that shall be allowed to use the Web Filter. The following modes of operation are available:

   - **Standard mode:** In standard mode, the Web Filter will listen for client requests on port 8080 by default and will allow any client from the networks listed in *Source networks* box to connect. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.
     Select the default authentication mode.

     - **None:** Select to not use any authentication.
     - **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Definitions & Users > Authentication Services > Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

       Note – When defining the Active Directory user group, we highly recommend to add the desired entries to the *Active Directory groups* box by manually entering the plain Active Directory group or user names instead of the LDAP strings. Example: Instead of an LDAP string `CN=ads_group1,CN=Users,DC=example,DC=com`, just enter the name `ads_group1`.

       Note – When using Kerberos, only add groups to the *Active Directory groups* box, as entries for users are not be accepted by the Web Filter.

     - **Agent:** Select to use the Sophos Authentication Agent (SAA). Users need to start the agent and authenticate in order to be able to use the Web Filter.
     - **Apple OpenDirectory SSO:** Select when you have configured *LDAP* on the *Definitions & Users > Authentication Services > Servers* tab and you are

using Apple OpenDirectory. Additionally, you have to upload a MAC OS X Single Sign-On Kerberos keyfile on the *Web Protection* > *Filtering Options* > *Misc* tab for the proxy to work properly. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration. Note that the Safari browser does not support SSO.

- **Basic user authentication:** In this mode, each client must authenticate itself against the proxy before using it. For more information about which authentication methods are supported, see *Definitions & Users* > *Authentication Services*. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.
- **Browser:** When selected the users will be presented a login dialog window in their browser to authenticate themselves at the Web Filter. This mode allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by users to be able to go on. For more information on the disclaimer, please refer to chapter *Management* > *Customization* > *Web Messages*.
- **eDirectory SSO:** Select when you have configured *eDirectory* on the *Definitions & Users* > *Authentication Services* > *Servers* tab. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

Note – For eDirectory and Active Directory Single-Sign-On (SSO) modes, the Web Filter caches accessing IP addresses and credentials for up to fifteen minutes, for Apple OpenDirectory SSO it caches only the group information. This is done to reduce the load on the authentication servers. However it also means that changes to users, groups, or the login status of accessing users may take up to fifteen minutes to be reflected by the Web Filter.

If you chose an authentication mode that requires user authentication, select **Block access on authentication failure** to deny access to users that fail authentication.

- **Transparent mode:** In transparent mode, all connections made by client browser applications on port `80` (port `443`, respectively, if SSL is used) are intercepted and redirected to the Web Filter without client-side configuration. The client is entirely unaware of the Web Filter server. The advantage of this mode is that no

additional administration or client-side configuration is necessary, the disadvantage however is that only HTTP (port 80) requests can be processed. Thus, when you select the transparent mode, the client's proxy settings will become ineffective.

Note – In transparent mode, the Web Filter will strip NTLM authentication headers from HTTP requests. Furthermore, the Web Filter cannot handle FTP requests in this mode. If your clients want to access such services, you must open the port (`21`) in the firewall. Note further that some webservers transmit some data, in particular streaming video and audio, over a port different from port 80. These requests will not be noticed when the Web Filter operates in transparent mode. To support such traffic, you must either use a different mode or enter an explicit firewall rule allowing them.

- **None:** Select to not use any authentication.
- **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Definitions & Users* > *Authentication Services* > *Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

  Note – When defining the Active Directory user group, we highly recommend to add the desired entries to the *Active Directory groups* box by manually entering the plain Active Directory group or user names instead of the LDAP strings. Example: Instead of an LDAP string `CN=ads_group1,CN=Users,DC=example,DC=com`, just enter the name `ads_group1`.

  Note – When using Kerberos, only add groups to the *Active Directory groups* box, as entries for users are not be accepted by the Web Filter.

- **Agent:** Select to use the Sophos Authentication Agent (SAA). Users need to start the agent and authenticate in order to be able to use the Web Filter.
- **Browser:** When selected the users will be presented a login dialog window in their browser to authenticate themselves at the Web Filter. This mode

allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by users to be able to go on. For more information on the disclaimer, please refer to chapter *Management > Customization >* Web Messages.

- **Full transparent** (optional): Select to preserve the client source IP instead of replacing it by the gateway's IP. This is useful if your clients use public IP addresses that should not be disguised by the Web Filter. The option is only meaningful and therefore only available when running in bridged mode.

  Select the default authentication mode:

  - **None:** Select to not use any authentication.
  - **Active Directory SSO:** Select when you have configured *Active Directory Single Sign-On* (SSO) on the *Definitions & Users > Authentication Services > Servers* tab. This has the effect that NTLM user authentication will be used to authenticate clients. Note that this is only guaranteed to work with Internet Explorer. When used in this mode, clients must have specified the Web Filter as HTTP proxy in their browser configuration.

    Note – When defining the Active Directory user group, we highly recommend to add the desired entries to the *Active Directory groups* box by manually entering the plain Active Directory group or user names instead of the LDAP strings. Example: Instead of an LDAP string `CN=ads_group1,CN=Users,DC=example,DC=com`, just enter the name `ads_group1`.

    Note – When using Kerberos, only add groups to the *Active Directory groups* box, as entries for users are not be accepted by the Web Filter.

  - **Agent:** Select to use the Sophos Authentication Agent (SAA). Users need to start the agent and authenticate in order to be able to use the Web Filter.
  - **Browser:** When selected the users will be presented a login dialog window in their browser to authenticate themselves at the Web Filter. This mode allows for username-based tracking, reporting, and surfing without client-side browser configuration. Moreover, you can enable a disclaimer that is additionally displayed on that dialog window and needs to be accepted by

users to be able to go on. For more information on the disclaimer, please refer to chapter *Management* > *Customization* > *Web Messages*.

7. **Enable Device-specific Authentication.**
   To configure authentication modes for specific devices, select the *Enable Device-specific Authentication* checkbox. Once enabled you can click the green Plus icon to add device types and associated authentication modes.

8. **Click *Next*, or select *Policies* from the top of the wizard.**

9. **Review and create policies for your filter profile.**
   To create a new policy, proceed as follows:
   1. **Click the Plus icon on the upper right.**
      The *Add Policy* dialog is displayed.

   2. **Make the following settings:**
      Name: Enter a descriptive name for this policy.

      Users/Groups: Select the users or user groups or add new users to be assigned to the policy. How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.

      Advanced settings: If you select *Apply this policy to requests that have skipped authentication due to an exception,* it will apply this policy to items exempted from authentication on the *Filtering Options* > *Exceptions* page.

      Time event: The policy will be active for the time period you select. Choose *Always* to enable the policy at all times. Time period definitions are managed on the *Definitions & Users* > *Time Period Definitions* tab.

      Filter action: Select an existing filter action or click the Plus icon to create a new one using the Filter Action Wizard. There is a *Default content filter action* that you can edit, or you can create a new one. A filter action defines the types of web protection you want to apply in a policy. Filter actions can also be managed on the *Web Filter Profiles* > *Filter Actions* tab.

      Comment (optional): Add a description or other information.

   3. **Click *Save*.**
      The new policy appears at the top of the *Policies* list.

   4. **Enable the policy.**
      The new policy is disabled by default (toggle switch is gray). Click the toggle switch to enable the policy. The policy is now enabled (toggle switch is green).

10. **Click *Save*.**
    The new profile appears on the *Filter Profiles* list.

Important Note – When SSL scanning is enabled in combination with the transparent mode, certain SSL connections are destined to fail, e.g. SSL VPN tunnels. To enable SSL VPN connections, add the respective target host to the *Transparent Mode Skiplist* (see *Web Protection* > *Filtering Options* > *Misc*).
Furthermore, to access hosts with a self-signed certificate you need to create an exception for those hosts, selecting the option *Certificate Trust Check*. The proxy will then not check their certificates.

To either edit or delete a filter profile, click the name of the profile in the list.

9.2.2 Filter Actions

On the *Web Filter Profiles* > *Filter Actions* tab you can create and edit a set of web protection configuration settings that can be used to customize different types and levels of protection. Filter actions can be assigned to different users and user groups, providing a flexible way to control web access.

You can create a new filter action by clicking the *New filter action* button, or edit an existing filter action by clicking the corresponding *Edit* button. Either of these actions will launch the Filter Action Wizard. For more information, see *Web Protection* > *Policies* > *Filter Action Wizard*.

On the *Web Protection* > *Web Filter Profiles* > *Filter Actions* page you can also search, clone, delete or browse the list of existing filter actions.

9.2.3 Parent Proxies

Some network topologies require an upstream web proxy server. On the *Web Protection* > *Web Filter Profiles* > *Parent Proxies* page you can configure a parent proxy.

To configure a parent proxy, do the following:

1. **Click *New Parent Proxy*.**
   The *Create New Parent Proxy* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this parent proxy.

Comment (optional): Add a description or other information.

Use proxy for these hosts: Add hosts to this box for which the parent proxy is to be used, e.g. `*.wikipedia.org`. Note that you can use pattern matching here. Regular expressions, however, are not allowed. If you leave the box empty, an asterisk (*) is automatically added when clicking *Save*, which matches all hosts. Such a proxy definition can therefore be regarded as a fallback proxy which matches when none of the other proxies, if existent, do.

Parent proxy: Select or add the network definition of the parent proxy.

Port: The default port for the connection to the parent proxy is 8080. If your parent proxy requires a different port, you can change it here.

Proxy requires authentication: If the parent proxy requires authentication, select the checkbox and enter username and password in the appearing textboxes.

3. **Click *Save*.**
   The new parent proxy appears on the *Parent Proxies* list.

The proxy can now be used in filter actions or globally.

To either edit or delete a parent proxy, click the corresponding buttons.

9.3 Filtering Options

On the *Web Protection* > *Filtering Options* page you can configure various options to web filtering. The tabs accessible from this page allow you to configure exceptions to filtering, users that can bypass filtering, filtering categories, HTTPS certificates and authorities, and various other options.

9.3.1 Exceptions

On the *Web Protection* > *Filtering Options* > *Exceptions* tab you can define whitelist client networks, users/groups, and domains. All entries contained in these lists can be excluded from certain web protection services.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this exception.

   Comment (optional): Add a description or other information.

   Skip These Checks: Select the security checks that should be skipped:

   - **Authentication:** If the Web Filter runs in *Authentication* mode, you can skip authentication for the source hosts/networks or target domains.
   - **Caching:** Select to disable caching for specific domains or source hosts/networks.
   - **Block by download size:** Select to disable blocking content according to the size of the download.
   - **Antivirus:** Select to disable virus scanning, which checks messages for unwanted content such as viruses, trojan horses and the like.
   - **Extension blocking:** Select to disable the file extension filter, which can be used to block content that contains certain types of files based on their extensions.
   - **MIME type blocking:** Select to disable the MIME type filter, which can be used to block content that has a certain MIME type.
   - **URL filter:** Select to disable the URL filter, which controls the access to certain kinds of websites.
   - **Content removal:** Select to bypass the removal of special content in webpages such as embedded objects (e.g., multimedia files) or JavaScript.
   - **SSL scanning:** Select to skip SSL scanning for the webpage in request. This is useful with online banking websites or with websites that do not play well with SSL interception. Note that for technical reasons this option does not work for any transparent Web Filter mode. With transparent mode, use the *Transparent Mode Skiplist* instead (see *Filtering Options > Misc* tab). In standard mode, exceptions can only be made based on the destination host or IP address depending on what the client sends. With exceptions based on categories, instead of the whole URL, only the hostname will be classified.
   - **Certificate trust check:** Select to skip the trust check of the HTTPS server certificate. Note that, when the Web Filter works in transparent mode with authentication, skipping the certificate trust check based on a users/groups match (*For all requests Coming from these users/groups*) is technically impossible.

- **Certificate date check:** Select to skip the check of whether the HTTPS certificate's date is valid.

The following two options are useful if there are persons or members of e.g. a works council whose activities must not be logged at all:

- **Accessed pages:** Select to not log pages that have been accessed. Those page requests will also be excluded from reporting.
- **Blocked pages:** Select to not log pages that have been blocked. Those page requests will also be excluded from reporting.

For all requests: Select at least one condition for which the security checks are to be skipped. You can logically combine several conditions by selecting either *And* or *Or* from the drop-down list in front of a condition. The following conditions can be set:

- **Coming from these source networks:** Select to add source hosts/networks that should be exempt from the security checks of this exception rule. Enter the respective hosts or networks in the *Hosts/Networks* box that opens after selecting the condition.
- **Coming from these source endpoint groups:** Select to add computer groups (see *Endpoint Protection* > *Computer Management* > *Manage Groups* tab) that should be exempt from the security checks of this exception rule. Enter the respective groups in the *Source Endpoint Groups* box that opens after selecting the condition.
- **Matching these URLs:** Select to add target domains that should be exempt from the security checks of this exception rule. Add the respective domains to the *Target Domains* box that opens after selecting the condition. Regular expressions are allowed here. Example: `^https?://[^.]*\.domain.com` matches HTTP (S) connections to all subdomains of the domain.

Cross Reference – For detailed information on using regular expressions for web filtering, see the Sophos Knowledgebase.

Note – When using *Transparent* mode with SSL scanning enabled, you need to enter the target domain(s) as IP addresses. Otherwise the exception will fail for technical reasons.

- **Coming from these users/groups:** Select to add users or user groups that should be exempt from the security checks of this exception rule. Enter the respective users or groups in the *Users/Groups* box that opens after selecting the condition. Also, in Standard mode, matching for certain users/groups does not work due to the missing authentication.
- **Going to these categories of websites:** Select to skip security checks for certain categories. Select then the categories from the list that opens after selecting the condition.

3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

9.3.2 Websites

On the *Web Protection* > *Filtering Options* > *Websites* tab you can maintain lists of sites for which you want to override the default category or reputation.

To add an entry to the *Local Site List*:

1. **Click the *Add Site* button.**
2. **Enter the sites you wish to override.**
   The text box in the *Add Local Site(s)* dialog will accept URLs, domains, IP addresses, or CIDR ranges.
3. **Optionally, select the *Include subdomains* checkbox.**
   Selecting this checkbox will apply the overrides to all subdomains. For instance, if you add example.com and select the *Include subdomains* checkbox, mail.example.com will be included in the override.
4. **Select a *Category* or *Reputation* to override.**
   You can override either *Category*, *Reputation*, or both. Sites defined in the *Local Site List* are processed by filter actions using these overridden values.
5. **Add an optional comment.**

For large lists of sites you can page through entries by using the *Next* and *Previous* icons at the top of the tab, or search for items using the search text box. To delete entries click the *Delete* icon next to the entry, or select multiple items and click the *Delete* icon at the top of the list.

9.3.3 Bypass Users

On the *Web Protection* > *Filtering Options* > *Bypass Users* tab you can specify which users are allowed to bypass block pages..

To add an existing group or user:

1. **Click the Folder icon next to *Users/Groups allowed to bypass blocking*.**
   The list of existing users and groups appears in the left navigation pane.
2. **Select and drag the user or group to the *Users/Groups allowed to bypass blocking* box.**
   The item will now be listed on the *Bypass Users* tab.

To add a new user:

1. **Click the green Plus icon next to *Users/Groups allowed to bypass blocking*.**
   The *Add user* dialog appears.
2. **Enter user information into the *Add User* dialog**.
   How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.
3. **Click *Apply*.**
   Your settings will be saved.

9.3.4 Potentially Unwanted Applications

On the *Web Protection* > *Filtering Options* > *PUAs* tab you can maintain lists of authorized Potentially Unwanted Applications (PUAs). Your UTM can identify applications that are potentially unwanted in a business environment and block them. To allow specific PUAs when blocking is enabled, add the name as reported in the block page or the logs.

To add an entry to the *Local Site List*:

1. **Click the *Plus icon* on the Authorized PUAs list.**
2. **Enter the PUA definition.**
   To find PUA definitions, go to Logging & *Reporting* > *Web Protection* > *Web Usage Report* and select *PUA Downloaders* from the *Available Reports* drop-down.
3. **Click *Apply*.**

By clicking the *Open Actions menu* icon, next to the green *Plus icon*, you can import or export a text list of PUAs and clear the *Authorized PUAs* list.

9.3.5 Categories

On the *Web Protection* > *Filtering Options* > *Categories* tab you can customize the mapping of website categories to category groups, which can be selected on the *Filter Action* tab or on the *Website Filtering* page. Sophos UTM can identify and block access to 60 different categories of websites. Sophisticated URL classification methods ensure accuracy and completeness in identifying questionable websites. If a user requests a webpage that is not included in the database, the URL is sent to the web crawlers and classified automatically.

Note – If you are of the opinion that a website is wrongly categorized, you can use the following URL report form to suggest new categories.

To assign website categories to a category group, proceed as follows:

1. **Click *Edit* in the category group you want to edit.**
   The *Edit Filter Category* dialog box opens.
2. **Select the subcategories.**
   Select or clear the checkboxes of the subcategories you want to add to or remove from the group.
3. **Click *Save*.**
   The group will be updated with your settings.

Alternatively, you can also create a new filter category. Proceed as follows:

1. **Click the *New Filter Category* button on the top of the page.**
   The *Create Filter Category* dialog box opens.
2. **Enter a name.**
   Enter a descriptive name for the new filter category.
3. **Select the subcategories.**
   Select the checkboxes of the subcategories you want to add to the group.
4. **Click *Save*.**
   The group will be updated with your settings.

To either edit or delete a category, click the corresponding buttons.

9.3.6 HTTPS CAs

On the *Web Protection* > *Web Filtering* > *HTTPS CAs* tab you can manage Signing and Verification Certificate Authorities (CAs) for HTTPS connections.

Signing CA

In this area you can upload your Signing CA certificate, regenerate the Signing CA certificate, or download the existing Signing CA certificate. By default, the Signing CA certificate is created according to the information provided during setup, i.e. it is consistent with the information on the *Management* > *System Settings* > *Organizational* tab—unless there have been any changes applied since.

To upload a new Signing CA certificate, proceed as follows:

1. **Click the button *Upload*.**
   The *Upload PKCS#12 Certificate File* dialog window opens.
2. **Browse for the certificate to upload.**
   Click the Folder icon next to the *File* box, click *Browse* in the opening *Upload File* dialog window, select the certificate to upload and click *Start Upload*.

   You can only upload certificates in PKCS#12 format which are password protected.
3. **Enter the password.**
   Enter the password twice into the corresponding fields and click *Save*.

   The new Signing CA certificate will be installed.

To regenerate your Signing CA certificate, proceed as follows:

1. **Click the button *Regenerate*.**
   The *Create New Signing CA* dialog box opens.
2. **Change the information.**
   Change the given information according to your needs and click *Save*.

   The new Signing CA certificate will be generated. The Signing CA information in the *Signing CA* area will change accordingly.

To download the Signing CA certificate, proceed as follows:

1. **Click the button *Download*.**
   The *Download Certificate File* dialog window opens.

2. **Select the file format to download.**
   You can choose between two different formats:
   - **PKCS#12:** This format will be encrypted, so enter an export password.
   - **PEM:** Unencrypted format.
3. **Click *Download*.**
   The file will be downloaded.

If you use certificates for your internal webservers signed by a custom CA, it is advisable to upload this CA certificate to WebAdmin as Trusted Certificate Authority. Otherwise users will be prompted with an error message by the Web Filter claiming to be confronted with an untrustworthy server certificate.
To facilitate supplying client PCs with the proxy CA certificate, users can download the certificate themselves via http://passthrough.fw-notify.net/cacert.pem and install it in their browser. The website request is directly accepted and processed by the proxy. It is therefore necessary to enable the Web Filter on the *Web Filtering* > *Global* tab first.

Note – In case the proxy's operation mode is not *Transparent Mode* the proxy has to be enabled in the user's browser. Otherwise the certificate download link will not be accessible.

Alternatively, if the User Portal is enabled, users can download the proxy CA certificate from the User Portal, tab *HTTPS Proxy*.

Preventing HTTPS Problems

When using HTTPS, Windows system programs like Windows Update and Windows Defender will not be able to establish connections because they are run with `system user` rights. However, this user, by default, does not trust the proxy CA. It is therefore necessary to import the HTTPS proxy CA certificate for the system user. Do the following:

1. **In Windows, open the *Microsoft Management Console* (`mmc`).**
2. **Click on the *File* menu and then *Add/Remove Snap-in*.**
   The *Add or Remove Snap-ins* dialog window opens.
3. **Click *Add* at the bottom of the window.**
   The dialog window *Add Standalone Snap-In* opens.
4. **Select *Certificates* from the list and click *Add*.**
   A wizard appears.

5. **Select *Computer account* and click *Next*.**
6. **Make sure that *Local computer* is selected and click *Finish* and then *Close*.**
   The first dialog window now contains the item *Certificates (Local Computer)*.
7. **Click *OK*.**
   The dialog window closes and the Console Root now contains the item *Certificates (Local Computer)*.
8. **In the *Console Root* window on the left open *Certificates > Trusted Root Certification Authorities*, right-click *Certificates* and select *All Tasks > Import* from the context menu.**
   The import dialog wizard opens.
9. **Click *Next*.**
   The next wizard step is displayed.
10. **Browse to the previously downloaded HTTPS proxy CA certificate, click *Open* and then *Next*.**
    The next wizard step is displayed.
11. **Make sure that *Place all certificates in the following store* is selected and click *Next* and *Close*.**
    The wizard reports the import success.
12. **Confirm the wizard's message.**
    The proxy CA certificate is now displayed among the trusted certificates.
13. **Save the changes.**
    Click on the *File* menu and then *Save* to save the changes on the Console Root.

After importing, the CA is system-widely accepted and connection problems resulting from the HTTPS proxy should not occur.

Verification CAs

This area allows you to manage Verifications CAs. Those are Certificate Authorities you trust in the first place, i.e. websites presenting valid certificates signed by these CAs are regarded trustworthy by the HTTPS proxy.

Local Verification CAs: You can upload Verification CAs additionally to the CA list below. Proceed as follows:

1. **Click the Folder icon next to the *Upload local CA* field.**
   The *Upload File* dialog window opens.

2. **Select the certificate to upload.**
   Click *Browse* and select the CA certificate to upload. Only PEM certificate extensions are supported:
3. **Upload the certificate.**
   Click *Start Upload* to upload the selected CA certificate.

   The certificate will be installed and displayed in the *Local Verification CAs* area.

Global Verification CAs: The list of Verification CAs shown here is identical to the Verification CAs pre-installed by Mozilla Firefox. However, you can disable one or all Verification CAs of the list if you do not regard them as trustworthy. To revoke a CA's certificate click its toggle switch. The toggle switch turns gray and the HTTPS proxy will no longer accept websites signed by this CA.

Tip – Click the blue Info icon to see the fingerprint of a CA.

The HTTPS proxy will present a "Blocked Content" error page to a client if the CA is unknown or disabled. However, you can create an exception for such pages: either via the *Create Exception* link on the error page of the Web Filter or via the *Web Protection > Web Filtering > Exceptions* tab.

Note – When clicking the *Create Exception* link on the Web Filter error page a login dialog window is presented. Only users with admin rights are allowed to create exceptions.

9.3.7 Misc

The *Web Protection > Filtering Options > Misc* tab contains various other configuration options of the Web Filter such as caching, streaming, or port settings.

Misc Settings

Web filtering port: Here you can define the port number that the Web Filter will use for client requests. The default is `8080`.

Note – This only applies if you do not operate the proxy in transparent mode.

MIME blocking inspects HTTP body: Not only the HTTP header but also the HTTP body is checked for blocked MIME types. Note that turning on this feature may have a negative impact on performance.

Block unscannable and encrypted files: Select this option to block files that could not be scanned. The reason for that may be, among other things, that files are encrypted or corrupt.

Allowed target services: In the *Allowed target services* box you can select the target services the Web Filter should be allowed to access. The default setting consists of target services (ports) that are usually safe to connect to and which are typically used by browsers, namely *HTTP* (port `80`), *HTTPS* (port `443`), *FTP* (port `21`), *LDAP* (port `389`), *LDAP-SSL* (port `636`), *Web Filter* (port `8080`), *UTM Spam Release* (ports `3840-4840`), and *UTM WebAdmin* (port `4444`).

Default charset: This option affects how the proxy displays file names in the *Download Manager* window. URLs (and file names that they may reference) that are encoded in foreign charsets will be converted to UTF-8 from the charset specified here unless the server sends a different charset. If you are in a country or region that uses a double-byte charset, you should set this option to the "native" charset for that country or region.

Search domain: You can add an additional domain here, which will be searched when the first DNS lookup returns no result ("NXDOMAIN"). Then, a second DNS request is initiated which appends the domain given here to the original hostname. Example: A user enters `http://wiki`, meaning to address *wiki.intranet.example.com*. However, the URL can only be resolved when you enter `intranet.example.com` into the *Search domain* field.

Authentication timeout: This setting allows you to set the length of time (in seconds) that a user can browse after logging in with browser mode authentication. If the user has a logout tab open, the user can continue to browse without re-authenticating until that tab is closed, plus the authentication timeout.

This setting also allows you to set the length of time (in seconds) that a *Block Override* or a *Warning Proceed* lasts.

Authentication realm: The authentication realm is the name of the source which a browser displays along with the authentication request when the proxy works in *Basic User Authentication* mode. It defines the protection space according to RFC 2617. You can give any string here.

Transparent Mode Skiplist

Using this option is only meaningful if the Web Filter runs in transparent mode. Hosts and networks listed in the *Skip transparent mode hosts/nets* boxes will not be subject to the transparent interception of HTTP traffic. There is one box for source and one for destination hosts/networks. To allow HTTP traffic (without proxy) for these hosts and networks, select the *Allow HTTP/S traffic for listed hosts/nets* checkbox. If you do not select this checkbox, you must define specific firewall rules for the hosts and networks listed here.

Proxy Auto Configuration

The proxy auto configuration is a feature that enables you to centrally provide a proxy auto configuration file (PAC file) which can be fetched by browsers. The browsers will in turn configure their proxy settings according to the details outlined in the PAC file.

The PAC file is named *wpad.dat*, has the MIME type `application/x-ns-proxy-autoconfig` and will be provided by the UTM. It contains the information you enter into the text box, for example:

```
function FindProxyForURL(url, host)
 { return "PROXY proxy.example.com:8080; DIRECT"; }
```

The function above instructs the browser to redirect all page requests to the proxy of the server `proxy.example.com` on port `8080`. If the proxy is not reachable, a direct connection to the Internet will be established.

The hostname can also be written as a variable called `${asg_hostname}`. This is especially useful when you want to deploy the same PAC file to several Sophos UTM appliances using Sophos UTM Manager. The variable will then be instantiated with the hostname of the respective UTM. Using the variable in the example above would look like the following:

```
function FindProxyForURL(url, host)
 { return "PROXY ${asg_hostname}:8080; DIRECT"; }
```

To provide the PAC file for your network, you have the following possibilities:

- Providing via browser configuration: If you select the option *Enable Proxy Auto Configuration*, the PAC file will be available via the UTM Web Filter under the URL of the following type: `http://IP-of-UTM:8080/wpad.dat`. To use this file, enter its URL in the automatic proxy configuration setting of those browsers which are to use the proxy.
- Providing via DHCP: You can have your DHCP server(s) hand out the URL of the PAC file together with the client IP address. To do that, select the option *Enable HTTP Proxy*

Auto Configuration in your DHCP server configuration (see chapter *Network Services* > *DHCP*). A browser will then automatically fetch the PAC file and configure its settings accordingly.

Note – Providing via DHCP works with Microsoft's Internet Explorer only. Regarding all other browsers you need to provide the PAC file manually.

URL Categorization Parent Proxy

Enter a proxy server for URL categorization lookups if you do not have direct internet access. This option is only available if you have endpoint protection enabled, or if you are doing local lookups. For local lookups, this option sets the proxy that will be used to download categorization updates to the UTM.

Web Caching

Enable caching: When this option is enabled, the Web Filter keeps an on-disk object cache to speed up requests to frequently visited webpages.

- **Cache SSL content:** With this option enabled, SSL-encrypted data will be stored unencrypted on disk as well.
- **Cache content that contains cookies:** Cookies are often used for authentication purposes. With this option enabled, HTTP answers containing cookies will be cached as well. This may be critical, as users requesting the same page are likely to get the cached page, containing the cookie of another user.

  Important Note – Caching SSL and/or cookie content is an important security issue as the content is readable by every user with SuperAdmin rights.

- **Force caching for Sophos Endpoint updates:** If enabled, certain data related to Sophos Auto Update (SAU) requests from endpoints will be cached. We recommend to enable this feature when using endpoint protection. If disabled, this type of data will not be cached. This can lead to uplink saturation when many endpoints simultaneously try to download data from the update servers in the Internet.

Clear Cache: You can delete all cached pages by clicking *Clear Cache*.

Streaming Settings

Bypass content scanning for streaming content: When this option is active, typical audio and video streaming content is not subject to content scanning. Disabling this option will

effectively disable most media streams, since they cannot be scanned in a reasonable time-frame. It is therefore recommended to leave this option turned on.

Apple OpenDirectory Single Sign-On

When you are using *Apple OpenDirectory SSO* as authentication method, you need to upload a MAC OS X Single Sign-On Kerberos keyfile for authentication to work properly. Generate that keyfile and upload it by clicking the Folder icon. For more information on how to generate that keyfile please refer to the Kerberos documentation.

Certificate for End-User Pages

The UTM uses HTTPS to provide user notification, perform browser authentication and secure other user interactions. By default, the UTM uses an automatically generated certificate for these HTTPS connections. You can use this option to use a custom certificate for HTTPS pages that are presented to the end user. To use your own custom certificate for these HTTPS connections, first upload it using *Remote Access* > *Certificate Management* > *Certificates*, then select it and update the settings here.

Note –The *Hostname:* specified is the base domain for the certificate you are using. The UTM will then prepend *passthrough.* or *passthrough6.* to that domain. The certificate must be valid for *passthrough* (and *passthough6*) as a Common Name, Subject Alternate Name, or most commonly as a wildcard certificate, so you can prepend any host at the domain. In addition, you must set up DNS for *passthrough* and *passthrough6* to specific IP addresses. If you use the UTM as your DNS server this is done automatically. If you are using an alternate DNS server you must create those entries there.

9.4 Policy Test

Use the *Web Protection* > *Policy Test* page to test URLs against your existing *Web Filter Profiles*. To test a URL against your current policy, proceed as follows:

1. **Enter the URL you want to test.**
2. **Set the source IP address.**
   Different source networks may have different *Web Filter Profiles*.
3. **Optionally, enter a user to test the request as.**
   Users can fall under different *Web Filter Profiles*.

4. **Optionally, enter a time for the request.**
   Web Filter Profiles can be configured to have rules based on the time of day.
5. **Click Test.**

The results of your test parameters will be displayed in the *Policy Test Results* box.

Note – When you test a URL against your *Web Filter Profiles*, the *Web Protection* > *Policy Test* page does not download content, or check for malware, MIME types, or file extensions. The actual filtering behavior may be different depending on what content the URL is hosting.

Note – The correct Authentication Server must be added on the *Definitions & Users* > *Authentication Services* > *Servers* page for the test to work properly.

9.5 Application Control

The Application Control functionality of UTM allows you to shape and block network traffic based on the type of traffic. In contrast to the Web Filtering functionality of UTM (see chapter Web Filtering), the application control classification engine distinguishes network traffic not only by protocol or by URL but more fine-grained. This is especially useful regarding web traffic: traffic to websites normally uses the HTTP protocol on port 80 or the HTTPS protocol on port 443. When you want to block traffic to a certain website, e.g. facebook.com, you can do that either based on that website's URL (Web Filtering). Or you can block facebook traffic independent from any URL by relying on network traffic classification.

The classification engine of UTM uses layer 7 packet inspection to classify network traffic.

Application control can be used in two ways. In a first step, you need to generally enable application control on the *Network Visibility* page which makes applications "visible" in a way. Now you can leave it that way (or for a certain time) to see which applications are used by your users (e.g. in Flow Monitor, logging, reporting). In a second step you can block certain applications and allow others. This is achieved by rules which can be created on the *Application Control Rules* page. Additionally, you can use traffic shaping to privilege traffic of defined applications which can be configured via Sophos' Quality of Service function.

9.5.1 Network Visibility

On the *Web Protection* > *Application Control* > *Network Visibility* page, you can enable and disable application control.

When application control is enabled all network traffic is classified and logged according to its classification. Current network traffic can be viewed via the Flow Monitor with in-depth information about its type (see chapter *Flow Monitor*). For example information on HTTP traffic is drilled down to the underlying applications, e.g. "twitter", "facebook", etc. To open the Flow Monitor, select the desired interface in the *Flow Monitor* section and click the *Open Flow Monitor* button.

Regarding logging and reporting, there is extensive information available on network traffic and its classification, as well as clients and servers which use those applications. For more information on logging and reporting see chapter *Logging & Reporting*, section *View Log Files* for logging and section *Network Usage* > *Bandwidth Usage* and *Web Protection* > *Application Control* for reporting.

9.5.2 Application Control Rules

On the *Web Protection* > *Application Control* > *Application Control Rules* page you can create rules based on network traffic classification which define applications whose traffic should be blocked or explicitly allowed for your network.

By default, all network traffic is allowed when application control is enabled.

Application control rules can be created either via this page or via the Flow Monitor. The latter method may be more convenient, however you can only create rules for traffic currently monitored in your network.

To create an application control rule, proceed as follows:

1. **On the *Application Control Rules* tab, click *New Rule*.**
   The *Create New Rule* dialog box opens.
2. **Make the following settings:**
   Name (optional): You can enter a name for the rule. If you leave the field empty the system is going to generate a name for the rule.

Group: The *Group* option is useful to group rules logically. With the drop-down list on top of the list you can filter the rules by their group. Grouping is only used for display purposes, it does not affect rule matching. To create a new group select the << *New group* >> entry and enter a descriptive name in the *Name* field.

Position: The position number, defining the priority of the rule. Lower numbers have higher priority. Rules are matched in ascending order. Once a rule has matched, rules with a higher number will not be evaluated anymore.

Action: Select whether the traffic is to be blocked or allowed.

Control by: Select whether to control traffic based on its application type or by a dynamic filter based on categories.

- **Applications:** The traffic is controlled application-based. Select one or more applications in the box *Control These Applications*.
- **Dynamic filter:** The traffic is controlled category-based. Select one or more categories in the box *Control These Categories*.

Control these applications/categories: Click the Folder icon to select applications/categories. A dialog window opens, which is described in detail in the next section.

Note – Some applications cannot be blocked. This is necessary to ensure a flawless operation of Sophos UTM. Such applications miss a checkbox in the application table of the *Select Application* dialog window, e.g. *WebAdmin*, *Teredo* and *SixXs* (for IPv6 traffic), *Portal* (for User Portal traffic), and some more. When using dynamic filters, blocking of those applications is also prevented automatically.

Productivity (only with *Dynamic filter*): Reflects the productivity score you have chosen.

Risk (only with *Dynamic filter*: Reflects the risk score you have chosen.

For: Select or add networks or hosts to this box whose network traffic is to be controlled by this rule. This applies only to source hosts/networks. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Log: This option is selected by default and enables logging of traffic which matches the rule.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new rule appears on the *Application Control Rules* list.

The Select Application or Category Dialog Window

When creating application control rules you need to choose applications or application categories from a dialog window called *Select one or more applications/categories to control*.

The table in the lower part of the dialog window displays the applications you can choose from or which belong to a defined category. By default, all applications are displayed.

The upper part of the dialog window provides three configuration options to limit the number of applications in the table:

- **Category:** Applications are grouped by category. This list contains all available categories. By default, all categories are selected, which means that the table below displays all applications available. If you want to limit the displayed applications to certain categories, click into the category list and select only one or more categories relevant to you.
- **Productivity:** Applications are also classified by their productivity impact which means how much they influence productivity. Example: Salesforce, a typical business software, has the score 5 which means its usage adds to productivity. On the contrary, Farmville, an online game, has the score 1 which means its usage is counterproductive. The network service DNS has the score 3 which means its productivity impact is neutral.
- **Risk:** Applications are also classified by the risk they carry when used with regard to malware, virus infections, or attacks. A higher number means a higher risk.

Tip – Each application has an Info icon which, when clicked, displays a description of the respective application. You can search the table by using the filter field in the table header.

Now, depending on the type of control you selected in the *Create New Rule* dialog box, do the following:

- Control by dynamic filter: Select the categories from the *Category* box and click *Apply* to adopt the selected categories to your rule.
- Control by application: From the table, select the applications you want to control by clicking the checkbox in front. Click *Apply* to adopt the selected applications to your rule.

After clicking *Apply*, the dialog window closes and you can continue to edit the settings of your application rule.

9.5.3 Advanced

On the *Web Protection* > *Application Control* > *Advanced* page you can configure advanced options for application control.

Application Control Skiplist

Hosts and networks listed in this box will not be monitored by application control and can therefore neither be controlled by application control nor by the application selector of Quality of Service. This applies both to source and destination hosts/networks.

9.6 FTP

On the *Web Protection* > *FTP* tab you can configure the FTP proxy. The *File Transfer Protocol* (FTP) is a widely used protocol for exchanging files over the Internet. Sophos UTM presents a proxy service acting as a go-between for all FTP traffic passing your network. The FTP proxy provides such useful features as virus scanning of FTP traffic or blocking of certain file types that are transferred via the FTP protocol.

The FTP proxy can work transparently, that is, all FTP clients within your network would establish a connection to the proxy instead of their ultimate destination. The proxy would then initiate a new network connection on behalf of the request, invisible to the client. The advantage of this mode is that no additional administration or client-side configuration is necessary.

9.6.1 Global

On the *Web Protection* > *FTP* > *Global* tab you can configure the basic settings of the FTP proxy.

To configure the FTP proxy, proceed as follows:

1. **On the *Global* tab, enable the FTP proxy.**
   Click the toggle switch.

   The toggle switch turns amber and the *FTP Settings* area becomes editable.

2. **Select the allowed networks.**
   Select the networks that are allowed to use the FTP proxy.

3. **Select an operation mode.**
   Select an operation mode for the FTP proxy. The following modes are available:
   - **Transparent:** The proxy forwards the client request to the target server and scans the content. No configuration on client side is necessary.
   - **Non-Transparent:** Using this mode you need to configure the FTP clients. Use the gateway's IP address and port `2121`.
   - **Both:** This mode allows you to use transparent mode for some clients and non-transparent mode for others. Configure FTP clients that are to work in non-transparent mode to use a proxy with the gateway's IP address and port `2121`.
4. **Click *Apply*.**
   Your settings will be saved.

Note – The FTP proxy is unable to communicate with FTP servers that use Active Directory authentication. To enable FTP clients to connect to an FTP server of that kind, add the server to the FTP proxy skiplist, which is configured on the *Advanced* tab.

9.6.2 Antivirus

The *Web Protection* > *FTP* > *Antivirus* tab contains all measures that can be taken against FTP traffic that carries harmful and dangerous content such as viruses, worms, or other malware.

Use Antivirus scanning: When selecting this option, FTP traffic will be scanned. Sophos UTM features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings* > *Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.

Max scanning size: Specify the maximum size of files to be scanned by the antivirus engine (s). Files exceeding this size will be exempt from scanning.

Click *Apply* to save your settings.

Note – Files within archives (e.g. `zip` files) will not be scanned for blocked file types, blocked extensions or blocked MIME types. To protect your network from these within archived files, consider blocking archive file types such as zip, rar, etc.

File Extension Filter

This feature filters FTP transfers that transmit certain types of files based on their extensions (e.g., executable binaries) from web traffic that have a file extension listed in the *Blocked File Extensions* box. You can add additional file extensions or delete file extensions that are not to be blocked. To add a file extension, click the Plus icon in the *Blocked File Extensions* box and enter the file extension you want to block, for example `exe` (without the delimiting dot). Click *Apply* to save your settings.

9.6.3 Exceptions

On the *FTP > Exceptions* tab you can define whitelist hosts/networks that should be excluded from selectable security options offered by the FTP proxy.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this exception.

   Skip these checks: Select the security checks that should be skipped:

   - **Antivirus checking:** Select to disable virus scanning, which checks traffic for unwanted content such as viruses, trojan horses, and the like.
   - **Extension blocking:** Select to disable the file extension filter, which can be used to block file transfers based on file extensions.
   - **Allowed servers:** Select to disable checks for allowed servers which can be set on the *Advanced* tab. If selected, the selected client hosts/networks will have access to any FTP server, whereas the selected server hosts/networks will be allowed for any client.

For these client hosts/networks: When selecting this option, the *Client Hosts/Networks* box opens. Select the client hosts/networks that should be exempt from the security checks of this exception rule.

OR For these server hosts/networks: When selecting this option, the *Server Hosts/Networks* box opens. Select the server hosts/networks that should be exempt from the security checks of this exception rule.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

9.6.4 Advanced

On the *FTP > Advanced* tab you can specify hosts and networks that can skip the transparent mode of the FTP proxy. Additionally, you can define which FTP servers are allowed to be accessed.

FTP Proxy Skiplist

Hosts and networks (FTP clients as well as FTP servers) listed here are excluded from the transparent interception of FTP traffic. However, to allow FTP traffic for these hosts and networks, select the *Allow FTP traffic for listed hosts/nets* checkbox. If you do not select this checkbox, you must define specific firewall rules for the hosts and networks listed here.

Note – The FTP proxy is unable to communicate with FTP servers that use Active Directory authentication. To enable FTP clients to connect to an FTP server of that kind, add the server to the FTP proxy skiplist.

FTP Servers

Select or add FTP servers or networks that are allowed to be accessed from your hosts/networks. You can create exceptions for some FTP clients or FTP servers to bypass this list on the *Exceptions* tab.

10 Email Protection

This chapter describes how to configure basic email protection features of Sophos UTM. The *Email Protection Statistics* page in WebAdmin shows an overview of today's top ten email senders, email recipients, spammers (by country), recognized malware, and concurrent connections. Each of the sections contains a *Details* link. Clicking the link redirects you to the respective reporting section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

10.1 SMTP

The menu *Email Protection > SMTP* allows you to configure the SMTP proxy. SMTP is the abbreviation of *Simple Mail Transfer Protocol*, a protocol used to deliver emails to a mail server. Sophos UTM includes an application level gateway for SMTP, which can be used to protect your internal mail server from remote attacks and additionally provides powerful virus scanning and email filtering services.

Note – To use the SMTP proxy correctly, a valid name server (DNS) must be configured.

10.1.1 Global

On the *Email Protection > SMTP > Global* tab you can decide whether to use *Simple Mode* for SMTP configuration or *Profile Mode*.

1. **Enable SMTP.**
   Click the toggle switch.

   The toggle switch turns green and the *Configuration Mode* area becomes editable.

2. **Select a configuration mode.**
   Simple Mode: Use this mode if all domains share the same settings. However, you can still define exceptions based on domain name, email addresses, and hosts. There is no functionality restriction compared with *Profile Mode*.

   Profile Mode: (Not available with BasicGuard subscription.) In this mode you can override or extend global settings e.g., of antispam and antivirus, for individual domains or domain groups by creating profiles for them in the menu *SMTP Profiles*. Settings made in the *SMTP* menu still apply to their assigned domains and, moreover, serve as defaults for profiles. In *Profile Mode*, you will find additional notes with some of the settings regarding recommendations for profile mode and behavior of the UTM.

3. **Click *Apply*.**
   The selected mode will be enabled.

SPX Global Template

If SPX Encryption is enabled, this section is available. From the drop-down list, select the SPX template that will be globally used. If using SMTP Simple mode, this template will be used for all SMTP users. If using SMTP Profile mode, this template will be used for all SMTP profiles that do not have an individual SPX template selected.

Live Log

The *POP3 Live Log* logs the POP3 proxy activities, showing all incoming emails. Click the button to open the live log in a new window.

10.1.2 Routing

On the *Routing* tab you can configure domain and routing targets for the SMTP proxy and define how recipients are to be verified.

To configure the SMTP proxy routing, proceed as follows:

1. **Enter your internal domain(s).**
   To enter your email domains, click the Plus icon in the *Domains* box.

In the appearing text box, enter the domain in the form `example.com` and click *Apply*. Repeat this step until all domains are listed.

In *Profile Mode*: Enter only domains that use global settings. All other domains should be listed in their respective profiles.

2. **Specify the internal server.**
From the drop-down list *Route by*, select the host to which emails for the domains listed above should be forwarded to. A typical target host would be the Microsoft Exchange Server on your local network. You can choose between different server types:

   - **Static host list:** Select a host definition of the target route in the *Host list* box. Note that you can select several host definitions for basic failover purposes. If delivery to the first host fails, mail will be routed to the next one. However, the (static) order of hosts cannot be determined with the current version of Sophos UTM and is somewhat accidental. To randomize delivery to a group of hosts so as to additionally achieve basic load balancing capability, use the *DNS hostname* route type and specify a hostname that has multiple A records (an *A record* or *address record* maps a hostname to an IP address).
   - **DNS hostname:** Specify the *fully qualified domain name* (FQDN) of your target route (e.g., `exchange.example.com`). Note that when you select a DNS name having multiple A records, mail to each server will be delivered randomly. In addition, if one server fails, all mail destined for it will automatically be routed to the remaining servers.
   - **MX records:** You can also route mail to your domain(s) by means of MX record (s). If you select this route type, the mail transfer agent of Sophos UTM makes a DNS query requesting the MX record for the recipient's domain name, which is the portion of the email address following the "@" character. Make sure that the gateway is not the primary MX for the domain(s) specified above, since it will not deliver mail to itself.

3. **Click *Apply*.**
Your settings will be saved.

Recipient verification

Verify recipients: Here you can specify whether and how email recipients are to be verified.

- **With callout:** A request is sent to the server to verify the recipient.
- **In Active Directory:** A request is sent to the Active Directory server to verify the recipient. To be able to use Active Directory you must have an Active Directory server

specified in *Definitions & Users > Authentication Services > Servers*. Enter a base DN into the *Alternative Base DN* field.

Note – The use of Active Directory recipient verification may lead to bounced messages in case the server does not respond.

- **Off:** You can turn off recipient verification completely but this is not recommended for it will lead to higher spam traffic volume and dictionary attacks. Thus your quarantine is likely to be flooded with unsolicited messages.

Click *Apply* to save your settings.

10.1.3 Antivirus

The *Antivirus* tab contains various measures against emails that carry harmful and dangerous content such as viruses, worms, or other malware.

Note – Outgoing emails will be scanned if the checkbox *Scan relayed (outgoing) messages* on the *Relaying* tab is selected.

Scan During SMTP Transaction

Select the checkbox *Reject malware during SMTP transaction* if you want to have messages scanned already during SMTP transaction and to have them rejected in case they contain malware.

In *Profile Mode*: This setting cannot be changed per profile. Messages with more than one recipient will skip this feature if one of the recipient profiles has *Antivirus Scanning* turned off. This means it is advisable to leave the regular antivirus setting below set to either *Blackhole* or *Quarantine*.

Click *Apply* to save your settings.

Antivirus Scanning

When using this option, emails will be scanned for unwanted content such as viruses, trojan horses, or suspicious file types. Messages containing malicious content will be blocked and stored in the email quarantine. Users can review and release their quarantined messages either through the Sophos User Portal or the daily Quarantine Report. However, messages containing malicious content can only be released from the quarantine by the administrator in the Mail Manager.

Antivirus: You can configure how to proceed with messages that contain malicious content. The following actions are available:

- **Off:** There will be no antivirus scans.
- **Blackhole:** Incoming messages will be accepted and instantly removed. Outgoing messages will never be blackholed to avoid unintended mail loss. They will be quarantined instead.
- **Quarantine:** The message will be blocked and stored in the email quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report. Note that messages containing malicious content can only be released from the quarantine by an administrator.

Sophos UTM features several antivirus engines for best security:

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings* > *Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.

Quarantine unscannable and encrypted content: Select this option to quarantine emails whose content could not be scanned. Unscannable content may be encrypted or corrupt archives or oversized content, or there may be a technical reason like a scanner failure.

Click *Apply* to save your settings.

MIME Type Filter

The MIME type filter reads the MIME type of email contents. You can define how the different MIME types are to be dealt with.

- **Quarantine audio content:** When you select this checkbox audio content like e.g., mp3 or wav files, will be quarantined.
- **Quarantine video content:** When you select this checkbox video content like e.g., mpg or mov files, will be quarantined.
- **Quarantine executable content:** When you select this checkbox executable content like e.g., exe files, will be quarantined.

Additional types to quarantine: To add a MIME type other than above that shall be quarantined, click the Plus icon in the *Additional Types To Quarantine* box and enter the MIME type

(e.g., `image/gif`). You can use wildcards (`*`) on the right side of the slash, e.g., `application/*`.

Whitelisted content types: You can use this box to allow generally certain MIME types. To add a MIME type click the Plus icon in the *Whitelisted content types* box and enter the MIME type. Click *Apply* to save your settings.

MIME type	MIME type class
audio/*	audio files
video/*	video files
application/x-dosexec	applications
application/x-msdownload	
application/exe	
application/x-exe	
application/dos-exe	
vms/exe	
application/x-winexe	
application/msdos-windows	
application/x-msdos-program	

Table 2: MIME types known by the MIME Type Filter

File Extension Filter

This feature filters and quarantines emails (with warnings) that contain certain types of files based on their extensions (e.g., executables). To add file extensions, click the Plus icon in the *Blocked file extensions* box and enter a critical file extension you want to be restricted, e.g., `exe` or `jar` (without the dot delimiter). Click *Apply* to save your settings.

Note – Archives cannot be scanned for forbidden file extensions. To protect your network from malware included in archives you might want to consider blocking the respective archive file extensions altogether.

Antivirus Check Footer

For each outgoing email, you can add and customize a special footer informing users that the email has been scanned for malicious content. However, the footer will only be added if the checkbox *Scan Relayed (Outgoing) Messages* on the *Relaying* tab is selected. In addition, the antivirus check footer will not be appended to the email if the email is a reply (i.e. having *In-Reply-To* header) or if the content type of the email could not be determined. Click *Apply* to save your settings.

Note – Adding a footer to messages already signed or encrypted by an email client (e.g., Microsoft's Outlook or Mozilla's Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the antivirus check footer option. However, if you do not wish to forgo the privacy and authentication of your email communication and still want to apply a general antivirus check footer, consider using the built-in email encryption feature of Sophos UTM. Email encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.

10.1.4 Antispam

Sophos UTM can be configured to detect unsolicited spam emails and to identify spam transmissions from known or suspected spam purveyors. Configuration options located on the *Antispam* tab let you configure SMTP security features aimed at preventing your network from receiving unsolicited commercial emails.

Note – Outgoing emails will be scanned if the checkbox *Scan relayed (outgoing) messages* on the *Relaying* tab is selected.

Note – Some of the features on this tab are not available with BasicGuard subscription.

Spam Detection During SMTP Transaction

You have the possibility to reject spam already during SMTP transaction. Select one of the following settings for the option *Reject at SMTP Time*:

- **Off:** Spam detection is disabled and no email is going to be rejected for spam reasons.
- **Confirmed spam:** Only confirmed spam is rejected.

- **Spam:** All emails that the system regards as spam are rejected. Note that there may be a higher false positive rate because emails regarded as probable spam may be rejected such as newsletters.

Emails which are not rejected during SMTP transaction will be treated according to your settings in the *Spam Filter* section below.

In *Profile Mode*: This setting cannot be changed per profile. Messages with more than one recipient will skip this feature if one of the recipient profiles has spam scanning completely turned off. This means it is advisable to leave the regular spam scanning setting set to either *Spam* or *Confirmed spam*.

RBLs (Realtime Blackhole Lists)

A *Realtime Blackhole List* (RBL) is a means by which an Internet site may publish a list of IP addresses linked to spamming.

Use recommended RBLs: Selecting this option causes the mail transfer agent to query external databases of known spam senders (so-called *Realtime Blackhole Lists*). Messages sent from a site included in one or more of such lists can easily be rejected. Several services of this type are available on the Internet. This function massively helps to reduce the amount of spam.
By default, the following RBLs are queried:

- Commtouch IP Reputation (ctipd.org)
- cbl.abuseat.org

Note – The list of RBLs queried by Sophos UTM is subject to change without notice. Sophos does not warrant for the contents of these databases.

You can also add further RBL sites to enhance the antispam capability of Sophos UTM. To do so, click the Plus icon in the *Extra RBL zones* box. In the appearing textbox, enter the RBL zone.

Click *Apply* to save your settings.

Spam Filter

Sophos UTM includes a heuristic check of emails for characteristics suggestive of spam. It uses SMTP envelope information and an internal database of heuristic tests and characteristics. This spam filtering option scores messages based on their content and SMTP envelope information. Higher scores indicate a higher spam probability.

With the following two options you can specify what to do with messages that have been assigned a certain spam score. This ensures that potential spam emails are treated differently by the gateway.

- **Spam action:** Here you can define what to do with messages that are classified as probable spam. Note that there may be false positives, such as newsletters, thus blackholing may lead to email loss.
- **Confirmed spam action:** Here you can define what to do with confirmed spam messages.

You can choose between different actions for those two types of spam:

- **Off:** No messages will be marked as spam or filtered out.
- **Warn:** No messages will be filtered out. Instead, for incoming messages, a spam flag will be added to the message's header and a spam marker will be added to the message's subject. Outgoing messages will be sent without action.
- **Quarantine:** Messages will be blocked and stored in the email quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report.
- **Blackhole:** Incoming messages will be accepted and instantly removed. Outgoing messages will never be blackholed to avoid unintended mail loss. They will be quarantined instead.

Spam marker: With this option you can specify a spam marker, that is, a string that will be added to the message's subject line making it easy to identify spam messages quickly. By default, the string `*SPAM*` is used to tag messages as spam.

Sender Blacklist

The envelope sender of incoming SMTP sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the message will be blackholed.
To add a new address pattern to the blacklist click the Plus icon in the *Blacklisted Address Patterns* box, enter (a part of) an address, and click *Apply*. You can use an asterisk (*) as a wildcard, e.g., `*@abbeybnknational.com`.

Tip – End-users can create their personal blacklist and whitelist in the User Portal.

Expression Filter

The expression filter scans messages' content passing through the SMTP proxy for specific expressions. Suspicious emails will be blocked. Expressions can be entered as *Perl Compatible*

Regular Expressions. Simple strings such as "online dating" are interpreted in a case-insensitive manner. Click *Apply* to save your settings.

Cross Reference – For detailed information on using regular expressions in the expression filter, see the Sophos Knowledgebase.

Advanced Antispam Features

This area gathers various other advanced options increasing the antispam capability of Sophos UTM.

Reject invalid HELO/missing RDNS: Select this option if you want to reject hosts that send invalid HELO entries or lack RDNS entries. If you want to exempt hosts from this check, please refer to the *Exceptions* tab.

> **Do strict RDNS checks:** Select this option if you want to additionally reject mail from hosts with invalid RDNS records. An RDNS record is invalid if the found hostname does not resolve back to the original IP address.

Use Greylisting: Greylisting basically means the temporary rejection of emails for a certain amount of time. Typically, a mail server using greylisting will record the following pieces of information for all incoming messages:

- The sender address
- The IP address of the host the message is sent from
- The recipient address
- The message subject

This data set is checked against the SMTP proxy's internal database; if the data set has not been seen before, a record is created in the database along with a special time stamp describing it. This data set causes the email to be rejected for a period of five minutes. After that time the data set is known to the proxy and the message will be accepted when it is sent again. Note that the data set will expire after a week if it is not updated within this period.
Greylisting uses the fact that most senders of spam messages use software based on the "fire-and-forget" method: Try to deliver the mail and if it doesn't work, forget it! This means that senders of spam mail do not try to send emails again when there is a temporary failure, contrary to RFC-conform mail servers. The assumption is that since temporary failures are built into the RFC specifications for email delivery, a legitimate server will try again to send the email later, at which time the destination will accept it.

Use BATV: BATV is a draft of the IETF, facing the challenge to distinguish legitimate uses from unauthorized uses of email addresses. BATV provides a method to sign the envelope sender of outgoing mail by adding a simple shared key to encode a hash of the address and time-varying information as well as some random data proving that the email was really sent by you. It is basically used to reject bounce messages not sent by you. By using BATV, you can now check if bounces you receive are really caused by your initial email, and not from a spammer forging an email with your address. If a bounce returns and the email address is not signed according to BATV, the SMTP proxy will not accept the message. Note that the signature provided by BATV expires after seven days. To change the key (also known as *BATV secret*) that is used to encode the hash of an email's envelope `MAIL FROM` address, go to the *Email Protection* > *SMTP* > *Advanced* tab.

Note – Some mail transfer agents may reject a message whose envelope sender address was modified using BATV. In this case, you need to create an exception rule for the senders, recipients, or domains affected.

Perform SPF check: SPF (*Sender Policy Framework*) is a framework where domain owners can publish information about their outgoing email servers. Domains use public records to direct requests for different services (web, email, etc.) to the machines that perform those services. All domains already publish MX records for email related services to let others know what machines receive mail for the domain. SPF works by domains publishing some sort of "reverse MX" records to tell the world what machines send mail from the domain. When receiving a message from a certain domain, the recipient can check those records to make sure that mail is coming from where it should be coming from.

Cross Reference – Further information is available at the Sender Policy Framework website.

As an additional antispam feature, the SMTP proxy tacitly checks each recipient address it receives with your backend mail server(s) before accepting mail for this address. Emails for invalid recipient addresses will not be accepted. In order for this function to work, your backend mail server(s) must reject mails for unknown recipients at the SMTP stage. The general rule is that if your backend server rejects a message, the SMTP proxy will reject it, too.

Note, however, that recipient verification is *not* done for trusted (authenticated) or relay hosts, because some user agents may encounter problems when recipients get rejected in the SMTP

transaction. In the usual scenario (backend mail server rejects unknown recipients in the SMTP transaction), Sophos UTM will only generate bounces in the following cases:

- When a trusted or relay source sends a message to an undeliverable recipient.
- When the backend mail server has been down so that Sophos UTM was not able to verify the recipient.

However, Sophos UTM does not prevent your backend mail server(s) from sending non-delivery reports (NDRs) or bounces. In addition, Sophos UTM caches positive callout replies from the mail server for 24 hours, and negative ones for two hours.

10.1.5 Data Protection

On the *SMTP > Data Protection* tab, the Data Protection feature allows you to reduce accidental data loss from workstations by monitoring and restricting the transfer of files containing sensitive data. Accidental data loss is commonly caused by employees mishandling sensitive data. For example, a user sends a file containing sensitive data home via email (SMTP). Data Protection scans outgoing emails including subject line, message body and attachments for sensitive or confidential information. Based on the outcome, the email can be encrypted using SPX encryption, or the email can be rejected or sent.

To configure Data Protection, define the settings in the following sections. As long as no Sophos content control rule is selected, and no custom rule is defined, the feature is disabled.

Data Protection Policy

Scan within attachments: If selected, attachments will be scanned for sensitive data, additionally to the message itself.

Action on rule match: Select how to handle an email if the policy is triggered:

Reject: An email that triggers the policy will not be sent.

Send with SPX encryption: An email that triggers the policy will automatically be sent SPX encrypted (see *Email Protection > SPX Encryption* tab). If SMTP is used in Simple Mode, the SPX Template selected on the *SMTP > Global* tab will be used for SPX encryption. If SMTP is used in Profile Mode, the SPX template used depends on the SMTP profile the sender's domain is assigned to (see *SMTP Profiles* tab). If the sender's domain is not assigned to any profile, the default template selected on the *SMTP > Global* tab will be used.

Allow: An email that triggers the policy will be sent nevertheless.

On match, notify: Select if you want to notify the email sender, the administrator, other, or all of them. Next to other you have to enter a email address. The notification email can be customized on the *Management* > *Customization* > *Email Messages* tab.

Click *Apply* to save your settings.

Sophos Content Control Rules

Type: Select an entry from the drop-down list to reduce the number of displayed rules accordingly.

Region: Select an entry from the drop-down list to reduce the number of displayed rules accordingly.

Show selected only: If enabled, only selected rules will be displayed in the list.

Rules: Select the rules you want to use for the Data Protection feature. Hovering the cursor on an entry, a tool-tip with additional information concerning the rule appears.

Click *Apply* to save your settings.

Custom Rules

Custom expression: Enter expressions that you want to use for the Data Protection feature, in addition to the rules selected above. You can add regular expressions.

Cross Reference – For detailed information on using regular expressions here, see the Sophos Knowledgebase.

Click *Apply* to save your settings.

10.1.6 Exceptions

On the *SMTP* > *Exceptions* tab you can define whitelist hosts, networks, senders, and recipients that can be excluded from antispam, antivirus, or other security checks.

Note – Since emails can have many recipients, and Sophos UTM implements inline scanning for the SMTP protocol, scanning of an email is skipped for all recipients if one of the email's recipients is listed in the *Recipients* box.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this exception.

   Skip these checks: Select the security checks that should be skipped. For more information, see *Email Protection > SMTP >* Antivirus, Antispam, and Data Protection.

   For these source hosts/networks: Select or add the source hosts/networks (i.e., the host or network messages originate from) that should skip the security checks defined by this exception rule. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Note – No exception needs to be created for localhost because local messages will not be scanned by default.

   When selecting this option, the *Hosts/Networks* box opens. You can add a host or network by either clicking the Plus icon or the Folder icon.

   OR these sender addresses: Select the senders' email addresses that should skip the defined security checks.
   When selecting this option, the *Senders* box opens. You can either enter a complete valid email address (e.g., `jdoe@example.com`) or all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`).

   Note – Use the *Senders* option with caution, as sender addresses can easily be forged.

   OR these recipient addresses: Select the recipients' email addresses that should skip the defined security checks.

   When selecting this option, the *Recipients* box opens. You can either enter a complete valid email address (e.g., `jdoe@example.com`) or all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`).

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

10.1.7 Relaying

The SMTP proxy can be used as a mail relay. A mail relay is an SMTP server configured in such a way that it allows specific users, user groups, or hosts to relay (i.e., send) emails through it to domains that are not local.

Note – Some of the features on this tab are not available with BasicGuard subscription.

Upstream Host List

An upstream host is a host that forwards email to you, e.g., your ISP or external MX. If you get inbound email from static upstream hosts, it is necessary that you enter the hosts here. Otherwise spam protection will not work properly.

To add an upstream host either click the Plus icon or the Folder icon for drag-and-drop from the *Networks* object list. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page. If you would like to only allow upstream hosts select the checkbox *Allow upstream/relay hosts only*. SMTP access will then be limited to the defined upstream hosts. Upstream hosts can authenticate to get relaying rights. Click *Apply* to save your settings.

Authenticated Relay

SMTP clients can authenticate to get relaying privileges. Select the checkbox *Allow authenticated relaying* and specify the users and user groups that should be able to use this feature. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page. Click *Apply* to save your settings.

Note – If the checkbox *Allow upstream/relay hosts only* is enabled then *Authenticated Relay* does only work when the sending host is configured as upstream/relay host.

Host-based Relay

Mail relaying can also be enabled host-based. If your local mail server or mail clients should be able to use the SMTP proxy as a mail relay, you need to add the networks and hosts which should be able to send mail through the relay to the *Allowed hosts/networks* box. The networks and hosts listed are allowed to send messages to any addresses. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Caution – It is extremely important not to select *Any* in the *Allowed hosts/networks* box, because this would result in an open relay, allowing anyone on the Internet to send messages through the SMTP proxy. Spammers will quickly recognize this, leading to massive email traffic. In the worst case, you will be listed on 3rd party spammer blacklists. In most configurations, the only hosts that should be allowed to relay mail are the mail servers in your network.

Click *Apply* to save your settings.

Host/Network Blacklist

Here you can define hosts and networks that shall be blocked by the SMTP proxy. Click *Apply* to save your settings.

Content Scan For Relayed Messages

When this option is enabled, also messages sent by either authenticated or host-based relays will be scanned for malicious content. If there are many outgoing mails, turning this option off can improve your performance. Click *Apply* to save your settings.

Note that your global antivirus and antispam settings also apply to outgoing messages. But regardless of those settings, infected or spam messages are never blackholed but always sent to quarantine to avoid unintended mail loss.

10.1.8 Advanced

On the *SMTP > Advanced* tab you can configure additional security options of the SMTP proxy such as smarthost settings or transparent mode skiplist, among others.

Parent Proxy

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

Use a parent proxy: Select the checkbox to enable parent proxy use. Select or add the host and enter the port of the proxy. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Proxy requires authentication: If the parent proxy requires authentication, enter username and password here.

Transparent Mode

To enable transparent mode for SMTP select the checkbox and click *Apply*.
Hosts and networks listed in the *Skip transparent mode hosts/nets* box will not be subject to the transparent interception of SMTP traffic. However, to allow SMTP traffic for these hosts and networks, select the *Allow SMTP traffic for listed hosts/nets* checkbox. If you do not select this checkbox, you must define specific firewall rules for the hosts and networks listed here. Click *Apply* to save your settings.

TLS Settings

TLS certificate: Select a certificate from the drop-down list which will be used to negotiate TLS encryption with all remote hosts supporting it. You can create or upload certificates on the *Site-to-site VPN > Certificate Management > Certificates* tab.

Require TLS negotiation host/nets: Add or select hosts or nets here which always require TLS encryption for email communication. The UTM will then hold back emails if TLS encryption is not available for those hosts/nets for some reason, that means messages will stay in the mail queue until TLS becomes available again. In case TLS is not available within a reasonable period of time, sending attempts will be stopped and the user will get a notification that their email could not be sent.

Require TLS negotiation sender domains: If you want to enforce TLS encryption for incoming emails for certain domains, enter those domains here. Emails sent from those domains without TLS will be rejected immediately.

Skip TLS negotiation host/nets: If a particular host or network should encounter problems with TLS encryption, you can enter it in the box and select the appropriate TLS certificate from the drop-down menu. This will cause the UTM to skip TLS negotiation for this host or network. Click *Apply* to save your settings.

Domain Keys Identified Mail (DKIM)

DKIM is a method to cryptographically sign outgoing messages. To use DKIM signing, enter your private RSA key and the corresponding key selector into the respective fields and add the domains you want to sign emails for to the *DKIM domains* box. Click *Apply* to save your settings.

Confidentiality Footer

For each outgoing email, you can add and customize a confidentiality footer informing users, for example, that the email may contain confidential or privileged information. However, the con-

fidentiality footer will not be appended to the email if the email is a reply (i.e. having an *In-Reply-To* header) or if the content type of the email could not be determined.

Note – Adding a footer to messages already signed or encrypted by an email client (e.g., Microsoft's Outlook or Mozilla's Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the antivirus check footer option. However, if you do not wish to forgo the privacy and authentication of your email communication and still want to apply a general antivirus check footer, consider using the built-in email encryption feature of Sophos UTM. Email encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.

Advanced Settings

Here you can configure the SMTP hostname and the postmaster address, among other things.

SMTP hostname: Setting the SMTP hostname will cause the proxy to use the specified name in HELO and SMTP banner messages. By default, the normal system hostname is selected.

Postmaster address: Specify the email address of the postmaster of the UTM to whom messages are to be forwarded that are sent in the form of `postmaster@[192.168.16.8]`, where the IP literal address is one of the IP addresses of the UTM. Accepting such messages is an RFC requirement.

BATV secret: Here you can change the automatically generated BATV secret used by the SMTP proxy. The BATV secret is a shared key used to sign an email's envelope `MailFrom` address, thus enabling detection of invalid bounce addresses. If you are using several MXs for your domains, you can change the BATV secret to be the same on all systems.

Max message size: The maximum message size that is accepted by the proxy. This setting applies to both incoming and outgoing emails. If your backend server has a limitation with regard to message sizes, you should set the same or a lower value here.

Max connections: The maximum number of concurrent connections the proxy allows. Default is 20.

Max connections/host: The maximum number of connections per host the proxy allows. Default is 10.

Max mails/connection: The maximum number of mails per connection the proxy allows. Default is 1000.

Max rcpt/mail: The maximum number of recipients per mail the proxy allows. Default is 100.

Footers mode: Here you can define how footers will be added to mails. *MIME part* will add the footer as extra MIME part. Existing part encodings are not changed and national language characters are preserved. The other method is *Inline* which means that the footer is separated from the main mail by the -- separator. With this mode you can choose whether the footer should be Unicode (UTF-8) converted or not. Unicode conversion upgrades the message to preserve national language characters in the footer.

Smarthost Settings

A smarthost is a type of mail relay server which allows an SMTP server to route mail to an upstream mail server rather than directly to the recipient's server. Often this smarthost requires authentication from the sender to verify that the sender has privileges to have mail forwarded through the smarthost.

Use a smarthost: If you want to use a smarthost to send mail, select the checkbox. In that case, the proxy will never deliver mail itself, but rather send anything to the smarthost.

- **Smarthost:** Select or add a smarthost object. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.
- **Smarthost port:** The default port for the smarthost connection is 25. You can change it if required.
- **This smarthost requires authentication:** Select this checkbox if the smarthost requires authentication. Both *Plain* and *Login* authentication types are supported. Enter a username and password into the respective fields.

10.2 SMTP Profiles

The SMTP proxy of Sophos UTM lets you create alternative SMTP profiles, which can then be associated with different domains. That way you can specify domains that should use a different profile other than the default profile configured in *Email Protection* > *SMTP*. The order of the functions, structured as tabs, reflects how each step gets processed one after the other during SMTP time.

To create an SMTP profile, proceed as follows:

1. **Enable the SMTP profile mode.**
   On the *Email Protection* > *SMTP* > *Global* tab select *Profile Mode* and click *Apply*.

   The SMTP profiles creation in the *Email Protection* > *SMTP Profiles* menu is enabled.

2. **On the *SMTP Profiles* tab, click *New Profile*.**
   A dialog box opens.
3. **Enter a descriptive name for the profile.**
4. **Add one or more domains.**
   Add one or more domains to the *Domains* box.

   Settings of this profile will be applied for those domains.
5. **Make the following settings:**
   You only need to make settings for functions you want to use. For each of the following functions you can decide whether to use individual settings defined here or global settings defined under *Email Protection* > *SMTP*. By default, the global settings option is selected. The individual settings for each function are described below.

   Note – Encrypted emails whose sender address includes a domain name configured here cannot be decrypted when using the email encryption/decryption engine of Sophos UTM. Therefore, no profile should be added for external email domains.

   All settings that you can define here can also be set globally in *Email Protection* > *SMTP*. Therefore only a list of settings and the differences from the global settings are given here, along with cross-references to the respective global setting where detailed information can be found.

   The following settings can be made:

   - **Routing:** On the *Routing* tab you can configure domain and routing targets for the SMTP proxy and define how recipients shall be verified.
     - Static Host List
     - DNS Hostname
     - MX Records

     For detailed information please refer to *Email Protection* > *SMTP* > *Routing*.
   - **Recipient Verification**
     Verify recipients: Here you can specify whether and how email recipients are to be verified.

- **With callout:** A request is sent to the server to verify the recipient.
- **In Active Directory:** A request is sent to the Active Directory server to verify the recipient. To be able to use Active Directory you must have an Active Directory server specified in *Definitions & Users > Authentication Services >* Servers. Enter a base DN into the *Alternative Base DN* field.

  Note – The use of Active Directory recipient verification may lead to bounced messages in case the server does not respond.

- **Off:** You can turn off recipient verification completely but this is not recommended for it will lead to higher spam traffic volume and dictionary attacks. Thus your quarantine is likely to be flooded with unsolicited messages.

For detailed information please refer to *Email Protection > SMTP >* Routing.

- **Sophos UTM RBLs:** Here you can block IP addresses linked to spamming.
  - Use recommended RBLs

  For detailed information please refer to *Email Protection > SMTP >* Antispam.
- **Extra RBLs:** You can add further RBL sites to enhance the antispam capability of Sophos UTM. For detailed information please refer to *Email Protection > SMTP >* Antispam. Note that, as a third option, you can add the global settings to your individual settings here.
- **BATV/RDNS/HELO/SPF/Greylisting:** This tab gathers various other advanced options increasing the antispam capability of Sophos UTM.
  - Reject Invalid HELO/Missing RDNS
  - Use Greylisting
  - Use BATV
  - Perform SPF Check

  For detailed information please refer to *Email Protection > SMTP >* Antispam.
- **Antivirus Scanning:** You can configure how to proceed with messages that contain malicious content. The following actions are available:
  - Off
  - Quarantine
  - Blackhole

You can choose between the following antivirus scan options:

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings* > *Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.

Quarantine unscannable and encrypted content: Select this option to quarantine emails whose content could not be scanned. Unscannable content may be encrypted or corrupt archives or oversized content, or there may be a technical reason like a scanner failure.

For detailed information please refer to *Email Protection* > *SMTP* > *Antivirus*.

- **Antispam Scanning:** Here you can decide how to deal with unsolicited commercial emails. Both for spam and confirmed spam you can choose between the following actions:
  - Off
  - Warn
  - Quarantine
  - Blackhole

  For detailed information please refer to *Email Protection* > *SMTP* > *Antispam*.
- **Sender Blacklist:** The envelope sender of incoming SMTP sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the message will be blackholed. For detailed information please refer to *Email Protection* > *SMTP* > *Antispam*. Note that, as a third option, you can add the global settings to your individual settings here.
- **MIME Audio/Video/Executables blocking:** The MIME type filter reads the MIME type of email contents. You can select which content types you would like to quarantine:
  - Audio Content
  - Video Content
  - Executable Content

  For detailed information please refer to *Email Protection* > *SMTP* > *Antivirus*.

- **MIME Type Blacklist:** Here you can add additional MIME types to quarantine. For detailed information please refer to *Email Protection > SMTP >* Antivirus. Note that, as a third option, you can add the global settings to your individual settings here.
- **MIME Type Whitelist:** Here you can add MIME types not to quarantine. For detailed information please refer to *Email Protection > SMTP >* Antivirus. Note that, as a third option, you can add the global settings to your individual settings here.
- **Blocked File Extensions:** Using the *File extension filter* you can quarantine emails (with warnings) that contain certain types of files based on their extensions (e.g., executables). For detailed information please refer to *Email Protection > SMTP >* Antivirus. Note that, as a third option, you can add the global settings to your individual settings here.
- **Blocked Expressions:** The expression filter scans messages' content passing through the SMTP proxy for specific expressions. Suspicious emails will be blocked. For detailed information please refer to *Email Protection > SMTP >* Antispam. Note that, as a third option, you can add the global settings to your individual settings here.
- **Confidentiality Footer:** For each outgoing email, you can add and customize a confidentiality footer informing users, for example, that the email may contain confidential or privileged information. However, the confidentiality footer will not be appended to the email if the email is a reply (i.e. having an *In-Reply-To* header) or if the content type of the email could not be determined. Note that the footer is appended depending on the sender domain. To use a footer, select the checkbox and enter the footer text.
- **SPX Template Selection:** The SPX template is used for SPX Encryption. It defines how encrypted emails will be sent to the recipients. For detailed information please refer to *Email Protection > SPX Encryption > SPX Templates*.
- **Data Protection Configuration:** Here you can add attachments to the scan list, set notifications and select items from the *SophosLabs Content Control List*. For detailed information please refer to *SMTP > Data Protection*.

6. **Click *Apply*.**
   Your settings will be saved.The new profile appears on the *SMTP Profiles* list.

Note – When you select *Use global settings* for a topic and click *Apply*, the icon of the function changes to the global settings icon. By this, you can easily get an overview on which functions global settings or individual settings are applied.

To either disable, rename or delete a profile click the corresponding buttons at the top below the profile drop-down list.

10.3 POP3

The menu *Email Protection* > *POP3* lets you configure the POP3 proxy for incoming emails. The *Post Office Protocol 3* (POP3) is an application-layer Internet standard protocol that allows the retrieval of emails from a remote mail server. The POP3 proxy works transparently, meaning that all POP3 requests coming from the internal network on port `110` (and `995` if scanning of TLS encrypted traffic is enabled) are intercepted and redirected through the proxy invisible to the client. The advantage of this mode is that no additional administration or client-side configuration is necessary.

Note – It might be necessary to increase the server timeout settings in the email clients' configuration. Usual default settings of about one minute or less might be too low, especially when fetching large emails.

The POP3 protocol does not have server-side tracking of which mails have already been retrieved. Generally, a mail client retrieves a mail and deletes it on the server afterwards. However, if the client is configured to not delete mails, then server-side deleting is omitted and the client keeps track of which mail has already been fetched.

10.3.1 Global

On the *Email Protection* > *POP3* > *Global* tab you can configure basic settings for the POP3 proxy.

To configure the POP3 proxy, proceed as follows:

1. **Enable the POP3 proxy.**
   Click the toggle switch.

   The toggle switch turns amber and the *POP3 Settings* area becomes editable.

2. **Select the allowed networks.**
   Add or select the networks that should be allowed to proxy POP3 traffic. Typically, this is the internal network. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Caution – It is extremely important not to select an *Any* network object, because this introduces a serious security risk and opens your appliance up to abuse from the Internet.

3. **Click *Apply*.**
   Your settings will be saved.

To cancel the configuration, click the amber colored toggle switch.

Live Log

The *POP3 Live Log* logs the POP3 proxy activities, showing all incoming emails. Click the button to open the live log in a new window.

10.3.2 Antivirus

The *Antivirus* tab contains various measures against emails that carry harmful and dangerous content such as viruses, worms, or other malware.

Antivirus Scanning

When using this option, emails will be scanned for unwanted content such as viruses, trojan horses, or suspicious file types. Messages containing malicious content will be blocked and stored in the email quarantine. Users can review and release their quarantined messages either through the Sophos User Portal or the daily Quarantine Report. However, messages containing malicious content can only be released from the quarantine by the administrator in the Mail Manager.

Sophos UTM features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings > Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.

Quarantine unscannable and encrypted content: Select this option to quarantine emails whose content could not be scanned. Unscannable content may be encrypted or corrupt archives or oversized content, or there may be a technical reason like a scanner failure.

Max scanning size: Specify the maximum size of files to be scanned by the antivirus engine (s). Files exceeding this size will be exempt from scanning.

Click *Apply* to save your settings.

File Extension Filter

This feature filters and quarantines emails (with warnings) that contain certain types of files based on their extensions (e.g., executables). To add file extensions, click the Plus icon in the *Blocked File Extensions* box and enter a critical file extension you want to be scanned, e.g., `exe` or `jar` (without the dot delimiter). Click *Apply* to save your settings.

Note – Archives cannot be scanned for forbidden file extensions. To protect your network from malware included in archives you might want to consider blocking the respective archive file extensions altogether.

10.3.3 Antispam

Sophos UTM can be configured to detect unsolicited spam emails and to identify spam transmissions from known or suspected spam purveyors. Configuration options located on the *Antispam* tab let you configure POP3 security features aimed at preventing your network from receiving unsolicited commercial emails.

Spam Filter

Sophos UTM includes a heuristic check of incoming emails for characteristics suggestive of spam. It uses SMTP envelope information and an internal database of heuristic tests and characteristics. This spam filtering option scores messages based on their content and SMTP envelope information. Higher scores indicate a higher spam probability.

With the following two options you can specify what to do with messages that have been assigned a certain spam score. This ensures that potential spam emails are treated differently by the gateway.

- **Spam action:** Here you can define what to do with messages that are classified as probable spam.

- **Confirmed spam action:** Here you can define what to do with confirmed spam messages.

You can choose between different actions for those two types of spam:

- **Off:** No messages will be marked as spam or filtered out.
- **Warn:** No messages will be filtered out. Instead, a spam flag will be added to the message's header and a spam marker will be added to the message's subject.
- **Quarantine:** The message will be blocked and stored in the email quarantine. Quarantined messages can be reviewed either through the User Portal or the daily Quarantine Report.

Spam marker: With this option you can specify a spam marker, that is, a string that will be added to the message's subject line making it easy to identify spam messages quickly. By default, the string `*SPAM*` is used to tag messages as spam.

Expression Filter

The expression filter scans the message's subject and body for specific expressions. Emails that contain an expression listed here will be blocked. However, if the prefetch option is enabled on the *Email Protection* > *POP3* > *Advanced* tab, the email will be sent to the quarantine. Expressions can be entered as *Perl Compatible Regular Expressions*. Simple strings such as "online dating" are interpreted in a case-insensitive manner.

Cross Reference – For detailed information on using regular expressions in the expression filter, see the Sophos Knowledgebase.

Click *Apply* to save your settings.

Sender Blacklist

The envelope sender of incoming POP3 sessions will be matched against the addresses on this blacklist. If the envelope sender is found on the blacklist the message will be quarantined and marked as *Other* in the subject line.
To add a new address pattern to the blacklist click the Plus icon in the *Blacklisted Address Patterns* box, enter (a part of) an address, and click *Apply*. You can use an asterisk (*) as a wildcard, e.g., `*@abbeybnknational.com`.

Tip – End-users can create their personal blacklist and whitelist in the User Portal.

10.3.4 Exceptions

On the *POP3 > Exceptions* tab you can define client hosts/networks and sender addresses that shall be excluded from various security features.

To create an exception, proceed as follows:

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this exception.

   Skip these checks: Select the security checks that should be skipped. For more information, see *Email Protection > POP3 >* *Antivirus* and *Antispam*.

   For these client hosts/networks: Add or select the source hosts/networks (i.e., the hosts or networks messages originate from) that should skip the security checks. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Note – No exception needs to be created for localhost because local messages will not be scanned by default.

   When selecting this option, the *Client hosts/networks* dialog box opens. You can add a host or network by either clicking the plus symbol or the folder symbol.

   OR these sender addresses: Select the senders' email addresses that should skip the defined security checks.
   When selecting this option, the *Senders* box opens. You can either enter a complete valid email address (e.g., `jdoe@example.com`) or all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`).

   Note – Use the *Senders* option with caution, as sender addresses can easily be forged.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

10.3.5 Advanced

On the *POP3* > *Advanced* tab you can specify those hosts and networks that can skip the transparent mode of the POP3 proxy. In addition, it contains the POP3 proxy's prefetch option, which allows the prefetching of messages from a POP3 server and storing them in a database.

Transparent Mode Skiplist

Hosts and networks listed in the *Skip transparent mode hosts/nets* box will not be subject to the transparent interception of POP3 traffic. However, to allow POP3 traffic for these hosts and networks, select the *Allow POP3 traffic for listed hosts/nets* checkbox. If you do not select this checkbox, you must define specific firewall rules for the hosts and networks listed here.

POP3 Servers and Prefetch Settings

You can enter one or more POP3 servers here that are used in your network or by your end-users, so that the servers are known to the proxy. Additionally, you can turn on prefetching.

To define a POP3 server, do the following:

1. **Add the DNS name of the POP3 server(s).**
   In the *POP3 servers* box, click the Plus icon. In the *Add Server* dialog window, enter the DNS name and click *Save*.

   A new entry with the entered DNS name and the suffix *Servers* is displayed in the box. The UTM automatically creates a DNS group with the specified DNS name and associates it with the new POP3 server entry.

2. **Specify the POP3 server's properties.**
   In the *POP3 servers* box, click the Edit icon in front of the POP3 server. The *Edit Server* dialog window opens. Make the following settings:

   Name: If you want, modify the POP3 server's name.

   Hosts: The box automatically contains a DNS group with the DNS name specified above. Add or select additional hosts or DNS groups. Make sure to add only such hosts or DNS groups that serve the same POP3 accounts. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

TLS certificate: Select a certificate from the drop-down list which will be used to negotiate TLS encryption with all remote hosts supporting it. You can create or upload certificates on the *Site-to-site VPN > Certificate Management > Certificates* tab.

Note – For TLS encryption to work, the *Scan TLS encrypted POP3 traffic* checkbox in the *TLS Settings* section has to be enabled. For POP3 servers not defined here or not having a TLS certificate, you can select a default TLS certificate in the *TLS Settings* section.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The POP3 server is defined.

If no POP3 server is specified and a mail gets caught by the proxy, the proxy replaces the mail with a notification to the recipient right away in the same connection stating that the mail has been quarantined. The quarantined mail can be viewed in *Mail Manager*, but is not associated to a server or account and therefore cannot be released in a later connection. Generally, releasing of emails from quarantine does only work for prefetched messages.

There are two scenarios:

- If POP3 server(s) are given and prefetching is disabled, the proxy keeps track which quarantined mails belong to which server/account. Thus, quarantined mail can be released when the client polls the mailbox next time. For this to work, the proxy has to safely identify which IP addresses belong to which server (by their FQDN which you have entered in your mail client).
- If POP3 server(s) are given and prefetching is enabled, the POP3 proxy periodically checks the POP3 server(s) for new messages. If a new message has arrived, it will be copied to the POP3 proxy, scanned and stored into a database on the UTM. The message remains on the POP3 server. When a client tries to fetch new messages, it communicates with the POP3 proxy instead and only retrieves messages from this database.

A POP3 proxy supporting prefetching has a variety of benefits, among others:

- No timeout problems between client and proxy or vice versa.
- Delivery of messages is much faster because emails have been scanned in advance.
- Blocked messages can be released from the User Portal—they will then be included in the next fetch.

If a message was blocked because it contained malicious content or because it was identified as spam, it will not be delivered to the client. Instead, such a message will be sent to the quarantine. A message held in quarantine is stored in the *Mail Manager* section of the User Portal, from where it can be deleted or released.

Use prefetch mode: To enable prefetch mode, select the checkbox and add one or more POP3 servers to the *POP3 Servers* box.

Prefetch interval: Select the time interval at which the POP3 proxy contacts the POP3 server to prefetch messages.

Note – The interval at which mail clients are allowed to connect to the POP3 server may vary from server to server. The prefetch interval should therefore not be set to a shorter interval than allowed by the POP3 server, because otherwise the download of POP3 messages would fail as long as the access to the POP3 server is blocked.
Note further that several mail clients may query the same POP3 account. Whenever messages were successfully fetched from a POP3 server, this will restart the timer until the server can be accessed for the next time. If for that reason the POP3 proxy cannot access a POP3 server four times in a row (default is every 15 minutes), the account password will be deleted from the proxy's mail database and no emails will be fetched until a mail client sends the password to the POP3 server again and successfully logs in.

Delete quarantined mails from server: When you select this option, quarantined messages will be deleted from the POP3 server immediately. This is useful to prevent that users get spam or virus messages when they connect to the POP3 server not via the UTM, but for example via the POP3 server's web portal.

If the email client is configured to delete messages from the server after retrieving them, this information will be stored in the database, too. The next time the proxy is going to prefetch messages for this POP3 account, it will delete the messages from the server. This means, as long as no client fetches the messages from the Sophos UTM *and* no delete command is configured, no message will be deleted from the POP3 server. Therefore, they can still be read, for example, via the web portal of the email provider.
Quarantined messages are deleted from the POP3 server in the following cases:

- Messages are manually deleted via the Mail Manager.
- Messages are manually deleted by the user via the User Portal.

- The message was released (either through the Quarantine Report or the User Portal) and the user's email client is configured to delete messages upon delivery.
- The notification message has been deleted.
- After the storage period has expired (see section *Configuration* in chapter *Mail Manager*).

In prefetch mode however, spam messages in quarantine cannot be deleted from the POP3 server directly by means of a client command.

Note – The email client must successfully connect to the POP3 server at least once for the prefetch function to operate properly. This is because Sophos UTM needs to store the name of the POP3 server, the username, and the user's password in a database in order to fetch POP3 messages on behalf of this user. This, however, *cannot* be achieved by configuring POP3 account credentials in the Sophos User Portal. The POP3 account credentials in the User Portal are needed for prefetched messages to appear in this user's portal and daily Quarantine Report.

Note for fetchmail users: The `TOP` method is not supported to download emails from the mail server for security reasons—messages that are received through `TOP` cannot be scanned. It will work if you specify the `fetchall` option (`-a` on command line). For more information please read "RETR or TOP" in the fetchmail manual.

Preferred Charset

In this section you can select a charset different than UTF-8 that will be used for those mail headers, which have been in some way changed by the UTM (e.g. BATV). This is useful if your users who use mail clients which do not understand UTF-8. Generally the default charset for mail headers works fine for every region. Therefore only change this setting if you are sure this is what you want. If in doubt keep the default *UTF-8*.

TLS Settings

Scan TLS encrypted POP3 traffic: If enabled, the UTM will scan TLS encrypted POP3 traffic. For this to work, TLS certificates have to be defined for the POP3 servers accessed by the POP3 clients (see *POP3 Servers and Prefetch Settings* section above and *TLS certificate* checkbox below).

If disabled, and a POP3 client tries to access a POP3 server via TLS, the connection will not be established.

TLS certificate: Select a certificate from the drop-down list which will be used for TLS encryption with all POP3 clients supporting TLS and trying to access a POP3 server that either is not listed in the *POP3 servers* box above or does not have a matching TLS certificate associated. The selected certificate will be presented to the POP3 client. POP3 clients usually verify that the TLS certificate presented by the POP3 server matches the configured POP3 server name. For this reason, most POP3 clients will display a warning that the certificate's hostname does not match the expected configured POP3 server's name. However, the user can dismiss the warning and connect nevertheless. If you want to avoid this warning, add all used POP3 servers to the *POP3 servers* box above and configure matching TLS certificates for each of them.

If no certificate is selected here, and a POP3 client tries to access a POP3 server via TLS that is not listed in the *POP3 servers* box or does not have a matching TLS certificate associated, the connection will not be established.

Tip – You can create or upload certificates on the *Site-to-site VPN* > *Certificate Management* > *Certificates* tab.

10.4 Encryption

Ever since email became the primary electronic communication medium for personal and business purposes, a legitimate concern over privacy and authentication has arisen. In general terms, the email format is transmitted in clear text, similar to a postcard which anyone could read. Moreover, as assimilating false identities is an easy process, it is important for the recipient to be able to tell if the sender is who they claim to be.

Solutions to these issues are typically accomplished with email encryption and digital certificates, where an email message is electronically signed and cryptographically encoded. This assures that the message recipient exclusively can open and view the contents of the email (privacy), verifying the identity of the sender (authentication). In other words, this process negates the idea of being sent an "e-postcard", and introduces a process much like registered or certified mail.

Modern cryptography has two methods to encrypt email: symmetric and asymmetric. Both have become standard methods and are utilized in several types of applications. Symmetric key cryptography refers to encryption methods in which both, the sender and receiver, share the same key.

On the other hand, asymmetric key cryptography (also known as public key cryptography) is a form of cryptography in which each user has a pair of cryptographic keys; a public key, which encrypts data, and a corresponding private or secret key for decryption. Whereas the public key is freely published, the private key will be securely kept by the user.

One drawback with symmetric encryption is that for a sender and recipient to communicate securely, they must agree upon a key and keep it secret between themselves. If they are in different physical locations, they must prevent the disclosure of the secret key during transmission. Therefore, the persistent problem with symmetric encryption is key distribution: how do I get the key to the recipient without someone intercepting it? Public key cryptography was invented to exactly address this problem. With public key cryptography, users can securely communicate over an insecure channel without having to agree upon a shared key beforehand.

The need for email encryption has produced a variety of public key cryptography standards, most notably S/MIME and OpenPGP, both of which are supported by Sophos UTM. S/MIME (*Secure Multipurpose Internet Mail Extensions*) is a standard for asymmetric encryption and the signing of emails encapsulated in MIME. It is typically used within a public key infrastructure (PKI) and is based on a hierarchical structure of digital certificates, requiring a trusted instance as Certificate Authority (CA). The CA issues a digital certificate by binding an identity to a pair of electronic keys; this can be seen as a digital counterpart to a traditional identity document such as a passport. Technically speaking, the CA issues a certificate binding a public key to a particular *Distinguished Name* in the X.500 standard, or to an *Alternative Name* such as an email address.

A digital certificate makes it possible to verify someone's claim that they have the right to use a given key. The idea is that if someone trusts a CA and can verify that a public key is signed by this CA, then one can also be assured that the public key in question really does belong to the purported owner.

OpenPGP (*Pretty Good Privacy*), on the other hand, uses asymmetric encryption typically employed in a *web of trust* (WOT). This means that public keys are digitally signed by other users who, by that act, endorse the association of that public key with the person.

Note – Although both standards offer similar services, S/MIME and OpenPGP have very different formats. This means that users of one protocol cannot communicate with the users of the other. Furthermore, authentication certificates also cannot be shared.

The entire email encryption is transparent to the user, that is, no additional encryption software is required on the client side. Generally speaking, encryption requires having the destination

party's certificate or public key on store. For incoming and outgoing messages, email encryption functions as follows:

- By default, outgoing messages from internal users will be scanned, automatically signed, and encrypted using the recipient's certificate (S/MIME) or public key (OpenPGP), provided the S/MIME certificate or OpenPGP public key of the recipient is existent on the UTM.
- Encrypted incoming messages from external users whose S/MIME certificate or OpenPGP public key are known to the UTM will automatically be decrypted and scanned for malicious content. To decrypt the message, the S/MIME key or OpenPGP private key of the internal user must be existent on the UTM.
- Encrypted incoming messages from external users or for internal users unknown to the UTM will be delivered, although they cannot be decrypted and therefore not scanned for viruses or spam. It is then the responsibility of the recipient (internal user) to ensure that the email does not contain any malware, for example, by using a personal firewall.
- Outgoing messages already encrypted on the client side will directly be sent to the recipient if the recipient's S/MIME certificate or OpenPGP public key are unknown. However, if the recipient's S/MIME certificate or OpenPGP public key are available, the message will be encrypted a second time. Note that pre-encrypted messages cannot be scanned for malicious content.
- Decryption is only possible for incoming emails, where "incoming" means that the domain name of the sender's email address must not be part of any SMTP profile. For example, to decrypt a message sent by `jdoe@example.com`, the domain `example.com` must *not* be configured in either the routing settings or any SMTP profile.
- A summary of the signing/encryption result is written into the subject line of each email. For example, an email that was correctly signed and encrypted with S/MIME, has " (S/MIME: Signed and encrypted)" appended to the subject line.

Note – Adding a footer to messages already signed or encrypted by an email client (e.g., Microsoft's Outlook or Mozilla's Thunderbird) will break their signature and render them invalid. If you want to create digital signatures on the client side, disable the antivirus check footer option. However, if you do not wish to forgo the privacy and authentication of your email communication and still want to apply a general antivirus check footer, consider using the built-in email encryption feature of Sophos UTM. Email encryption done on the gateway means that the footer is added to the message prior to creating the digital signature, thus leaving the signature intact.

10.4.1 Global

On the *Email Protection* > *Encryption* > *Global* tab you can configure the basic settings of the email encryption functionality.

Note – Encryption is only working for SMTP, not for POP3.

Before you can use email encryption, you must first create a *Certificate Authority* (CA) consisting of a CA certificate and CA key. The CA certificate can be downloaded and stored locally. In addition, it can be installed as an external CA (S/MIME Authority) in other units as illustrated in the diagram to enable transparent email encryption between two Sophos UTM units.

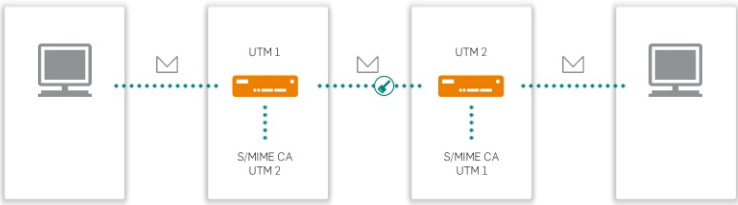

Figure 20 Email Encryption: Using Two Sophos UTM Units

To configure email encryption, proceed as follows:

1. **On the *Global* tab, enable email encryption.**
   Click the toggle switch.

   The toggle switch turns amber and the *Email Encryption Certificate Authority (CA)* area becomes editable.

2. **Create a certificate authority (CA).**
   Fill out the form in the *Email Encryption Certificate Authority (CA)* area. By default, the form is filled out with the values of the *Management* > *System Settings* > *Organizational* tab.

3. **Click *Save*.**
   The toggle switch turns green and the following certificates and keys are being created:

   - S/MIME CA Certificate
   - OpenPGP Postmaster Key

Note that this may take several minutes to complete. If you do not see the fingerprints of the S/MIME CA certificate or the OpenPGP Postmaster key, click the *Reload* button in the upper right corner of WebAdmin. The certificate and the key can be downloaded and locally stored.

Use the *Reset Email Encryption System Now* button to reset all settings in the *Encryption* menu to the factory default configuration.

10.4.2 Options

On the *Encryption* > *Options* tab you can define the default policy to be used within the public key cryptography framework of Sophos UTM.

Default Policy: Specify your default policy for emails in terms of cryptography. These settings can, however, be overwritten by customized settings.

The following actions are available:

- Sign outgoing email
- Encrypt outgoing email
- Verify incoming email
- Decrypt incoming email

Click *Apply* to save your settings.

Note – For encryption to work, the sender must be within the *Internal Users* list. Outgoing emails for recipients whose S/MIME certificate or OpenPGP public key are existent on the gateway will be encrypted by default. If you want to disable encryption for these recipients, delete their S/MIME certificates or OpenPGP public keys. If certificates or public keys are unknown to the UTM, emails will be sent unencrypted.

Automatic Extraction of S/MIME Certificates

When this option is selected, S/MIME certificates will automatically be extracted from incoming emails provided the certificate that is appended to the email is signed by a trusted certificate authority, that is, a CA present on the unit as shown on the *Email Protection* > *Encryption* > *S/MIME Authorities* tab. In addition, the time and date of Sophos UTM must be within the certificate's validity period for the automatic extraction of certificates to work. Once a certificate has been successfully extracted, it will appear on the *Email Protection* > *Encryption* > *S/MIME*

Certificates tab. Note that this may take five to ten minutes to complete. Click *Apply* to save your settings.

OpenPGP Keyserver

OpenPGP keyserver host public PGP keys. You can add an OpenPGP keyserver here. For signed incoming emails and for outgoing emails that shall be encrypted, the UTM will try to retrieve the public key from the given server if the respective public key is yet unknown to the UTM.

10.4.3 Internal Users

For signing and decrypting messages, either the S/MIME key or the OpenPGP private key must be existent on the UTM. On the *Encryption* > *Internal Users* tab you can create both an individual S/MIME key/certificate and/or OpenPGP key pair for those users for whom email encryption should be enabled.

To create an internal email user, proceed as follows:

1. **On the *Internal Users* tab, click *New Email Encryption User*.**
   The *Create New User* dialog box opens.
2. **Make the following settings:**
   Email address: Enter the email address of the user.

   Full name: Enter the name of the user.

   Signing: The following signing options are available:

   - Use default policy: The policy from the *Options* tab will be used.
   - On: Emails will be signed using the certificate of the user.
   - Off: Emails will not be signed.

   Encryption: The following encryption options are available:

   - Use default policy: The policy from the *Options* tab will be used.
   - On: Emails will be encrypted using the public key of the recipient.
   - Off: Emails will not be encrypted.

   Verifying: The following verification options are available:

- Use default policy: The policy from the *Options* tab will be used.
- On: Emails will be verified using the public key of the sender.
- Off: Emails will not be verified.

Decryption: The following decryption options are available:

- Use default policy: The policy from the *Options* tab will be used.
- On: Emails will be decrypted using the certificate of the user.
- Off: Emails will not be decrypted.

S/MIME: Select whether you want to have the S/MIME certificate and key automatically generated by the system or whether you want to upload a certificate in `PKCS#12` format. When uploading the certificate, you must know the passphrase the `PKCS#12` file was protected with. Note that the `PKCS#12` file must both contain the S/MIME key and certificate. Any CA certificate that may be included in this `PKCS#12` file will be ignored.

OpenPGP: Select whether you want to have the OpenPGP key pair consisting of a private key and the public key automatically generated by the system or whether you want to upload the key pair in `ASCII` format. Note that both private and public key must be included in one single file and that the file must not contain a passphrase.

Note – If you configure both S/MIME and OpenPGP for an individual user, emails sent by this user will be signed using S/MIME.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new user appears on the *Internal Users* list.

Use the toggle switch to turn the usage of one or both keys off without having to delete the key (s).

Note – For security reasons, the files offered for download only contain the S/MIME certificate and the OpenPGP public key, respectively. The S/MIME key and the OpenPGP private key cannot be downloaded from the system.

10.4.4 S/MIME Authorities

On the *Encryption* > *S/MIME Authorities* tab you can manage certificate authorities (CA) for email encryption. In addition to pre-installed CAs, you can upload certificates of external certificate authorities. All incoming emails whose certificates are signed by one of the CAs listed and enabled here will be trusted automatically.

Note – If you have selected the *Enable automatic S/MIME certificate extraction* option on the *Email Protection* > *Encryption* > *Options* tab, certificates signed by a CA listed and enabled here will be extracted automatically and placed on the *Email Protection* > *Encryption* > *S/MIME Certificates* tab.

Local S/MIME Authorities

You can import the certificate (i.e., the public key) of an external certification authority you trust. That way, all incoming emails whose certificates were signed by this CA will be trusted, too. For example, you can install the CA of another Sophos UTM unit, thus enabling transparent email encryption between two Sophos UTM units.

To import an external S/MIME authority certificate, proceed as follows:

1. **Click the Folder icon next to the *Upload local authority* field.**
   The *Upload File* dialog window opens.
2. **Select the certificate to upload.**
   Click *Browse* and select the CA certificate to upload. The following certificate extensions are supported:
   - `cer`, `crt`, or `der`: These certificate types are binary and basically the same.
   - `pem`: Base64 encoded DER certificates.
3. **Upload the certificate.**
   Click *Start Upload* to upload the selected CA certificate.

   The certificate will be installed and displayed in the *Local S/MIME Authorities* area.

You can delete or disable an S/MIME authority certificate if you do not regard the CA as trustworthy. To revoke an S/MIME authority's certificate click its toggle switch. The toggle switch turns gray and the SMTP proxy will no longer accept mails signed by this S/MIME authority. To delete a certificate, click the Empty icon.

Tip – Click the blue Info icon to see the fingerprint of a CA.

Global S/MIME Authorities

The list of S/MIME CAs shown here is identical to the S/MIME CAs pre-installed by Mozilla Firefox. This facilitates email encryption between your company and your communication partners who maintain a PKI based on those CAs. However, you can disable an S/MIME authority certificate if you do not regard the CA as trustworthy. To revoke an S/MIME authority's certificate click its toggle switch. The toggle switch turns gray and the SMTP proxy will no longer accept mails signed by this S/MIME authority.

The following links point to URLs of notable root certificates:

- Trustcenter
- S-TRUST
- Thawte
- VeriSign
- GeoTrust

10.4.5 S/MIME Certificates

On the *Encryption* > *S/MIME Certificates* tab, you can import external S/MIME certificates. Emails for recipients whose certificates are listed here will automatically be encrypted. If you want to disable encryption for a particular recipient, simply delete its certificate from the list.

Note – If for a recipient an OpenPGP public key is imported additionally to an S/MIME certificate, emails will be encrypted using OpenPGP.

Note – When you upload an S/MIME certificate manually, messages from the email address associated with the certificate are always trusted, although no CA certificate is available that may identify the person noted in the certificate. That is to say, manually uploading an S/MIME certificate labels the source as trusted.

To import an external S/MIME certificate, proceed as follows:

1. **On the *S/MIME Certificates* tab, click *New External S/MIME Certificate*.**
   The *Add S/MIME Certificate* dialog box opens.

2. **Make the following settings:**
   Format: Select the format of the certificate. You can choose between the following formats:

   - `der` (binary)
   - `pem` (ASCII)

   Note – Microsoft Windows operating systems use the `cer` file extension for both `der` and `pem` formats. You must therefore determine in advance whether the certificate you are about to upload is in binary or ASCII format. Then select the format from the drop-down list accordingly.

   Certificate: Click the Folder icon to open the *Upload File* dialog window. Select the file and click *Start Upload*.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new S/MIME certificate appears on the *S/MIME Certificates* list.

10.4.6 OpenPGP Public Keys

On the *Encryption* > *OpenPGP Public Keys* tab you can install OpenPGP public keys. Files must be provided in `.asc` format. The upload of entire keyrings is supported.

Note – Do not upload a keyring that is protected by a passphrase.

All public keys included in the keyring will be imported and can be used to encrypt messages. Emails for recipients whose public keys are listed here will automatically be encrypted. If you want to disable encryption for a particular recipient, simply delete its public key from the list.

Note – Only one email address per key is supported. If there are multiple addresses attached to a key, only the "first" one will be used (the order may depend on how OpenPGP sorts addresses). If the key you want to import has several addresses attached, you must remove the unneeded addresses with OpenPGP or other tools prior to importing the key into Sophos UTM.

To import an OpenPGP public key, proceed as follows:

1. **On the *OpenPGP Public Keys* tab, click *Import Keyring File*.**
   The *Import OpenPGP Keyring File* dialog box opens.
2. **Upload the OpenPGP key(s).**
   Click the Folder icon to open the *Upload File* dialog window. Select the file and click *Start Upload*.

   The key or, if the file contains several keys, a list of keys is displayed.
3. **Select one or more keys and click *Import Selected Keys*.**
   The key(s) appear(s) on the *OpenPGP Public Keys* list.

Note – An email address must be attached to the key. Otherwise the installation will fail.

10.5 SPX Encryption

SPX (Secure PDF Exchange) encryption is a next-generation version of email encryption. It is clientless and extremely easy to set up and customize in any environment. Using SPX encryption, unencrypted email messages and any attachments sent to the UTM are converted to a PDF document, which is then encrypted with a password. You can configure the UTM to allow senders to select passwords for the recipients, or the server can generate the password for the recipient and store it for that recipient, or the server can generate one-time passwords for recipients.

When SPX encryption is enabled, there are two ways how emails can be SPX encrypted:

- The Administrator can download a Microsoft Outlook plugin (see chapter *Email Protection > SPX Encryption > Sophos Outlook Add-in*). After having it installed, an *Encrypt* button is displayed in the Microsoft Outlook user interface. To encrypt a single message, the user needs to enable the *Encrypt* button and then write and send the message. Only if something goes wrong, for example the sender does not enter a valid password, a notification will be sent, if configured.

  Note – If you are not using Outlook you can also trigger SPX encryption by setting the header field X-Sophos-SPX-Encrypt to *yes*.

- In the Data Protection feature, you can specify to automatically SPX encrypt emails containing sensitive data (see *SMTP > Data Protection* tab).

The encrypted message is then sent to the recipient's mail server. Using Adobe Reader, the recipient can decrypt the message with the password that was used to encrypt the PDF. SPX-encrypted email messages are accessible on all popular smartphone platforms that have native or third-party PDF file support, including Blackberry and Windows Mobile devices.

Using the SPX reply portal, the recipient is able to answer the email in a secure way. It is possible to set expiry times for the secure reply and unused passwords (see chapter *Email Protection > SPX Encryption > SPX Configuration*).

SPX encryption can be activated in both SMTP configuration modes, Simple Mode and Profile Mode. If using Simple mode, a global SPX template can be chosen. The SPX template defines the layout of the PDF file, password settings, recipient instructions, and SPX reply portal settings. If using Profile mode, you can define different SPX templates for different SMTP profiles. So, if you are managing various customer domains, you can assign them customized SPX templates containing for example different company logos and texts.

10.5.1 SPX Configuration

On the *SPX Encryption > SPX Configuration* tab you enable SPX encryption, and you configure general settings for all SMTP users.

To configure SPX encryption, proceed as follows:

1. **Enable SPX encryption.**
   Click the toggle switch.

   The toggle switch turns green.
2. **In the following sections of this tab, make the required global settings.**
3. **On the *SPX Templates* tab, modify the existing Sophos Default Template and/or add new SPX templates.**
4. **On the *SMTP > Global* tab, select the Global SPX Template.**
5. **Optionally, if using SMTP Profile Mode, select the desired SPX templates for the respective SMTP profiles.**
6. **If you want the users to SPX encrypt email messages via the Microsoft Outlook plugin, make sure that they have access to the *Email Protection > SPX Encryption > Sophos Outlook Add-in* tab. If you use another email messenger you have to set the Header manually by yourself.**

SPX Password Settings

Minimum length: The minimum number of characters allowed for a password specified by the sender.

Require special characters: If enabled, the password specified by the sender has to contain at least one special character (non alphanumeric characters and whitespace are treated like special characters).

Click *Apply* to save your settings.

SPX Password Reset

Reset password for: Here you can delete the password of a recipient. Enter the recipient's email address and click *Apply*.

SPX Portal Settings

Interface used for SPX reply portal: Select the interface that provides the SPX reply portal. This web interface allows recipients of SPX encrypted messages to securely reply to the sender. In many configurations this would be the external interface.

Port: Enter the port on which the SPX reply portal should listen.

Click *Apply* to save your settings.

SPX Portal and Password Expiry Settings

Allow secure reply for: Specify for how long the recipient of an SPX encrypted message is allowed to send a reply via the SPX reply portal.

Keep unused password for: Specify the expiry time of a password that was not used meanwhile.

Note – If for example the *Keep Unused Password* is set to 3 days the password will expire at 0 o'clock if there was no SPX encrypted message sent for a specific recipient.

Note – If the *Keep Unused Password* option is set to 0 days, the password will be saved and expires at 0 o'clock.

Click *Apply* to save your settings.

SPX Notification Settings

Send notification on error to: Specify whom to send a notification when an SPX error occurs. You can send the notification to the administrator, to the sender, or to both, or you can send no notification at all. Error messages will always be listed in the SMTP log.

Tip – SPX error messages can be customized on the *Management* > *Customization* > *Email Messages* tab.

Click *Apply* to save your settings.

10.5.2 SPX Templates

On the *SPX Encryption* > *SPX Templates* tab you can modify the existing Default SophosTemplate, and you can define new SPX templates. If using SMTP Simple mode, a global SPX template can be selected for all SMTP users on the *SMTP* > *Global* tab. If using SMTP Profile mode, you can assign different SPX templates to different SMTP profiles on the *SMTP Profiles* tab.

To configure SPX encryption, proceed as follows:

1. **Click *New Template*.**
   The *Create SPX Template* dialog box opens.

   Tip – The Sophos Default Template contains useful settings and example texts. Therefore you should consider to clone the existing template using its *Clone* button instead of creating a new template from scratch.

   Note – The notification sender is the mail address which is configured in *Management* > *Notifications* > *Sender*.

2. **Make the following settings:**
   Template name: Enter a descriptive name for the template.
3. **Make the following basic settings:**
   Comment (optional): Add a description or other information.

   Organization Name: The organization name will be displayed on notifications concerning SPX, sent to the administrator or the email sender, depending on your settings.

PDF Cover Page: Select if you want the encrypted PDF file to have an additional first page. You can use the default page or a custom page. In case of the custom page, upload a one page PDF file via the Folder icon.

PDF Encryption: Select the encryption mode of the PDF file. Note that some PDF viewers cannot read AES / 256 encrypted PDF files.

Label Languages: Select the display language of the labels in the email forwarded to the recipient. The email contains fields such as *From*, *To*, *Sender*, or *Subject*, for example.

Page Size: Select the page size of the PDF file.

Remove Sophos Logos: Enable this option to replace the default Sophos logo with your company logo specified on the *Management* > *Customization* > *General* tab. The logo will be displayed in two places: on the footer of the encryption email sent to the recipient and in the footer of the reply message generated via the *Reply* button in the PDF file.

4. **Make the following password settings:**
Password Type: Select how you want to generate the password for accessing the encrypted email message. No matter which type you select, the sender always has to take care of transferring the password in a safe way to the recipient.

   - **Specified by Sender:** Select if the email sender should generate the password himself. In this case, the sender has to enter the password into the *Subject* field, using the following format: `[secure:<password>]<subject text>` where `<password>` is the password to open the encrypted PDF file and `<subject text>` is the random subject. Of course, the password will be removed by the UTM before the email is sent to the recipient.

     Note – A template with this option should not be used in combination with Data Protection. With Data Protection, the sender does not know beforehand that an email will be encrypted and thus will not enter the password into the *Subject* field. When the UTM tries to SPX encrypt an email with no password specified, the sender will receive an error message with the information that the password is missing.

   - **Generated and Stored for Recipient:** The UTM automatically creates a recipient-specific password when the first email is sent to a recipient. This password will be sent to the sender. With the next email, the same password is used

automatically. The password will expire when it is not used for a certain time, and it can be reset by the administrator, see the *SPX Configuration* tab.

- **Generated one-time Password for every Email:** The UTM automatically creates a new password for each affected email. This password will be sent to the sender.

Notification Subject (not with the *Specified by sender* option): The subject of the email that is sent from the UTM to the email sender containing the password. Here you can use variables, e.g. `%%ENVELOPE_TO%%`, for the recipient's name.

Notification Body (not with the *Specified by sender* option): The body of the email that is sent from the UTM to the email sender containing the password. Here you can use variables, e.g., `%%GENERATED_PASSWORD%%`, for the password.

Tip – The Sophos Default SPX Template on this tab contains all available variables and gives a useful example of a notification.

5. **Make the following recipient instructions settings:**
Instructions for Recipient: The body of the email that is sent from the UTM to the email recipient containing instructions concerning the encrypted email. Simple HTML markup and hyperlinks are allowed. You can also use variables, e.g., `%%ORGANIZATION_NAME%%`.

Tip – The Sophos Default SPX Template on this tab contains all available variables and gives a useful example of recipient instructions.

Header Image/Footer Image: Select if the email from the UTM to the email recipient should have a header and/or a footer image. You can use the default image, which is an orange envelope with an appropriate text, or a custom image. In case of the custom image, upload a JPG, GIF, or PNG file via the Folder icon. The recommended size is 752 x 69 pixels.

6. **Make the following SPX portal settings:**
Enable SPX Reply Portal: If enabled, the encrypted PDF file sent to the recipient will contain a *Reply* button. With this button the recipient can access the SPX reply portal to send an encrypted email reply to the sender.

Include Original Body into Reply: If enabled, the reply from the recipient will automatically contain the body of the original email.

Portal header image/Portal footer image: Select if the SPX reply portal should have a header and/or a footer image. You can use the default image, which is an orange envelope with an appropriate text, or a custom image. In case of the custom image, upload a JPG, GIF, or PNG file via the Folder icon. The recommended size is 752 x 69 pixels.

7. **Click *Save*.**
   The SPX template will be created and appears on the *SPX Templates* list.

To either edit or delete an SPX template, click the corresponding buttons.

10.5.3 Sophos Outlook Add-in

On the *Email Protection* > *SPX Encryption* > *Sophos Outlook Add-in* tab you can navigate to the Sophos website and with your MySophos credentials you are able to download the Sophos Outlook Add-in.

The Outlook Add-in simplifies the encryption of messages which contain sensitive or confidential information leaving your organization. For downloading and for the installing documentation visit the Sophos website.

Run the installer with the parameters: msiexec /qr /i SophosOutlookAddInSetup.msi T=1 EC=3 C=1 I=1

10.6 Quarantine Report

Sophos UTM features an email quarantine containing all messages (SMTP and POP3) that have been blocked and redirected to the quarantine for various reasons. This includes messages waiting for delivery as well as messages that are infected by malicious software, contain suspicious attachments, are identified as spam, or simply contain unwanted expressions.

To minimize the risk of messages being withheld that were quarantined mistakenly (so-called *false positives*), Sophos UTM sends a daily Quarantine Report to the users informing them of messages in their quarantine. If users have several email addresses configured, they will get an individual Quarantine Report for each email address. This also applies if a user has additional POP3 accounts configured in his User Portal, provided the POP3 proxy of Sophos UTM is in *prefetch* mode, which allows the prefetching of messages from a POP3 server and storing them

in a local database. In a Quarantine Report a user can click on any spam entry to release the message from the quarantine or to whitelist the sender for the future.

The following list contains some more information about the Quarantine Report:

- Quarantine Reports are only sent to those users whose email address is part of a domain contained in any SMTP profile. This includes the specification in the *Domains* box on the *SMTP* > *Routing* tab as well as the specifications in the *Domains* box of any SMTP Profile.
- If the POP3 *prefetch* option is disabled, quarantined messages sent to this account will not appear in the Quarantine Report. Instead, each user will find the typical Sophos POP3 blocked message in his inbox. It is therefore not possible to release the message by means of the Quarantine Report or the User Portal. The only way to deliver such an email is to download it in `zip` format from the Mail Manager by the administrator.
- On the *Advanced* tab, the administrator defines which types of quarantined mail can be released by the users. By default, only spam emails can be released from the quarantine. Messages quarantined for other reasons, for example because they contain viruses or suspicious file attachments, can only be released from the quarantine by the administrator in the Mail Manager of Sophos UTM. In addition, users can also review all of their messages currently held in quarantine in the Sophos User Portal.
- If a spam email has multiple recipients, as is the case with mailing lists, when any one recipient releases the email, it is released for that recipient only, provided the email address of the mailing list is configured on the system. Otherwise the email will be sent to all recipients simultaneously. For more information, see the *Define internal mailing lists* option on the *Email Protection* > *Quarantine Report* > *Exceptions* tab.
- Emails sent to an SMTP email address for which no user is configured in Sophos UTM can be released (but not whitelisted) from the Quarantine Report or in the Mail Manager by the administrator. However, as this user is not configured, no access to the User Portal is possible.
- Spam emails sent to mailing lists cannot be whitelisted.
- Some email clients do not encode the header of an email correctly, which may result in an awkward representation of the email in the daily Quarantine Report.

10.6.1 Global

On the *Quarantine Report* > *Global* tab you can define at what time the daily Quarantine Report shall be sent and write a message text that will appear in the Quarantine Reports.

To edit the Quarantine Report settings, enable the Quarantine Report: Click the toggle switch. The toggle switch turns green.

Time to Send Report

Here you can define when the daily Quarantine Report will be sent. Select the time using the drop-down lists and click *Apply*.
You can also send an additional report. For this, select the checkbox *Send Additional Report*, set the time, and click *Apply*.

Customizable Message Text

Here you can customize the text which forms the introduction of the Quarantine Report. Change the message text according to your needs and click *Apply*.

Note – It is not possible to use HTML tags in the customizable message text box.

Note – Customization is not possible when using a home use license.

Note– The notification sender is the mail address which is configured in *Management* > *Notifications* > *Sender*.

10.6.2 Exceptions

On the *Quarantine Report* > *Exception* tab you can define a skiplist of email addresses that should be exempt from receiving daily Quarantine Reports.

Skipping Quarantine Reports

Here you can configure internal email addresses for which no quarantine notifications should be sent. Users whose email addresses are listed here will not receive daily Quarantine Reports. You can enter full email addresses or use an asterisk (*) as wildcard, for example `*@example.com`.

Note – The skiplist only applies for the SMTP Quarantine Report. If there is a POP3 account specified for the respective user, the POP3 Quarantine Report will be sent nonetheless.

Define Internal Mailing Lists

If the email address of a mailing list is configured in the *Mailing list address patterns* box (e.g., `newsletter@example.com`) and a spam message sent to this mailing list was detected and redirected to the email quarantine, the Quarantine Report of all recipients included in this

mailing list will contain a link to this spam message. Thus, each recipient can release this spam message individually by entering his email address in a user prompt that appears once the recipient has clicked the *Release* link in the Quarantine Report.

Note – Mailing lists cannot be whitelisted in the Quarantine Report or the User Portal.

Alternatively, you could enter the email address of that particular mailing list as an additional email address in a local user's profile; this user becoming some sort of a mail manager. Then only this user's Quarantine Report will contain a link to the spam message that was sent to the mailing list. Clicking the *Release* link will deliver the spam message to all recipients of that mailing list at once.

Note – If the email address of a mailing list is configured as an additional email address in a user's profile, no recipient included in that mailing list gets displayed the links to spam messages that were sent to this mailing list.

However, if the email address of a mailing list is both configured as an additional email address in a user's profile and in the *Mailing list address patterns* box, then the *Release* link in that user's Quarantine Report will open a user prompt. The user is then to decide who is going to receive the spam mail by manually entering the respective email address(es) to forward the spam message to.

Finally, if the email address of a mailing list is neither configured as an additional email address in a user's profile nor as a mailing list address pattern, a spam message sent to the mailing list is handled like a normal email, meaning that if any one recipient releases the spam mail, it will be sent to all recipients of the mailing list.

To sum up, whenever the email address of a mailing list is configured as a mailing list address pattern, each user having a link to the spam message in his Quarantine Report is prompted to enter an email address to release the spam message to.

10.6.3 Advanced

On the *Quarantine Report > Advanced* tab you can configure an alternative hostname and port number for the *Release* links contained in daily Quarantine Reports. Additionally, you can change the release options for spam emails.

Advanced Quarantine Report Options

Hostname: By default, this is the gateway's hostname as given on the *Management > System Settings > Hostname* tab. The quarantine report, for example, which is sent by the gateway, contains hyperlinks a user can click to release messages from the email quarantine. By default, these links point to the hostname specified here. If you want to enable users to release their emails from across the Internet, it might be necessary to enter an alternative hostname here that can be publicly resolved.

Port: By default, port `3840` is configured. You can change the port to any value in the range from `1024` to `65535`.

Allowed networks: You can also specify the networks that should be allowed to connect to the email release service. By default, only the internal network is selected.

Click *Apply* to save your settings.

Release Options

Here you can select which types of quarantined messages shall be releasable by users. You can choose between the following options:

- Malware
- Spam
- Expression
- File extension
- Unscannable
- MIME type
- Other

Click *Apply* to save your settings.

10.7 Mail Manager

The Mail Manager is an administrative tool to manage and organize all email messages currently stored on the unit. This includes messages waiting for delivery as well as quarantined messages that are infected by malicious software, contain suspicious attachments, are identified as

spam, or contain unwanted expressions. You can use the Mail Manager to review all messages before downloading, releasing, or deleting them. The Mail Manager is fully UTF-8 capable.

10.7.1 Mail Manager Window

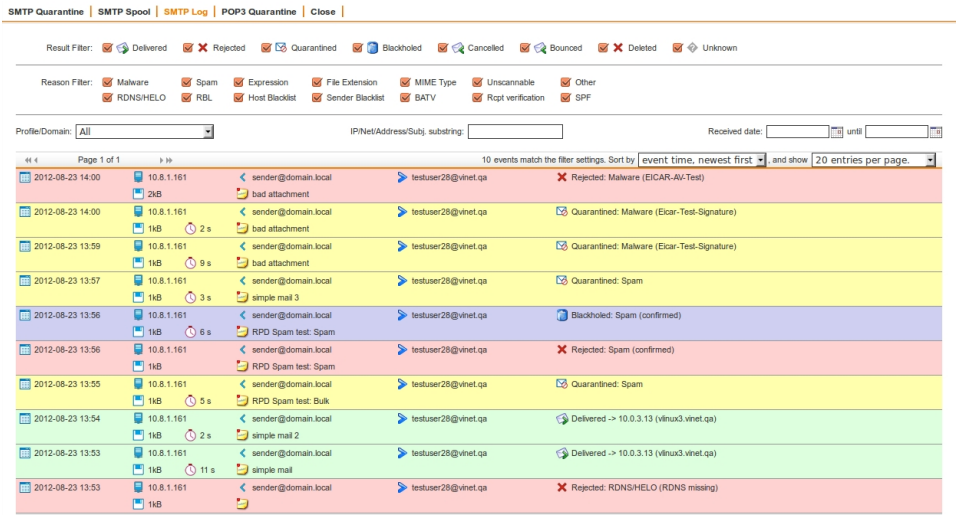

Figure 21 Mail Manager of Sophos UTM

To open the Mail Manager window click the button *Open Mail Manager in New Window* on the *Email Protection* > *Mail Manager* > *Global* tab. The Mail Manager is divided into five different tabs:

- **SMTP Quarantine:** Displays all messages that are currently quarantined.
- **SMTP Spool:** Displays all messages currently in `/var/spool`. This may be due to them waiting for delivery or because of an error.
- **SMTP Log:** Displays the delivery log for all messages processed via SMTP.
- **POP3 Quarantine:** Displays all messages fetched via POP3 that are currently quarantined.
- **Close:** Click here to close the Mail Manager window.

10.7.1.1 SMTP/POP3 Quarantine

Messages in SMTP and POP3 Quarantine can be displayed according to their respective quarantine cause:

- Malware
- Spam
- Expression
- File Extension
- MIME Type (SMTP only)
- Unscannable
- Other

Use the checkboxes to select/unselect quarantine causes. Double-click the checkbox of a cause to solely select this cause.

Tip – Double-click a message to view it.

Profile/Domain: Select a profile/domain to show its messages only.

Sender/Rcpt/Subject substring: Here you can enter a sender, recipient, or subject to search for in the messages.

Received date: To only show messages processed during a certain time frame, enter a date, or select a date from the calendar icon.

Sort by: By default, the list is sorted by time of arrival. Messages can be sorted by date, subject line, sender address, and message size.

and show: The checkbox allows to display 20, 50, 100, 250, 500, 1000, or all messages per page. Note that showing all messages may take a lot of time.

Use the checkbox in front of each message or click a message to select it to apply actions on the selected messages. The following actions are available:

- **View** (only available for an individual message): Opens a window with the contents of the email.
- **Download:** Selected messages will be downloaded.

- **Delete:** Selected messages will be deleted irrevocably.
- **Release:** Selected messages will be released from quarantine.
- **Release and report as false positive:** Selected messages will be released from quarantine and reported as false positive to the spam scan engine.

Note that only the administrator can release *all* messages held in quarantine. Users reviewing their messages in the Sophos User Portal can only release messages they are explicitly allowed to. The authorization settings for this can be found on the *Email Protection* > *Quarantine Report* > *Advanced* tab.

Select global cleanup action: Here you find several deletion options that will be applied on messages globally, that is, regardless whether they are selected and/or displayed or not.

Caution – Deleted messages are irrevocable.

10.7.1.2 SMTP Spool

Here you see messages that are either waiting for delivery or have produced an error. The delivery log is also part of the message header. Use the following checkboxes to select only one type of messages for display:

- **Waiting:** Messages waiting for delivery.
- **Error:** Messages that caused an error. If a messages produces an error more than once, please report the case to your Sophos Partner or the Sophos Support Team.

Hint – Double-click a message to view it.

Profile/Domain: Select a profile/domain to show its messages only.

Sender/Rcpt/Subject substring: Here you can enter a sender, recipient, or subject to search for in the messages.

Received date: To only show messages processed during a certain time frame, enter a date, or select a date from the calendar icon.

Sort by: By default, the list is sorted by time of arrival. Messages can be sorted by date, subject line, sender address, and message size.

and show: The checkbox allows to display 20, 50, 100, 250, 500, 1000, or all messages per page. Note that showing all messages may take a lot of time.

Use the checkbox in front of each message or click a message to select it to apply actions on the selected messages. The following actions are available:

- **Download:** Selected messages will be downloaded.
- **Retry:** For selected messages delivery will be retried immediately.
- **Delete:** Selected messages will be deleted irrevocably.
- **Bounce:** Selected messages will be bounced, that is the sender will receive a message that the delivery of their message has been canceled.

Select Global Cleanup Action: Here you find a retry option and several deletion options that will be applied on messages globally, that is, regardless whether they are selected and/or displayed or not.

Caution – Deleted messages are irrevocable.

10.7.1.3 SMTP Log

The *SMTP Log* displays the log messages for all messages processed via SMTP.

Result Filter: Select which type of message will be displayed by selecting the corresponding checkboxes.

- **Delivered:** Successfully delivered messages.
- **Rejected:** Messages rejected by the UTM.
- **Quarantined:** Quarantined messages.
- **Blackholed:** Messages that have been deleted without notification.
- **Canceled:** Messages that have been manually bounced in *SMTP Spool*.
- **Bounced:** Messages that could not be delivered, for example because of false routing settings.
- **Deleted:** Messages that have been manually deleted.
- **Unknown:** Messages whose status is unknown.

Use the checkboxes to select/unselect *Result Filter* items. Double-click an item to solely select this item.

Reason Filter: Use the checkboxes to further filter the message log display.

Note – Double-click a message log to view it. Click on the server icon of a message to resolve the IP address. An asterisk (*) denotes a successful reverse DNS lookup.

Profile/Domain: Select a profile/domain to show its messages only.

IP/Net/Address/Subj. Substring: Here you can enter an IP address, network address, or subject to search for in the SMTP log messages.

Received Date: To only show messages processed during a certain time frame, enter a date, or select a date from the calendar icon.

Sort by: By default, the list is sorted by event time. Messages can be sorted by event time, sender address, and message size.

and show: The checkbox allows to display 20, 50, 100, 250, 500, 1000, or all messages per page. Note that showing all messages may take a lot of time.

10.7.2 Global

In the upper part of the *Mail Manager* > *Global* tab you can open the Mail Manager by clicking the *Open Mail Manager in New Window* button.

In the lower part, the *Statistics Overview* area provides an overview of all messages currently stored on the unit. Data is divided into messages that were delivered via the SMTP or POP3 protocol. For both types, the following information is displayed:

- **Waiting for Delivery (Spooled)** (SMTP only): Mails that are currently in spool, for example because they were being scanned and could not be delivered yet.
- **Clean total** (POP3 only): Mails that have been prefetched by the unit and have not yet been collected by a client/user.
- **Quarantined Malware:** The total of messages that contain malware, such as viruses or other harmful content.
- **Quarantined Spam:** The total of messages that were identified as spam.
- **Quarantined Expression:** The total of messages that were diverted to the quarantine because they contain forbidden expressions.
- **Quarantined File Extension:** The total of messages held in quarantine because they contain suspicious attachments (identified by their file extension).

- **Quarantined Unscannable:** The total of messages held in quarantine because it could not be scanned.
- **Quarantined MIME Type** (SMTP only): The total of messages held in quarantine because they contain MIME types that are to be filtered according to the SMTP settings.
- **Quarantined Total:** The total of messages that are held in quarantine.

Note – The numbers for *Waiting for Delivery* represent a real-time snapshot for SMTP messages. However, for POP3 messages, the numbers presented are the accumulation of data since the last time prefetching was enabled.

Below you see a short statistic for SMTP quarantining and rejections of the last 24 hours:

- **Malware Quarantined/Rejected:** Messages quarantined/rejected because they contain harmful content.
- **Spam Quarantined/Rejected:** Messages quarantined/rejected because they have been identified as spam.
- **Blacklist Rejects:** Messages rejected because the sender is on a blacklist.
- **Address Verification Rejects:** Messages rejected because the sender address could not be verified.
- **SPF Rejects:** Messages rejected because sending host is not allowed.
- **RBL Rejects:** Messages rejected because the sender is on a real time blackhole list.
- **BATV Rejects:** Messages rejected because BATV tag could not be validated.
- **RDNS/HELO Rejects:** Messages rejected due to invalid HELO or missing RDNS entries.

Whether there are any rejects depends on your settings in *Email Protection > SMTP*.

10.7.3 Configuration

On the *Mail Manager > Configuration* tab you can configure how long the database log will be kept and after how many days quarantined messages are to be deleted from the quarantine. Any logs and messages that are older than the number of days in the expiration settings will be deleted automatically.

The default settings are as follows:

- Database log will be deleted after three days. Maximum number permitted: 30 days.
- Quarantined messages will be deleted after 14 days. Maximum number permitted: 999 days.

The minimum number of days permitted for both database log and quarantine is one day.

Flush Database Log

This option is useful if your database log has accumulated an immense amount of data to clear the log immediately. That way you do not have to wait for the normal cleanup action to apply.

11 Endpoint Protection

The *Endpoint Protection* menu allows you to manage the protection of endpoint devices in your network, e.g. desktop computers, servers, and laptops. UTM is the configuration side of endpoint protection where you deploy the software for endpoints, get an overview of the protected endpoints, set up antivirus and device control policies, group endpoints, and assign the defined policies to endpoint groups.

Endpoint protection uses a central service called Sophos LiveConnect. This cloud-based service is automatically set up for the use with your UTM once you enable endpoint protection. LiveConnect allows you to always manage all of your endpoints, whether they are on your local network, at remote sites, or with traveling users. The LiveConnect service provides:

- A pre-configured installation package for the endpoint agent
- Policy deployment & updates for endpoints
- Security updates and definitions for endpoints
- Central logging & reporting data to monitor endpoints centrally through WebAdmin

As LiveConnect is a cloud-based service you will need an active Internet connection in order for the service to work. Managed endpoints will need an Internet connection to receive policy and security updates, too.

The figure below shows a deployment example of Sophos UTM Endpoint Protection with the use of the LiveConnect Service.

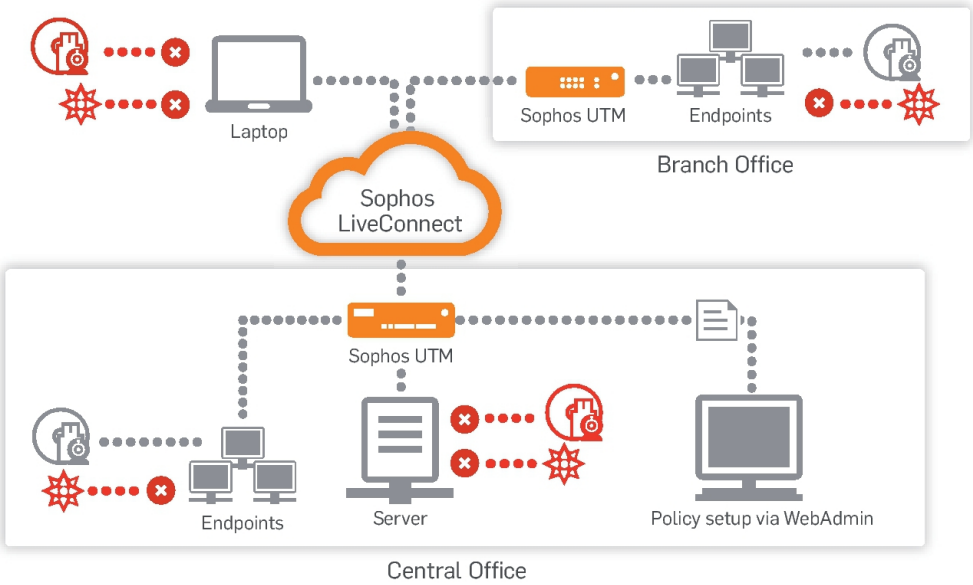

Figure 22 Endpoint Protection: Overview

The following topics are included in this chapter:

- Computer Management
- Antivirus
- Device Control

If endpoint protection is enabled, the overview page gives you general information on registered computers and their status. You can sort and search this list. If the status of an endpoint is not *Ok*, you can click on the status to open a window with more information. The status *Not Compliant* indicates that the device's settings are currently not the same as configured on the UTM. To resolve this problem you find a link in the window to send the current endpoint settings to the endpoint. For the other statuses you can acknowledge the information and decide what actions have to be taken.

Open Endpoint Protection Live Log

The endpoint protection live log gives you information about the connection between the endpoints, LiveConnect, and the UTM, as well as security information concerning the endpoints.

Click the *Open Endpoint Protection Live Log* button to open the endpoint protection live log in a new window.

11.1 Computer Management

On the *Endpoint Protection* > *Computer Management* pages you can enable and manage the protection of individual computers connected to your Sophos UTM.

You can find and deploy an installation file for endpoints and you get an overview of all computers where the endpoint protection software is installed. You can define computer groups with differing protection settings.

11.1.1 Global

On the *Endpoint Protection* > *Computer Management* > *Global* tab you can enable or disable endpoint protection.

To enable endpoint protection, do the following:

1. **On the *Global* tab, enable endpoint protection.**
   Click the toggle switch.

   The toggle switch turns amber and some fields with your organization details become visible.

2. **Enter your organization details.**
   By default the settings from the *Management* > *System Settings* > *Organizational* tab is used.

3. **Optionally, configure a parent proxy:**
   If your UTM does not have direct HTTP internet access, Endpoint Protection can use a proxy server to reach Sophos LiveConnect. Select *Use a parent proxy* and enter the host and port if necessary.

4. **Click *Activate Endpoint Protection*.**
   The toggle switch turns green and endpoint protection is activated.

   To cancel the configuration, click the amber colored toggle switch.

On the *Deploy Agent* page you can now continue by deploying an endpoint protection installation package to computers to be monitored.

Note – When using endpoint protection, we recommend to enable the *Force caching for Sophos Endpoint updates* feature on the *Web Protection* > *Filtering Options* > *Misc* tab, section *Web Caching*, to prevent uplink saturation when endpoints download data from the update servers in the Internet.

Note – The administrator can configure alerts for endpoint virus detection under *Management* > *Notifications* > *Notifications* tab, section *Endpoint*.

Note – If the Web Filter is activated and works in transparent mode, additional settings are necessary to ensure that endpoints can correctly use endpoint protection: As soon as endpoint protection is enabled, the UTM automatically creates a DNS group named *Sophos LiveConnect*. Add this DNS group to the *Skip transparent mode destination hosts/nets* box on the *Web Protection* > *Filtering Options* > *Misc* tab.

To disable endpoint protection, do the following:

1. **On the *Global* tab, disable endpoint protection.**
   Click the toggle switch.

   The toggle switch turns amber and two options are available.

2. **Select whether you want to delete your endpoint data.**
   Keep ALL data: Use this option if you want to temporarily disable endpoint protection. Your endpoint settings will be preserved. When enabling the feature again, the previously installed endpoints will automatically connect again and all defined policies will be available.

   Delete ALL data: Use this option if you want to reset all endpoint settings and start from scratch. All connections to endpoints and all policy settings will be deleted. After enabling the feature again, deploy new installation packages to the endpoints for them to get the new registration data (see section *Computer Management* > *Advanced*).

3. **Click *Disable Endpoint Protection*.**

The toggle switch turns gray and endpoint protection is disabled.

11.1.2 Deploy Agent

On the *Endpoint Protection* > *Computer Management* > *Deploy Agent* tab you can deploy the installation files for the individual computers to be monitored via endpoint protection.

With the package there are two different ways to deploy the endpoint protection software to endpoints:

- Use the *Download Endpoint Installation Package Now* button to download and save the installation package. Then give endpoint users access to the package.
- Copy the URL which is displayed in the gray box and send it to the endpoint users. Using the URL, endpoint users can download and install the installation package by themselves.

Note – The name of the installation packages must not be changed. During installation LiveConnect compares the package name with the current registration data of the UTM. If the information does not match, the installation will be aborted.

After installation on an endpoint, the respective computer will be displayed on the *Manage Computers* tab. Additionally it will automatically be assigned to the computer group defined on the *Advanced* tab.

Note – The installation package can be invalidated using the *Reset Registration Token* button on the *Advanced* tab.

11.1.3 Manage Computers

The *Endpoint Protection* > *Computer Management* > *Manage Computers* tab gives you an overview of the computers which have endpoint protection installed for your UTM. The computers are added to the list automatically. You can assign a computer to a group, add additional information, modify a computer's tamper protection settings, or delete a computer from the list.

To edit the settings of a listed computer proceed as follows:

1. **Click the *Edit* button of the respective computer.**
   The *Edit Computer* dialog box opens.

2. **Make the following settings:**
   Computer group: Select the computer group you want to assign the computer to. The computer will receive the protection settings of the assigned group.

   Type: Select the computer type, i.e. desktop, laptop, or server. The type serves to filter the list.

   Tamper protection: If enabled, modification of the protection settings on the computer locally is only possible with a password. The password is defined on the *Advanced* tab. If disabled, the endpoint user can modify protection settings without password. By default, the setting matches the setting of the group the computer belongs to.

   Inventory # (optional): Enter the inventory number of the computer.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   Your settings will be saved.

To delete a computer from the list, click the *Delete* button.

Note – When you delete a computer from the list it will no longer be monitored by the UTM. However, the installed endpoint software will not automatically be uninstalled, and the policies last deployed will still be active.

11.1.4 Manage Groups

On the *Endpoint Protection* > *Computer Management* > *Manage Groups* tab you can combine the protected computers to groups, and define endpoint protection settings for groups. All computers belonging to a group share the same antivirus and device policies.

Note – Every computer belongs to exactly one group. Initially, all computers belong to the Default group. After adding groups, on the *Advanced* tab you can define which group should be the default, i.e., which group a newly installed computer will be assigned to automatically.

To create a computer group, proceed as follows:

1. **Click *Add Computer Group*.**
   The *Add Computer Group* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this group.

   Antivirus policy: Select the antivirus policy to be applied to the group. The policies are defined on the *Antivirus > Policies* tab. Note that you can define group-specific exceptions from this policy on the *Antivirus > Exceptions* tab.

   Device policy: Select the device policy to be applied to the group. The policies are defined on the *Device Control > Policies* tab. Note that you can define group-specific exceptions from this policy on the *Device Control > Exceptions* tab.

   Tamper protection: If enabled, modification of the protection settings on the respective endpoints locally is only possible with a password. The password is defined on the *Advanced* tab. If disabled, the endpoint user can modify protection settings without password. Note that you can change the tamper protection setting for individual computers on the *Manage Computers* tab.

   Web Control: If enabled, endpoints in this group can enforce and report on web filtering policy, even if they are not on a Sophos UTM network. To enable Endpoint Web Control, see the *Endpoint Protection > Web Control* tab.

   Use proxy for AutoUpdate: If enabled, the proxy attributes specified in the fields below will be sent to the endpoints of this group. The endpoints will use the proxy data to connect to the Internet.

   Note – Make sure to enter the correct data. If the endpoints receive wrong proxy data they cannot connect to the Internet and to the UTM any more. In this case you will have to change the configuration on each affected endpoint manually.

   Address: Enter the proxy's IP address.

   Port: Enter the proxy's port number.

   User: Enter the proxy's username if required.

   Password: Enter the proxy's password if required.

   Computers: Add the computers to belong to the group.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The group will be created and appears on the *Manage Groups* list. Please note that it may take up to 15 minutes until all computers are reconfigured.

To either edit or delete a group, click the corresponding buttons.

11.1.5 Advanced

On the *Endpoint Protection* > *Computer Management* > *Advanced* tab, the following options can be configured:

Tamper Protection: With tamper protection enabled, protection settings can only be changed on endpoints using this password.

Default Computers Group: Select the computer group a computer will be assigned to automatically, shortly after installation of endpoint protection.

Sophos LiveConnect – Registration: This section contains registration information about your endpoint protection. Amongst others, the information is used to identify installation packages, and it can be used for support purposes.

If you use Sophos Enterprise Console to manage endpoints, you can use this UTM to provide their Web Control policy. *Under SEC Information*, copy the *Hostname* and the *Shared-Key*into the Web Control policy editor in Sophos Enterprise Console

- **Reset registration token**: Click this button to prevent endpoints from being installed with a previously deployed installation package. Typically you do this to finish your rollout. If you want new endpoints to be installed, provide a new installation package via the *Deploy Agent* tab.

Parent Proxy: Use a parent proxy if your UTM does not have direct internet access.

11.2 Antivirus

On the *Endpoint Protection* > *Antivirus* pages you can define antivirus settings for the endpoint protection feature. You can create antivirus policies, i.e., sets of antivirus settings, which you can subsequently apply to your computer groups to be monitored by endpoint protection. Additionally you can define exceptions for the antivirus features to be applied to specific computer groups.

11.2.1 Policies

On the *Endpoint Protection* > *Antivirus* > *Policies* tab you can manage different sets of antivirus settings which you can subsequently apply to the computer groups monitored by endpoint protection.

By default, the antivirus policy *Basic protection* represents the best balance between protecting your computer against threats and overall system performance. It cannot be modified.

To add a new antivirus policy, proceed as follows:

1. **Click the *Add Policy* button.**
   The *Add Policy* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this policy.

   On-access scanning: If enabled, whenever you copy, move, or open a file, the file will be scanned and access will only be granted if it does not pose a threat to your computer or has been authorized for use.

   - **Scan for PUA:** If enabled, the on-access scanning will include a check for potentially unwanted applications (PUAs).

   Automatic cleanup: If enabled, items that contain viruses or spyware will automatically be cleaned up, any items that are purely malware will be deleted, and any items that have been infected will be disinfected. These disinfected files should be considered permanently damaged, as the virus scanner cannot know what the file contained before it was damaged.

   Sophos Live Protection: If the antivirus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the Sophos threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis.

   The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.

   - **Send sample file:** If a file is considered suspicious, but cannot be positively identified as malicious based on the file data alone, you can allow Sophos to request a sample of the file. If this option is enabled, and Sophos does not already hold a

sample of the file, the file will be submitted automatically. Submitting sample files helps Sophos to continuously enhance detection of malware without the risk of false positives.

Suspicious behavior (HIPS): If enabled, all system processes are watched for signs of active malware, such as suspicious writes to the registry, file copy actions, or buffer overflow techniques. Suspicious processes will be blocked.

Web protection: If enabled, the website URLs are looked up in the Sophos online database of infected websites.

- **Block malicious sites:** If enabled, sites with malicious contents will be blocked.
- **Download scanning:** If enabled, during a download data will be scanned by antivirus scanning and blocked if the download contains malicious content.

Scheduled scanning: If enabled, a scan will be executed at a specified time.

- **Rootkit scan:** If enabled, with each scheduled scan the computer will be scanned for rootkits.
- **Low priority scan:** If enabled, the on-demand scans will be conducted with a lower priority. Note that this only works from Windows Vista Service Pack 2 onwards.
- **Time event:** Select a time event when the scans will take place, taking the time zone of the endpoint into account.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new policy appears on the antivirus policies list. Please note that settings changes may need up to 15 minutes until all computers are reconfigured.

To either edit or delete a policy, click the corresponding buttons.

11.2.2 Exceptions

On the *Endpoint Protection* > *Antivirus* > *Exceptions* tab you can define computer group-specific exceptions from the antivirus settings of endpoint protection. An exception serves to exclude items from scanning which would be scanned due to an antivirus policy setting.

To add an exception, proceed as follows:

On the *Exceptions* tab, click *Add Exception*.

1. The *Add Exception* dialog box opens.

2. **Make the following settings:**
   Type: Select the type of items you want to skip from on-access and on-demand scanning.

   - **Adware and PUA:** If selected, you can exclude a specific adware or PUA (Potentially Unwanted Applications) from scanning and blocking. Adware displays advertising (for example, pop-up messages) that may affect user productivity and system efficiency. PUAs are not malicious, but are generally considered unsuitable for business networks. Add the name of the adware or PUA in the *Filename* field, e.g., `example.stuff`.
   - **Scanning exclusions:** If selected, you can exclude a file, a folder, or a network drive from antivirus scanning. Enter the file, folder, or network drive in the *File/Path* field, e.g., `C:\Documents\` or `\\Server\Users\Documents\CV.doc`.
   - **Scanning extensions:** If selected, you can add files with a specific extension so that they will be scanned by antivirus scanning. Enter the extension in the *Extension* field, e.g., `html`.
   - **Buffer overflow:** If selected, you can prevent an application using buffer overflow techniques from being blocked through behavior monitoring. Optionally enter the name of the application file in the *Filename* field and upload the file via the *Upload* field.
   - **Suspicious files:** If selected, you can prevent a suspicious file from being blocked through antivirus scanning. Upload the file via the *Upload* field. UTM generates the MD5 checksum of the file. The name of the uploaded file will automatically be used for the *Filename* field. Optionally modify the filename. If a file having the defined filename and the stored MD5 sum is found on the client, it will not be blocked through antivirus scanning.
   - **Suspicious behaviors:** If selected, you can prevent a file from being blocked through suspicious behavior detection. Optionally enter the name of the file in the *Filename* field and upload the file via the *Upload* field.
   - **Websites:** If selected, websites matching the properties specified in the *Web format* field will not be scanned through antivirus protection.
     Web format: Specify the server(s) with the websites you want to allow to visit.
     - **Domain name:** Enter the name of the domain to be allowed into the *Website* field.

- **IP address with subnet mask:** Enter the IPv4 address and netmask of the computers to be allowed.
- **IP address:** Enter the IPv4 address of the computer to be allowed.

Upload (only with types *Buffer overflow*, *Suspicious files*, and *Suspicious behaviors*): Upload the file that should be skipped from antivirus scanning.

Computers Groups: Select the computer groups for which this exception is valid.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new exception appears on the *Exceptions* list.

To either edit or delete an exception, click the corresponding buttons.

11.3 Device Control

On the *Endpoint Protection* > *Device Control* pages you can control devices attached to computers monitored by endpoint protection. Basically, in a device policy, you define which types of devices are allowed or blocked for the computer groups the policy is assigned to. As soon as a device is detected, the endpoint protection checks if it is allowed according to the device policy applied to the computer group of the respective computer. If it is blocked or restricted due to the device policy it will be displayed on the *Exceptions* tab, where you can add an exception for the device.

11.3.1 Policies

On the *Endpoint Protection* > *Device Control* > *Policies* tab you can manage different sets of device control settings which can subsequently be applied to the computer groups monitored by endpoint protection. These sets are called device policies.

By default two device policies are available: *Blocked All* prohibits the usage of all types of devices, whereas *Full Access* permits all rights for all devices. These policies cannot be modified.

To add a new policy, proceed as follows:

1. **Click the *Add Policy* button.**
   The *Add Policy* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this policy.

   Storage Devices: For different types of storage devices you can configure whether they should be *Allowed* or *Blocked*. Where applicable, a *Read only* entry is available, too.

   Network Devices: For modems and wireless networks you can configure whether they should be *Allowed*, *Block bridged*, or *Blocked*.

   Short Range Devices: For Bluetooth and infrared devices you can configure whether they should be *Allowed* or *Blocked*.

3. **Comment** (optional): Add a description or other information.

4. **Click *Save*.**
   The new policy appears on the device control policies list. It can now be applied to a computer group. Please note that settings changes may need up to 15 minutes until all computers are reconfigured.

To either edit or delete a policy, click the corresponding buttons.

11.3.2 Exceptions

On the *Endpoint Protection* > *Device Control* > *Exceptions* tab you can create protection exceptions for devices. An exception always allows something which is forbidden by the device policy assigned to a computer group. Exceptions are made for computer groups, therefore an exception always applies to all computers of the selected group(s).

The *Exceptions* list automatically shows all detected devices that are blocked or access-restricted by the applied device control policies. For floppy drives technically cannot be distinguished, if multiple floppy drives are connected, only one entry will be displayed which serves as a placeholder for all floppy drives.

To add an exception for a device, proceed as follows:

1. **Click the *Edit* button of the device.**
   The *Edit Device* dialog box opens.

2. **Make the following settings:**
   Allowed: Add the computer groups for which this device should be allowed.

Read only or bridged: Add the computer groups for which this device should be allowed in read-only mode (applies to storage devices) or bridged mode (applies to network devices).

Apply to all: If you select this option, the current settings will be applied to all devices with the same device ID. This is for example useful if you want to assign a generic exception to a set of USB sticks of the same type.

Mode: This option is only available when you unselect the *Apply to all* checkbox. In this case you have to specify what becomes of other devices having the generic exception. If you want to keep the generic exception for the affected devices, select *Keep for others*. If you want to delete the generic exception, click *Delete for others*.

Tip – For more information and examples concerning generic exceptions, see section Working With Generic Device Exceptions below.

Comment (optional): Add a description or other information.

3. **Click *Save*.**

   The computer groups along with their exceptions will be displayed with the edited device.

Note – Once a device exists on the *Exceptions* list, it will stay on the list until you delete it using the *Delete* button. Typically you would delete a device after the corresponding hardware device has been removed irrevocably (e.g., optical drive does not exist any longer) or after changing your device policies (e.g., wireless network adapters are now generally allowed). When you delete a device which is still in use, a message box opens that you need to confirm with *OK*. After that the device will be deleted from the list. If an exception existed for this device, the exception will automatically be invalidated, i.e. the current device policy will be applied to the device.

Working With Generic Device Exceptions

A generic device exception is an exception which is automatically applied to all devices having the same device ID.

Creating a Generic Exception

1. Click the *Edit* button of a device that does not have a generic exception, i.e., the *Apply to all* checkbox is unselected.

2. Configure the exception and select the *Apply to all* checkbox.
3. Save the exception.
   The exception will be applied to all devices having the same device ID.

Excluding a Device From a Generic Exception

1. Click the *Edit* button of the device you want to exclude from an existing generic exception.
2. Configure the individual exception and unselect the *Apply to all* checkbox.
3. In the *Mode* drop-down list, select *Keep for others*.
4. Save the exception.
   The edited device will have an individual exception, whereas the others will keep the generic exception.

Changing the Settings for All Devices Having the Generic Exception

1. Click the *Edit* button of one of the devices having a generic exception.
2. Configure the exception while keeping the *Apply to all* checkbox selected.
3. Save the exception.
   The settings of all devices having the same device ID where the *Apply to all* checkbox is selected will be changed accordingly.

Deleting a Generic Exception

1. Click the *Edit* button of one of the devices having the generic exception.
2. Unselect the *Apply to all* checkbox.
3. In the *Mode* drop-down list, select *Delete for others*.
4. Save the exception.
   The exceptions of all devices having the same device ID where the *Apply to all* checkbox was selected will be deleted. Only the edited device still has an exception—an individual one.

11.4 Endpoint Web Control

While the Sophos UTM provides security and productivity protection for systems browsing the web from within your corporate network, Endpoint Web Control extends this protection to

user's machines. This provides protection, control, and reporting for endpoint machines that are located, or roam, outside your corporate network. When enabled, all policies that are defined in *Web Protection* > *Web Filtering* and *Web Protection* > *Web Filter Profiles* > *Proxy Profiles* are enforced by Endpoint Web Control, even if the computer is not on a UTM network. Sophos UTM and Sophos endpoints communicate through LiveConnect, a cloud service that enables instant policy and reporting updates by seamlessly connecting Sophos UTM and roaming Sophos endpoints. For instance, a roaming laptop at home or in a coffee shop would still enforce Web Control policy, and the Sophos UTM will receive logging information from the roaming laptop.

11.4.1 Global

On the *Endpoint Protection* > *Web Control* > *Global* tab you can enable or disable endpoint web control. To configure filtering policies for Endpoint Web Control, Web Control must be enabled for the relevant group on the *Endpoint Protection* > *Computer Management* > *Manage Groups* page, and that group must be referenced in a proxy profile on the *Web Protection* > *Web Filter Profiles* > *Proxy Profiles* tab.

11.4.2 Advanced

On the *Endpoint Protection* > *Web Control* > *Advanced* tab you can select *Scan traffic on both gateway and endpoint* . By default, the Sophos UTM does not scan web traffic for endpoints that have Web Control enabled. If this option is selected, both the endpoint and the Sophos UTM will filter web traffic. To help provide additional security, configure *Web Protection* > *Web Filtering* > *Policies* > *Antivirus* to use *Dual Scan (Maximum Security)*. Alternately, select a different scan engine on the *Management* > *System Settings* > *Scan Settings* tab. Either option will provide a different antivirus scanning engine on the Sophos UTM than is included on the endpoint, increasing security.

11.4.3 Features not Supported

While there are many benefits to extending Web Control to the Endpoint, some features are only available from within a Sophos UTM network. The following features are supported on the Sophos UTM, but not supported by Endpoint Web Control:

- **Scan HTTPS (SSL) Traffic:** HTTPS traffic cannot be scanned by the Endpoint. If the Endpoint is proxying through the UTM and this feature is turned on, the traffic will be scanned by the UTM.

- **Authentication Mode:** The Endpoint will always use the currently logged on user (SSO). The Endpoint cannot perform authentication because if the Endpoint is roaming it will not be able to talk to the UTM to authenticate.
- **Antivirus/Malware:** Sophos endpoint antivirus settings are configured on the *Endpoint Protection > Antivirus page*. If Web Protection (Download scanning) is turned on it will always perform a virus single scan for all web content. Dual scan and max scanning size are not supported.
- **Active Content Removal**
- **YouTube for Schools**
- **Streaming Settings:** The Sophos Endpoint will always scan streaming content for viruses.
- **Block Unscannable and Encrypted Files**
- **Block by Download Size**
- **Allowed Target Services:** This feature applies only to the Sophos UTM.
- **Web Caching:** This feature applies only to the Sophos UTM.

12 Wireless Protection

The *Wireless Protection* menu allows you to configure and manage wireless access points for your Sophos UTM, the corresponding wireless networks, and the clients which use wireless access. The access points are automatically configured on your UTM, so there is no need to configure them individually. The communication between the UTM and the access point, which is used to exchange the access point configuration and status information, is encrypted using AES.

Important Note – When the lights of your access point blink furiously, do not disconnect it from power! Furiously blinking lights mean that a firmware flash is currently in progress. A firmware flash takes place for example after an UTM system update that comes with a Wireless Protection update.

The following topics are included in this chapter:

The Wireless Protection overview page gives you general information on connected access points, their status, connected clients, wireless networks, mesh networks, and mesh peer links.

In the *Currently Connected* section, you can sort the entries by SSID or by access point, and you can expand and collapse the individual entries by clicking the Collapse icon on the left.

Live Log

You can click the *Open Wireless Protection Live Log* button to see detailed connection and debug information for the access points and clients trying to connect.

12.1 Global Settings

On the *Wireless Protection* > *Global Settings* pages you can enable Wireless Protection, configure network interfaces for Wireless Protection and WPA/WPA2 enterprise authentication.

12.1.1 Global Settings

On the *Wireless Protection* > *Global Settings* > *Global Settings* tab you can enable or disable Wireless Protection.

To enable Wireless Protection do the following:

1. **On the *Global Settings* tab, enable Wireless Protection.**
   Click the toggle switch.

   The toggle switch turns amber and the *Access Control* area becomes editable.

   When enabling Wireless Protection for the first time, the *Initial Setup* section appears. It shows the configuration which will be created: A separate wireless "Guest" network using WPA2 personal encryption with DHCP for wireless clients, which will be allowed to use DNS on the UTM and the *Web Surfing* service. The pre-shared key is auto-generated and will only be shown in this section. This initial configuration is intended as a template. You can edit the settings at any time on the *Wireless Protection* > *Wireless Networks* page.

   Skip Automatic Configuration: You can also skip the initial setup by selecting this option. You will then need to configure the wireless settings manually.

2. **Select a network interface for the access point.**
   Click the Folder icon in the *Allowed interfaces* section to select a configured interface where the access point is going to be plugged in. Make sure that a DHCP server is associated to this interface.

3. **Click *Apply*.**

   Your settings will be saved. The toggle switch turns green to indicate that Wireless Protection is active.

   You can now continue by plugging the access point into the configured network interface. If you decided to skip the automatic configuration, proceed the configuration on the *Wireless Networks* page.

To cancel the configuration, click the amber colored toggle switch.

As soon as you plug in an access point it will automatically connect to the system. Newly connected, unconfigured access points are listed as *Pending Access Points* on the *Access Points* > *Overview* page.

12.1.2 Advanced

On the *Wireless Protection* > *Global Settings* > *Advanced* tab you can configure your access points to use WPA/WPA2 enterprise authentication.

For enterprise authentication, you need to provide some information of your RADIUS server. Note that the AP(s) do not communicate with the RADIUS server for authentication but only the UTM. Port `414` is used for the RADIUS communication between the UTM and the AP(s).

To use WPA/WPA2 enterprise authentication, make the following settings:

RADIUS server: Select or create a server where clients are to authenticate themselves, e.g. your Active Directory server.

RADIUS port (optional): The default RADIUS port 1812 is selected. You can change the port if necessary.

RADIUS secret: Enter the RADIUS passphrase which is needed by the access point to be able to communicate with the RADIUS server.

Test settings: Click to verify if the connection to the RADIUS server can successfully been established.

Click *Apply* to save your settings.

12.2 Wireless Networks

On the *Wireless Protection* > *Wireless Networks* page you can define your wireless networks, such as their SSID and encryption method. Moreover, you can define whether the wireless network should have a separate IP address range or be bridged into the LAN of the access point.

To define a new wireless network, do the following:

1. **On the *Wireless Networks* page, click *Add Wireless Network*.**
   The *Add Wireless Network* dialog box opens.

2. **Make the following settings:**
   Network name: Enter a descriptive name for the network.

   Network SSID: Enter the Service Set Identifier (SSID) for the network which will be seen by clients to identify the wireless network. The SSID may consist of 1-32 ASCII printable characters[1]. It must not contain a comma and must not begin or end with a space.

   Encryption mode: Select an encryption mode from the drop-down list. Default is *WPA 2 Personal*. We recommend to prefer *WPA2* over *WPA*, if possible. For security reasons, it is recommended to not use WEP unless there are clients using your wireless network that do not support one of the other methods. When using an enterprise authentication method, you also need to configure a RADIUS server on the *Global Settings > Advanced* tab. As NAS ID of the RADIUS server enter the wireless network name.

   Passphrase/PSK: Only available with *WPA/WPA2 Personal* encryption mode. Enter the passphrase to protect the wireless network from unauthorized access and repeat it in the next field. The passphrase may consist of 8-63 ASCII printable characters.

   128-bit WEP key: Only available with *WEP* encryption mode. Enter a WEP key here that exactly consists of 26 hexadecimal characters.

   Client traffic: Select a method how the wireless network is to be integrated into your local network.

   - **Separate zone** (default): The wireless network is handled as a separate network, having an IP address range of its own. Using this option, after adding the wireless network you have to continue your setup as described in the section below (Next Steps for Separate Zone Network).

     Note – When switching an existing *Separate Zone* network to *Bridge to AP LAN* or *Bridge to VLAN*, already configured WLAN interfaces on the UTM will be disabled and the interface object will become *unassigned*. However, you can assign a new hardware interface to the interface object by editing it and thus re-enable it.

   - **Bridge to AP LAN:** You can also bridge the wireless network into the network of the access point, that means that the wireless clients share the same IP address

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

range.

Note – If VLAN is enabled, the wireless clients will be bridged into the VLAN network of the access point.

- **Bridge to VLAN:** You can decide to have this wireless network's traffic bridged to a VLAN of your choice. This is useful when you want the access points to be in a common network separate from the wireless clients.
  Bridge to VLAN ID: Enter the VLAN ID of the network that the wireless clients should be part of.

  Client VLAN ID (only available with an *Enterprise* encryption mode): Select how the VLAN ID is defined:

  - **Static:** Uses the VLAN ID defined in the *Bridge to VLAN ID* field.
  - **RADIUS & Static:** Uses the VLAN ID delivered by your RADIUS server: When a user connects to one of your wireless networks and authenticates at your RADIUS server, the RADIUS server tells the access point what VLAN ID to use for that user. Thus, when using multiple wireless networks, you can define per user who has access to which internal networks. If a user does not have a VLAN ID attribute assigned, the VLAN ID defined in the *Bridge to VLAN ID* field will be used.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Algorithm (only available with WPA/WPA2 encryption mode): Select an encryption algorithm which can be either *AES* or *TKIP & AES*. For security reasons, it is recommended to use *AES*.

   Frequency band: The access points assigned to this wireless network will transmit on the selected frequency band(s). The 5 GHz band generally has higher performance, lower latency, and is typically less disturbed. Hence it should be preferred for e.g. VoIP communication. Note that only AP 50 is able to send on the 5 GHz band.

   Time-based access: Select this option if you want to automatically enable and disable the wireless network according to a time schedule.

Select active time: Select a time period definition which determines when the wireless network is enabled. You can add a new time period definition by clicking the Plus icon.

Client isolation: Clients within a network normally can communicate with one another. If you want to prevent this, for example in a guest network, select *Enabled* from the drop-down list.

Hide SSID: Sometimes you want to hide your SSID. Select *Yes* from the drop-down list to do so. Please note that this is no security feature.

MAC filtering type: To restrict the MAC addresses allowed to connect to this wireless network, select *Blacklist* or *Whitelist*. With *Blacklist*, all MAC addresses are allowed except those listed on the MAC address list selected below. With *Whitelist*, all MAC addresses are prohibited except those listed on the MAC address list selected below.

MAC addresses: The list of MAC addresses used to restrict access to the wireless network. MAC address lists can be created on the *Definitions & Users > Network Definitions > MAC Address Definitions* tab. Note that a maximum of 200 MAC addresses is allowed.

4. **Click *Save*.**
   Your settings will be saved. The wireless network appears on the *Wireless Networks* list.

Next Steps for Separate Zone Networks

When you created a wireless network with the option *Separate Zone*, a new corresponding virtual hardware interface will be created automatically, e.g., *wlan0*. To be able to use the wireless network, some further manual configuration steps are required. Proceed as follows:

1. **Configure a new network interface.**
   On the *Interfaces & Routing > Interfaces > Interfaces* tab create a new interface and select your wlan interface (e.g., wlan0) as hardware. Make sure that type is “Ethernet” and specify the IP address and netmask of your wireless network.
2. **Enable DHCP for the wireless clients.**
   For your clients to be able to connect to UTM, they need to be assigned an IP address and a default gateway. Therefore, on the *Network Services > DHCP > Servers* tab, set up a DHCP server for the interface.

3. **Enable DNS for the wireless clients.**
   For your clients to be able to resolve DNS names they have to get access to DNS servers. On the *Network Services* > *DNS* > *Global* tab, add the interface to the list of allowed networks.
4. **Create a NAT rule to mask the wireless network.**
   As with any other network you have to translate the wireless network's addresses into the address of the uplink interface. You create the NAT rule on the *Network Protection* > *NAT* > *Masquerading* tab.
5. **Create one or more packet filter rules to allow traffic from and to the wireless network.**
   As with any other network you have to create one or more packet filter rules to allow the traffic to pass the UTM, e.g., web surfing traffic. You create packet filter rules on the *Network Protection* > *Firewall* > *Rules* tab.

12.3 Access Points

The *Wireless Protection* > *Access Points* pages provide an overview of the access points (AP) known to the system. You can edit AP attributes, delete or group APs and assign wireless networks to APs or AP groups.

Note – With BasicGuard subscription, only one access point can connect to UTM. The maximum number of access points is limited to 223 by any UTM appliance.

Types of Access Points

Currently, Sophos provides four different access points:

- AP 5: standards 802.11b/g/n, 2.4 GHz band
  It can only be connected to a RED rev2 or rev3 with USB connector and exactly supports one SSID with the WLAN type *Bridge to AP LAN* and a maximum of 7 wireless clients.
- AP 10: standards 802.11b/g/n, 2.4 GHz band
- AP 30: standards 802.11b/g/n, 2.4 GHz band
- AP 50: standards 802.11a/b/g/n, 2.4/5 GHz dual-band/dual-radio
  There are two different AP 50 models available where the available channels differ:

- FCC regulatory domain (mainly US): channels 1-11, 36, 40, 44, 48
- ETSI regulatory domain (mainly Europe): channels 1–13, 36, 40, 44, 48

Note that the country setting of an AP regulates the available channels to be compliant with local law.

Cross Reference – For detailed information about access points see the *Operating Instructions* in the Sophos UTM Resource Center.

12.3.1 Overview

The *Wireless Protection* > *Access Points* > *Overview* page provides an overview of access points (AP) known to the system. The Sophos UTM distinguishes between active, inactive and pending APs. To make sure that only genuine APs connect to your network, APs need to be authorized first.

Note – If you want to use an AP 5, first enable RED management and set up the RED. Then make sure that the RED interface is added to the allowed interfaces on the *Wireless Protection* > *Global Settings* page. After connecting the AP 5 to the RED the AP 5 should be displayed in the *Pending Access Points* section.

Access points can be temporarily disabled on the *Grouping* tab. When an AP is physically removed from your network, you can delete it here by clicking the *Delete* button. As long as the AP remains connected to your network, it will automatically re-appear in *Pending* state after deletion.

Tip – Each section of this page can be collapsed and expanded by clicking the Collapse icon on the right of the section header.

Active Access Points

Here, APs are listed that are connected, configured, and running. To edit an AP, click the *Edit* button (see *Editing an Access Point* below).

Inactive Access Points

Here, APs are listed that have been configured in the past but are currently not connected to the UTM. If an AP remains in this state for more than five minutes, please check the network connectivity of the AP and the configuration of your system. A restart of the Wireless Protection

service will erase *Last Seen* timestamps. To edit an AP, click the *Edit* button (see *Editing an Access Point* below).

Pending Access Points

Here, APs are listed that are connected to the system but not yet authorized. To authorize an access point, click the *Accept* button (see *Editing an Access Point* below).

After receiving its configuration, the now authorized access point will be immediately displayed in one of the above sections, depending on whether it is currently active or not.

Editing an Access Point

1. **Click the *Edit* or *Accept* button of the respective access point.**
   The *Edit Access Point* dialog window opens.
2. **Make the following settings:**
   Label (optional): Enter a label to easily identify the AP in your network.

   Country: Select the country where the AP is located.

   Important Note – The country code regulates which channels will be available for transmit. To comply with local law, always select the correct country (see also chapter *Access Points*).

   Group (optional): You can organize APs in groups. If a group has been created before, you can select it from the drop-down list. Otherwise select << *New group* >> and enter a name for the group into the appearing *Name* text box. Groups can be organized on the *Grouping* tab.
3. **In the *Wireless Networks* section, make the following settings:**
   Wireless network selection (only if no group or a new group is selected): Select the wireless networks the access point should broadcast. This is useful if you have, for example, a company wireless network that should only be broadcasted in your offices, and a guest wireless network that should only be broadcasted in public parts of your building. You can search the wireless network list by using the filter field in the list header.

   Note – For an access point to broadcast a wireless network some conditions have to be fulfilled. They are explained in section Rules for Assigning Networks to APs below.

4. **Optionally, in the *Mesh Networks* section, make the following settings** (only available with AP 50 and only if a mesh network is defined on the *Mesh Networks* tab):
   Mesh roles: Click the Plus icon to select mesh networks that should be broadcasted by the access point. A dialog window opens.

   - **Mesh:** Select the mesh network.
   - **Role:** Define the access point's role for the selected mesh network. A root access point is directly connected to the UTM. A mesh access point, after having received its initial configuration, once unplugged from the UTM will connect to a root access point via the mesh network. Note that an access point can be mesh access point only for one single mesh network.

   After saving, the access point icon in the *Mesh roles* list designates the access point's role. Via the functional icons you can edit a mesh role or delete it from the list.

   Important Note – If you delete a mesh role from the *Mesh roles* list, you have to plug the access point into your Ethernet again to get its initial configuration. To change the mesh network without having to plug the access point into your Ethernet again, do not delete the mesh role but instead click the Edit icon of the mesh role, and select the desired mesh network.

5. **Optionally, make the following advanced settings:**
   Channel 2.4 GHz: You can keep the default setting *Auto* which will automatically select the least used channel for transmit. Or you can select a fix channel.

   Channel 5 GHz (only available with AP 50): You can keep the default setting *Auto* which will automatically select the least used channel for transmit. Or you can select a fix channel.

   Tip – When you select *Auto*, the currently used channel will be announced in the access point entry.

   TX power 2.4 GHz: You can keep the default setting *100 %* for the access point to send with maximum power. Or you can down-regulate the power to reduce the operating distance, e.g., to minimize interference.

   TX power 5 GHz (only available with AP 50): For AP 50 you can down-regulate the power output for the 5 GHz band separately.

STP: To enable Spanning Tree Protocol, select *Enabled* from the drop-down list. This network protocol detects and prevents bridge loops. STP is mandatory if the access point broadcasts a mesh network.

VLAN tagging: VLAN tagging is disabled by default. If you want to connect the AP with an existing VLAN Ethernet interface, you need to enable VLAN tagging by selecting the checkbox. Make sure that the VLAN Ethernet interface is added to the *Allowed interfaces* box on the *Global Settings* > *Global Settings* page.

Note – To introduce the usage of VLAN for your access points in your network, take the following steps: Connect the AP to the UTM using standard LAN for at least a minute. This is necessary for the AP to get its configuration. Connecting it via VLAN from the beginning, the AP would not know of being in a VLAN and therefore would not be able to connect to the UTM to get its configuration. When the AP is displayed, enable VLAN tagging and enter the VLAN ID. Then connect the AP to its intended VLAN, e.g., a switch.

Note – VLAN tagging is not possible with AP 5.

AP VLAN ID: When *VLAN tagging* is enabled, enter the VLAN tag of the VLAN the access point should use to connect to the UTM. Do not use the VLAN tags `0` and `1` as they usually have a special meaning on networking hardware like switches, and `4095` is reserved by convention.

Note – When VLAN tagging is configured, the AP will try DHCP on the configured VLAN for 60 seconds. If no IP address is received during that time, the AP will try DHCP on the regular LAN as a fallback.

6. **Click *Save*.**
The access point receives its configuration or configuration update, respectively.

Note – A configuration change needs approximately 15 seconds until all interfaces are reconfigured.

If VLAN tagging is configured but the AP cannot contact the UTM via VLAN, the AP will reboot itself and try again after receiving the configuration.

Rules for Assigning Networks to APs

An access point can only be assigned to a wireless network if the *Client traffic* option of the wireless network and the *VLAN tagging* option of the access point fit together. The following rules apply:

- Wireless network with client traffic *Separate Zone*: VLAN tagging of the access point can be enabled or disabled.
- Wireless network with client traffic *Bridge to AP LAN*: VLAN tagging of the access point has to be disabled.
- Wireless network with client traffic *Bridge to VLAN*: VLAN tagging of the access point has to be enabled. The respective wireless clients will use the *Bridge to VLAN ID* specified for the wireless network, or they will receive their VLAN ID from the RADIUS server, if specified.

Note – An AP 5 can only be assigned one single wireless network with the *Client traffic* option *Bridge to AP LAN*.

12.3.2 Grouping

On the *Wireless Protection* > *Access Points* > *Grouping* page you can organize access points in groups. The list provides an overview of all access point groups and ungrouped access points. Access points and groups can be distinguished by their respective icon.

To create an access point group, proceed as follows:

1. **On the *Grouping* page, click *New Group*.**
   The *New Access Point Group* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the access point group.

   VLAN tagging: VLAN tagging is disabled by default. If you want to connect the AP with an existing VLAN Ethernet interface, you need to enable VLAN tagging by selecting the checkbox. Make sure that the VLAN Ethernet interface is added to the *Allowed interfaces* box on the *Global Settings* > *Global Settings* page.

   - **AP VLAN ID:** Enter the VLAN tag that should be used by this group of APs to connect to UTM. Do not use the VLAN tags `0` and `1` as they usually have a special

meaning on networking hardware like switches, and `4095` is reserved by convention.

Access point selection: Select the access points that should become members of the group. Only access points that are not assigned to any other group are displayed.

Wireless network selection: Select the wireless networks that should be broadcasted by the access points of this group.

Note – For an access point to broadcast a wireless network some conditions have to be fulfilled. They are explained in chapter *Access Points* > *Overview*, section Rules for Assigning Networks to APs.

3. **Click *Save*.**
   The new access point group appears on the *Grouping* list.

To either edit or delete a group, click the corresponding buttons of a group.

To either edit or delete an access point, click the corresponding buttons of an access point. For more information about editing and deleting access points see chapter *Access Points* > *Overview*.

12.4 Mesh Networks

On the *Wireless Protection* > *Mesh Networks* page you can define mesh networks, and associate access points that should broadcast them. In general, in a mesh network multiple access points communicate with each other and broadcast a common wireless network. On the one hand, access points connected via a mesh network can broadcast the same wireless network to clients, thus working as a single access point, while covering a wider area. On the other hand, a mesh network can be used to bridge Ethernet networks without laying cables.

Access points associated with a mesh network can play one of two roles: root access point or mesh access point. Both broadcast the mesh network, thus the amount of other wireless networks they can broadcast is reduced by one.

- **Root access point:** It has a wired connection to the UTM and provides a mesh network. An access point can be root access point for multiple mesh networks.
- **Mesh access point:** It needs a mesh network to connect to the UTM via a root access

point. An access point can be mesh access point for only one single mesh network at a time.

A mesh network can be used for two main use cases: you can implement a wireless bridge or a wireless repeater:

- **Wireless bridge:** Using two access points, you can establish a wireless connection between two Ethernet segments. A wireless bridge is useful when you cannot lay a cable to connect those Ethernet segments. While the first Ethernet segment with your UTM is connected to the Ethernet interface of the root access point, the second Ethernet segment has to be connected to the Ethernet interface of the mesh access point. Using multiple mesh access points, you can connect more Ethernet segments.

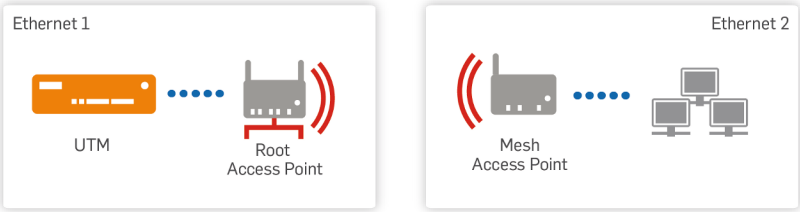

Figure 23 Mesh Network Use Case Wireless Bridge

- **Wireless repeater:** Your Ethernet with your UTM is connected to the Ethernet interface of a root access point. The root access point has a wireless connection via the mesh network to a mesh access point, which broadcasts wireless networks to wireless clients.

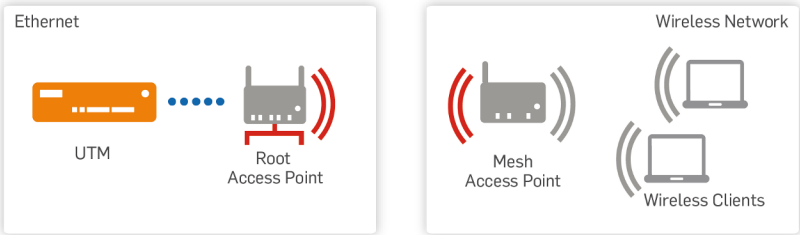

Figure 24 Mesh Network Use Case Wireless Repeater

To define a new mesh network, do the following:

1. **On the *Mesh Networks* page, click *Add Mesh Network*.**
   The *Add Mesh Network* dialog box opens.

2. **Make the following settings:**
   Mesh-ID: Enter a unique ID for the mesh network.

   Frequency band: Access points assigned to this network will transmit the mesh network on the selected frequency band. Generally, it is a good idea to use a different frequency band for the mesh network than for the broadcasted wireless networks.

   Comment (optional): Add a description or other information.

   Access points: Click the Plus icon to select access points that should broadcast the mesh network. A dialog window *Add Mesh Role* opens:

   - **AP:** Select an access point. Note that only AP 50 access points can be used for broadcasting mesh networks at the moment.
   - **Role:** Define the access point's role for the selected mesh network. A root access point is directly connected to the UTM. A mesh access point, after having received its initial configuration, once unplugged from the UTM will connect to a root access point via the mesh network. Note that an access point can be mesh access point only for one single mesh network.

   Note – It is crucial for the initial configuration to plug the mesh access point like every other access point into one of the Ethernet segments selected in the *Allowed interfaces* box on the *Global Settings* tab.

   Use the Delete icon in the *Access Points* list to delete an access point from the list.

   Important Note – If you delete a mesh access point from the *Access Points* list, you have to plug the access point into your Ethernet again to get its initial configuration. To change the mesh network without having to plug the access point into your Ethernet again, do not delete the access point but instead click the access point's *Edit* button on the *Access Points* > *Overview* tab, click the Edit icon in the *Mesh Networks* section, and select the desired mesh network.

   The access point icon designates an access point's role. You can search the access point list by using the filter field in the list header.

3. **Click *Save*.**
   Your settings will be saved. The mesh network appears on the *Mesh Networks* list.

12.5 Wireless Clients

The *Wireless Protection* > *Wireless Clients* page gives you an overview of clients that are currently connected to an access point or have been connected in the past.

As not all clients transmit their name you can give them a name here to ease distinguishing known clients in the overview. If clients transmit their NetBIOS name during the DHCP request, their name is displayed in the table. Otherwise they will be listed as *[unknown]*. You can change the name of (unknown) clients by clicking the Key icon in front of the name. Then enter a name and click *Save*. It takes a few seconds for the change to take effect. Click the Reload button in the upper right corner of WebAdmin to see the name of the client.

You can also delete clients from the table by clicking the Empty icon in the first column.

A restart of the Wireless Protection service will erase *Last seen* timestamps.

Note – IP addresses assigned to clients can only be displayed if the UTM serves as DHCP server for the corresponding wireless network. Additionally, for static DHCP mappings the IP address `0.0.0.0` is displayed at the moment.

12.6 Hotspots

On the *Wireless Protection* > *Hotspots* pages you can manage access with the captive portal system. The Hotspot feature allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests. The feature is available within the wireless subscription, but also works with wired networks.

Note – Technically, the Hotspot feature serves to restrict traffic which is basically allowed by the firewall. Therefore you have to ensure that a firewall rule exists which allows the traffic to be managed via the hotspots. It is recommended to test the traffic with the hotspot feature disabled before enabling the hotspots.

Note – If the Hotspot feature is used in combination with an active-active cluster setup, the respective traffic cannot be distributed between master and workers. All traffic from and to the hotspot interfaces will be directed through the master.

Hotspot Generation

In a first step, the administrator creates and enables a hotspot with a specific type of access. The following types are available:

- **Terms of use acceptance:** The guest is presented a terms of use, which you can define, and has to select a checkbox to get access.
- **Password of the day:** The guest has to enter a password to get access. The password changes on a daily basis.
- **Voucher:** The guest gets a voucher and has to enter the voucher code to get access. The voucher can be limited in the number of devices, in time, and traffic.

Distribution of Access Information to Guests

With the types *Password of the day* and *Voucher*, the access information has to be handed out to the guests. Therefore you can define users who are allowed to manage and distribute access information. Those users receive and distribute the access information via the *Hotspot* tab of the User Portal:

- **Password of the day:** The current password can be sent via email and the users find the password in the User Portal. The users forward the password to the guests. They can generate or enter a new password. Hereby, the former password automatically becomes invalid and active sessions will be terminated. Potential other users will be informed of the new password, either by email or via the User Portal, depending on what is configured for them.
- **Voucher:** In the User Portal, users have the possibility to create vouchers, each with a unique code. Different types of vouchers can be available if specified by the administrator. The vouchers can be printed or exported and given to the guests. A list of created vouchers gives an overview about their usage and helps to manage them.

Legal Information

In many countries, operating a public wireless LAN is subject to specific national laws, restricting access to websites of legally questionable content (e.g., file sharing sites, extremist websites, etc.). To meet this requirement, you can combine the hotspot with the web protection capabilities of the Sophos UTM, which allow you to control web access by blocking and allowing everything from an entire website category type to a single URL. The UTM gives you complete

control over what is allowed to be accessed, by whom, and when. That way you can put the hotspot under heavy restrictions, if national or corporate policies require you to do so.

Using the built-in HTTP proxy of Sophos UTM also gives you advanced logging and reporting capabilities. The reporting will show who visited what site, when, and how many times, allowing you to identify inappropriate usage in case you want to operate a hotspot without any access restrictions.

In addition to that, legal regulations may require you to register your hotspot at the national's regulatory body.

12.6.1 Global

On the *Wireless Protection > Hotspots > Global* tab you can enable the Hotspots feature and define users who are allowed to view and distribute hotspot access information.

To configure hotspots, proceed as follows:

1. **On the *Global* tab, enable the Hotspots.**
   Click the toggle switch.

   The toggle switch turns green and the *Global Hotspot Settings* area becomes editable.
2. **Select the allowed users.**
   Select the users or groups or add new users that should be able to provide hotspot access information via the User Portal. Users selected here can change the password of the day and are able to create hotspot vouchers. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.
3. **Click *Apply*.**
   Your settings will be saved.

Live Log

The Hotspots live log gives you information on the usage of the hotspots. Click the *Open Live Log* button to open the Hotspots live log in a new window.

Download Templates

Here you can download the hotspot login template and the voucher template that are used by default when adding a new hotspot. You can modify the default templates to customize your hotspot login page or the voucher design without the need to create them from scratch. You can upload the customized HTML and PDF template on the *Wireless Protection > Hotspots > Hotspots* tab.

1. **Click the blue Download icon.**
   The *Download Certificate File* dialog window opens.
2. **Save the file.**
   The file will be downloaded.

12.6.2 Hotspots

On the *Wireless Protection* > *Hotspots* > *Hotspots* tab you can manage different hotspots.

Note – A hotspot has to be assigned to an existing interface, typically a WLAN interface. All hosts using this interface will automatically be restricted by the hotspot. Therefore, before you create a hotspot you would typically create a wireless network with client traffic *Separate Zone*, then create an interface for the respective WLAN interface hardware. For more information see *Wireless Protection* > *Wireless Networks*.

To create a hotspot, proceed as follows:

1. **Click *Add Hotspot*.**
   The *Add Hotspot* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this hotspot.

   Interfaces: Add the interfaces which are to be restricted by the hotspot. Please ensure that for the selected interfaces a firewall rule exists which allows the desired traffic. An interface can only be used by one hotspot.

   Caution – You should not select an uplink interface here because traffic to the Internet will completely be blocked afterwards. Additionally, we strongly advise against using interfaces used by servers which provide essential services like authentication. You may irreversibly lock yourself out of WebAdmin!

   Hotspot type: Select the hotspot type for the selected interfaces.

   - **Password of the day:** A new password will be created automatically once a day. This password will be available in the User Portal on the *Hotspots* tab which is available to all users specified on the *Global* tab. Additionally it will be sent to the specified email addresses.

- **Voucher** (not available with BasicGuard subscription): With this hotspot type, in the User Portal tokens with different limitations and properties can be generated, printed and given to customers. After entering the code, the customers can then directly access the Internet.
- **Terms of Use Acceptance:** Customers can access the Internet after accepting the Terms of Use.
- **Backend Authentication:** With this hotspot type, users can authenticate via any supported backend mechanism (see *Definitions & Users > Authentication Services*). With this type, the user credentials are stored to periodically check if the user is still authorized.

Note – If you select *Backend Authentication* a new entry field for OTP token appears on the Login Form if Hotspot is configured as an OTP facility.

Password creation time (only with Hotspot type *Password of the day*): The assigned time of the day at which the new password will be created. At this time the former password will immediately get invalid and current sessions will be cut off.

Send password by email to (only with Hotspot type *Password of the day*): Add email addresses to which the password shall be sent.

Voucher definitions (only with Hotspot type *Voucher*): Add or select the voucher definitions you want to use for the hotspot. How to add a voucher definition is explained on the *Voucher Definitions* page.

Devices per voucher (only with Hotspot type *Voucher*): Enter the number of devices which are allowed to log in with one voucher during its lifetime. It is not recommended to use the *unlimited* entry.

Hotspot users (only with Hotspot type *Backend Authentication*): Select the users or user groups or add the users that should be able to access the hotspot via backend authentication. Typically, this is a backend user group.

Session expires (only with Hotspot type *Terms of Use Acceptance* or *Backend Authentication*): Select the time span after which the access will expire. After that, with the hotspot type *Terms of Use Acceptance*, the users have to accept the terms of use again to log in. With the hotspot type *Backend Authentication*, the users have to authenticate again.

Users have to accept terms of use (not with Hotspot type *Terms of Use Acceptance*): Select this option if you want the hotspot users to accept your terms of use before accessing the Internet.

- **Terms of use:** Add the text to be displayed as terms of use. Simple HTML markup and hyperlinks are allowed.

Redirect to URL after login: If selected, after entering the password or the voucher data, the users will be redirected automatically to a particular URL, e.g., your hotel's website or a webpage stating your portal system policies.

- **URL:** URL to which the user is redirected.

Comment (optional): Add a description or other information.

3. **Optionally, make the following hotspot customization settings:**
   By default, the user will be presented a login page with the Sophos logo. You can use a customized HTML file with your own images and stylesheets. Additionally, you can customize the voucher layout.

   Customization type: Select the customization type. The following types are available:

   - **Basic:** Use the default login page template. If required, change logo, title, and text.
     Logo: Upload a logo for the login page. Supported image file types are jpg, png and gif. A maximum image width of 300 px and height of 100 px is recommended (depending on the title length). Use the *Restore Default* button to select the default Sophos logo again.

     Scale logo to recommended size: If selected, a logo exceeding the recommended width or height will be scaled down and displayed in the recommended size. If not selected, the logo will be displayed in the original size.

     Title: Add a title for the login page. Simple HTML markup and hyperlinks are allowed.

     Custom text: Add an additional text for the login page. You can for example enter the SSID of the wireless network to be used. Simple HTML markup and hyperlinks are allowed.

   - **Full:** Select an individual login HTML page.
     Login page template: Select the HTML template you want to use for your individual login page. Clicking the Folder icon opens a window where you can select

and upload the file. Use the *Restore Default* button to select the default Sophos HTML template again. In this template, you can use variables that can dynamically insert information for each hotspot. For example, you can add the company name and administrator information, the terms of use and the login form. See detailed information below, in *Using Variables in Login Page Template*. You can download the default HTML template on the *Wireless Protection > Hotspots > Global* tab.

Images / Stylesheets: Add files that are referenced in your login page template, e.g., images, stylesheets, or JavaScript files. Clicking the Folder icon opens a window where you can select and upload the files.

Voucher template (only with hotspot type *Voucher*): Clicking the Folder icon opens a window where you can select and upload the PDF file with the voucher layout. By default, a default template is used. You can restore the default clicking the *Restore Default* button. The voucher PDF file has to have a PDF version PDF 1.5 or lower. It may have any page size and format—both size and format will be adjust during voucher creation in the User Portal, depending on page size and number of vouchers per page specified there. You can download the default PDF template on the *Wireless Protection > Hotspots > Global* tab.

The PDF file may contain the following variables that will be replaced with the respective values during voucher generation in the User Portal:

- Wireless network name (SSID): `<?ssid0?>` (and `<?ssid1?>`, `<?ssid2?>` and so on, if the WLAN has more than one SSIDs)
- Wireless network password: `<?psk0?>` (and `<?psk1?>`, `<?psk2?>` and so on, if the WLAN has more than one SSIDs)
- Voucher code: `<?code?>`
- Voucher validity time: `<?validity?>`
- Voucher data limit: `<?datalimit?>`
- Voucher time limit: `<?timelimit?>`
- QR code with the hotspot access data encoded: `<?qrX?>`. The upper left corner of the QR code will be placed on the lower left corner of the variable.

Note – When using variables, the PDF file must include the entire character sets of the fonts used. When a variable is replaced by its value, and one of the substitute

characters is not available, it will be displayed incorrectly. We recommend to add the string `<?abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789?>` to your PDF file, which will automatically be removed during voucher generation. Additionally, it is recommended to use a separate line for the variables as the layout could get corrupted if the substituted text is too long.

4. **Click *Save*.**
   The hotspot will be created and appears on the *Hotspots* list.

Tip – You can open a preview of the login page after saving the hotspot. In the *Hotspots* list just click the button *Preview Login Page* of the respective hotspot.

To either edit or delete a hotspot, click the corresponding buttons.

Using Variables in Login Page Template

The HTML template for the login page may contain various variables that can dynamically insert information for the hotspot login page. When the UTM processes a template in order to display a login page, it replaces any template variables with the relevant value. Valid variables are:

- General variables

  `<?company_text?>`: Custom company text as defined on *Management* > *Customization* > *Global*

  `<?company_logo?>`: Company logo as defined on *Management* > *Customization* > *Global*. The variable will be replaced by the path of the logo file, usage e.g., `<img src="<?company_logo?>">`

  `<?admin_contact?>`: Administrator name or address as defined on *Management* > *Customization* > *Web Messages*

  `<?admin_message?>`: Administrator information label as defined on *Management* > *Customization* > *Web Messages* (default: *Your cache administrator is:*)

  `<?error?>`: Error message that arose while trying to log in.

- Variables used for all hotspot types
  `<?terms?>`: Terms of use (as defined on *Hotspots* page)

<?redirect_host?>: Redirect URL that is specified for the hotspot (as defined on *Hotspots* page)

<?location?>: URL the user requested

<?location_host?>: Hostname of the URL the user requested

<?login_form?>: Login form suitable for the respective hotspot type: *Password* text box, *Token* text box, *Username* and *Password* text boxes, or *Accept* checkbox, and *Login* button. For creating customized login forms, see *User Specific Login Form* below.

<?asset_path?> (only important for customization mode *Full*): Hotspot-specific directory for storage of images or stylesheets (example usage: <img src="<?asset_path?>/logo.png">)

- Variables only used for Voucher type hotspots
  <?maclimit?> Number of allowed devices per voucher of this hotspot (as defined on *Hotspots* page)

  <?numdevices?>: Number of devices used for this voucher

  <?timeend?>: End of validity period (as defined on *Voucher Definitions* page)

  <?time_total?>: Total time quota allowed (as defined on *Voucher Definitions* page)

  <?time_used?>: Time quota used up (as defined on *Voucher Definitions* page)

  <?traffic_total?>: Total data volume allowed (as defined on *Voucher Definitions* page)

  <?traffic_used?>: Data volume used up (as defined on *Voucher Definitions* page)

Templates can contain *if* variables that make up sections like the ones shown below. Each section has an opening and a closing variable. The contents of an *if* section is only displayed on a specific condition.

If Section	Meaning
<?if_loggedin?> <?if_loggedin_end?>	Section is displayed when the user has successfully logged in.
<?if_notloggedin?> <?if_notloggedin_end?>	Section is displayed when the user has not yet logged in, e.g., because terms of use have to be accepted or because an error occurred.

If Section	Meaning
<?if_authtype_password?> <?if_authtype_password_end?>	Section is displayed when hotspot type is *Password of the day*.
<?if_authtype_disclaimer?> <?if_authtype_disclaimer_end?>	Section is displayed when hotspot type is *Terms of Use Acceptance*.
<?if_authtype_token?> <?if_authtype_token_end?>	Section is displayed when hotspot type is *Voucher*.
<?if_authtype_backend?> <?if_authtype_backendtoken_end?>	Section is displayed when hotspot type is *Backend Authentication*.
<?if_location?> <?if_location_end?>	Section is displayed when the user has been redirected.
<?if_redirect_url?> <?if_redirect_url_end?>	Section is displayed when the checkbox *Redirect to URL after login* is enabled.
<?if_not_redirect_url?> <?if_not_redirect_url_end?>	Section is displayed when the checkbox *Redirect to URL after login* is disabled.
<?if_timelimit?> <?if_timelimit_end?>	Section is displayed when a validity period is set for a voucher.
<?if_trafficlimit?> <?if_trafficlimit_end?>	Section is displayed when a data volume is set for a voucher.

If Section	Meaning
<?if_timequota?> <?if_timequota_ end?>	Section is displayed when a time quota is set for a voucher.
<?if_maclimit?> <?if_maclimit_ end?>	Section is displayed when a *Devices per voucher* value is specified.
<?if_terms?> <?if_terms_end?>	Section is displayed when Terms of Use are defined and enabled.
<?if_error?> <?if_error_end?>	Section is displayed when an error occurred while trying to log in.

User-Specific Login Form

If you want to create your own login form instead of using the pre-defined `<?login_form?>` variable, consider the following:

- Enclose the form in the following tags:
  `<form action="?action=login" method="POST">...</form>`
- For a Terms of Use Acceptance hotspot, add a checkbox named "accept":
  `<input type="checkbox" name="accept">`
- For Password of the Day or Voucher hotspots, add a text box named "token":
  `<input type="text" name="token">`
- For a Backend Authentication hotspot, add the two text boxes named "username" and "password":
  `<input type="text" name="username">`
  `<input type="password" name="password">`
- Add a means to submit the form, e.g., a Login button:
  `<input type="submit" name="login" value="Login">`

12.6.3 Voucher Definitions

On the *Wireless Protection* > *Hotspots* > *Voucher Definitions* tab you can manage different voucher definitions for voucher type hotspots.

To create a voucher definition, proceed as follows:

1. **Click *Add Voucher Definition*.**
   The *Add Voucher Definition* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this voucher definition.

   Validity period: Enter the time span for which a voucher with this definition will be valid. Counting is started at the first login. It is highly recommended to enter a time period.

   Note – The maximum time for the *Validity Period* is two years.

   Time quota: Here you can restrict the allowed online time. Enter the maximum online time after which a voucher of this definition expires. Counting is started at login and is stopped at logout. Additionally, counting is stopped after 5 minutes of inactivity.

   Note – The maximum time for the *Time Quota* is two years.

   Data volume: Here you can restrict the allowed data volume. Enter the maximum data volume to be transmitted with this voucher definition.

   Note – The maximum *Data Volume* is 100 GB.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The voucher definition will be created. It can now be selected when creating a voucher-type hotspot.

To either edit or delete a voucher definition, click the corresponding buttons.

12.6.4 Advanced

General Voucher Options

Here you can decide if and after which time interval you want to delete expired vouchers from the database. In the hotspot log you will still find information about the deleted vouchers.

Walled Garden

Add or select specific hosts or networks to be always accessible by all users, without entering a password or a voucher code. How to add a definition is explained on the *Definitions & Users* >

Network Definitions > *Network Definitions* page.

13 Webserver Protection

This chapter describes how to configure the web application firewall of Sophos UTM which protects your webservers against attacks and malicious behavior.

The following topics are included in this chapter:

13.1 Web Application Firewall

Using the Web Application Firewall (WAF), also known as reverse proxy, Sophos UTM lets you protect your webservers from attacks and malicious behavior like cross-site scripting (XSS), SQL injection, directory traversal, and other potent attacks against your servers. You can define external addresses (virtual servers) which should be translated into the "real" machines in place of using the DNAT rule(s). From there, servers can be protected using a variety of patterns and detection methods. In simpler terms, this area of UTM allows the application of terms and conditions to requests which are received and sent from the webserver. It also offers load balancing across multiple targets.

13.1.1 Virtual Webservers

On the *Web Application Firewall* > *Virtual Webservers* tab you can create virtual webservers. Those webservers, as part of the UTM, build the firewall between the Internet and your webservers. That is why this kind of intervention is also known as reverse proxy. The UTM picks up the requests for the webservers and protects the real webservers from various attacks. Each virtual server maps to a real webserver and determines what level of protection is applied. You can also use more than one real webserver in one virtual webserver definition. That way you get load balancing for your real webservers.

To add a virtual server, do the following:

1. **Click the *New Virtual Webserver* button.**
   The *Create Virtual Webserver* dialog box opens.

2. **Make the following settings:**
Name: Enter a descriptive name for the virtual webserver.

Interface: Select an interface from the drop-down list over which the webserver can be reached.

Note – If there are interfaces with a IPv4 and a IPv6 address, only the IPv4 address will be taken for the Web Application Firewall. It is not possible to use link local addresses as frontend interface.

Type: Determine whether you want the communication between the client and the virtual webserver to be *Encrypted (HTTPS)* or *Plaintext (HTTP)*. When you want to use reverse authentication, we highly recommend to select *Encrypted (HTTPS)* for security reasons.

Port: Enter a port number on which the virtual webserver can be reached from external. Default is port 80 with *Plaintext (HTTP)* and port 443 with *Encrypted (HTTPS)*.

Redirect from HTTP to HTTPS (only with *Encrypted (HTTPS)*): If enabled, users entering the URL without `https://` will be redirected automatically to the virtual webserver.

Certificate (only with *Encrypted (HTTPS)*): Select the webserver's certificate from the drop-down list. The certificate needs to be created beforehand on the web server, and be uploaded on the *Certificate Management* > *Certificates* tab.

Domain: This field displays the hostname for which the certificate had been created.

Domains (only with SAN certificates): The WAF supports Subject Alternative Name (SAN) certificates. All hostnames covered by a certificate will be listed in this box. You can then select one or more hostnames by selecting the checkbox in front of a hostname.

Domains (only with *Plaintext (HTTP)* or *Encrypted (HTTPS)* with wildcard certificate): Enter the domains the webserver is responsible for as FQDN, e.g. `shop.example.com`, or use the Action icon to import a list of domain names. You can use an asterisk (*) as a wildcard for the prefix of the domain, e.g.,`*.mydomain.com`. Domains with wildcards are considered as fallback settings: The virtual webserver with the wildcard domain entry is only used when no other virtual webserver with a more specific domain name is

configured. Example: A client request to `a.b.c` will match `a.b.c` before `*.b.c` before `*.c`.

If *Redirect from HTTP to HTTPS* is enabled, at least one non-wildcard domain must be configured as the target of the redirection (a wildcard domain is not a valid redirection target). The first non-wildcard domain in the domain list is used as the redirection target.

Real webservers: Create a new real webserver or select the checkbox in front of the webserver you want to apply the firewall profile to. If you have mirroring webservers you can also select more than one webserver. By default, traffic will be load-balanced between the selected webservers. The implemented request counting algorithm automatically assigns each new request to the webserver with the lowest number of active requests at present. On the *Site Path Routing* tab you can specify detailed balancing rules.

Firewall profile: Select a firewall profile from the drop-down list. This profile is applied to protect the selected webservers. You can also select *No Profile* to not use any firewall profile.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
Disable compression support (optional): By default, this checkbox is disabled and the content is sent compressed when both the client requests compressed data and the real webserver supports one of the requested compression schemas. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your webservers, it can be necessary to disable compression support. When the checkbox is enabled, the WAF will request uncompressed data from the real webservers of this virtual webserver and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

Rewrite HTML (optional): Select this option to have the UTM rewrite links of the returned webpages in order for the links to stay valid. Example: One of your real webserver instances has the hostname `yourcompany.local` but the virtual server's hostname on the UTM is `yourcompany.com`. Thus, absolute links like `<a href="http://yourcompany.local/">` will be broken if the link is not rewritten to `<a href="http://yourcompany.com/">` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your webserver or if internal links on your webpages are always realized as relative links. It is

recommended to use the option with Microsoft's Outlook Web Access and/or Sharepoint Portal Server.

Note – It is likely that some links cannot be rewritten correctly and are therefore rendered invalid. Ask your website author(s) to format links consistently.

Apart from URL rewriting, the HTML rewriting feature also fixes malformed HTML, for example:

- `<title>` tags are moved in DOM tree from node `html > title` to correct `html > head > title`
- Quotes around HTML attribute values are fixed (e.g., `name="value"` becomes `name="value"`)

Note – HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.

Cross Reference – Please see the libxml documentation for further information (http://xmlsoft.org/html/libxml-HTMLparser.html).

Rewrite Cookie (optional, only visible if *Rewrite HTML* is enabled): Select this option to have the UTM rewrite cookies of the returned webpages.

Note – If *Rewrite HTML* is disabled the *Rewrite Cookie* option will be also disabled.

Pass host header (optional): When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the webserver. Whether passing the host header is necessary in your environment however depends on the configuration of your webserver.

4. **Click *Save*.**
   The server is added to the *Virtual Webservers* list.
5. **Enable the virtual webserver.**
   The new virtual webserver is disabled by default (toggle switch is gray). Click the toggle switch to enable the virtual webserver.

   The virtual webserver is now enabled (toggle switch is green).

The *Virtual Webservers* list displays a status icon for each real webserver assigned to a virtual webserver. The status icon of a real webserver is red when the real webserver has not been enabled. It is amber when the real webserver is down or unavailable and green if everything is working.

13.1.2 Real Webservers

On the *Web Application Firewall > Real Webservers* tab you can add the webservers that are to be protected by the WAF.

To add a webserver, do the following:

1. **Click the *New Real Webserver* button.**
   The *Create Real Webserver* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the webserver.

   Host: Add or select a host, which can either be of the type *Host* or *DNS Host*. We highly recommend to use the DNS hostname here because hosts listed with their IP address transmit empty host headers which leads to problems with some browsers. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Type: Determine whether you want the communication between the UTM and the webserver to be *Encrypted (HTTPS)* or *Plaintext (HTTP)*.

   Port: Enter a port number for the communication between the UTM and the webserver. Default is port 80 with *Plaintext (HTTP)* and port 443 with *Encrypted (HTTPS)*.

   Comment (optional): Add a description or other information.
3. **Optionally, make the following advanced settings:**
   Enable HTTP keepalive: By default, the WAF uses HTTP keepalive, i.e., HTTP persistent connections, which helps to reduce CPU and memory usage. In rare cases where the real webserver does not support HTTP keepalive properly, this feature can provoke reading errors or timeouts and should then be disabled for the affected webserver. When a virtual webserver is assigned at least one real webserver with HTTP keepalive disabled, the feature will automatically be disabled for all real webservers assigned to this virtual webserver.
4. **Click *Save*.**
   The server is added to the *Real Webservers* list.

The webservers present can now be assigned firewall profiles on the *Virtual Webservers* tab.

13.1.3 Firewall Profiles

On the *Web Application Firewall* > *Firewall Profiles* tab you can create WAF profiles that define the modes and levels of protection for your webservers.

To create a WAF profile, do the following:

1. **Click the *New Firewall Profile* button.**
   The *Create Firewall Profile* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the profile.

   Pass Outlook Anywhere: Allows external Microsoft Outlook clients to access the Microsoft Exchange Server via the WAF. Microsoft Outlook traffic will not be checked or protected by the WAF.

   Note – If you select *Pass Outlook Anywhere* the conditions below are disabled.

   Mode: Select a mode from the drop-down list:

   - **Monitor:** HTTP requests are monitored and logged.
   - **Reject:** HTTP requests are rejected.

   The selected mode is applied when an HTTP request meets any one of the conditions selected below.

   Note – If you select one of the conditions below *Pass Outlook Anywhere* is disabled.

   Common Threats filter: If enabled, you can protect your webservers from several threats. You can specify the threat filter categories you want to use in the *Threat Filter Categories* section below. All requests will be checked against the rule sets of the selected categories. Depending on the results, a notice or a warning will be shown in the live log or the request will be blocked directly.

   Rigid Filtering: If enabled, several of the selected rules will be tightened. This may lead to false positives.

Skip filter rules: Some of the selected threat categories may contain rules that lead to false positives. To avoid false positives induced by a specific rule, add the rule number that you want to skip to this box. WAF rule numbers can for example be retrieved on the *Logging & Reporting* > *Webserver Protection* > *Details* page, via the *Top Rules* filter.

Cookie signing: Protects a webserver against manipulated cookies. When the webserver sets a cookie, a second cookie is added to the first cookie containing a hash built of the primary cookie's name, its value and a secret, where the secret is only known by the WAF. Thus, if a request cannot provide a correct cookie pair, there has been some sort of manipulation and the cookie will be dropped.

URL hardening: Protects against URL rewriting. For that, when a client requests a website, all URLs of the website are signed. The signing uses a similar procedure as with cookie signing. Additionally the response from the webserver is analyzed regarding what links can be validly requested next. Hardened URLs can furthermore be bookmarked and visited later. Select one of the following methods to define entry URLs:

- **Entry URLs specified manually:** Enter URLs that serve as kind of entry URLs of a website and therefore do not need to be signed. They need to comply with the syntax of the following examples: `http://shop.example.com/products/`, `https://shop.example.com/products/` or `/products/`.
- **Entry URLs from uploaded Google sitemap file:** You can upload a sitemap file here which contains information on your website structure. Sitemap files can be uploaded in XML or in plain-text format, the latter simply containing a list of URLs. As soon as the profile is saved, the sitemap file is going to be parsed by the WAF.
- **Entry URLs from Google sitemap URL:** You can have the UTM download a sitemap file from a defined URL which contains information on your website structure. This file can be checked for updates at a regular interval. As soon as the profile is saved, the sitemap file is going to be downloaded and parsed by the WAF.

  URL: Enter the path to the sitemap as absolute URL.

  Update: Select an update interval from this drop-down list. When you select *Manual* the sitemap is going to be updated only when you save this profile anew.

Note – When using Reverse Authentication with Frontend Mode *Form* on a designated path, it is not necessary to specify entry URLs for the login form and for

this path. How to configure the path is described on the *Webserver Protection > Web Application Firewall > Site Path Routing* page.

Note – URL hardening affects all files with a HTTP content type of `text/*` or `*xml*`, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the URL hardening feature.

Form hardening: Protects against web form rewriting. Form hardening saves the original structure of a web form and signs it. Therefore, if the structure of a form has changed when it is submitted the server will reject the request.

Note – Form hardening affects all files with a HTTP content type of `text/*` or `*xml*`, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the form hardening feature.

Antivirus: Select this option to protect a webserver against viruses.

Mode: Sophos UTM features several antivirus engines for best security.

- **Single Scan:** Default setting; provides maximum performance using the engine defined on the *System Settings* > *Scan Settings* tab.
- **Dual Scan:** Provides maximum recognition rate by scanning the respective traffic twice using different virus scanners. Note that dual scan is not available with BasicGuard subscription.

Direction: Select from the drop-down list whether to scan only up- or downloads or both.

Block unscannable content: Select this option to block files that cannot be scanned. The reason for that may be, among other things, that files are encrypted or corrupt.

Block clients with bad reputation: Based on GeoIP and RBL information you can block clients which have a bad reputation according to their classification. Sophos uses the following classification providers:

RBL sources:

- Commtouch IP Reputation (ctipd.org)
- dnsbl.proxybl.org
- http.dnsbl.sorbs.net

The GeoIP source is Maxmind. The WAF blocks clients that belong to one of the following Maxmind categories:

- A1: Anonymous proxies or VPN services used by clients to hide their IP address or their original geographical location.
- A2: Satellite providers are ISPs that use satellites to provide Internet access to users all over the world, often from high risk countries.

Skip remote lookups for clients with bad reputation: As reputation lookups include sending requests to remote classification providers, using reputation-based blocking may slow down your system. Select this checkbox to only use GeoIP-based classification which uses cached information and is therefore much faster.

Comment (optional): Add a description or other information.

3. **Optionally, select the following threat filter categories** (only available when *Common Threats filter* is enabled):
Protocol Violations: Enforces adherence to the RFC standard specification of the HTTP protocol. Violating these standards usually indicates malicious intent.

Protocol Anomalies: Searches for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers like 'Host' and 'User-Agent'.

Request Limits: Enforces reasonable limits on the amount and ranges of request arguments. Overloading request arguments is a typical attack vector.

HTTP Policy: Narrows down the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely used options protects against attackers aiming at these often less well supported options.

Bad Robots: Checks for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your webservers are less likely to be discovered.

Generic Attacks: Searches for attempted command executions common to most attacks. After having breached a webserver, an attacker usually tries to execute

commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.

SQL Injection Attacks: Checks for embedded SQL commands and escape characters in request arguments. Most attacks on webservers target input fields that can be used to direct embedded SQL commands to the database.

(XSS) Attacks: Checks for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target webserver, often in a legitimate way.

Tight Security: Performs tight security checks on requests, like checking for prohibited path traversal attempts.

Trojans: Checks for usage patterns characteristic of trojans, thus searching for requests indicating trojan activity. It does not, however, prevent the installation of such trojans as this is covered by the antivirus scanners.

Outbound: Prevents webservers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.

4. **Click *Save*.**
   The WAF profile is added to the *Firewall Profiles* list.

Additional Information on URL Hardening and Form Hardening

It would be best practice to always enable both URL hardening and form hardening because those two functions are complementary, especially in the way that they prevent issues you may have when enabling just one of them:

- Only form hardening is activated: When a webpage contains hyperlinks with appended queries (which is the case with certain CMSs), e.g. `http://example.com/?view=article&id=1`, such page requests are blocked by form hardening because it expects a signature which is missing.
- Only URL hardening is activated: When a web browser appends form data to the action URL of the `form` tag of a web form (which is the case with GET requests), the form data becomes part of the request URL sent to the webserver, by that rendering the URL signature invalid.

The reason why activating both functions solves those issues is that in case either form hardening or URL hardening find that a request is valid, the server accepts the request.

Outlook Web Access

The configuration of the WAF for Outlook Web Access (OWA) is a bit tricky since OWA handles requests from a public IP differently than internal requests from an internal LAN IP to the OWA website. There are redirects attached in the URLs of OWA, where for external access the external FQDN is used, whereas for internal requests the internal server's IP address is used.

The solution is to set the OWA directory as *Entry URL* in the WAF profile of your OWA webserver (e.g. `http://webserver/owa/`). Additionally, you need to create an exception which skips URL hardening for the path `/owa/*` and to disable cookie signing completely for the virtual server.

13.1.4 Exceptions

On the *Web Application Firewall > Exceptions* tab you can define web requests or source networks that are to be exempt from certain checks.

1. **On the *Exceptions* tab, click *New Exception List*.**
   The *Create Exception List* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the exception.

   Skip these checks: Select the security check(s) that should be skipped. See *Firewall Profiles* for descriptions.

   Skip these categories: Select the threat filter categories that should be skipped. See *Firewall Profiles* for descriptions.

   Virtual webservers: Select the virtual webservers that are to be exempt from the selected check(s).

   For all requests: Select a request definition from the drop-down list. Note that you can logically combine two request definitions by either AND or OR.

   Networks: Add or select the source networks where the client request comes from and which are to be exempt from the selected check(s). How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Paths: Add the paths that are to be exempt from the selected check(s), in the form of e.g. `/products/images/*`.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   Never change HTML during URL Hardening or Form Hardening: If selected, no data matching the defined exception settings will be modified by the WAF engine. With this option, e.g., binary data wrongly supplied with a text/html content type by the real webserver will not be corrupted. On the other hand, web requests may be blocked due to activated URL hardening, HTML rewriting, or form hardening. Those three features use an HTML parser and therefore to some extent depend on the modification of webpage content. To prevent undesired blocking, skip URL hardening and/or form hardening for requests affected by blocking; you might need to do this in another/new exception to reflect dependencies between webservers and/or webpages.
4. **Click *Save*.**
   The new exception appears on the *Exceptions* list.
5. **Enable the exception.**
   The new exception is disabled by default (toggle switch is gray). Click the toggle switch to enable the exception.

   The exception is now enabled (toggle switch is green).

To either edit or delete an exception, click the corresponding buttons.

13.1.5 Site Path Routing

On the *Web Application Firewall* > *Site Path Routing* tab you can define to which real webservers incoming requests are forwarded. You can for example define that all URLs with a specific path, e.g., `/products`, are sent to a specific webserver. On the other hand you can allow more than one webserver for a specific request but add rules how to distribute the requests among the servers. You can for example define that each session is bound to one webserver throughout its lifetime (sticky session). This may for example be necessary if you host an online shop and want to make sure that a user sticks to one server during his shopping session. You can also configure to send all requests to one webserver and use the others only as a backup.

For each virtual webserver, one default site path route (with path `/`) is created automatically. The UTM automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no

other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, e.g., because the default route was deleted, the request will be denied.

Note – The *Site Path Routing* tab can only be accessed after at least one real webserver and one virtual webserver have been created.

To create a site path route, proceed as follows:

1. **Click the *New Site Path Route* button.**
   The *Create Site Path Route* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the site path route.

   Virtual webserver: Select the original target host of the incoming traffic.

   Path: Enter the path for which you want to create the site path route, e.g., `/products`.

   Reverse Authentication: Select the authentication profile with the users or groups that should have access to this site path route. When no profile is selected, no authentication is required.

   Caution – Using a reverse authentication profile on a Virtual Webserver running in plain text mode will expose user credentials. Continuing will cause the Web Application Firewall to send user credentials in an unsafe manner.

   Caution – An authentication profile with frontend mode *Form* can only be deployed once on any one Virtual Webserver.

   Real webservers: Select the checkboxes in front of the real webservers which are to be used for the specified path. The order of the selected webservers is only relevant for the *Enable hot-standby mode* option. With the Sort icons you can change the order.

   Comment (optional): Add a description or other information.
3. **Optionally, make the following advanced settings:**
   Enable sticky session cookie: Select this option to ensure that each session will be bound to one real webserver. If enabled, a cookie is passed to the user's browser, which provokes the UTM to route all requests from this browser to the same real webserver. If

the server is not available, the cookie will be updated, and the session will switch to another webserver.

Enable hot-standby mode: Select this option if you want to send all requests to the first selected real webserver, and use the other webservers only as a backup. The backup servers are only used in case the main server fails. As soon as the main server is back working, the sessions will switch back—unless you selected the *Enable sticky session cookie* option.

4. **Click *Save*.**
   The site path route is added to the *Site Path Routing* list.

To either edit or delete a site path route, click the corresponding buttons.

13.1.6 Advanced

On the *Web Application Firewall > Advanced* tab you can define the keys used for cookie signing and URL hardening.

Cookie Signing

Here you can enter a custom secret that is used as signing key for cookie signing.

URL Hardening

Here you can enter a custom secret that is used as signing key for URL hardening.

Form Hardening

Here you can enter a custom secret that is used as encryption key for the form hardening token. The secret must consist of at least eight characters.

13.2 Reverse Authentication

On the *Webserver Protection > Reverse Authentication* pages, you can define how to use the web application firewall to authenticate users directly instead of leaving the authentication to the real webservers. Via authentication profiles, the reverse authentication can be used to assign specific authentication settings to each site path route.

An authentication profile is basically defined by two authentication modes: the authentication mode used between the user and the WAF and the authentication mode used between the WAF and the real webservers. Thus, even if a real webserver does not support authentication,

the WAF can enforce authentication of the users. On the other hand, reverse authentication ensures that a user only has to authenticate once, even if more than one real webserver is assigned to the respective virtual webserver.

Using forms for user authentication, you can specify company-specific form templates.

13.2.1 Profiles

On the *Webserver Protection* > *Reverse Authentication* > *Profiles* tab, you specify authentication profiles for the web application firewall. With profiles you can assign different authentication settings to different users or user groups. After specifying the authentication profiles, you can assign them to site path routes on the *Web Application Firewall* > *Site Path Routing* tab.

To add an authentication profile, do the following:

1. **On the *Profiles* tab, click *New Authentication Profile*.**
   The *Create Authentication Profile* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the profile.

   Frontend mode: Select how the users should authenticate at the web application firewall.

   Basic: Users authenticate with HTTP basic authentication, entering username and password. As the credentials are sent unencrypted with this mode, it should be used over HTTPS. With this mode, no session cookies will be generated and a dedicated logout is not possible.

   Form Template: Users will be presented a form where they have to enter their credentials. With this mode, session cookies will be generated and a dedicated logout is possible. The form template to be used can be selected in the *Form template* drop-down list. Besides the default form template, the list shows the forms that have been defined on the *Form Templates* tab.

   Frontend realm: The realm is a unique string that is used to define the path to the URL authentication form. It is important to enter a string that is not used as a path on the related real webserver, otherwise the real webserver path would not be accessible by the users.

Note – These characters are allowed for the *Frontend Realm*: A-Z a-z 0-9 , ; . : - _ # ' + =) (& % $! ^ < > | @

Form template: Select the form template that will be presented to the users for authentication. Form templates are defined on the *Form Templates* page.

Backend mode: Select how the web application firewall authenticates against the real webservers. The backend mode has to match the real webservers' authentication settings.

Basic: Authentication works with HTTP basic authentication, providing username and password.

None: There is no authentication between the WAF and the real webservers. Note that even if your real webservers do not support authentication, users will be authenticated via the frontend mode.

Users/Groups: Select the users or user groups or add new users that should be assigned to this authentication profile. After assigning this profile to a site path route, these users will have access to the site path with the authentication settings defined in this profile. Typically, this would be a backend user group. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

Note - Sometimes users should be required to use the User Principal Name notation 'user@domain' when entering their credentials, for example when using Exchange servers in combination with Active Directory servers. How to use User Principal Name notation on the *Definitions & Users > Authentication Services > Servers > Active Directory* page.

Comment (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
Enable Session Timeout: To limit the session.

Session Timeout: To set the time value.

Session Timeout Scope: To set the scope to *day(s)*, *hour(s)* or *minute(s)*.

Limit Session Lifetime: To limit the lifetime of the session.

Session Lifetime: To set the lifetime value.

Session Lifetime Scope: To set the scope to *day(s)*, *hour(s)* or *minute(s)*.

Note - The *Cookie Encryption Secret* is displayed if the *Frontend Mode* is set to *Form*.

Strip Basic Authentication (if *Frontend Mode* is *Form* and *Backend Mode* is *None*): To pass through HTTP Basic Authentication header *Authorize* so that double-layered HTTP authentication can be used.

4. **Optionally, make the following advanced settings:**
Enable Session Timeout: Select this option to enable a timeout for the user session which will confirm user credentials by having them log in again if they do not perform any action on the Virtual Webserver.

Session Timeout: Set a interval for the Session Timeout.

Session Timeout Scope: Set a scope for the Session Timeout.

Limit Session Lifetime: Select this option to enable a hard limit for how long users may remain logged in, regardless of activity in the mean time.

Session Lifetime: Set a interval for the Limit Session Lifetime.

Session Lifetime Scope: Set a scope for the Session Lifetime.

Cookie Encryption Secret: Set the secret for the Cookie encryption.

Note – The *Cookie Encryption Secret* is only available when the *Frontend Mode* is set to *Form* in the Authentication Profile.

Strip Basic Authentication: Activate the checkmark to strip the basic authentication.

Note – *Strip Basic Authentication* is only available when the *Backend Mode* is set to *None* in the Authentication Profile.

Caution – When using Reverse Authentication in combination with OTP the OTP tokens will only be checked once when a user session is set up. Once a session is set up, any subsequent request by the same user will not have their OTP tokens evaluated. This is because malicious users might exploit the OTP configuration by sending an overwhelming amount of requests to authentication protected paths, thereby invoking OTP

checks and effectively running a DoS attack on the authentication daemon. Passwords and all other request aspects will still be checked to match the configuration.

5. **Click *Save*.**
   The new profile appears on the *Profiles* list.

To either edit or delete a profile, click the corresponding buttons.

13.2.2 Form Templates

On the *Webserver Protection* > *Reverse Authentication* > *Form Templates* tab, you can upload HTML forms for reverse authentication. A form template can be assigned to an authentication profile with frontend mode *Form*. The respective form will be presented when a user tries to access a site path to which the authentication profile is assigned.

To add a form template, do the following:

1. **On the *Form Templates* tab, click *New Form Template*.**
   The *Create Form Template* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the form template.

   Filename: Click the folder icon to select and upload the HTML template.

   Images/stylesheets: Select and upload the images, stylesheets, or Javascript files that are used by the selected form template.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new form template appears on the *Form Templates* list.

To either edit or delete a form template, click the corresponding buttons.

13.3 Certificate Management

Using the *Webserver Protection* > *Certificate Management* menu, which contains the same configuration options as the *Site-to-site VPN* > *Certificate Management* menu, you can manage all certificate-related operations of Sophos UTM. This includes creating or importing X.509

certificates as well as uploading so-called *Certificate Revocation Lists* (CRLs), among other things.

13.3.1 Certificates

See *Site-to-site VPN* > *Certificate Management* > *Certificates*.

13.3.2 Certificate Authority

See *Site-to-site VPN* > *Certificate Management* > *Certificate Authority*.

13.3.3 Revocation Lists (CRLs)

See *Site-to-site VPN* > *Certificate Management* > *Revocation Lists (CRLs)*.

13.3.4 Advanced

See *Site-to-site VPN* > *Certificate Management* > *Advanced*.

14 RED Management

This chapter describes how to configure Sophos RED. RED is short for *Remote Ethernet Device* and is a means to connect remote branch offices and the like to your main office as if the branch office is part of your local network.

The setup consists of the Sophos UTM in your main office and a Remote Ethernet Device (RED) in your remote office. Establishing a connection between the two is utmost easy as the RED appliance itself does not need to be configured at all. As soon as the RED appliance is connected to your UTM it behaves like any other Ethernet device on your UTM. All traffic of your branch office is safely routed via your UTM which means that your branch office is as secure as your local network.

There are currently two types of RED appliances available:

- RED 10: RED solution for small remote offices
- RED 50: RED solution for bigger remote offices which comes with two uplink interfaces.

The following topics are included in this chapter:

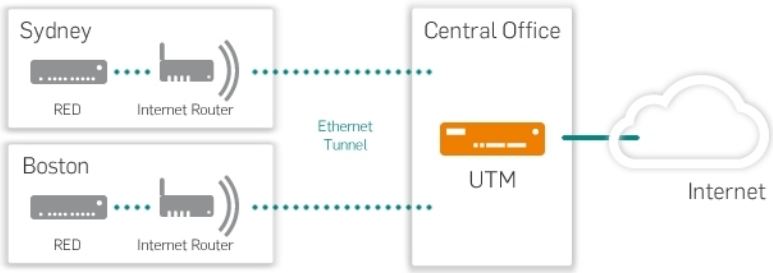

Figure 25 RED: Setup Sketch

Setting up a RED environment involves the following steps:

1. Activation of RED support.
2. Configuration of the RED appliance on your UTM.
3. Connecting the RED appliance to the Internet on the remote site.

Note – The overview page of RED displays general information on the RED architecture as long as no RED appliance is configured. When a RED appliance has been configured, the page will display information on the RED status.

14.1 Overview

The page *Overview* provides general information on what RED is meant for, how it works, and how a typical RED setup looks like.

Cross Reference – For detailed information about RED devices see the *Quick Start guides* and *Operating Instructions* in the Sophos UTM Resource Center. The LED blink codes of the RED 10 appliances are described in the Sophos Knowledgebase.

Open RED Live Log

You can use the live log to monitor the connection between your Sophos UTM and the RED appliance. Click the *Open RED Live Log* button to open the live log in a new window.

14.2 Global Settings

On the *Global Settings* tab you can enable or disable the support for RED which means that your UTM acts as a RED hub. You need to enable the RED support before any RED appliances can connect to the UTM.

RED Configuration

To enable RED support, do the following:

1. **On the *Global Settings* tab, enable RED support.**
   Click the toggle switch.

   The toggle switch turns amber and the *RED Hub Configuration* area becomes editable.

2. **Enter your organization details.**
   By default the settings from the *Management* > *System Settings* > *Organizational* tab is used.
3. **Click *Activate RED*.**
   The toggle switch turns green and RED support is activated. Your UTM is now registered at the RED Provisioning Service (RPS) of Sophos to act as a RED hub.

   You can now continue by adding one or more RED appliances on the *Client Management* page, or use the wizard on the *Deployment Helper* page.

To cancel the configuration, click the amber colored toggle switch.

Automatic Device Deauthorization

When RED support is enabled, you can specify if disconnected RED appliances should automatically be deauthorized after a certain time span. With this feature, you can prevent stolen RED appliances from connecting to the UTM.

Note –The *Automatic Device Deauthorization* does not work for RED Tunnel between 2 UTMs.

1. **Enable automatic deauthorization.**
   Select the *Enable Automatic Device Deauthorization* checkbox.
2. **Specify a time span after which the RED appliance should be deauthorized.**
   Enter the desired value into the *Deauthorize After* text box. The minimum time span is 5 minutes.
3. **Click *Apply*.**
   The automatic device deauthorization is now activated.

When a RED appliance reconnects after being disconnected for a time span longer than the defined time span, it will automatically be disabled. This is indicated by the toggle switches on the *Client Management* page. A respective warning will be displayed on the *Overview* page as well. To permit a deauthorized RED appliance to connect again, enable that RED appliance on the *Client Management* page.

14.3 Client Management

On the *RED Management > Client Management* page you can enable remote UTMs to connect to your UTM using a Remote Ethernet Device (RED) tunnel. The remote UTMs then simply act like RED appliances. Furthermore you can configure RED appliances manually (expert mode) instead of using the deployment helper. The deployment helper is a more convenient way to configure RED appliances and can be found on the next WebAdmin page.

Each RED appliance or UTM that is configured here is able to establish a connection to your UTM.

The *[Server]* tag in front of the page name indicates that this page only needs configuration if the UTM should act as server (RED hub).

Note – For RED appliances to be able to connect, you need to enable RED support on the *Global Settings* page first.

Setting Up a RED Tunnel Between Two UTMs

To enable another UTM to connect to your local UTM using a RED tunnel, do the following:

1. **On the *Client Management* tab, click *Add RED*.**
   The *Add RED* dialog box opens.
2. **Make the following settings:**
   Branch Name: Enter a name for the branch where the client UTM is located, e.g. "Office Munich".

   Client Type: Select *UTM* from the drop-down list.

   Tunnel ID: By default, *Automatic* is selected. Tunnels will be numbered consecutively. You need to make sure that the tunnel ID is unique for both UTMs. In this case you might need to select another ID from the drop-down list.
3. **Click *Save*.**

   The UTM object is being created.
4. **Download the provisioning file.**

To provide the remote (client) UTM with the configuration data download the provisioning file using the *Download* button and transfer the file to the remote UTM in a secure way.

Configuring a RED Appliance

To enable a RED appliance to connect to your local UTM, do the following:

1. **On the *Client Management* tab, click *Add RED*.**
   The *Add RED* dialog box opens.
2. **Make the following settings:**
   Branch Name: Enter a name for the branch where the RED appliance is located, e.g. "Office Munich".

   Client Type: Select *RED 10* or *RED 50* from the drop-down list, depending on the type of RED appliance you want to connect.

   Note – The RED 50 appliance has an LCD display. It can be used to show you important information about the device. With the Left button you can enter the menu. Navigate with the Up and Down button and enter with the Right button. Please see the Operating Instructions for further information.

   RED ID: Enter the ID of the RED appliance you are configuring. This ID can be found on the back of the RED appliance and on its packaging.

   Tunnel ID: By default, *Automatic* is selected. Tunnels will be numbered consecutively. In case you have conflicting IDs, select another ID from the drop-down list.

   Unlock Code (optional): For the first deployment of a RED appliance, leave this box empty. In case the RED appliance you are configuring has been deployed before, you need to provide its unlock code. The unlock code is generated during the deployment of a RED appliance, and is emailed instantly to the address provided on the *Global Settings* tab. This is a security feature, which ensures that a RED appliance cannot simply be removed and installed elsewhere.

   Note – For manual deployment via USB stick and automatic deployment via RED Provisioning Service (see below), two separate unlock codes are generated. If

you switch a RED device from one deployment method to the other, make sure to use the corresponding unlock code: For manual deployment, provide the unlock code of the last manual deployment; for automatic deployment, provide the unlock code of the last automatic deployment.

If you are not in the possession of the unlock code, the only way to unlock the RED appliance is to contact the Sophos Support. The Support however can only help you if you deployed the configuration automatically, via the Sophos RED Provisioning Service.

Tip – The unlock code can also be found in the backup file of the UTM the RED was connected to in case that the backup contains host-specific data.

UTM Hostname: You need to enter a public IP address or hostname where the UTM is accessible.

2nd UTM Hostname: For RED 50 appliances, you can enter another public IP address or hostname of the same UTM. Note that you cannot enter the IP or hostname of a different UTM.

Use 2nd hostname for (only with RED 50, see images below): You can configure what the second hostname should be used for.

- **Failover:** Select to only use the second hostname in case the first hostname fails.
- **Balancing:** Select to activate active load balancing between both hostnames. This makes sense if both uplinks the first and the second hostname correlate to, are equal in latency and throughput.

Uplink mode/2nd Uplink mode: You can define how the RED appliance receives an IP address, which can be either via DHCP or by directly assigning a static IP address. For RED 50 appliances you define the uplink mode for each RED uplink Ethernet port separately.

- **DHCP Client:** The RED pulls an IP address from a DHCP server.
- **Static Address:** Enter an IPv4 address, a corresponding netmask, a default gateway and a DNS server.

Note – There is no one-to-one association between UTM hostname and RED uplink Ethernet port. Each RED port will try to connect to each defined UTM hostname.

Use 2nd uplink for (only with RED 50, see images below): You can configure what the second uplink should be used for.

- **Failover:** Select to only use the second uplink in case the first uplink fails.
- **Balancing:** Select to activate active load balancing between both uplinks. This makes sense if both uplinks on the RED 50 appliance are equal in latency and throughput.

Operation mode: You can define how the remote network will be integrated into your local network.

- **Standard/Unified:** The UTM completely controls the network traffic of the remote network. Additionally, it serves as DHCP server and as default gateway. All remote network traffic will be routed through the UTM.
- **Standard/Split:** The UTM completely controls the network traffic of the remote network. Additionally, it serves as DHCP server and as default gateway. In contrast to the Unified mode, only certain traffic will be routed through the UTM. Define local networks in the *Split Networks* box below which can be accessed by remote clients.

  Note – VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED appliance, use the *Standard* operation mode instead.

- **Transparent/Split:** The UTM does not control the network traffic of the remote network, it does neither serve as DHCP server nor as default gateway. On the contrary, it pulls an IP address from the DHCP server of the remote network to become a part of that network. However, you can enable access for remote clients to your local network. For that you need to define *Split Networks* that are allowed to be accessed by the remote network. Additionally, you can define one or more *Split Domains* to be accessible. If your local domains are not publicly resolvable, you need to define a *Split DNS Server*, which can be queried by remote clients.

> **Note –** VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED appliance, use the *Standard* operation mode instead.

You can find examples for all the operation modes on the *Deployment Helper* tab.

3. **For RED 50, optionally make the following switch port configuration settings:**
   LAN port mode: RED 50 offers four LAN ports that can be configured either as simple switches or for intelligent VLAN usage. When set to *Switch*, all traffic will basically be sent to all ports. When set to *VLAN*, traffic can be filtered according to the Ethernet frames' VLAN tag, thus allowing to tunnel more than one network into the RED tunnel.

   LAN modes: When using the VLAN switch port configuration, you can configure each LAN port separately. For each LAN port, the following options are available:

   Untagged: Ethernet frames with the VLAN IDs specified in the *LAN VID(s)* field below will be sent to this port. The frames are sent without tags, thus the end devices do not have to support VLAN. This port allows just one VLAN ID.

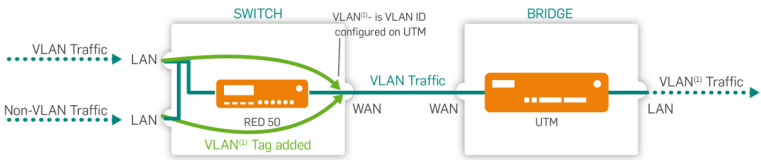

Figure 26 LAN mode: Untagged

Untagged, drop tagged: Ethernet frames with the VLAN IDs specified in the *LAN VID(s)* field below will not be sent to this port. The frames are sent without tags, thus the end devices do not have to support VLAN.

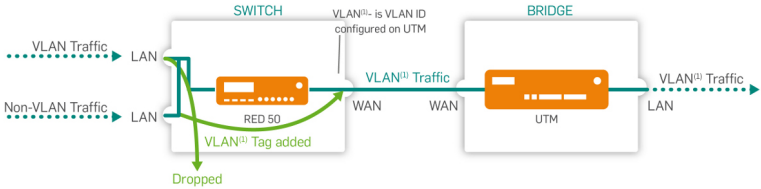

Figure 27 LAN mode: Untagged, drop tagged

Tagged: Ethernet frames with the VLAN IDs specified in the *LAN VID(s)* field below will be sent to this port. The frames are sent with tags, and the end devices have to support VLAN. Frames without VLAN IDs will not be sent to this port. This port allows up to 64 different VLAN ID(s) separated by comma.

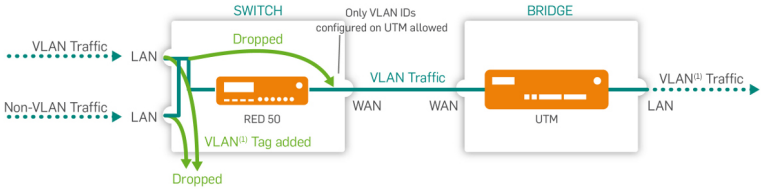

Figure 28 LAN mode: Tagged

Disabled: This Port is closed. No frames with or without VLAN IDs specified in the *LAN VID(s)* will be sent to this port.

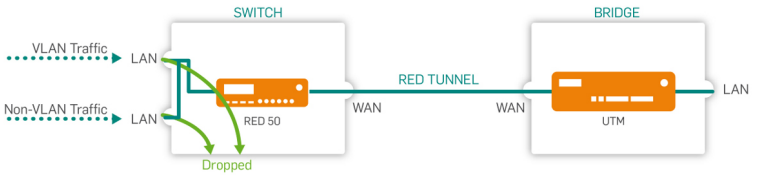

Figure 29 LAN mode: Disabled

Note – The *LAN modes* have different names in the Cisco/HP documentation. *Untagged* also known as 'Hybrid Port', *Untagged, drop tagged* also known as 'Access Port' and *Tagged* also known as 'Trunk Port'.

4. **Optionally, make the following advanced settings:**

   MAC filtering type: To restrict the MAC addresses allowed to connect to this RED appliance, select *Blacklist* or *Whitelist*. With *Blacklist*, all MAC addresses are allowed except those listed on the MAC address list selected below. With *Whitelist*, all MAC addresses are prohibited except those listed on the MAC address list selected below.

   MAC addresses: The list of MAC addresses used to restrict access to the RED appliance. MAC address lists can be created on the *Definitions & Users > Network Definitions > MAC Address Definitions* tab. Note that for RED 10, a maximum of 200 MAC addresses is allowed, whereas for RED 50, the list may contain up to 400 MAC addresses.

   Note – MAC filtering only works for RED rev. 2 or newer.

   Device deployment: Select how you want to provide the necessary configuration settings for the RED. By default, the UTM provides the RED's configuration data automatically via Sophos' RED Provisioning Service. In this case, the RED appliance receives its configuration via Internet. If for example your RED does not have an Internet connection, you can provide the configuration manually, via USB stick.

   Note – Once you deployed a RED device offline you need to deploy it online to check with the RED Provisioning Service before you can deploy it offline again. Manual device deployment only works for RED appliances with firmware version 9.1 or newer.

   Caution – If you select manual deployment, it is extremely important to keep the unlock code, which is sent by email. If you lose the unlock code, you can never again connect the RED appliance to another UTM.

   Data compression: Enabling data compression will compress all traffic that is sent through the RED tunnel. Data compression might increase the throughput of the RED appliance in areas with a very slow Internet connection such as 1-2 Mbps. However, any performance increase mainly depends on the entropy of the data being sent (for example, already compressed data such as HTTPS or SSH cannot be compressed any further). In some circumstances it might therefore be possible that enabling data compression could actually reduce the throughput of the RED appliance. In that case, please disable data compression.

Note – Data compression is not available for RED 10 rev.1.

3G/UMTS failover: Starting with RED rev. 2, the RED appliance offers a USB port, where you can plug in a 3G/UMTS USB stick. If selected, this stick can serve as Internet uplink failover in case of a WAN interface failure. For the necessary settings please refer to your Internet provider's data sheet.

- **Username/Password** (optional): If required, enter a username and password for the mobile network.
- **PIN** (optional): Enter the PIN of the SIM card if a PIN is configured.

  Note – If you enter a wrong PIN, in case of a WAN interface failure, the connection via 3G/UMTS cannot be established. Instead, the *3G/UMTS failover* checkbox of the RED appliance will automatically be unselected. Thus, the wrong PIN will only be used once. When the WAN interface comes up again, a warning will be displayed for the RED appliance: *A wrong PIN was entered for 3G/UMTS failover uplink. Please change the login data.* When you open the *Edit RED* dialog box, a message is displayed which tells you that the *3G/UMTS failover* was automatically unselected. Correct the PIN before selecting the checkbox again. Please note that after three connection attempts with a wrong PIN, the SIM card will be locked. Unlocking cannot be done via the RED appliance or the UTM. The signal strength for the most supported *3G/UMTS* USB Sticks is displayed in the Live Log and the RED 50 LCD display.

- **Mobile network:** Select the mobile network type, which is either GSM or CDMA.
- **APN:** Enter your provider's Access Point Name information.
- **Dial string** (optional): If your provider uses a different dial string, enter it here. Default is *99#.

Note – You always have to make the following configurations manually: 1) Creating the necessary firewall rules (*Network Protection* > *Firewall* > *Rules*). 2) Creating the necessary masquerading rules (*Network Protection* > *NAT* > *Masquerading*).

5. **Click *Save*.**
   The RED appliance is being created and appears on the *RED* list.

With automatic device deployment, as soon as the RED has booted, it will fetch its configuration at the Sophos RED Provisioning Service (RPS). After that the connection between your UTM and the RED appliance is going to be established.

With manual device deployment, the new entry in the *RED* list will have a *Download* button. Download the configuration file and save it to the root directory of a USB stick. Then plug the USB stick into the RED appliance before turning it on. The RED will fetch its configuration from the USB stick. After that the connection between your UTM and the RED appliance is going to be established.

Caution – It is crucial that you keep the unlock code, which is emailed instantly to the address provided on the *Global Settings* tab as soon as the RED appliance receives its configuration. (In case of switching between manual and automatic deployment, make sure to keep both unlock codes.) You need the unlock code when you want to use the RED appliance with another UTM. If you then do not have the unlock code ready, the only way to unlock the RED appliance is to contact the Sophos Support. The Support however can only help you if you deployed the configuration automatically, via the Sophos RED Provisioning Service.

To edit a RED appliance, click the corresponding button. You can see the appliance status of all configured RED appliances on the *RED* overview page of WebAdmin.

The following images give an overview of the four balancing/failover combinations RED 50 provides. Solid lines reflect balancing, dotted lines failover behavior:

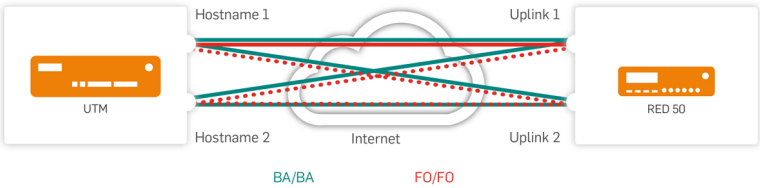

Figure 30 RED 50: Hostname and Uplink Balancing (turquoise) and Hostname and Uplink Failover (red)

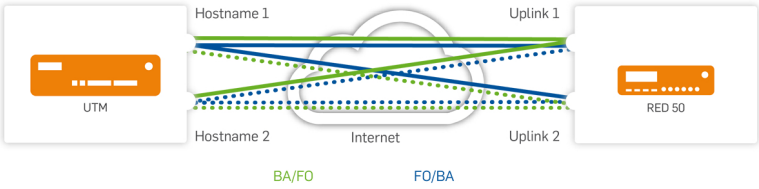

Figure 31 RED 50: Hostname Balancing and Uplink Failover (green) and Hostname Failover and Uplink Balancing (blue)

Deleting a RED Appliance

To delete a RED appliance, click the *Delete* button next to the appliance name.
There will be a warning that the RED object has dependencies. Be aware that deleting a RED appliance will *not* delete associated interfaces and their dependencies. This is intentional, since it enables you to move an interface from one RED appliance to another.

If you want to remove a RED appliance setup completely, you need to delete potential interface and other definitions manually.

14.4 Deployment Helper

The *RED Management* > *Deployment Helper* tab provides a wizard that facilitates setting up and integrating a RED environment. The wizard is meant to be a simple alternative to the normal configuration on the *Client Management* tab. You only need to fill in the requested fields, if needed also fields marked *optional*, and to click *Deploy RED*.

The *[Server]* tag in front of the page name indicates that this page only needs configuration if the UTM should act as server (RED hub).

Note – For your convenience, with *Standard* and *Standard/Split* mode, in contrast to the *Client Management* tab, the deployment helper automatically creates the following objects: a local interface with the specified IP address; a DHCP server for the remote network, covering half of the available IP address range; access to the local DNS resolver. In *Transparent/Split* mode, the deployment helper only creates a DHCP client (*Ethernet DHCP*) interface.

The deployment helper provides short descriptions for every option and a sketch for each of the three operation modes offered by the RED technology.

Below you find a description and use case examples for the three operation modes of RED.

Standard/Unified

The UTM manages the whole remote network. It acts as DHCP server and as default gateway.

Example: You have a branch office and, for security reasons, you want all its traffic to be routed via your headquarter UTM. That way the remote site becomes a part of your local network as if it were connected via LAN.

Standard/Split

Note – VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED appliance, use the *Standard* operation mode instead.

As with the *Standard* mode, the UTM manages the whole remote network. It acts as DHCP server and as default gateway. The difference is that only traffic targeted to networks listed in the *Split Networks* box is redirected to your local UTM. All traffic not targeted to the defined split networks is directly routed to the Internet.

Example: You have a branch office and you want it to have access to your local intranet or you want to route traffic of the remote network via your UTM for security reasons, e.g. to have the traffic checked for viruses or to use an HTTP proxy.

Transparent/Split

Note – VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED appliance, use the *Standard* operation mode instead.

The remote network stays independent, the UTM is a part of this network by getting an IP address from the remote DHCP server. Only certain traffic of the remote network is allowed to access certain networks or local domains of yours. Since the UTM has no control of the remote network, local domains, which are not publicly resolvable, cannot be resolved by the remote router unless you define a *Split DNS Server*. This is a local DNS server of yours which can then be queried by remote clients.

Technically, the local interface of the RED appliance and its uplink interface to your local UTM as well as its link to the remote router are bridged. (For RED 50 appliances, LAN ports are bridged only to WAN 1.) Since the UTM is only a client of the remote network, routing traffic to the split networks the same way as with the other modes is not possible. Therefore, the RED appliance intercepts all traffic: Traffic targeting to a network listed in the *Split Networks* box or going to a domain listed in the *Split Domains* box is redirected to the UTM interface. This is accomplished by replacing the default gateway's MAC address in the respective data packets with the UTM's MAC address.

Example: There is a partner or a service provider who should have access to your intranet or a certain server in your local network. Using a RED appliance, that partner's network will stay completely independent of your network, but they can access a defined part of your network for certain purposes, as if they were connected via LAN.

Note – Using the deployment helper, the uplink mode of the RED appliance is *DHCP Client* in either operation mode. If you need to assign it a static IP address instead, you need to configure the RED appliance on the *Client Management* tab.

14.5 Tunnel Management

On the *RED Management* > *Tunnel Management* page you can configure your UTM to act as a RED appliance to be able to establish a RED tunnel to another UTM. The remote host UTM will then serve as RED hub for your UTM.

The *[Client]* tag in front of the page name indicates that this page only needs configuration if the UTM should act as RED client.

To connect your UTM to the host UTM you need a provisioning file. This file needs to be generated on the host UTM (see *Client Management*).

To connect your UTM to the host UTM, proceed as follows:

1. **On the host UTM, add your local UTM to the *Client Management* list.**
2. **On the host UTM, download the provisioning file for your UTM.**
3. **On your local UTM, click *Add Tunnel*.**
   The *Add Tunnel* dialog box opens.
4. **Make the following settings:**
   Tunnel Name: Enter a descriptive name for this tunnel.

UTM Host: Select the remote UTM host.

Prov. File: Click the Folder icon, select the provisioning file you want to upload, and click *Start Upload*.

Comment (optional): Add a description or other information.

5. **Click *Save*.**
   The RED tunnel will be established and displayed on the *Tunnel Management* list.

15 Site-to-site VPN

This chapter describes how to configure site-to-site VPN settings of Sophos UTM. Site-to-site VPNs in Sophos UTM are realized by means of *Virtual Private Networks* (VPNs), which are a cost effective and secure way for remote networks to communicate confidentially with each other over a public network such as the Internet. They use the cryptographic tunneling protocol IPsec to provide confidentiality and privacy of the data transmitted over them.

Cross Reference – More information on how to configure site-to-site VPN connections can be found in the Sophos Knowledgebase.

The following topics are included in this chapter:

- Amazon VPC
- IPsec
- SSL
- Certificate Management

The *Site-to-site VPN* overview page in WebAdmin shows all configured Amazon VPC, IPsec, and SSL connections and their current status. The state of each connection is reported by the color of its status icons. There are two types of status icons. The larger ones next to the connection name inform about the overall status of a connection. The different colors mean:

- Green – All SAs (*Security Association*) have been established. Connection is fully functional.
- Yellow – Not all SAs have been established. Connection is partly functional.
- Red – No SAs have been established. Connection is not functional.

The smaller ones next to the tunnel information report the status for that tunnel. Here the colors mean:

- Green – All SAs have been established. Tunnel is fully functional.
- Yellow – IPsec SA has been established, ISAKMP SA (*Internet Security Association and Key Management Protocol*) is down. Tunnel is fully functional.
- Red – No SAs have been established. Connection is not functional.

15.1 Amazon VPC

Amazon Virtual Private Cloud (VPC) is a commercial cloud computing service. A user can create virtual private clouds, which can subsequently be connected to a local network and centrally managed over IPsec tunnels.

You can connect your Amazon VPC to your Sophos UTM if the UTM has a static public IP address. The entire configuration of the VPN connections has to be done in the Amazon environment. Afterwards you just import the connection data using your Amazon access data or a configuration file.

15.1.1 Status

The *Site-to-site VPN* > *Amazon VPC* > *Status* page shows a list of all connections to your Amazon VPCs.

Here you can enable and disable the connections.

To enable connections to Amazon VPC, proceed as follows:

1. **On the *Setup* page, import at least one VPC connection.**
2. **On the *Status* page, enable Amazon VPC.**
   Click the toggle switch.

   The toggle switch turns green and the imported VPC connections are displayed.
3. **Enable the desired connection.**
   Click the toggle switch of the connection you want to enable.

   The toggle switch turns green and the two tunnels of the VPC connection are displayed.

   Note – Each connection consists of two tunnels for redundancy reasons: an active and a backup tunnel. Active tunnels can be identified by having a netmask at the end of their BGP line. The status icons of the tunnels are displayed for control purposes only—you cannot enable or disable a single tunnel.

To disable all Amazon VPC connections click the topmost toggle switch. To disable a single connection click the toggle switch of the respective connection.

To close a connection and delete it from the list, click the red Delete icon of the respective connection.

Note – As the connections are configured on Amazon VPC's side, you can re-import a deleted connection into Sophos UTM with the same data as before.

15.1.2 Setup

On the *Site-to-site VPN > Amazon VPC > Setup* page you add connections to your Amazon Virtual Private Cloud (VPC). You can either import all connections configured with one Amazon Web Service (AWS) account and using the IP address of your Sophos UTM as *Customer Gateway* (Amazon term for your endpoint of a VPC VPN connection). Or you add connections one by one using the configuration file which you can download from Amazon.

Import Via Amazon Credentials

You can import all connections configured with one AWS account and using the IP address of your Sophos UTM as Customer Gateway, at once. Just enter the AWS credentials you have been given when you created your Amazon Web Service account.

Note – All existing connections listed in the *Status* tab will be deleted during the import.

To import connections, proceed as follows:

1. **Make the following settings:**
   Access Key: Enter the Amazon Access Key ID. It is a 20-character, alphanumeric sequence.

   Secret Key: Enter the Secret Access Key. It is a 40-character sequence.

2. **Click *Apply*.**

   The connections are imported and subsequently displayed on the *Status* page.

Import Via Amazon Configuration

To add a single connection to the existing list of connections you have to upload the configuration file of the respective connection.

To import a single connection, proceed as follows:

1. **Download the configuration file of your Amazon VPC connection.**
   In Amazon's download dialog make sure to select *Sophos* from the *Vendor* drop-down list.
2. **Open the *Upload file* dialog window.**
   Click the Folder icon next to the *VPC Config File* box.
3. **Select the configuration file and upload it.**
   To upload the selected file click the button *Start Upload*.

   The filename is displayed in the *VPC Config File* box.
4. **If you use static routing, enter the remote network.**
   The remote network is not part of the configuration file. Therefore you need to enter it separately into the *Remote network* field, e.g. 10.0.0.0/8. This field is only important if you have configured the use of static routing instead of dynamic routing in Amazon VPC.
5. **Click *Apply*.**
   The connection is imported and subsequently displayed on the *Status* page.

Route Propagation

You can configure networks which are being pushed in route propagation enabled Routing Tables in the Amazon VPC.

To select local networks, proceed as follows:

1. **Add local networks.**
   Add or select a local network that should be pushed in route propagation. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.
2. **Click *Apply*.**
   The Route Propagation networks are applied.

15.2 IPsec

IP Security (IPsec) is a standard for securing *Internet Protocol* (IP) communications by encrypting and/or authenticating all IP packets.

The IPsec standard defines two service modes and two protocols:

- Transport mode
- Tunnel mode
- *Authentication Header* (AH) authentication protocol
- *Encapsulated Security Payload* (ESP) encryption (and authentication) protocol

IPsec also offers methods for manual and automatic management of *Security Associations* (SAs) as well as key distribution. These characteristics are consolidated in a *Domain of Interpretation* (DOI).

IPsec Modes

IPsec can work in either transport mode or tunnel mode. In principle, a host-to-host connection can use either mode. If, however, one of the endpoints is a security gateway, the tunnel mode must be used. The IPsec VPN connections on this UTM always use the tunnel mode.

In transport mode, the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent either in clear text (AH) or encrypted (ESP). Either the complete packet can be authenticated with AH, or the payload can be encrypted and authenticated using ESP. In both cases, the original header is sent over the WAN in clear text.

In tunnel mode, the complete packet—header and payload—is encapsulated in a new IP packet. An IP header is added to the IP packet, with the destination address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then authenticated with AH or encrypted and authenticated using ESP.

IPsec Protocols

IPsec uses two protocols to communicate securely on the IP level.

- **Authentication Header (AH):** A protocol for the authentication of packet senders and for ensuring the integrity of packet data.
- **Encapsulating Security Payload (ESP):** A protocol for encrypting the entire packet and for the authentication of its contents.

The *Authentication Header* protocol (AH) checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a *Hash-based Message*

Authentication Code (HMAC) in connection with a key. One of the following hashing algorithms will be used:

- **Message Digest Version 5 (MD5):** This algorithm generates a 128-bit checksum from a message of any size. This checksum is like a fingerprint of the message, and will change if the message is altered. This hash value is sometimes also called a digital signature or a message digest.
- **The Secure Hash (SHA-1):** This algorithm generates a hash similar to that of MD5, though the SHA-1 hash is 160 bits long. SHA-1 is more secure than MD5, due to its longer key.

Compared to MD5, an SHA-1 hash is somewhat harder to compute, and requires more CPU time to generate. The computation speed depends, of course, on the processor speed and the number of IPsec VPN connections in use at the Sophos UTM.

In addition to encryption, the *Encapsulated Security Payload* protocol (ESP) offers the ability to authenticate senders and verify packet contents. If ESP is used in tunnel mode, the complete IP packet (header and payload) is encrypted. New, unencrypted IP and ESP headers are added to the encapsulating packet: The new IP header contains the address of the receiving gateway and the address of the sending gateway. These IP addresses are those of the VPN tunnel.

For ESP with encryption normally the following algorithms are used:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Of these, AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 bits. Sophos UTM supports a number of encryption algorithms. Either the MD5 or SHA-1 algorithms can be used for authentication.

NAT Traversal (NAT-T)

NAT traversal is a technology for establishing connections between hosts in TCP/IP networks which use NAT devices. This is achieved by using UDP encapsulation of the ESP packets to establish IPsec tunnels through NAT devices. UDP encapsulation is only used if NAT is detected between the IPsec peers; otherwise normal ESP packets will be used.

With NAT traversal you are able to place the gateway or a road warrior behind a NAT router and still establish an IPsec tunnel. Both IPsec peers must support NAT traversal if you want to use this feature, which is automatically negotiated. Make sure that the NAT device has IPsec-passthrough turned off, because this could impair the use of NAT traversal.

If road warriors want to use NAT traversal, their corresponding user object in WebAdmin must have a static remote access IP address (RAS address) set (see also *Use Static Remote Access IP* on the *Users* page in WebAdmin).

By default, a NAT traversal keep-alive signal is sent at intervals of 60 seconds to prevent an established tunnel from expiring when no data is transmitted. The keep-alive messages are sent to ensure that the NAT router keeps the state information associated with the session so that the tunnel stays open.

TOS

Type of Service bits (TOS bits) are several four-bit flags in the IP header. These bits are referred to as *Type of Service* bits because they allow the transferring application to tell the network which type of service quality is necessary.

With the IPsec implementation of Sophos UTM the TOS value is always copied.

15.2.1 Connections

On the *Site-to-site VPN > IPsec > Connections* tab you can create and edit IPsec connections.

To create an IPsec connection, proceed as follows:

1. **On the *Connections* tab, click *New IPsec Connection*.**
   The *Add IPsec Connection* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this connection.

   Remote gateway: Select a remote gateway definition. Remote gateways are configured on the *Site-to-site VPN > IPsec > Remote Gateways* tab.

   Local interface: Select the name of the interface which is used as the local endpoint of the IPsec tunnel.

   Policy: Select the IPsec policy for this IPsec connection. IPsec policies can be defined on the *Site-to-site VPN > IPsec > Policies* tab.

   Local networks: Select or add the local networks that should be reachable through the VPN tunnel. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Automatic firewall rules: By selecting this option you can automatically add firewall rules that allow traffic for this connection. The rules are added as soon as the connection is enabled, and they are removed when the connection is disabled. If you want to use a stricter IPsec connection, disable *Automatic firewall rules* and use IPsec objects in the firewall rule set instead.

Strict routing: If strict routing is enabled, VPN routing is done according to source and destination IP address (instead of only destination IP address). In this case, only those packets exactly matching the VPN tunnel definition are routed into the VPN tunnel. As a consequence, you cannot use SNAT to add networks or hosts to the VPN tunnel, that are originally not part of the tunnel definition. On the other hand, without strict routing, you cannot have a mixed unencrypted/encrypted setup to the same network from different source addresses.

Bind tunnel to local interface: By default, the option is unselected and all traffic originating from the selected local networks and going to the defined remote networks will always be sent through this IPsec tunnel. It is not possible to have multiple identical tunnels on different interfaces because the selector would always be the same. However, if enabled, the defined IPsec selector will be bound to the selected local interface. Thus it is possible to either bypass IPsec policies with static routes or define redundant IPsec tunnels over different uplinks and use multipath rules to balance traffic over the available interfaces and their IPsec tunnels. Use cases for this setting are for example:

- Bypass IPsec policies for local hosts which belong to the remote network through static routes.
- Balance traffic based on layer 3 and layer 4 with multipath rules over multiple IPsec tunnels or MPLS links with automatic failover.

Note – This option cannot be used in combination with an interface group.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new connection appears on the IPsec *Connections* list.

To either edit or delete a connection, click the corresponding buttons.

Open Live Log: The IPsec VPN live log displays monitoring information about established IPsec connection. Click the button to open the live log in a new window.

15.2.2 Remote Gateways

On the *Site-to-site VPN* > *IPsec* > *Remote Gateways* tab you can define the remote gateways for your site-to-site VPN tunnels. These remote network definitions will become available when creating IPsec connections on the *IPsec* > *Connections* tab.

To add a remote gateway, proceed as follows:

1. **On the *Remote Gateways* tab, click *New Remote Gateway*.**
   The *Add Remote Gateway* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this remote gateway.

   Gateway type: Select the type of the gateway. The following types are available:

   - **Initiate connection:** Select if the remote endpoint has a static IP address so that a connection to the remote gateway can be initiated by the gateway. If selected, specify the remote gateway in the *Gateway* box. Note that you can also select this option if the remote gateway is resolved through DynDNS.
   - **Respond only:** Select if the IP address of the remote endpoint is unknown or cannot be resolved through DynDNS. The gateway is not able to initiate a connection to the remote gateway but waits for incoming connections to which it only needs to respond.

   Authentication type: Select the authentication type for this remote gateway definition. The following types are available:

   - **Preshared key:** Authentication with *Preshared Keys* (PSK) uses secret passwords as keys. These passwords must be distributed to the endpoints before establishing the connection. When a new VPN tunnel is established, each side checks that the other knows the secret password. The security of PSKs depends on the quality of the passwords used: common words and phrases are subject to dictionary attacks. Permanent or long-term IPsec connections should use certificates instead.
   - **RSA key:** Authentication using RSA keys is much more sophisticated. In this scheme, each side of the connection generates a key pair consisting of a public key and a private key. The private key is necessary for the encryption and authentication during the key exchange. Both endpoints of an IPsecVPN connection using this authentication method need their own key pair. Copy the public RSA key of the

remote unit (*Site-to-site VPN > IPsec > Local RSA Key*) into the *Public Key* box of the local unit and vice versa. In addition, enter the VPN ID types and VPN identifiers that correspond to the respective RSA keys.

- **Local X.509 certificate:** Similarly, the X.509 certificate authentication scheme uses public keys and private keys. An X.509 certificate contains the public key together with information identifying the owner of the key. Such certificates are signed and issued by a trusted *Certificate Authority* (CA). During the key exchange process, the certificates are exchanged and authenticated using a locally stored CA certificate. Select this authentication type if the X.509 certificate of the remote gateway is locally stored on the unit.
- **Remote X.509 certificate:** Select this authentication type if the X.509 certificate of the remote gateway is not locally stored on the unit. You must then select the VPN ID type and VPN identifier of the certificate being used on the remote unit, that is, the certificate which is selected in the *Local X.509 Certificate* area of the *Site-to-site VPN > IPsec > Advanced* tab.

VPN ID type: Depending on the authentication type you must select a VPN ID type and VPN identifier. The VPN identifier entered here must match the values configured on the remote site. Suppose you are using two UTM appliances for establishing a site-to-site VPN tunnel. If you select *RSA Key* as authentication type on the local unit, the VPN ID type and the VPN identifier must match what is configured on the *Site-to-site VPN > IPsec > Local RSA Key* tab on the remote unit. You can select among the following VPN ID types:

- **IP address**
- **Hostname**
- **Email address**
- **Distinguished name:** Only available with *Remote X.509 Certificate* authentication.
- **Any:** Default with *Respond Only* gateway type.

Remote networks: Select the remote networks that should be reachable via the remote gateway.

Comment (optional): Add a description or other information.

3. **Make advanced settings if necessary.**
   The following advanced settings should only be made when you know what their impact is:

   Support path MTU discovery: PMTU (Path Maximum Transmission Unit) refers to the size of data packets transmitted. It is usually preferable that IP data packets be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. If any of the data packets are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return *ICMP Destination Unreachable* messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path.
   If you enable this option, UTM enables PMTU if it is enabled on the server side.

   Support congestion signaling (ECN): ECN (Explicit Congestion Notification) is an extension to the Internet Protocol and allows end-to-end notifications of network congestion without dropping packets. Select this option if you want to copy ECN information from the original IP packet header into the IPsec packet header. Note that the remote endpoint must support it as well as the underlying network and involved routers.

   Enable XAUTH client mode: XAUTH is an extension of IPsec IKE to authenticate users via username and password at a VPN gateway. To use XAUTH for authentication with this remote gateway, select the option and provide username and password (twice) as required by the remote gateway.

4. **Click *Save*.**
   The gateway definition appears on the *Remote Gateways* list.

To either edit or delete a remote gateway definition, click the corresponding buttons.

15.2.3 Policies

On the *IPsec* > *Policies* tab you can customize parameters for IPsec connections and unite them into a policy. An IPsec policy defines IKE (Internet Key Exchange) and IPsec proposal parameters of an IPsec connection. Note that each IPsec connection needs an IPsec policy.

Note – Sophos UTM only supports the main mode in IKE phase 1. The aggressive mode is not supported.

To create an IPsec policy, proceed as follows:

1. **On the *Policy* tab, click *New IPsec Policy*.**
   The *Add IPsec Policy* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this policy.

   IKE encryption algorithm: The encryption algorithm specifies the algorithm used for encrypting the IKE messages. Supported algorithms are:

   - *DES* (56 bit)
   - *3DES* (168 bit)
   - *AES 128* (128 bit)
   - *AES 192* (192 bit)
   - *AES 256* (256 bit)
   - *Blowfish* (128 bit)
   - *Twofish* (128 bit)
   - *Serpent* (128 bit)

   Security Note – We strongly recommend against using DES, as it is a weak algorithm, and therefore represents a potential vulnerability.

   IKE authentication algorithm: The authentication algorithm specifies the algorithm used for integrity checking of the IKE messages. Supported algorithms are:

   - *MD5* (128 bit)
   - *SHA1* (160 bit)
   - *SHA2 256* (256 bit)
   - *SHA2 384* (384 bit)
   - *SHA2 512* (512 bit)

   IKE SA lifetime: This value specifies the timeframe in seconds for which the IKE SA (security association) is valid and when the next rekeying should take place. Valid values are between 60 sec and 28800 sec (8 hrs). The default value is 7800 seconds.

   IKE DH group: When negotiating a connection, the communicating parties also settle the actual keys used to encrypt the data. In order to generate a session key, IKE uses the

Diffie-Hellman (DH) algorithm, which utilizes random data. The random data generation is based on pool bits. The IKE group basically tells the number of pool bits. The more pool bits, the larger the random numbers. The larger the numbers, the harder it is to crack the Diffie-Hellman algorithm. As a consequence, more pool bits mean more security but also the consumption of more CPU resources. Currently, the following Diffie-Hellman groups are supported:

- *Group 1: MODP 768*
- *Group 2: MODP 1024*
- *Group 5: MODP 1536*
- *Group 14: MODP 2048*
- *Group 15: MODP 3072*
- *Group 16: MODP 4096*

Security Note – Group 1 (MODP 768) is considered weak and only supported for interoperability reasons. We strongly recommend against using it, as it represents a potential vulnerability.

IPsec encryption algorithm: The same encryption algorithms as for IKE. Additionally there are the following entries:

- *No encryption (null)*
- *AES 128 CTR* (128 bit)
- *AES 192 CTR* (192 bit)
- *AES 256 CTR* (256 bit)
- *AES 128 GCM (96 bit)*
- *AES 192 GCM (96 bit)*
- *AES 256 GCM (96 bit)*
- *AES 128 GCM (128 bit)*
- *AES 192 GCM (128 bit)*
- *AES 256 GCM (128 bit)*

Security Note – We strongly recommend against using no encryption or DES, as this represents a potential vulnerability.

IPsec authentication algorithm: The same authentication algorithms as for IKE. Additionally there are the following algorithms:

- *SHA2 256* (96 bit)
- *SHA2 384* (96 bit)
- *SHA2 512* (96 bit)

Those are available for compliance with tunnel endpoints not adhering to RFC 4868, for example UTM (i.e., ASG) versions older than V8, and therefore do not support truncated checksums longer than 96 bit.

IPsec SA lifetime: This value specifies the timeframe in seconds for which the IPsec SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 86400 sec (1 day). The default value is 3600 seconds.

IPsec PFS group: *Perfect Forward Secrecy* (PFS) refers to the notion that if a session key is compromised, it will permit access only to data of this specific session. In order for PFS to exist, the key used to protect the IPsec SA must not be derived from random keying material used to get the keys for the IKE SA. Therefore, PFS initiates a second Diffie-Hellman key exchange proposing the selected DH group for the IPsec connection to get a new randomly generated key. Supported Diffie-Hellman groups are the same as for IKE.
Enabling PFS is considered to be more secure, but it takes also more time for the exchange. It is not recommended to use PFS on slow hardware.

Note – PFS is not fully interoperable with all vendors. If you notice problems during the negotiation, you might consider disabling PFS.

Strict policy: If an IPsec gateway makes a proposition with respect to an encryption algorithm and to the strength, it might happen that the gateway of the receiver accepts this proposition, even though the IPsec policy does not correspond to it. If you select this option and the remote endpoint does not agree on using exactly the parameters you specified, the IPsec connection will not be established. Suppose the IPsec policy of your UTM requires AES-256 encryption, whereas, for example, a road warrior with SSH Sentinel

wants to connect with AES-128; with the strict policy option enabled, the connection would be rejected.

Note – The compression setting will not be enforced via *Strict policy*.

Compression: This option specifies whether IP packets should be compressed by means of the *IP Payload Compression Protocol* (IPComp) prior to encryption. IPComp reduces the size of IP packets by compressing them to increase the overall communication performance between a pair of communicating hosts or gateways. Compression is turned off by default.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new policy appears on the *Policies* list.

To either edit or delete a policy, click the corresponding buttons.

15.2.4 Local RSA Key

With RSA authentication, RSA keys are used for authentication of the VPN endpoints. The public keys of the endpoints are exchanged manually before the connection is established. If you want to use this authentication type, you have to define a VPN identifier and create a local RSA key. The public RSA key of the gateway must be made available to remote IPsec devices that use IPsec RSA authentication with Sophos UTM.

Current Local Public RSA Key

Displayed is the public portion of the currently installed local RSA key pair. Click into the box, then press `CTRL-A` and `CTRL-C` to copy it to the clipboard.

Local RSA Key VPN Options

Select the VPN ID type which best suits your needs. By default, the hostname of the gateway is taken as the VPN identifier. If you have a static IP address as local VPN endpoint, select *IP address*. Alternatively, use an email address as VPN ID for mobile IPsec road warriors.

- **Hostname:** Default setting; the hostname of the gateway. However, you can enter a different hostname here.
- **Email address:** By default, this is the email address of the gateway's admin account.

However, you can enter a different email address here.

- **IP address:** The IP address of the external interface of the gateway.

Click *Apply* to save your settings. Changing the settings does not modify the RSA key.

Re-generate Local RSA Key

To generate a new RSA key, select the desired key size and click *Apply*. This will start the key generation process, which can take from a few minutes up to two hours, according to your selected key length and used hardware. The key size (key length) is a measure of the number of keys which are possible with a cipher. The length is usually specified in bits. The following key sizes are supported:

- 1024 bits
- 2048 bits
- 4096 bits

Once the RSA key has been generated, the appropriate public key will be displayed in the *Current Local Public RSA Key* box. Generating a new RSA key will overwrite the old one.

15.2.5 Advanced

On the *Site-to-site VPN > IPsec > Advanced* tab you can configure advanced options of IPsec VPN. Depending on your preferred authentication type, you can define the local certificate (for X.509 authentication) and the local RSA key (for RSA authentication), among other things. Note that this should only be done by experienced users.

Local X.509 Certificate

With X.509 authentication, certificates are used to verify the public keys of the VPN endpoints. If you want to use this authentication type, you have to select a local certificate from the drop-down list in the *Local X.509 Certificate* area. The selected key/certificate is then used to authenticate the gateway to remote peers if X.509 authentication is selected.

You can only select certificates where the appropriate private key is present, other certificates are not available in the drop-down list.

If there is no certificate available for selection, you have to add one in the *Certificate Management* menu, either by creating a new one or by importing one using the upload function.

After selecting the certificate, enter the passphrase the private key was protected with. During the saving process, the passphrase is verified and an error message is displayed if it does not match the encrypted key.

Once an active key/certificate is selected, it is displayed in the *Local X.509 Certificate* area.

Dead Peer Detection (DPD)

Use Dead Peer Detection: The dead peer detection option is used for automatically terminating a connection if the remote VPN gateway or client is unreachable. For connections with static endpoints, the tunnel will be re-negotiated automatically. Connections with dynamic endpoints require the remote side to re-negotiate the tunnel. Usually it is safe to always enable this option. The IPsec peers automatically determine whether the remote side supports dead peer detection or not, and will fall back to normal mode if necessary.

NAT Traversal (NAT-T)

Use NAT Traversal: Select to enable that IPsec traffic can pass upstream systems which use *Network Address Translation* (NAT). Additionally, you can define the keepalive interval for NAT traversal. Click *Apply* to save your settings.

CRL Handling

There might be situations in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For this purpose, so-called *Certificate Revocation Lists* or CRLs are used. They normally contain the serial numbers of those certificates of a certifying instance, that have been held invalid and that are still valid according to their respective periods of validity.
After the expiration of these periods the certificate will no longer be valid and must therefore not be maintained in the block list.

Automatic Fetching: This function automatically requests the CRL through the URL defined in the partner certificate via HTTP, Anonymous FTP or LDAP version 3. On request, the CRL can be downloaded, saved and updated, once the validity period has expired. If you use this feature but not via port 80 or 443, make sure that you set the firewall rules accordingly, so that the CRL distribution server can be accessed.

Strict Policy: If this option is enabled, any partner certificate without a corresponding CRL will be rejected.

Preshared Key Probing

For IPsec connections using the respond-only mode you can decide to use different preshared keys (PSK) for each IPsec connection.

Enable probing of preshared keys: Select the checkbox to enable this option. This will affect L2TP-over-IPsec, remote access IPsec, and VPN IPsec connections.

15.2.6 Debug

IKE Debugging

In the *IKE Debugging* section you can configure IKE debug options. Select the checkboxes for which types of IKE messages or communication you want to create debug output.

Note – The *IKE Debugging* section is identical across the *Debug* tabs of the menus *Site-to-site VPN IPsec*, *Remote Access IPsec*, *L2TP over IPsec* and *Cisco VPN Client*.

The following flags can be logged:

- **Control Flow:** Displays control messages of IKE state
- **Outbound packets:** Displays content of outgoing IKE messages
- **Inbound packets:** Displays content of incoming IKE messages
- **Kernel messaging:** Displays communication messages with the Kernel
- **High availability:** Displays communication with other HA nodes

15.3 SSL

Site-to-site VPN tunnels can be established via an SSL connection. SSL VPN connections have distinct roles attached. The tunnel endpoints act as either client or server. The client always initiates the connection, the server responds to client requests. Keep in mind that this contrasts IPsec where both endpoints normally can initiate a connection.

Note – If you run into problems in establishing a connection, check whether SSL scanning is activated with the Web Filter operating in transparent mode. If so, make sure that the target

host of the VPN connection has been added to the *Transparent Mode Skiplist* under *Web Protection > Filtering Options > Misc*.

15.3.1 Connections

To create an SSLVPN site-to-site tunnel, it is crucial to create the server configuration first. The configuration of the client has always to be the second step.

To create a server configuration, proceed as follows:

1. **On the *Connections* tab, click *New SSL Connection*.**
   The *Add SSL Connection* dialog box opens.
2. **Make the following settings:**
   Connection type: Select *Server* from the drop-down list.

   Connection name: Enter a descriptive name for the connection.

   Use static virtual IP address (optional): Only select this option if the IP address pool is not compatible with the client's network environment: By default clients are assigned an IP address from the *Virtual IP Pool* (configurable on *Settings* tab). Rarely, it may happen that such an IP address is already in use on the client's host. In that case enter a suitable IP address in the *Static Peer IP* field which will then be assigned to the client during tunnel setup.

   Local networks: Select or add one or more local networks that are allowed to be accessed remotely. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Remote networks: Select or add one or more remote networks that are allowed to connect to the local network(s).

   Note – You can change the *Local networks* and *Remote networks* settings later without having to reconfigure the client.

   Automatic firewall rules (optional): When enabled, the UTM will automatically allow access to the selected local networks for all accessing SSL VPN clients.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new SSL server connection appears on the *Connections* list.

4. **Download the configuration file.**
   Use the *Download* button, which is located in the newly created SSL server connection row, to download the client configuration file for this connection.

   Encrypt configuration file (optional): It is advisable to encrypt the configuration file for security reasons. Enter a password twice.
   Click *Download peer config* to save the file.
   This file is needed by the client-side administrator in order to be able to set up the client endpoint of the tunnel.

The next step is the client configuration which has to take place on client side and *not* on server side. Ensure that the downloaded client configuration file is at hand.

To create a client configuration, proceed as follows:

1. **On the *Connections* tab, click *New SSL Connection*.**
   The *Add SSL Connection* dialog box opens.

2. **Make the following settings:**
   Connection type: Select *Client* from the drop-down list.

   Connection name: Enter a descriptive name for the connection.

   Configuration file: Click the Folder icon, browse for the client configuration file and click *Start Upload*.

   Password (optional): If the file has been encrypted, enter the password.

   Use HTTP proxy server (optional): Select the checkbox if the client is located behind a proxy and enter the settings for the proxy.

      Proxy requires authentication (optional): Select the checkbox if the client needs to authenticate against the proxy and enter username and password.

   Override peer hostname (optional): Select the checkbox and enter a hostname here if the server system's regular hostname (or DynDNS hostname) cannot be resolved from the client host.

   Automatic firewall rules (optional): When enabled, the UTM will automatically allow traffic between hosts on the tunneled local and remote networks.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new SSL VPN client connection appears on the *Connections* list.

To either edit or delete a client connection, click the corresponding buttons.

Click on the *Site-to-site VPN* menu to see the status of the SSL VPN connection on the overview page. The status icon there turns green when the connection is established. Then information about the interconnected subnets on both sides of the tunnel becomes available, too.

15.3.2 Settings

On the *SSL* > *Settings* tab you can configure the basic settings for SSL VPN server connections.

Note – This tab is identical for *Site-to-site VPN* > *SSL* and *Remote Access* > *SSL*. Changes applied here always affect both SSL configurations.

Server Settings

You can make the following settings for the SSL VPN connection:

- **Interface Address:** Default value is *Any*. When using the web application firewall you need to give a specific interface address for the service to listen for SSL connections. This is necessary for the site-to-site/remote access SSL connection handler and the web application firewall to be able to differentiate between the incoming SSL connections.
- **Protocol:** Select the protocol to use. You can choose either *TCP* or *UDP*.
- **Port:** You can change the port. The default port is `443`. You cannot use port `10443`, the SUM Gateway Manager port `4422`, or the port used by the WebAdmin interface.
- **Override Hostname:** The value in the *Override Hostname* box is used as the target hostname for client VPN connections and is by default the hostname of the gateway. Only change the default if the system's regular hostname (or DynDNS hostname) cannot be reached under this name from the Internet.

Virtual IP Pool

Pool Network: This is the virtual IP address pool which is used to distribute IP addresses from a certain IP range to the SSL clients. By default, the *VPN Pool (SSL)* is selected. In case you select a different address pool, the netmask must not be greater than 29 bits, for OpenVPN cannot handle address pools whose netmask is `/30`, `/31`, or `/32`.

Duplicate CN

Select *Allow Multiple Concurrent Connections Per User* if you want to allow your users to connect from different IP addresses at the same time. When disabled, only one concurrent SSL VPN connection is allowed per user.

15.3.3 Advanced

On the *SSL* > *Advanced* tab you can configure various advanced server options ranging from the cryptographic settings, through compression settings, to debug settings.

Note – This tab is identical for *Site-to-site VPN* > *SSL* and *Remote Access* > *SSL*. Changes applied here always affect both SSL configurations.

Cryptographic Settings

These settings control the encryption parameters for all SSL VPN remote access clients:

- **Encryption Algorithm:** The encryption algorithm specifies the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported, which are all in *Cipher Block Chaining* (CBC) mode:
  - *DES-EDE3-CBC*
  - *AES-128-CBC* (128 bit)
  - *AES-192-CBC* (192 bit)
  - *AES-256-CBC* (256 bit)
  - *BF-CBC* (Blowfish (128 bit))
- **Authentication Algorithm:** The authentication algorithm specifies the algorithm used for checking the integrity of the data sent through the VPN tunnel. Supported algorithms are:
  - *MD5* (128 bit)
  - *SHA-1* (160 bit)
  - *SHA2 256* (256 bit)
  - *SHA2 384* (384 bit)
  - *SHA2 512* (512 bit)

- **Key Size:** The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.
- **Server Certificate:** Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.
- **Key Lifetime:** Enter a time period after which the key will expire. The default is 28,800 seconds.

Compression Settings

Compress SSL VPN Traffic: When enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

Debug Settings

Enable Debug Mode: When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

15.4 Certificate Management

The *Site-to-site VPN* > *Certificate Management* menu is the central place to manage all certificate-related operations of Sophos UTM. This includes creating or importing X.509 certificates as well as uploading so-called *Certificate Revocation Lists* (CRLs), among other things.

15.4.1 Certificates

On the *Site-to-site VPN* > *Certificate Management* > *Certificates* tab you can create or import public key certificates in the X.509 standard format. Such certificates are digitally signed statements usually issued by a *Certificate Authority* (CA) binding together a public key with a particular *Distinguished Name* (DN) in X.500 notation.

All certificates you create on this tab contain an RSA key. They are signed by the self-signed certificate authority (CA) *VPN Signing CA* that was created automatically using the information you provided during the initial login to the WebAdmin interface.

To generate a certificate, proceed as follows:

1. **On the *Certificates* tab, click *New Certificate*.**
   The *Add Certificate* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this certificate.

   Method: To create a certificate, select *Generate* (for more information on uploading certificates, see below).

   Key size: The length of the RSA key. The longer the key, the more secure it is. You can choose among key sizes of 1024, 2048, or 4096 bits. Select the maximum key size compatible with the application programs and hardware devices you intend to use. Unless longer keys cause critical performance issues for your specific purposes, do not reduce the key size in order to optimize performance.

   VPN ID type: You have to define a unique identifier for the certificate. The following types of identifiers are available:
   - Email address
   - Hostname
   - IP address
   - Distinguished name

   VPN ID: Depending on the selected VPN ID type, enter the appropriate value into this text box. For example, if you selected *IP address* from the *VPN ID type* list, enter an IP address into this text box. Note that this text box will be hidden when you select *Distinguished Name* from the *VPN ID type* list.

   Use the drop-down lists and text boxes from *Country* to *Email* to enter identifying information about the certificate holder. This information is used to build the *Distinguished Name*, that is, the name of the entity whose public key the certificate identifies. This name contains a lot of personal information in the X.500 standard and is supposed to be unique across the Internet. If the certificate is for a road warrior connection, enter the name of the user in the *Common name* box. If the certificate is for a host, enter a hostname.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The certificate appears on the *Certificates* list.

To delete a certificate click the button *Delete* of the respective certificate.

Alternatively, to upload a certificate, proceed as follows:

1. **On the *Certificates* tab, click *New Certificate*.**
   The *Add Certificate* dialog box opens.

2. **Make the following settings:**
   Name: Enter a descriptive name for this certificate.

   Method: Select *Upload*.

   File type: Select the file type of the certificate. You can upload certificates being one of the following types:

   - **PKCS#12 (Cert+CA):** PKCS refers to a group of *Public Key Cryptography Standards* (PKCS) devised and published by RSA laboratories. The `PKCS#12` file format is commonly used to store private keys with accompanying public key certificates protected with a container passphrase. You must know this container passphrase to upload files in this format.
   - **PEM (Cert only):** A Base64 encoded *Privacy Enhanced Mail* (`PEM`) file format with no password required.

   File: Click the Folder icon next to the *File* box and select the certificate you want to upload.

   Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The certificate appears on the *Certificates* list.

To delete a certificate click the button *Delete* of the respective certificate.

You can download the certificate either in `PKCS#12` or as `PEM` format. The `PEM` file only contains the certificate itself, while the `PKCS#12` file also contains the private key as well as the CA certificate with which it was signed.

15.4.2 Certificate Authority

On the *Site-to-site VPN* > *Certificate Management* > *Certificate Authority* tab you can add new *Certificate Authorities* to the unit. Generally speaking, a certificate authority or *Certification Authority* (CA) is an entity which issues digital certificates for use by other parties. A CA attests that the public key contained in the certificate belongs to the person, organization, host, or other entity noted in the certificate by signing the certificate signing request with the private key of the CA's own certificate. Such a CA is therefore called a signing CA.

On UTM, the signing CA was created automatically using the information you provided during the initial login to UTM. Thus, all certificates you create on the *Certificates* tab are self-signed certificates, meaning that the issuer and the subject are identical. However, you can

alternatively import a signing CA by third-party vendors. In addition, to verify the authenticity of a host or user requesting an IPsec connection, you can also use alternative CA certificates whose private keys are unknown. Those CA certificates are called verification CAs and can be added on this tab as well.

Important Note – You can have multiple verification CAs on your system, but only one signing CA. So if you upload a new signing CA, the previously installed signing CA automatically becomes a verification CA.

To import a CA, proceed as follows:

1. **On the *Certificate Authority* tab, click *Import CA*.**
   The *Import CA* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this CA.

   Type: Select the type of CA you are going to import. You can choose between verification CAs or signing CAs. A verification CA must be available in the `PEM` format, while a signing CA must be available in the `PKCS#12` format.

   CA Certificate: Click the Folder icon next to the *CA Certificate* box and select the certificate you want to import. Note that if you are to upload a new signing CA, you must enter the password with which the `PKCS#12` container was secured.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new CA certificate appears on the *Certificate Authority* list.

To delete a CA click the button *Delete* of the respective CA.

The signing CA can be downloaded in `PKCS#12` format. You will then be prompted to enter a password, which will be used to secure the `PKCS#12` container. In addition, verification CAs can be downloaded in `PEM` format.

15.4.3 Revocation Lists (CRLs)

A CRL is a list of certificates (more precisely, their serial numbers) which have been revoked, that is, are no longer valid, and should therefore not be relied upon. On the *Site-to-site VPN > Certificate Management > Revocation Lists (CRLs)* tab you can upload the CRL that is deployed within your PKI.

To upload a CRL, proceed as follows:

1. **On the *Revocation Lists (CRLs)* tab, click *Upload CRL*.**
   The *Upload CRL* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this CRL.

   CRL File: Click the Folder icon next to the *CRL File* box and select the CRL you want to upload.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**
   The new CRL appears on the list of revocation lists.

To delete a CRL click the button *Delete* of the respective CRL.

15.4.4 Advanced

On the *Site-to-site VPN > Certificate Management > Advanced* tab you can re-generate the VPN Signing CA that was created during the initial setup of the unit. The VPN Signing CA is the certificate authority with which digital certificates are signed that are used for remote access and site-to-site VPN connections. The old VPN signing CA will be kept as verification CA.

Re-generate Signing CA

You can renew all user certificates using the current signing CA. This becomes relevant once you have installed an alternative VPN Signing CA on the *Certificate Authority* tab.

Caution – The UTM and all user certificates will be re-generated using the new signing CA. This will break certificate-based site-to-site and remote access VPN connections.

16 Remote Access

This chapter describes how to configure remote access settings of Sophos UTM. Remote access using Sophos UTM is realized by means of *Virtual Private Networks* (VPNs), which are a cost effective and secure way to provide remote users such as telecommuting employees access to the corporate network. VPNs use cryptographic tunneling protocols such as IPsec and PPTP to provide confidentiality and privacy of the data transmitted over them.

Cross Reference – More information on how to configure remote access VPN connections can be found in the Sophos Knowledgebase.

The UTM automatically generates necessary installation and configuration files for the respective remote access connection type. Those files can be downloaded directly from the User Portal. However, only those files are available to a user that correspond to the connection types enabled for them, e.g., a user who has been enabled to use SSL remote access will find an SSL installation file only.

Note – You can download remote access configuration files of all or selected users on the *Definitions & Users* > *Users & Groups* > *Users* tab.

The *Remote Access Status* page contains an overview of all online users.

The following topics are included in this chapter:

16.1 SSL

The remote access SSL feature of Sophos UTM is realized by OpenVPN, a full-featured SSL VPN solution. It provides the ability to create point-to-point encrypted tunnels between remote employees and your company, requiring both SSL certificates and a username/password combination for authentication to enable access to internal resources. In addition, it offers a secure User Portal, which can be accessed by each authorized user to download a customized SSL VPN client software bundle. This bundle includes a free SSL VPN client, SSL certificates and a configuration that can be handled by a simple one-click installation procedure. This SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

Cross Reference – More information on how to use the SSL VPN client can be found in the Sophos Knowledgebase.

16.1.1 Profiles

On the *Remote Access* > *SSL* > *Profiles* tab you can create different profiles for remote access users defining basic settings for SSL VPN access.

To configure an SSL VPN profile, proceed as follows:

1. **On the *Profiles* tab, click *New Remote Access Profile*.**
   The *Add Remote Access Profile* dialog box opens.
2. **Make the following settings:**
   Profile name: Enter a descriptive name for this profile.

   Users and groups: Select the users or user groups or add new users that should be able to use SSL VPN remote access with this profile. How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.

   Local networks: Select or add the local network(s) that should be reachable to the selected SSL clients through the VPN SSL tunnel. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

Note – By default, the SSL VPN solution of Sophos UTM employs so-called split tunneling, that is, the process of allowing a remote VPN user to access a public network, for example, the Internet, at the same time that the user is allowed to access resources on the VPN. However, split tunneling can be bypassed if you select *Any* in the *Local networks* field. Thus, all traffic will be routed through the VPN SSL tunnel. Whether users are allowed to access a public network then depends on your firewall configuration.

Automatic firewall rules: Select this option to automatically add firewall rules that allow traffic for this profile. The rules are added as soon as the profile is enabled, and they are removed when the profile is disabled. If you do not select this option, you need to specify appropriate firewall rules manually.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new profile appears on the *Profiles* list.

To either edit or delete a profile, click the corresponding buttons.

Note – The *Remote Access* menu of the User Portal is only available to users who are selected in the *Users and groups* box *and* for whom a user definition does exist on the UTM (see *Definitions & Users > Users & Groups > Users*). Authorized users who have successfully logged in to the User Portal find the SSL VPN client software bundle as well as a link to installation instructions, which are available at the Sophos Knowledgebase. Downloading may fail with some browsers on Android if the CA certificate is not installed or if the hostname does not match the common name in the portal certificate. In this case, the user needs to install the CA certificate or try another browser.

Open Live Log

The *OpenVPN Live Log* logs remote access activities. Click the button to open the live log in a new window.

16.1.2 Settings

On the *SSL > Settings* tab you can configure the basic settings for SSL VPN server connections.

Note – This tab is identical for *Site-to-site VPN* > *SSL* and *Remote Access* > *SSL*. Changes applied here always affect both SSL configurations.

Server Settings

You can make the following settings for the SSL VPN connection:

- **Interface Address:** Default value is *Any*. When using the web application firewall you need to give a specific interface address for the service to listen for SSL connections. This is necessary for the site-to-site/remote access SSL connection handler and the web application firewall to be able to differentiate between the incoming SSL connections.
- **Protocol:** Select the protocol to use. You can choose either *TCP* or *UDP*.
- **Port:** You can change the port. The default port is `443`. You cannot use port `10443`, the SUM Gateway Manager port `4422`, or the port used by the WebAdmin interface.
- **Override Hostname:** The value in the *Override Hostname* box is used as the target hostname for client VPN connections and is by default the hostname of the gateway. Only change the default if the system's regular hostname (or DynDNS hostname) cannot be reached under this name from the Internet.

Virtual IP Pool

Pool Network: This is the virtual IP address pool which is used to distribute IP addresses from a certain IP range to the SSL clients. By default, the *VPN Pool (SSL)* is selected. In case you select a different address pool, the netmask must not be greater than 29 bits, for OpenVPN cannot handle address pools whose netmask is `/30`, `/31`, or `/32`.

Duplicate CN

Select *Allow Multiple Concurrent Connections Per User* if you want to allow your users to connect from different IP addresses at the same time. When disabled, only one concurrent SSL VPN connection is allowed per user.

16.1.3 Advanced

On the *SSL* > *Advanced* tab you can configure various advanced server options ranging from the cryptographic settings, through compression settings, to debug settings.

Note – This tab is identical for *Site-to-site VPN > SSL* and *Remote Access > SSL*. Changes applied here always affect both SSL configurations.

Cryptographic Settings

These settings control the encryption parameters for all SSL VPN remote access clients:

- **Encryption Algorithm:** The encryption algorithm specifies the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported, which are all in *Cipher Block Chaining* (CBC) mode:
  - *DES-EDE3-CBC*
  - *AES-128-CBC* (128 bit)
  - *AES-192-CBC* (192 bit)
  - *AES-256-CBC* (256 bit)
  - *BF-CBC* (Blowfish (128 bit))
- **Authentication Algorithm:** The authentication algorithm specifies the algorithm used for checking the integrity of the data sent through the VPN tunnel. Supported algorithms are:
  - *MD5* (128 bit)
  - *SHA-1* (160 bit)
  - *SHA2 256* (256 bit)
  - *SHA2 384* (384 bit)
  - *SHA2 512* (512 bit)
- **Key Size:** The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.
- **Server Certificate:** Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.
- **Key Lifetime:** Enter a time period after which the key will expire. The default is 28,800 seconds.

Compression Settings

Compress SSL VPN Traffic: When enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

Debug Settings

Enable Debug Mode: When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

16.2 PPTP

Point-to-Point Tunneling Protocol (PPTP) allows single Internet-based hosts to access internal network services through an encrypted tunnel. PPTP is easy to configure and requires no special client software on Microsoft Windows systems.

PPTP is included with versions of Microsoft Windows starting with Windows 95. In order to use PPTP with Sophos UTM, the client computer must support the MSCHAPv2 authentication protocol. Windows 95 and 98 users must apply an update to their systems in order to support this protocol.

16.2.1 Global

To configure global PPTP options, proceed as follows:

1. **On the *Global* tab, enable PPTP remote access.**
   Click the toggle switch.

   The toggle switch turns amber and the *Main Settings* area becomes editable.

2. **Make the following settings:**
   Authentication via: Select the authentication mechanism. PPTP remote access only supports local and RADIUS authentication.

   - **Local:** If you select *Local*, specify the users and user groups who should be able to use PPTP remote access. It is not possible to drag backend user groups into the field. Until a user account has been specified, PPTP remote access cannot be activated.

     Note – Username and password of the selected users may only contain ASCII printable characters[1].

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

Note – Similar to SSL VPN, the *Remote Access* menu of the User Portal is only available to users who are selected in the *Users and groups* box and for whom a user definition does exist on the UTM. Authorized users who have successfully logged in to the User Portal will find a link to installation instructions, which are available at the Sophos Knowledgebase.

- **RADIUS:** *RADIUS* can only be selected if a RADIUS server has been previously configured. With this authentication method users will be authenticated against an external RADIUS server that can be configured on the *Definitions & Users* > *Authentication Services* > *Servers* tab. The *Users and Groups* dialog box will be grayed out. However, its settings can still be changed, which has no effect. The RADIUS server must support MSCHAPv2 challenge-response authentication. The server can pass back parameters such as the client's IP address and DNS/WINS server addresses. The PPTP module sends the following string as NAS-ID to the RADIUS server: `pptp`. Note that when RADIUS authentication is selected, local users cannot be authenticated with PPTP anymore. Note further that clients must support MSCHAPv2 authentication as well.

Assign IP addresses by: IP addresses can be either assigned from a predefined IP address pool or distributed automatically by means of a DHCP server:

- **IP Address Pool:** Select this option if you want to assign IP addresses from a certain IP range to the clients gaining remote access through PPTP. By default, addresses from the private IP space `10.242.1.0/24` are assigned. This network definition is called the *VPN Pool (PPTP)* and can be used in all network-specific configuration options. If you want to use a different network, simply change the definition of the *VPN Pool (PPTP)* on the *Definitions & Users* > *Network Definitions* page. Alternatively, you can create another IP address pool by clicking the Plus icon next to the *Pool network* text box.
- **DHCP Server:** If you select *DHCP Server*, also specify the network interface through which the DHCP server is connected. The DHCP server does not have to be directly connected to the interface—it can also be accessed through a router. Note that the local DHCP server is not supported; the DHCP server selected here must be running on a physically different system.

3. **Click *Apply*.**
   Your settings will be saved.

Live Log

The *PPTP Daemon Live Log* logs all PPTP remote access activities. Click the button to open the live log in a new window.

16.2.2 iOS Devices

You can enable that iOS device users are offered automatic PPTP configuration in the User Portal.

However, only users that have been added to the *Users and groups* box on the *Global* tab will find configuration files on their User Portal site. The iOS device status is enabled by default.

Connection name: Enter a descriptive name for the PPTP connection so that iOS device users may identify the connection they are going to establish. The default name is your company name followed by the protocol PPTP.

Note – *Connection Name* must be unique among all iOS device connection settings (PPTP, L2TP over IPsec, Cisco VPN Client).

Override hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

To disable automatic iOS device configuration, click the toggle switch.

The toggle switch turns gray.

16.2.3 Advanced

On the *Remote Access > PPTP > Advanced* tab you can configure the encryption strength and the amount of debug output with regard to PPTP remote access. Note that advanced PPTP options can only be configured if PPTP remote access status is enabled on the *Global* tab.

Encryption Strength

You can choose between strong (128-bit) and weak (40-bit) tunnel encryption (MPPE). Do not use weak encryption unless you have endpoints that do not support 128-bit encryption.

Debug Mode

Enable Debug Mode: This option controls how much debug output is generated in the PPTP log. Select this option if you encounter connection problems and need detailed information about the negotiation of client parameters, for example.

16.3 L2TP over IPsec

L2TP, short for *Layer Two (2) Tunneling Protocol*, is a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet), better known as VPNs. Because of the lack of confidentiality inherent in the L2TP protocol, it is often combined with IPsec, which provides confidentiality, authentication, and integrity. The combination of these two protocols is also known as L2TP over IPsec. L2TP over IPsec allows you, while providing the same functions as PPTP, to give individual hosts access to your network through an encrypted IPsec tunnel.

16.3.1 Global

On the *L2TP over IPsec* > *Global* tab you can configure basic options for setting up remote access via L2TPover IPsec.

To use L2TP over IPsec, proceed as follows:

1. **On the *Global* tab enable L2TP over IPsec.**
   Click the toggle switch.

   The toggle switch turns amber and the *Server Settings and IP Address Assignment* area becomes editable.

2. **Make the following settings:**
   Interface: Select the network interface to be used for L2TP VPN access.

   Authentication mode: You can choose between the following authentication modes:

   - **Preshared key:** Enter a password which is subsequently used as preshared key. The *Preshared Key* method makes use of a shared secret that is exchanged by the communicating parties prior to the communication taking place. To communicate, both parties prove that they know the secret. The shared secret is a secure phrase or password that is used to encrypt the traffic using the encryption

algorithm for L2TP. For best security, you should take appropriate measures to increase the strength of the shared secret. The security of a shared secret depends on the quality of the password and how securely it has been transmitted. Passwords consisting of common words are extremely vulnerable to dictionary attacks. For that reason, the shared secret should be quite long and contain a variety of letters, capital letters, and numbers. Consequently, using a preshared secret as an authentication method should be replaced by certificates whenever possible.

Note – If you want to enable access for iOS devices you need to select *Preshared Key* because iOS devices only support PSK authentication.

- **X.509 CA check:** X.509 certificates ease the process of exchanging public authentication keys in large VPN setups with a lot of participants. A so-called CA gathers and checks the public keys of the VPN endpoints and issues a certificate for each member. The certificate contains the peer's identity along with its public key. Because the certificate is digitally signed, no one else can issue a forged certificate without being detected.
  During the key exchange, certificates are exchanged and verified using locally stored CA public keys. The actual authentication of the VPN endpoints is then done by using public and private keys. If you want to use this authentication mode, select an X.509 certificate.
  Note that for X.509 authentication to work, you need to have a valid CA configured on the *Remote Access* > *Certificate Management* > *Certificate Authority* tab.

Assign IP addresses by: IP addresses can be either assigned from a predefined IP address pool or distributed automatically by means of a DHCP server:

- **Pool network:** By default, *IP Address Pool* is selected as IP address assignment, having the pre-defined *VPN Pool (L2TP)* network definition selected as the *Pool Network*. The *VPN Pool (L2TP)* is a randomly generated network from the `10.x.x.x` IP address space for private Internets, using a class C subnet. It is normally not necessary to ever change this, as it ensures that the users have a dedicated pool of addresses to make connections from. If you want to use a different network, you can simply change the definition of the *VPN Pool (L2TP)*, or assign another network as IP address pool here.

> **Note –** If you use private IP addresses for your L2TP VPN Pool and you want IPsec hosts to be allowed to access the Internet, appropriate masquerading or NAT rules must be in place for the IP address pool.

- **DHCP Server:** If you select *DHCP Server*, also specify the network interface through which the DHCP server is connected. The DHCP server does not have to be directly connected to the interface—it can also be accessed through a router. Note that the local DHCP server is not supported; the DHCP server selected here must be running on a physically different system.

3. **Click *Apply*.**
   Your settings will be saved.

   To cancel the configuration, click the amber colored toggle switch.

Access Control

Authentication via: L2TP remote access only supports local and RADIUS authentication.

- **Local:** If you select *Local*, specify the users and user groups who should be able to use L2TP remote access. It is not possible to drag backend user groups into the field. For local users you need to add users in the usual way and enable L2TP for them. If no users or groups are selected, L2TP remote access is turned off. How to add a user is explained on the *Definitions & Users* > *Users & Groups* > *Users* page.

> **Note –** Username and password of the selected users may only contain ASCII printable characters[1].

> **Note –** Similar to SSLVPN the *Remote Access* menu of the User Portal is only available to users who are selected in the *Users and groups* box and for whom a user definition does exist on the UTM. Depending on the authentication mode, authorized users who have successfully logged in to the User Portal find the IPsec pre-shared key (authentication mode *Preshared key*) or the `PKCS#12` file (authentication mode *X.509 CA Check*) as well as a link to installation instructions, which are available at the Sophos Knowledgebase).

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

- **RADIUS:** If you select *RADIUS*, the authentication requests are forwarded to the RADIUS server. The L2TP module sends the following string as NAS-ID to the RADIUS server: `l2tp`.

The authentication algorithm gets automatically negotiated between client and server. For local users, Sophos UTM supports the following authentication protocols:

- MSCHAPv2
- PAP

By default, a Windows client negotiates MSCHAPv2.

For RADIUS users, Sophos UTM supports the following authentication protocols:

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

16.3.2 iOS Devices

You can enable that iOS device users are offered automatic L2TP over IPsec configuration in the User Portal.

However, only users that have been added to the *Users and groups* box on the *Global* tab will find configuration files on their User Portal site. The iOS device status is enabled by default.

Connection name: Enter a descriptive name for the L2TP over IPsec connection so that iOS device users may identify the connection they are going to establish. The default name is your company name followed by the protocol L2TP over IPsec.

Note – *Connection Name* must be unique among all iOS device connection settings (PPTP, L2TP over IPsec, Cisco VPN Client).

Override hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

To disable automatic iOS device configuration, click the toggle switch.

The toggle switch turns gray.

16.3.3 Debug

IKE Debugging

In the *IKE Debugging* section you can configure IKE debug options. Select the checkboxes for which types of IKE messages or communication you want to create debug output.

Note – The *IKE Debugging* section is identical across the *Debug* tabs of the menus *Site-to-site VPN IPsec*, *Remote Access IPsec*, *L2TP over IPsec* and *Cisco VPN Client*.

The following flags can be logged:

- **Control Flow:** Displays control messages of IKE state
- **Outbound packets:** Displays content of outgoing IKE messages
- **Inbound packets:** Displays content of incoming IKE messages
- **Kernel messaging:** Displays communication messages with the Kernel
- **High availability:** Displays communication with other HA nodes

L2TP Debugging

If *Enable debug mode* is selected, the *IPsec VPN* log file will contain extended information about L2TP or PPP connection negotiation.

16.4 IPsec

IP Security (IPsec) is a standard for securing *Internet Protocol* (IP) communications by encrypting and/or authenticating all IP packets.

The IPsec standard defines two service modes and two protocols:

- Transport mode
- Tunnel mode
- *Authentication Header* (AH) authentication protocol
- *Encapsulated Security Payload* (ESP) encryption (and authentication) protocol

IPsec also offers methods for manual and automatic management of *Security Associations* (SAs) as well as key distribution. These characteristics are consolidated in a *Domain of Interpretation* (DOI).

IPsec Modes

IPsec can work in either transport mode or tunnel mode. In principle, a host-to-host connection can use either mode. If, however, one of the endpoints is a security gateway, the tunnel mode must be used. The IPsec VPN connections on this UTM always use the tunnel mode.

In transport mode, the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent either in clear text (AH) or encrypted (ESP). Either the complete packet can be authenticated with AH, or the payload can be encrypted and authenticated using ESP. In both cases, the original header is sent over the WAN in clear text.

In tunnel mode, the complete packet—header and payload—is encapsulated in a new IP packet. An IP header is added to the IP packet, with the destination address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then authenticated with AH or encrypted and authenticated using ESP.

IPsec Protocols

IPsec uses two protocols to communicate securely on the IP level.

- **Authentication Header (AH):** A protocol for the authentication of packet senders and for ensuring the integrity of packet data.
- **Encapsulating Security Payload (ESP):** A protocol for encrypting the entire packet and for the authentication of its contents.

The *Authentication Header* protocol (AH) checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a *Hash-based Message Authentication Code* (HMAC) in connection with a key. One of the following hashing algorithms will be used:

- **Message Digest Version 5 (MD5):** This algorithm generates a 128-bit checksum from a message of any size. This checksum is like a fingerprint of the message, and will change if the message is altered. This hash value is sometimes also called a digital signature or a message digest.

- **The Secure Hash (SHA-1):** This algorithm generates a hash similar to that of MD5, though the SHA-1 hash is 160 bits long. SHA-1 is more secure than MD5, due to its longer key.

Compared to MD5, an SHA-1 hash is somewhat harder to compute, and requires more CPU time to generate. The computation speed depends, of course, on the processor speed and the number of IPsec VPN connections in use at the Sophos UTM.

In addition to encryption, the *Encapsulated Security Payload* protocol (ESP) offers the ability to authenticate senders and verify packet contents. If ESP is used in tunnel mode, the complete IP packet (header and payload) is encrypted. New, unencrypted IP and ESP headers are added to the encapsulating packet: The new IP header contains the address of the receiving gateway and the address of the sending gateway. These IP addresses are those of the VPN tunnel.

For ESP with encryption normally the following algorithms are used:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Of these, AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 bits. Sophos UTM supports a number of encryption algorithms. Either the MD5 or SHA-1 algorithms can be used for authentication.

NAT Traversal (NAT-T)

NAT traversal is a technology for establishing connections between hosts in TCP/IP networks which use NAT devices. This is achieved by using UDP encapsulation of the ESP packets to establish IPsec tunnels through NAT devices. UDP encapsulation is only used if NAT is detected between the IPsec peers; otherwise normal ESP packets will be used.

With NAT traversal you are able to place the gateway or a road warrior behind a NAT router and still establish an IPsec tunnel. Both IPsec peers must support NAT traversal if you want to use this feature, which is automatically negotiated. Make sure that the NAT device has IPsec-passthrough turned off, because this could impair the use of NAT traversal.

If road warriors want to use NAT traversal, their corresponding user object in WebAdmin must have a static remote access IP address (RAS address) set (see also *Use Static Remote Access IP* on the *Users* page in WebAdmin).

By default, a NAT traversal keep-alive signal is sent at intervals of 60 seconds to prevent an established tunnel from expiring when no data is transmitted. The keep-alive messages are

sent to ensure that the NAT router keeps the state information associated with the session so that the tunnel stays open.

TOS

Type of Service bits (TOS bits) are several four-bit flags in the IP header. These bits are referred to as *Type of Service* bits because they allow the transferring application to tell the network which type of service quality is necessary.

With the IPsec implementation of Sophos UTM the TOS value is always copied.

16.4.1 Connections

On the *IPsec* > *Connections* tab you can create and edit IPsec connections.

To create an IPsec connection, proceed as follows:

1. **On the *Connections* tab, click *New IPsec Remote Access Rule*.**
   The *Add IPsec Remote Access Rule* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this connection.

   Interface: Select the name of the interface which is used as the local endpoint of the IPsec tunnel.

   Local networks: Select or add the local networks that should be reachable through the VPN tunnel. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Virtual IP pool: The IP address pool where clients get an IP address assigned from in case they do not have a static IP address. The default pool is *VPN Pool (IPsec)* which comprises the private IP space `10.242.4.0/24`. You can, however, select or create a different IP address pool. How to add a definition is explained on the *Definitions & Users* > *Network Definitions* > *Network Definitions* page.

   Policy: Select the IPsec policy for this IPsec connection. IPsec policies can be defined on the *Remote Access* > *IPsec* > *Policies* tab.

   Authentication type: Select the authentication type for this remote gateway definition. The following types are available:

- **Preshared key:** Authentication with *Preshared Keys* (PSK) uses secret passwords as keys. These passwords must be distributed to the endpoints before establishing the connection. When a new VPN tunnel is established, each side checks that the other knows the secret password. The security of PSKs depends on the quality of the passwords used: common words and phrases are subject to dictionary attacks. Permanent or long-term IPsec connections should use certificates instead.
- **X.509 certificate:** The X.509 Certificate authentication scheme uses public keys and private keys. An X.509 certificate contains the public key together with information identifying the owner of the key. Such certificates are signed and issued by a trusted *Certificate Authority* (CA). Once selected, specify the users that should be allowed to use this IPsec connection. Unless you select the checkbox *Automatic firewall rules*, you need to specify appropriate firewall rules manually in the *Network Protection* menu.

  Note – The User Portal can only be accessed by users who are selected in the *Allowed users* box and for whom a user definition does exist on the UTM. Authorized users who have successfully logged in to the User Portal find the *Sophos IPsec Client* (SIC), its configuration file, the `PKCS#12` file as well as a link to installation instructions, which are available at the Sophos Knowledgebase.

- **CA DN match:** This authentication type uses a match of the *Distinguished Name* (DN) of CA certificates to verify the keys of the VPN endpoints. Once selected, select an *Authority* and choose a *DN mask* that matches the DNs of remote access clients. Now select or add a *Peer Subnet Range*. Clients are only allowed to connect if the DN mask matches the one in their certificate.

Enable XAUTH (optional): Extended authentication should be enabled to require authentication of users against configured backends.

Automatic firewall rules (optional): This option is only available with the authentication type *X.509 Certificate*. By selecting this option you can automatically add firewall rules that allow traffic for this connection. The rules are added as soon as the connection is enabled, and they are removed when the connection is disabled.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new remote access rule appears on the *Connections* list.

To either edit or delete a remote access rule, click the corresponding buttons.

16.4.2 Policies

On the *Remote Access* > *IPsec* > *Policies* tab you can customize parameters for IPsec connections and unite them into a policy. An IPsec policy defines IKE (Internet Key Exchange) and IPsec proposal parameters of an IPsec connection. Note that each IPsec connection needs an IPsec policy.

Note – Sophos UTM only supports the main mode in IKE phase 1. The aggressive mode is not supported.

To create an IPsec policy, proceed as follows:

1. **On the *Policy* tab, click *New IPsec Policy*.**
   The *Add IPsec Policy* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for this policy.

   IKE encryption algorithm: The encryption algorithm specifies the algorithm used for encrypting the IKE messages. Supported algorithms are:

   - *DES* (56 bit)
   - *3DES* (168 bit)
   - *AES 128* (128 bit)
   - *AES 192* (192 bit)
   - *AES 256* (256 bit)
   - *Blowfish* (128 bit)
   - *Twofish* (128 bit)
   - *Serpent* (128 bit)

   Security Note – We strongly recommend against using DES, as it is a weak algorithm, and therefore represents a potential vulnerability.

   IKE authentication algorithm: The authentication algorithm specifies the algorithm used for integrity checking of the IKE messages. Supported algorithms are:

- *MD5* (128 bit)
- *SHA1* (160 bit)
- *SHA2 256* (256 bit)
- *SHA2 384* (384 bit)
- *SHA2 512* (512 bit)

IKE SA lifetime: This value specifies the timeframe in seconds for which the IKE SA (security association) is valid and when the next rekeying should take place. Valid values are between 60 sec and 28800 sec (8 hrs). The default value is 7800 seconds.

IKE DH group: When negotiating a connection, the communicating parties also settle the actual keys used to encrypt the data. In order to generate a session key, IKE uses the *Diffie-Hellman* (DH) algorithm, which utilizes random data. The random data generation is based on pool bits. The IKE group basically tells the number of pool bits. The more pool bits, the larger the random numbers. The larger the numbers, the harder it is to crack the Diffie-Hellman algorithm. As a consequence, more pool bits mean more security but also the consumption of more CPU resources. Currently, the following Diffie-Hellman groups are supported:

- *Group 1: MODP 768*
- *Group 2: MODP 1024*
- *Group 5: MODP 1536*
- *Group 14: MODP 2048*
- *Group 15: MODP 3072*
- *Group 16: MODP 4096*

Security Note – Group 1 (MODP 768) is considered weak and only supported for interoperability reasons. We strongly recommend against using it, as it represents a potential vulnerability.

IPsec encryption algorithm: The same encryption algorithms as for IKE. Additionally there are the following entries:

- *No encryption (null)*
- *AES 128 CTR* (128 bit)

- *AES 192 CTR* (192 bit)
- *AES 256 CTR* (256 bit)
- *AES 128 GCM (96 bit)*
- *AES 192 GCM (96 bit)*
- *AES 256 GCM (96 bit)*
- *AES 128 GCM (128 bit)*
- *AES 192 GCM (128 bit)*
- *AES 256 GCM (128 bit)*

Security Note – We strongly recommend against using no encryption or DES, as this represents a potential vulnerability.

IPsec authentication algorithm: The same authentication algorithms as for IKE. Additionally there are the following algorithms:

- *SHA2 256* (96 bit)
- *SHA2 384* (96 bit)
- *SHA2 512* (96 bit)

Those are available for compliance with tunnel endpoints not adhering to RFC 4868, for example UTM (i.e., ASG) versions older than V8, and therefore do not support truncated checksums longer than 96 bit.

IPsec SA lifetime: This value specifies the timeframe in seconds for which the IPsec SA is valid and when the next rekeying should take place. Valid values are between 60 sec and 86400 sec (1 day). The default value is 3600 seconds.

IPsec PFS group: *Perfect Forward Secrecy* (PFS) refers to the notion that if a session key is compromised, it will permit access only to data of this specific session. In order for PFS to exist, the key used to protect the IPsec SA must not be derived from random keying material used to get the keys for the IKE SA. Therefore, PFS initiates a second Diffie-Hellman key exchange proposing the selected DH group for the IPsec connection to get a new randomly generated key. Supported Diffie-Hellman groups are the same as for IKE.

Enabling PFS is considered to be more secure, but it takes also more time for the exchange. It is not recommended to use PFS on slow hardware.

Note – PFS is not fully interoperable with all vendors. If you notice problems during the negotiation, you might consider disabling PFS.

Strict policy: If an IPsec gateway makes a proposition with respect to an encryption algorithm and to the strength, it might happen that the gateway of the receiver accepts this proposition, even though the IPsec policy does not correspond to it. If you select this option and the remote endpoint does not agree on using exactly the parameters you specified, the IPsec connection will not be established. Suppose the IPsec policy of your UTM requires AES-256 encryption, whereas, for example, a road warrior with SSH Sentinel wants to connect with AES-128; with the strict policy option enabled, the connection would be rejected.

Note – The compression setting will not be enforced via *Strict policy*.

Compression: This option specifies whether IP packets should be compressed by means of the *IP Payload Compression Protocol* (IPComp) prior to encryption. IPComp reduces the size of IP packets by compressing them to increase the overall communication performance between a pair of communicating hosts or gateways. Compression is turned off by default.

Comment (optional): Add a description or other information.

3. **Click *Save*.**
   The new policy appears on the *Policies* list.

To either edit or delete a policy, click the corresponding buttons.

16.4.3 Advanced

On the *Remote Access > IPsec > Advanced* tab you can configure advanced options of IPsec VPN. Depending on your preferred authentication type, you can define the local certificate (for X.509 authentication) and the local RSA key (for RSA authentication), among other things. Note that this should only be done by experienced users.

Local X.509 Certificate

With X.509 authentication, certificates are used to verify the public keys of the VPN endpoints. If you want to use this authentication type, you have to select a local certificate from the drop-down list in the *Local X.509 Certificate* area. The selected key/certificate is then used to authenticate the gateway to remote peers if X.509 authentication is selected.

You can only select certificates where the appropriate private key is present, other certificates are not available in the drop-down list.

If there is no certificate available for selection, you have to add one in the *Certificate Management* menu, either by creating a new one or by importing one using the upload function.

After selecting the certificate, enter the passphrase the private key was protected with. During the saving process, the passphrase is verified and an error message is displayed if it does not match the encrypted key.

Once an active key/certificate is selected, it is displayed in the *Local X.509 Certificate* area.

Dead Peer Detection (DPD)

Use Dead Peer Detection: The dead peer detection option is used for automatically terminating a connection if the remote VPN gateway or client is unreachable. For connections with static endpoints, the tunnel will be re-negotiated automatically. Connections with dynamic endpoints require the remote side to re-negotiate the tunnel. Usually it is safe to always enable this option. The IPsec peers automatically determine whether the remote side supports dead peer detection or not, and will fall back to normal mode if necessary.

NAT Traversal (NAT-T)

Use NAT Traversal: Select to enable that IPsec traffic can pass upstream systems which use *Network Address Translation* (NAT). Additionally, you can define the keepalive interval for NAT traversal. Click *Apply* to save your settings.

CRL Handling

There might be situations in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For this purpose, so-called *Certificate Revocation Lists* or CRLs are used. They normally contain the serial numbers of those certificates of a certifying instance, that have been held invalid and that are still valid according to their respective periods of validity.
After the expiration of these periods the certificate will no longer be valid and must therefore not be maintained in the block list.

Automatic Fetching: This function automatically requests the CRL through the URL defined in the partner certificate via HTTP, Anonymous FTP or LDAP version 3. On request, the CRL can be downloaded, saved and updated, once the validity period has expired. If you use this feature but not via port 80 or 443, make sure that you set the firewall rules accordingly, so that the CRL distribution server can be accessed.

Strict Policy: If this option is enabled, any partner certificate without a corresponding CRL will be rejected.

Preshared Key Probing

For IPsec connections using the respond-only mode you can decide to use different preshared keys (PSK) for each IPsec connection.

Enable probing of preshared keys: Select the checkbox to enable this option. This will affect L2TP-over-IPsec, remote access IPsec, and VPN IPsec connections.

16.4.4 Debug

IKE Debugging

In the *IKE Debugging* section you can configure IKE debug options. Select the checkboxes for which types of IKE messages or communication you want to create debug output.

Note – The *IKE Debugging* section is identical across the *Debug* tabs of the menus *Site-to-site VPN IPsec*, *Remote Access IPsec*, *L2TP over IPsec* and *Cisco VPN Client*.

The following flags can be logged:

- **Control Flow:** Displays control messages of IKE state
- **Outbound packets:** Displays content of outgoing IKE messages
- **Inbound packets:** Displays content of incoming IKE messages
- **Kernel messaging:** Displays communication messages with the Kernel
- **High availability:** Displays communication with other HA nodes

16.5 HTML5 VPN Portal

The HTML5 VPN Portal feature enables users from external networks to access internal resources via pre-configured connection types, using only a browser as a client, without installing plug-ins. To do so, the user logs into the User Portal of the UTM where on the *HTML5 VPN Portal* tab a list of all connections available to this user is shown. Clicking on the *Connect* button initiates the connection to the defined internal resource. As an administrator you have to generate these connections beforehand, specifying the allowed users, the connection type and other settings. Internal resources can be accessed using different connection types: either Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) to access remote desktops, a browser to use web applications (HTTP/HTTPS), or Telnet/Secure Shell (SSH) for terminal sessions. However, the HTML5 VPN Portal does not permit to download content, e.g. via HTTP, to the user's local computer.

Using this feature it is possible to give multiple users access to internal resources which do not support multi-user access themselves (e.g., network hardware like switches) or easily provide very granular access to just one specific service instead of giving access to entire systems or networks.

Examples:

- Give access to telephone service company to maintain your telephone system.
- Give access to a specific internal website, e.g., intranet.

Note – The user's browser has to be HTML5-compliant. The following browsers support the HTML5 VPN feature: Firefox 6.0 onwards, Internet Explorer 10 onwards, Chrome, Safari 5 onwards (on MAC only).

16.5.1 Global

On the *Remote Access* > *HTML5 VPN Portal* > *Global* tab you can activate the HTML5 VPN Portal and manage the respective VPN Portal connections. Note that the number of connections is limited to 100. For the allowed users, the enabled connections are available on the *HTML5 VPN Portal* tab of the User Portal.

To activate the HTML5 VPN Portal and create a new HTML5 VPN connection, proceed as follows:

1. **Enable the HTML5 VPN Portal.**
   Click the toggle switch.

   The toggle switch turns green and the elements on the page become editable. All existing, enabled connections will now be visible in the User Portal of the allowed users.

2. **Click the *New HTML5 VPN Portal Connection* button.**
   The *Add HTML5 VPN Portal Connection* dialog box opens.

3. **Make the following settings:**
   Name: Enter a descriptive name for this connection.

   Connection type: Select the connection type. Depending on the selected connection type, different parameters are displayed. The following types are available:

   - **Remote Desktop:** Remote access using the Remote Desktop Protocol (RDP), e.g., to open a remote desktop session to a Windows host.
   - **Webapp (HTTP):** Browser-based access to web applications via HTTP.
   - **Webapp (HTTPS):** Browser-based access to web applications via HTTPS.

     Note – The URL used for the HTTP/HTTPS connection is composed of the *Destination*, the *Port* and the *Path* options for this connection. The web application has to be compatible with Mozilla Firefox (version 6.0 onwards).

   - **Telnet:** Terminal access using the Telnet protocol, e.g., to give access to a switch or a printer.
   - **SSH:** Terminal access using SSH.

- **VNC:** Remote access using Virtual Network Computing (VNC), e.g., to open a remote desktop of a Linux/Unix host.

  Note – Currently only VNC classic authentication (password only) is supported. Make sure your server is set up accordingly.

Destination: Select or add the host which allowed users should be able to connect to. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Note – If the selected destination host supplies a self-signed certificate, make sure that the CN (Common Name) of the certificate matches your destination hostname. Otherwise the user will get a certificate warning in the portal browser. If you e.g. use a DNS host *www.mydomain.com*, make sure that the self-signed certificate contains this name. If you use a host instead of a DNS host, make sure that the self-signed certificate contains the host's IP address as a *Subject Alternative Name*.

Path (only with connection types *Webapp*): Enter the path which allowed users should be able to connect to.

Username (only with connection type *SSH*): Enter the username the user should use to connect.

Automatic login/**Automatic login (Basic Auth)**: If enabled, users can log in without knowing the authentication data. In this case, you have to provide the authentication data. The displayed options depend on the selected connection type:

- **Username:** Enter the username users should use to connect.
- **Password:** Enter the password users should use to connect.

  Note – When using the connection type *Telnet*, for security reasons automatic login only works when the banner length sent from the Telnet server does not exceed 4096 characters (including the password prompt). If the banner is longer, automatic login fails. In this case reduce the banner length or switch to manual login.

- **Authentication method** (only with connection type *SSH*): Select the SSH authentication method. You can either provide the *Password* for the selected username or add the *Private SSH key* for the SSH connection.

SSL host certificate (only with connection type *HTTPS*): Add the SSL host security certificate to identify the destination host.

- **SSL certificate:** Click the *Fetch* button to automatically add the certificate of the selected destination host.

Public host key (only with connection type *SSH*): Add the public key of the SSH host.

- **SSH public key:** Click the *Fetch* button to automatically retrieve the SSH public key of the selected destination host.

Allowed users (User Portal): Select the users or groups or add the new users that should be allowed to use the VPN Portal connection. By default, only one user can use a connection at the same time. If you want the users to share a session simultaneously, select the *Shared session* checkbox in the *Advanced* section. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

Note – When you add a group with backend membership, make sure that the group is also allowed for the User Portal. On the *Management > User Portal > Global* tab, either select *Allow all users* or *Allow only specific users* and explicitly add the group. If you only allow individual group members for the User Portal, they will not be provided the connections allowed for the group.

Comment (optional): Add a description or other information.

4. **Optionally, make the following advanced settings:**

Port: Enter a port number for the connection. By default the standard port of the selected connection type is selected.

Protocol security (only with connection type *Remote Desktop*): Select the security protocol for the Remote Desktop session. You can choose between RDP, TLS and NLA (Network Level Authentication). Your settings have to comply with the server settings. NLA requires to enable *Automatic login* above.

Share session: Select this option to allow users to use the connection simultaneously and see the same screen.

Allow external resources (only with connection types *Webapp (HTTP/S)*): Enter additional resources that are allowed to be accessed via this connection. This is useful if for example images or other resources are stored on a different server than the webpage itself. For the selected host(s) or network ranges port 80 and 443 will be allowed.

5. **Click *Save*.**
   The new connection appears on the *Connections* list.
6. **Enable the connection.**
   Click the toggle switch to activate the connection.

   The connection is now available for the allowed users. It is located on the *HTML5 VPN Portal* tab of the User Portal.

To either edit or delete a connection, click the corresponding buttons.

16.6 Cisco VPN Client

Sophos UTM supports IPsec remote access via Cisco VPN Client. The Cisco VPN Client is an executable program from Cisco Systems that allows computers to connect remotely to a *Virtual Private Network* (VPN) in a secure way.

16.6.1 Global

On the *Remote Access > Cisco VPN Client > Global* tab you can configure basic options for setting up remote access via Cisco VPN Client.

To configure Sophos UTM to allow Cisco VPN Client connections, proceed as follows:

1. **On the *Global* tab enable Cisco VPN Client.**
   Click the toggle switch.

   The toggle switch turns amber and the *Server Settings* area becomes editable.
2. **Make the following settings:**
   Interface: Select an interface to be used for Cisco VPN Client connections.

   Server certificate: Select the certificate with which the server identifies itself to the client.

Pool network: Select a network pool to choose virtual network addresses from to assign them to connecting clients. By default *VPN Pool (Cisco)* is selected.

Local networks: Select or add the local networks that should be reachable through the VPN tunnel. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

Users and groups: Select users or user groups, or add users that are allowed to connect to the UTM via Cisco VPN Client. How to add a user is explained on the *Definitions & Users > Users & Groups > Users* page.

Automatic firewall rules (optional): By selecting this option you can automatically add firewall rules that allow traffic for this connection. The rules are added as soon as the connection is enabled, and they are removed when the connection is disabled.

3. **Click *Apply*.**
   Your settings will be saved.

Live Log

Use the live log to track connection logs of the IPsec IKE daemon log. It shows information on establishing, upkeeping, and closing connections.

16.6.2 iOS Devices

You can enable that iOS device users are offered automatic Cisco IPsec configuration in the User Portal.

However, only users that have been added to the *Users and groups* box on the *Global* tab will find configuration files on their User Portal site. The iOS device status is enabled by default.

Connection name: Enter a descriptive name for the Cisco IPsec connection so that iOS device users may identify the connection they are going to establish. The default name is your company name followed by the protocol Cisco IPsec.

Note – *Connection Name* must be unique among all iOS device connection settings (PPTP, L2TP over IPsec, Cisco VPN Client).

Override hostname: In case the system hostname cannot be publicly resolved by the client, you can enter a server hostname here that overrides the internal preference of the *DynDNS Hostname* before the *System DNS Hostname*.

Establish VPN connection on demand: Select this option to automatically initiate a VPN connection whenever the location matches one of the hostnames or domains listed in the box.

- **Match domain or host:** Enter the domains or hostnames for which you want to establish VPN connections on demand. This could be your local intranet, for example.
- **Establish only when DNS lookup fails:** By default, the VPN connection is only established after a DNS lookup has failed. If unselected, the VPN connection is established regardless of whether the hostname can be resolved or not.

Note that connecting iOS devices get presented the server certificate specified on the *Global* tab. The iOS device checks whether the VPN ID of this certificate corresponds to the server hostname and refuses to connect if they differ. If the server certificate uses *Distinguished Name* as VPN ID Type it compares the server hostname with the *Common Name* field instead. You need to make sure the server certificate fulfills these constraints.

To disable automatic iOS device configuration, click the toggle switch.

The toggle switch turns gray.

16.6.3 Debug

IKE Debugging

In the *IKE Debugging* section you can configure IKE debug options. Select the checkboxes for which types of IKE messages or communication you want to create debug output.

Note – The *IKE Debugging* section is identical across the *Debug* tabs of the menus *Site-to-site VPN IPsec*, *Remote Access IPsec*, *L2TP over IPsec* and *Cisco VPN Client*.

The following flags can be logged:

- **Control Flow:** Displays control messages of IKE state
- **Outbound packets:** Displays content of outgoing IKE messages
- **Inbound packets:** Displays content of incoming IKE messages
- **Kernel messaging:** Displays communication messages with the Kernel
- **High availability:** Displays communication with other HA nodes

16.7 Advanced

On the *Remote Access > Advanced* page you can make the advanced configurations for remote access clients. The IP addresses of the DNS and WINS servers you enter here are provided for the use of remote access clients while establishing a connection to the gateway, thus providing full name resolution for your domain.

DNS Server: Specify up to two DNS servers of your organization.

WINS Server: Specify up to two WINS servers of your organization. *Windows Internet Naming Service* (WINS) is Microsoft's implementation of *NetBIOS Name Server* (NBNS) on Windows operating systems. Effectively, WINS is to NetBIOS names what DNS is to domain names—a central mapping of hostnames to IP addresses.

Domain Name: Enter the *fully qualified domain name* (FQDN) of your organization. The fully qualified domain name is an unambiguous domain name that specifies the node's absolute position in the DNS tree hierarchy, for example `intranet.example.com`.

Note – For PPTP and L2TP over IPsec the domain name *cannot* be distributed automatically, but needs to be configured on the client side.
With iOS devices using *Cisco VPN Client*, the DNS servers specified above are only used to resolve hosts that belong to the specified domain.

16.8 Certificate Management

Using the *Remote Access > Certificate Management* menu, which contains the same configuration options as the *Site-to-site VPN > Certificate Management* menu, you can manage all certificate-related operations of Sophos UTM. This includes creating or importing X.509 certificates as well as uploading so-called *Certificate Revocation Lists* (CRLs), among other things.

16.8.1 Certificates

See *Site-to-site VPN > Certificate Management >* Certificates.

16.8.2 Certificate Authority

See *Site-to-site VPN* > *Certificate Management* > *Certificate Authority*.

16.8.3 Revocation Lists (CRLs)

See *Site-to-site VPN* > *Certificate Management* > *Revocation Lists (CRLs)*.

16.8.4 Advanced

See *Site-to-site VPN* > *Certificate Management* > *Advanced*.

17 Logging & Reporting

This chapter describes the logging and reporting functionality of Sophos UTM.

Sophos UTM provides extensive logging capabilities by continuously recording various system and network protection events. The detailed audit trail provides both historical and current analysis of various network activities to help identify potential security threats or to troubleshoot occurring problems.

The reporting function of Sophos UTM provides real-time information of its managed devices by collecting current log data and presenting it in a graphical format.

The *Log Partition Status* page in WebAdmin shows the status of the log partition of your Sophos UTM unit, including information about the disk space left and fillup rate as well as a four-week histogram of the log partition utilization. As the fillup rate is the difference between the measurement point and the starting point divided by the time elapsed, the value is somewhat inaccurate in the beginning but becomes more precise the longer the system is up.

The following topics are included in this chapter:

Reporting Charts

Sophos UTM displays reporting data in line charts and pie charts. Due to their interactivity, those charts allow a fine-grained access to information.

Line Charts

Interacting with line charts is easy: When hovering the mouse cursor on a chart a big dot will appear, which gives detailed information of this part of the chart. The dot is clung to the line of the chart. As you move the mouse cursor the dot follows. In case a chart has several lines, the dot switches between them according to where you move the mouse cursor. Additionally, the dot changes its color depending on which line its information refer to, which is especially useful with lines running close to each other.

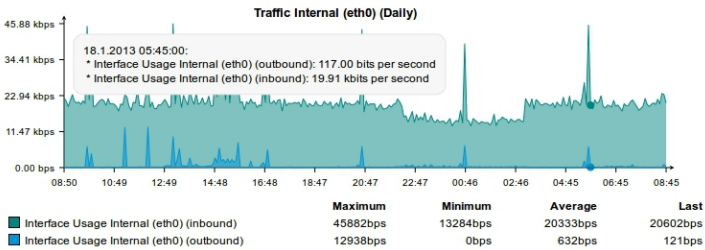

Figure 32 Reporting: Example of a Line Chart

Pie Charts

Similar to line charts, you can interact with pie charts: Direct the mouse cursor to a piece of a pie chart. This piece will immediately be extracted from the rest of the pie, the tooltip showing detailed information of the extracted piece.

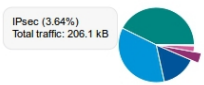

Figure 33 Reporting: Example of a Pie Chart

17.1 View Log Files

The *Logging & Reporting* > *View Log Files* menu offers the possibility to view different kind of log files and to search in log files.

17.1.1 Today's Log Files

On the *Logging & Reporting* > *View Log Files* > *Today's Log Files* tab all current logs can easily be accessed.

This tab provides various actions that can be applied to all log files. The following actions are available:

- **Live Log:** Opens a pop-up window allowing you to view the log file in real-time. New lines are added to the log file on the fly. If you select *Autoscroll*, the pop-up window will automatically scroll down to always display the most recent log. In addition, the pop-up window also contains a filter text box that allows you to limit the display of new logs to only those records that match the filter.
- **View:** Opens a pop-up window that shows the log file in its current state.
- **Clear:** Deletes the contents of the log file.

Using the drop-down list in the table footer, you can either download selected log files as a `zip` file or clear their contents simultaneously.

17.1.2 Archived Log Files

On the *Logging & Reporting* > *View Log Files* > *Archived Log Files* tab you can manage the log file archive. All log files are archived on a daily basis. To access an archived log file, select the subsystem of Sophos UTM for which logs are written as well as a year and month.

All available log files that match your selection will be displayed in chronological order. You can either view the archived log file or download it in `zip` file format.

Using the drop-down list in the table footer, you can either download selected log files as a `zip` file or delete them simultaneously.

17.1.3 Search Log Files

The tab *Logging & Reporting* > *View Log Files* > *Search Log Files* enables you to search through your local log files for various time periods. First, select the log file you want to search through, then enter the search term and select the time range. If you select *Custom Time Frame* from the *Select Time Frame* list, you can specify a start and end date. After clicking the *Start Search* button, a popup window will open presenting the results of your query. Depending on your browser it may be necessary to allow pop-up windows for WebAdmin.

If you select *Web Filtering* or *Endpoint Web Protection* from the Select log file to search list, you get 3 more filter categories. You can search for specific *User*, *URL* and *Action*

- **User:** Search for a full username in the logs.
- **URL:** Search for the substring match of a URL.
- **Action:** Dropdown list with all kinds of possible actions.

Note - If you select the *checkbox* under the *Search term*, you can optionally do the same search on *Web Filtering* and *Endpoint Protection* at the same time.

17.2 Hardware

The *Logging & Reporting* > *Hardware* menu provides overview statistics about the utilization of hardware components for several time periods.

17.2.1 Daily

The *Hardware* > *Daily* tab provides overview statistics about the following hardware components of the last 24 hours:

- CPU Usage
- Memory/Swap Usage
- Partition Usage

CPU Usage: The histogram displays the current processor utilization in percent.

Memory/Swap Usage: The utilization of memory and swap in percent. The swap usage heavily depends on your system configuration. The activation of system services such as Intrusion Prevention or the proxy servers will result in a higher memory usage. If the system runs out of free memory, it will begin to use swap space, which decreases the overall performance of the system. The used swap space should be as low as possible. To achieve that, increase the total amount of memory available to your system.

Partition Usage: The utilization of selected partitions in percent. All charts show three graphs, each representing one hard disk drive partition:

- **Root:** The root partition is the partition where the root directory of Sophos UTM is located. In addition, this partition stores update packages and backups.
- **Log:** The log partition is the partition where log files and reporting data is stored. If you run out of space on this partition, please adjust your settings under *Logging & Reporting* > *Log Settings* > *Local Logging*.
- **Storage:** The storage partition is the partition where proxy services store their data, for example images for the Web Filter, messages for the SMTP proxy, quarantined mails and the like. In addition, the database, temporary data, and configuration files are located there.

17.2.2 Weekly

The *Hardware* > *Weekly* tab provides overview statistics about selected hardware components for the last seven days. The histograms are described in the *Daily* section.

17.2.3 Monthly

The *Hardware* > *Monthly* tab provides overview statistics about selected hardware components for the last four weeks. The histograms are described in the *Daily* section.

17.2.4 Yearly

The *Hardware* > *Yearly* tab provides overview statistics about selected hardware components for the last twelve months. The histograms are described in the *Daily* section.

17.3 Network Usage

The tabs of the *Logging & Reporting* > *Network Usage* menu provide overview statistics about the traffic passing each interface of Sophos UTM for several time periods. Each chart presents its data using the following units of measurement:

- u (Micro, 10^{-6})
- m (Milli, 10^{-3})
- k (Kilo, 10^{3})
- M (Mega, 10^{6})
- G (Giga, 10^{9})

Note that the scaling can range from 10^{-18} to 10^{8}.

17.3.1 Daily

The *Network Usage* > *Daily* tab provides overview statistics about the traffic passing each configured interface of the last 24 hours.

Each histogram shows two graphs:

- **Inbound:** The average incoming traffic for that interface, in bits per second.
- **Outbound:** The average outgoing traffic for that interface, in bits per second.

The *Concurrent Connections* chart shows you the total of concurrent connections.

17.3.2 Weekly

The *Network Usage* > *Weekly* tab provides overview statistics about the traffic passing each configured interface of the last seven days. The histograms are described in the *Daily* section.

17.3.3 Monthly

The *Network Usage* > *Monthly* tab provides overview statistics about the traffic passing each configured interface of the last four weeks. The histograms are described in the *Daily* section.

17.3.4 Yearly

The *Network Usage* > *Yearly* tab provides overview statistics about the traffic passing each configured interface of the last twelve months. The histograms are described in the *Daily* section.

17.3.5 Bandwidth Usage

The *Network Usage* > *Bandwidth Usage* tab presents comprehensive data about the network traffic which was transferred to/from and through the device.

From the first drop-down list, select the type of data to display, e.g., *Top Clients* or *Top Services By Client*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *By Client* and *By Server* views you can manually provide an IP/Network, as well as network ranges (e.g., `192.168.1.0/24` or `10/8`). On the *By Services* views you can enter protocol and service, separated by comma (e.g., *TCP,SMTP*, *UDP,6000*). If you do not supply the protocol, TCP will be assumed (e.g. *HTTP* is also valid).

On the *Top Clients* and *Top Servers* views, if an IP or a hostname is clicked in the result table , it will automatically be used as a filter for the *Top Services By Client* or *Top Services By Server* view. On the *Top Services*, *Top Applications*, and *Top Application Categories* views, if you click a service, an application, or an application category in the result table, it will automatically be used as a filter for the *Top Clients by Service*, *Top Clients by Application*, or *Top Clients by Category* view.

Top Applications/Top Application Categories: If Application Control is turned off, network traffic will be displayed as "unclassified". If Application Control is active, network traffic will be displayed by type, e.g. "WebAdmin", "NTP", "facebook", etc. For more information on Application Control see chapter *Web Protection* > *Application Control*.

Please note that the labels *IN* and *OUT* for traffic may vary depending on the point of view. When running in proxy mode, the client connects to port `8080` on UTM (even in transparent mode), so data sent by the client (the request) is seen as *incoming* traffic and the data sent to the client (the response) is seen as *outgoing* traffic on the internal interface.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers. For example, if you want to sort all hosts by incoming traffic, click on *IN* in the table heading. Thus, hosts causing the most incoming traffic will be listed first. Note that the data for traffic is given in kibibytes (KiB) and mebibytes (MiB), both of which are base-2 units of computer storage (e.g., 1 kibibyte = 2^{10} bytes = 1 024 bytes).

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.4 Network Protection

The tabs of the *Logging & Reporting > Network Protection* menu provide overview statistics about relevant network protection events detected by Sophos UTM.

17.4.1 Daily

The *Network Protection > Daily* tab provides overview statistics about the following events of the last 24 hours:

- Firewall Violations
- Intrusion Prevention Statistics

Firewall Violations: Every data packet that is dropped or rejected is counted as a firewall violation. The number of firewall violations is calculated over a time span of five minutes.

Intrusion Prevention Statistics: All charts show two graphs:

- **Alert Events:** The number of data packets that triggered an intrusion alert.
- **Drop Events:** The number of data packets that where dropped by the intrusion prevention system.

17.4.2 Weekly

The *Network Protection* > *Weekly* tab provides overview statistics about firewall violations and intrusion prevention events of the last seven days. The histograms are described in the *Daily* section.

17.4.3 Monthly

The *Network Protection* > *Monthly* tab provides overview statistics about firewall violations and intrusion prevention events of the last four weeks. The histograms are described in the *Daily* section.

17.4.4 Yearly

The *Network Protection* > *Yearly* tab provides overview statistics about firewall violations and intrusion prevention events of the last twelve months. The histograms are described in the *Daily* section.

17.4.5 Firewall

The *Network Protection* > *Firewall* tab presents comprehensive data about the firewall activity, classified according to source IP, source hosts, number of received packets and number of services.

Note – Packets with a TTL less than or equal to one are dropped without being logged.

From the first drop-down list, select the type of data to display, e.g., *Top Source Hosts* or *Top Services By Destination*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *By Source* and *By Destination* views you can manually provide an IP/Network, as well as network ranges (e.g., `192.168.1.0/24` or `10/8`). On the *By Service* views you can enter protocol and service, separated by comma (e.g., *TCP,SMTP* or *UDP,6000*).

On the *Top Source Hosts* and *Top Destination Hosts* views, if you click an IP or a hostname in the result table, it will automatically be used as a filter for the *Top Services By Source* or *Top*

Services By Destination view. On the *Top Services* view, if you click a service in the result table, it will automatically be used as a filter for the *Top Source Host By Services* view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.4.6 Advanced Threat Protection

The *Network Protection* > *Advanced Threat Protection* tab presents comprehensive data about advanced threats in your network.

From the first drop-down list, select the type of data to display, e.g., *Recent Infections* or *Recent Infections by Host*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *Recent Infected by Malware* and *Recent Infections by Malware* views you can manually filter a specific threat. On the *Recent Infections by Host*views you can manually filter a specific host.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.4.7 IPS

The *Network Protection* > *IPS* tab presents comprehensive data about intrusion prevention activities on your network.

From the first drop-down list, select the type of data to display, e.g., *Top Source Hosts* or *Top Destinations By Source*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *By Source* and *By Destination* views you can manually provide an IP/Network, as well as network ranges (e.g., `192.168.1.0/24` or `10/8`). On the *Top Source Hosts* or *Top Destinations Hosts* views, if you click an IP in the result table, it will automatically be used as a filter for the *Top Destinations by Source* or *Top Sources by Destination* view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.5 Web Protection

The tabs of the *Logging & Reporting* > *Web Protection* menu provide overview statistics about the most active web users and most frequently visited websites.

17.5.1 Web Usage Report

The *Logging & Reporting* > *Web Protection* > *Web Usage Report* page is a mighty tool when you want to take a deeper look into your network traffic and your users' web usage. At a first glance, this page looks very complicated, but the best way to start is to use it and learn from the results.

Web Surfing Data Statistics

The collection of web surfing data is session-based. The UTM distinguishes between sessions per user ('How long has this user been surfing?') and sessions per user and domain ('How long has this user been surfing on this domain?'), where the domain is the top-level domain plus one significant level. To achieve good approximations, all data is gathered as follows: each web request is logged by taking the traffic volume and the duration between requests into account. If for a period of five minutes of inactivity no requests are recorded for a session, the session is considered closed. To take into account that users might still view a webpage within five minutes of inactivity, one minute is always added to the *Time Spent* values. Note further that reporting data is updated every 15 minutes.

Thus, if a user for example switches between two domains for 10 minutes, this will result in a total of 10 minutes for this user but 20 minutes for the domains surfed by this user. However, if the user uses different tabs or browsers to surf on the same domain, this will not influence the result.

When clients try to request invalid URLs, the Web Filter will log the request but will not be able to serve it. Those links will be counted as errors. They are not errors of the reporting or the Web Filter; in most cases, those errors occur because invalid or malformed links are placed in web content by the page creator.

Page Structure

Header Bar

First there is the header bar which consists of the following elements:

- **Home:** This icon takes you back to the beginning, clear of any clicks or filters.
- **Forward/Backward:** Use these icons to move back and forth along the history of your changes and settings. It works like in every web browser.
- **Available Reports:** This drop-down list contains all available report types including, if existent, your saved reports. It is set to *Sites* by default. The result table of the *Web Usage Report* page is directly dependent on this reporting type setting.

> **Note –** When using filters and clicking through reports notice how the *Available Reports* setting changes automatically. It always reflects the current reporting basis.

Standard: There are several report types available, see below for a detailed description.

Saved Web Reports: Here you can select saved web reports you created in the past.

- **Delete:** Click this icon to delete a saved web report. Standard reports cannot be deleted.
- **Save:** Click this icon to save a current view to be able to access this view easily in the future. It will be stored in the *Available Reports* drop-down list.

Filter Bar

Next there is the filter bar which consists of the following elements:

- **Plus:** Click this icon to create additional filters, see below for a detailed description.
- **Amount:** Use the drop-down list to reduce the amount of results in the table. You can limit the results to the top 10, top 50, or top 100 results.
- **Time:** Use the drop-down list to limit or expand the results in the table to certain time frames. The *Custom* timeframe allows you to specify your own timeframe.
- **Departments:** Use the drop-down list to limit the results in the table to defined departments. Departments can be created on the *Departments* page.

You can download the data in PDF or Excel format by clicking one of the corresponding icons on the right of the filter bar. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon you can get a pie chart displayed above the table. If you click the Send icon, a dialog window opens where you can enter one or more email recipients who should receive this report as well as a subject and a message before sending the data. You can also receive saved reports on a regular basis, see section *Scheduled Reports* for more information.

Results Table

Last, there is the results table. What you see here depends firstly on the selected report type (always reflected at *Available Reports* list) and secondly on possibly defined filters.

Note – When anonymization is enabled, users are not displayed by their name or IP address but they appear enumerated instead.

Depending on the report type, the table provides different information:

	Users	Categories	Sites	Domains	URLs	Overrides
#	✔	✔	✔	✔	✔	✔

	Users	Categories	Sites	Domains	URLs	Overrides
Traffic	✔	✔	✔	✔	✔	
%	✔	✔	✔	✔	✔	
Duration	✔		✔			
Pages	✔	✔	✔			
Requests	✔	✔	✔	✔	✔	
User						✔
Site						✔
Categories*					✔	✔
Action*					✔	✔
Reason*					✔	✔
Info*					✔	✔

* = Those cells can be clicked to further drill-down information.

#: Position with regard to traffic caused.

Traffic: Size of traffic caused.

%: Percentage on overall traffic.

Duration: Users report type: time spent by user(s). Sites report type: total time (sum over all users) spent on the website(s).

Pages: Number of pages (that is, all requests answered with code 200 and content-type text/html) requested.

Requests: Number of web requests for a category, site, domain, or URL.

User: Name of the user who bypassed blocking. If anonymization is enabled, *user_#* is displayed.

Site: Site for which blocking was bypassed.

Categories: Shows all categories a URL belongs to. With more than one category, clicking the category opens a small dialog field to select one of the categories from before a filter is created based on that category.

Action: Displays whether the website has been delivered to the client (*passed*), whether it has been *blocked* by an application control rule, or whether a user gained access to a blocked page using the bypass blocking feature (*overridden*).

Reason: Displays why a website request has been blocked or overridden. Example: A user tries to download an `msi` file and there is an application control rule which prohibits file transfers, then the cell displays *msi* for reason. In case of an overridden page, the reason entered by the user is displayed.

Info: If available, this cell displays additional information to why a website request has been blocked, e.g. when a file download was blocked due to its extension then the cell says *extension*.

Defining Filters

Filters are used to drill down the information displayed in the result table. They can be defined in two different ways: either by clicking the Plus icon in the Filter Bar or by clicking into the table.

Via Plus icon: After clicking the green Plus icon in the Filter Bar a small filter box with two fields is displayed. The first field, a drop-down list, lets you choose a report type, for example *Category*. The second field lets you choose or enter a value for the selected report type, e.g. *Adult Topics* when *Category* is selected. Click *Save* to save the filter and at the same time apply it to the result table.

Via table: Clicking into the table opens a dialog window *Reporting Direction* if there is more than one report type available for the item you clicked. You need to select one of the presented options for filtering. After that the *Reporting Direction* window closes, the relevant filter is created and displayed in the Filter Bar. The results table now shows the newly filtered results. Example: The default report of the *Web Usage Report* is *Sites*. In the results table you click on any row (e.g. amazon.com). The *Reporting Direction* window opens and gives you three options: either you want to see information on *Domains* for the site, on *Users* who visited the site, or on *Categories* the site belongs to. You see that several users visited amazon.com and you want to know more about this, so you click the *Users* box. The window closes. In the Header Bar you see that the report type changed to *Users* and in the Filter Bar you see that the result table for *Users* is filtered by the site you selected (amazon.com). Therefore the table shows all users who visited that site and additionally information on their sessions.

Note – Sometimes it makes a difference where you click into a table row as some table cells provide their own filter (see the items with an asterisk (*) in the section *Results Table* above).

17.5.2 Search Engine Report

The *Logging & Reporting* > *Web Protection* > *Search Engine Report* page provides information on search engines used by your users and searches they made. At a first glance, this page looks

very complicated, but the best way to start is to use it and learn from the results.

Page Structure

Header Bar

First there is the header bar which consists of the following elements:

- **Home:** This icon takes you back to the beginning, clear of any clicks or filters.
- **Forward/Backward:** Use these icons to move back and forth along the history of your changes and settings. It works like in every web browser.
- **Available Reports:** This drop-down list contains all available report types including, if existent, your saved reports. It is set to *Searches* by default. The result table of the *Search Engine Report* page is directly dependent on this reporting type setting.

  Note – When using filters and clicking through reports notice how the *Available Reports* setting changes automatically. It always reflects the current reporting basis.

  Standard: There are three report types available, see below for a detailed description.

  Saved Search Engine Reports: Here you can select saved search engine reports you created in the past.
- **Delete:** Click this icon to delete a saved search engine report. Standard reports cannot be deleted.
- **Save:** Click this icon to save a current view to be able to access this view easily in the future. It will be stored in the *Available Reports* drop-down list.

Filter Bar

Next there is the filter bar which consists of the following elements:

- **Plus:** Click this icon to create additional filters, see below for a detailed description.
- **Amount:** Use the drop-down list to reduce the amount of results in the table. You can limit the results to the top 10, top 50, or top 100 results.
- **Time:** Use the drop-down list to limit or expand the results in the table to certain time frames. The *Custom* timeframe allows you to specify your own timeframe.
- **Departments:** Use the drop-down list to limit the results in the table to defined departments. Departments can be created on the *Departments* page.

You can download the data in PDF or Excel format by clicking one of the corresponding icons on the right of the filter bar. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon you can get a pie chart displayed above the table. If you click the Send icon, a dialog window opens where you can enter one or more email recipients who should receive this report as well as a subject and a message before sending the data. You can also receive saved reports on a regular basis, see section *Scheduled Reports* for more information.

Results Table

Last, there is the results table. What you see here depends firstly on the selected report type (always reflected at *Available Reports* list) and secondly on possibly defined filters. The following report types are available:

- **Searches:** Displays the search terms your users used.
- **Search Engines:** Displays the search engines your users used.
- **Users Searches:** Displays the users who did searches.

Note – When anonymization is enabled, users are not displayed by their name or IP address but they appear enumerated instead.

For each report type, the table provides the following information:

#: Position with regard to frequency.

Requests: Number of requests for a search term, for a search engine, or by a user.

%: Percentage on overall searches.

Defining Filters

Filters are used to drill down the information displayed in the result table. They can be defined in two different ways: either by clicking the Plus icon in the Filter Bar or by clicking into the table.

Via Plus icon: After clicking the green Plus icon in the Filter Bar, a small filter box with two fields is displayed. The first field, a drop-down list, lets you choose a report type, for example *Search Engine*. The second field lets you choose or enter a value for the selected report type, e.g. *Google (google.com)* when *Search Engine* is selected. Click *Save* to save the filter and at the same time apply it to the result table. Search terms are case insensitive and support wildcards: '*' to match zero or more characters and '?' to match one character.

Via table: Clicking into the table opens a dialog window *Reporting Direction* if there is more than one report type available for the item you clicked. You need to select one of the presented options for filtering. After that the *Reporting Direction* window closes, the relevant filter is created and displayed in the Filter Bar. The results table now shows the newly filtered results. Example: The default report of the *Search Engine Report* is *Searches*. In the results table you click on any row (e.g. weather). The *Reporting Direction* window opens and gives you two options: either you want to see information on the search engines used for the search (*Search Engines*) or on users who searched for this term (*Users Searches*). You see that several users searched for weather and you want to know more about this, so you click the *Users Searches* box. The window closes. In the Header Bar you see that the report type changed to *Users Searches* and in the Filter Bar you see that the result table for *Users Searches* is filtered by the search you selected (weather). Therefore the table shows all users who searched for weather and additionally information on those searches.

17.5.3 Departments

On the *Logging & Reporting* > *Web Protection* > *Departments* page you can group users or hosts and networks to virtual departments. Those departments can then be used to filter web usage reports or search engine reports.

To create a department, proceed as follows:

1. **On the *Departments* tab, click *Add Department*.**
   The *Add New Department* dialog box opens.
2. **Enter a name**.

   In the *Name* field, enter a descriptive name for the department.
3. **Add users or hosts/networks.**
   A department definition can only contain users or hosts/networks, not both types at the same time.

   - **Users:** Add one or more users to the box who should be part of this department.
   - **Hosts/Networks:** Add one or more hosts or networks to the box which should be part of this department.

   Comment (optional): Add a description or other information.
4. **Click *Save*.**
   The new department appears on the *Departments* list.

To either edit, delete, or clone a department click the corresponding buttons.

For information on usage of departments please see sections *Web Usage Report* and *Search Engine Report*.

17.5.4 Scheduled Reports

On the *Logging & Reporting* > *Web Protection* > *Scheduled Reports* page you define which of your saved reports you would like to send by email on a regular basis. Before you can create a scheduled report, you need to have a least one saved report (for more information on saving reports see sections *Web Usage Report* or *Search Engine Report*).

To create a scheduled report, proceed as follows:

1. **On the *Scheduled Reports* tab, click *Add Scheduled Report*.**
   The *Add New Scheduled Report* dialog box opens.
2. **Make the following settings:**
   Name: Enter a descriptive name for the scheduled report.

   Interval: Select an interval from the drop-down list at which the report(s) should be sent.

   Reports: All saved reports are listed here. Select the checkbox in front of each report that should be sent at the selected interval.

   Recipients: Add recipients to the box who should receive the selected report(s). Note that you can add a list of recipients via the import button.

   Comment (optional): Add a description or other information.
3. **Click *Save*.**

   The new scheduled report appears on the *Scheduled Reports* list.

To either edit, delete, or clone a scheduled report, click the corresponding buttons. Use the toggle switch of a report to disable sending of reports without deleting the scheduled report itself.

17.5.5 Application Control

The *Logging & Reporting* > *Web Protection* > *Application Control* page contains comprehensive statistics about the most active sources, most frequently visited destinations, and the most popular applications given for various time ranges.

From the first drop-down list, select the type of data to display, e.g., *Top Sources* or *Top Applications*. Select the desired entry, and, if an additional box is displayed, specify the respective filter

argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *By Source* and *By Destination* views you can manually provide an IP/Network, as well as network ranges (e.g., `192.168.1.0/24` or `10/8`). On the *By Service* views you can enter protocol and service, separated by comma (e.g., *TCP,SMTP* or *UDP,6000*).

On the *Top Sources* view, if you click an IP or a hostname in the result table, it will automatically be used as a filter for the *Top Applications by Source* view. On the *Top Applications*and *Top Application Categories* views, if you click an application or application category in the result table, it will automatically be used as a filter for the *Top Sources by Application* or *Top Sources by Application Category* view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

The most active sources do not appear immediately in the table, but only after a session timeout had occurred. This is the case if a certain client (username or IP address) has ceased to surf the web for five minutes. The UTM determines this surfing session as "dead" and sends it to a database before it gets displayed on the most active sources list.

17.5.6 Deanonymization

The *Web Protection* > *Deanonymization* tab is only accessible if anonymization is activated (see *Logging & Reporting* > *Reporting Settings* > *Anonymizing*).

Here it is possible to abandon anonymization for specific users regarding web protection reports. Proceed as follows:

1. **Enter both passwords.**
   Enter the first and the second password that have been provided to enable anonymization.

2. **Add users to deanonymize.**
   To the *Deanonymize users* box add the usernames of those users you want to deanonymize.
3. **Click *Apply*.**
   Your settings will be saved.

17.6 Email Protection

The tabs of the *Logging & Reporting > Email Protection* menu provide overview statistics about mail flow, mail usage and email protection.

17.6.1 Usage Graphs

The *Email Protection > Usage Graphs* tab provides overview statistics about the mail flow on the UTM given for various time frames:

- Daily
- Weekly
- Monthly
- Yearly

17.6.2 Mail Usage

The *Email Protection > Mail Usage* tab contains comprehensive statistics about the most actively used email addresses and address domains given for various time ranges.

From the first drop-down list, select the type of data to display, e.g., *Top Senders* or *Top Domains*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *by Domain* and *by Address* views you can manually provide a domain or an address, respectively. Note that for specifying domains, you can use the percent sign (%) as a wildcard. By placing a percent sign at the end of your keyword, you are telling Sophos UTM to look for exact matches or sub-sets. Note that the filter field is case-sensitive.

On the *Top Addresses* and *Top Domains* views, if you click an address or a domain in the result table, it will automatically be used as a filter for the *Top Addresses by Domain* or *Top Peers by Address* view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.6.3 Blocked Mail

The *Email Protection* > *Blocked Mail* tab contains comprehensive statistics about all blocked email requests based on antivirus and antispam.

From the first drop-down list, select the type of data to display, e.g., *Top Blocked Spam Reason* or *Top Blocked Malware*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *Top Blocked Domain* view, if you click a domain in the result table, it will automatically be used as a filter for the *Top Blocked Addresses by Domain* view. On the *by Domain* view you can manually provide a domain. Note that you can use the percent sign (`%`) as a wildcard. By placing a percent sign at the end of your keyword, you are telling Sophos UTM to look for exact matches or sub-sets. Note that the filter field is case-sensitive.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.6.4 Deanonymization

The *Email Protection* > *Deanonymization* tab is only accessible if anonymization is activated (see *Logging & Reporting* > *Reporting Settings* > *Anonymizing*).

Here it is possible to abandon anonymization for specific email addresses and/or domains regarding email protection reports. Proceed as follows:

1. **Enter both passwords.**
   Enter the first and the second password that have been provided to enable anonymization.
2. **Make the following settings:**
   Deanonymize addresses: You can add email addresses you want to deanonymize.

   Deanonymize domains: You can add domains you want to deanonymize.
3. **Click *Apply*.**
   Your settings will be saved.

   Provided email addresses and domains become readable in reports.

17.7 Wireless Protection

The tabs of the *Logging & Reporting* > *Wireless Protection* menu provide overview statistics about relevant wireless protection events detected by Sophos UTM.

17.7.1 Daily

The *Wireless Protection* > *Daily* tab provides overview statistics of the last 24 hours about wireless networks and access points.

SSID Based Reporting

There is a chart for each wireless network. Each chart shows two graphs:

- **Connected clients:** The number of clients connected to the wireless network.
- **Failed connection attempts:** The number of failed connection attempts at the wireless network.

AP Based Reporting

For each access point the table shows the maximum and average connected users, the uptime (the accumulated time span the access point was up during the last 24 hours) as well as the number of reconnects.

17.7.2 Weekly

The *Wireless Protection* > *Weekly* tab provides overview statistics about wireless networks and access points of the last seven days. The histograms are described in the *Daily* section.

17.7.3 Monthly

The *Wireless Protection* > *Monthly* tab provides overview statistics about wireless networks and access points of the last four weeks. The histograms are described in the *Daily* section.

17.7.4 Yearly

The *Wireless Protection* > *Yearly* tab provides overview statistics about wireless networks and access points of the last twelve months. The histograms are described in the *Daily* section.

17.8 Remote Access

The tabs of the *Logging & Reporting* > *Remote Access* menu provide overview statistics about remote access activity and information on sessions.

17.8.1 Activity

The *Remote Access* > *Activity* tab provides overview statistics about the remote access activity on the UTM for IPsec, SSL VPN, PPTP, and L2TP given for various timeframes:

- Daily
- Weekly
- Monthly
- Yearly

Select Timeframe: Use the drop-down list to select a reporting timeframe. The page will reload automatically.

17.8.2 Session

The *Remote Access* > *Session* tab contains comprehensive statistics about completed sessions, failed logins, and current users given for various time ranges.

Note – The columns *Up* and *Down* show accounting data of the remote access connections. Accounting by default is disabled because it can increase the system load. You can enable it on the *Reporting Settings* > *Settings* tab in the *Remote Access Accounting* section.

From the first drop-down list, you can select the type of session you want to display: *Current Users*, *Completed Sessions*, or *Failed Logins*. Click the *Update* button to apply the filter.

Using the second drop-down list, you can filter the results. Depending on the selected session type, different filters are available, e.g., *By Service* or *By Source IP Address*. Some filters require to select or enter a filter argument.

Using the third drop-down list, you can filter the results by time. Always click *Update* to apply the filters.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.9 Webserver Protection

The tabs of the *Logging & Reporting* > *Webserver Protection* menu provide overview statistics about webserver requests, warnings, and alerts.

17.9.1 Usage Graphs

The *Webserver Protection > Usage Graphs* tab provides overview statistics about the web-server requests, warnings, and alerts on the UTM given for various time frames:

- Daily
- Weekly
- Monthly
- Yearly

17.9.2 Details

The *Webserver Protection > Details* tab contains comprehensive statistics about the most active clients, virtual hosts, backends, response codes, and various attacks given for various time ranges.

From the first drop-down list, select the type of data to display, e.g., *Top Clients* or *Top Attackers Per Virtual Host*. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click *Update* to apply the filters.

On the *By Client* and *By Attacker* views you can manually provide an IP/Network, as well as network ranges (e.g., `192.168.1.0/24` or `10/8`). On the *by Virtual Host* views you can manually provide a domain. Note that you can use the percent sign (`%`) as a wildcard. By placing a percent sign at the end of your keyword, you are telling Sophos UTM to look for exact matches or subsets. Note that the filter field is case-sensitive.

On the *Top Clients* or *Top Attackers* views, if you click an IP in the result table, it will automatically be used as a filter for the *Top Response Codes by Client* or *Top Rules by Attacker* view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the *Number of rows* drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers.

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected.

Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

17.10 Executive Report

In the menu *Logging & Reporting* > *Executive Report* you can create a collection of the most important reporting data presented in graphical format to show network utilization for a number of services.

17.10.1 View Report

On the *Logging & Reporting* > *Executive Report* > *View Report* tab you can create a complete executive report based on the individual reports in the tabs and pages of the *Reporting* menu. Click the button *Generate Report Now* to open a window showing the executive report.

17.10.2 Archived Executive Reports

The *Executive Report* > *Archived Executive Reports* tab provides an overview of all archived executive reports. Only those executive reports will be archived for which archiving has been selected on the *Configuration* tab.

17.10.3 Configuration

On the *Executive Report* > *Configuration* tab you can make the settings for executive reports.

Daily Executive Report

Daily executive report: If enabled, a daily executive report is created.

Archive PDF reports: If enabled, the daily executive report will be archived in PDF format. Archived executive reports can be accessed on the *Archived Executive Reports* tab.

Send reports as PDF instead of HTML: If enabled, the executive report sent by email is an attached PDF file. If unselected, it will be sent in HTML format.

Email addresses: Enter the email addresses of the recipients who should receive the executive report.

Weekly Executive Report

Most of the settings are described in the *Daily Executive Report* section.

You can additionally choose the weekday when the executive report should start to collect its data.

Monthly Executive Report

The settings are described in the *Daily Executive Report* section.

17.11 Log Settings

In the *Logging & Reporting > Log Settings* menu you can configure basic settings for local and remote logging.

17.11.1 Local Logging

On the *Logging & Reporting > Log Settings > Local Logging* tab you can make the settings for local logging. Local logging is enabled by default.

However, to activate local logging in case it was disabled, proceed as follows:

1. **On the *Local Logging* tab enable local logging.**
   Click the toggle switch.

   The toggle switch turns green and the areas on this tab become editable.
2. **Select a time frame when log files are to be deleted.**
   From the drop-down list select what action is to be applied automatically on log files. *Never delete log files* is selected by default.
3. **Click *Apply*.**
   Your settings will be saved.

Thresholds

Here you can define thresholds for local logging which are bound to certain actions that are to be carried out if a threshold is reached. The following actions are available:

- **Nothing:** No actions will be initiated.
- **Send Notification:** A notification will be sent to the administrator stating that the threshold was reached.

- **Delete Oldest Log Files:** Oldest log files will be deleted until the remaining amount is below the configured threshold or until the log file archive is empty. In addition, a notification of that event will be sent to the administrator.
- **Shutdown System:** The system will be shut down. A notification of that event will be sent to the administrator.
  In case of a system shutdown, the administrator has to change the configuration of the local logging, configure log file deletion or move away/delete log files manually. If the reason for the system shutdown persists, the system will shut down itself again the next time the log cleaning process runs, which happens daily at 12:00 AM (i.e., at midnight).

Click *Apply* to save your settings.

17.11.2 Remote Syslog Server

On the *Logging & Reporting > Log Settings > Remote Syslog Server* tab you can make the settings for remote logging. This function allows you to forward log messages from UTM to other hosts. This is especially useful for networks using a host to collect logging information from several UTMs. The selected host must run a logging daemon that is compatible to the syslog protocol.

To configure a remote syslog server, proceed as follows:

1. **On the *Remote Syslog Server* tab enable remote syslog.**
   Click the toggle switch.

   The toggle switch turns amber and the *Remote Syslog Settings* area becomes editable.
2. **Click the Plus icon in the *Syslog Servers* box to create a server.**
   The *Add Syslog Server* dialog box opens.
3. **Make the following settings:**
   Name: Enter a descriptive name for the remote syslog server.

   Server: Add or select the host that should receive log data from UTM. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Caution – Do not use one of UTM's own interfaces as a remote syslog host, since this will result in a logging loop.

Port: Add or select the service definition which is to be used for the connection. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

4. **Click *Apply*.**
   Your settings will be saved.

Remote Syslog Buffer

In this area you can change the buffer size of the remote syslog. The buffer size is the number of log lines kept in the buffer. Default is 1000. Click *Apply* to save your settings.

Remote Syslog Log Selection

This area is only editable when remote syslog is enabled. Select the checkboxes of the logs that should be delivered to the syslog server. You can select all logs at once by selecting the option *Select All*. Click *Apply* to save your settings.

17.11.3 Remote Log File Archives

On the *Logging & Reporting > Log Settings > Remote Log File Archives* tab you can make the settings for remote archiving of log files. If remote log file archiving is enabled, the log files of the past day are packed and compressed into one file, which is transferred to a remote log file storage. Using the drop-down list you can select your preferred transfer method.

To configure a remote log file archive, proceed as follows:

1. **Enable the *Remote Log File Archives* function.**
   Click the toggle switch.

   The toggle switch turns amber and the *Remote Log File Archive* area becomes editable.

2. **Select the log file archiving method.**
   From the drop-down list, select your preferred archiving method. Depending on your selection, the related configuration options for each archiving method will be displayed below. You can choose between the following archiving methods:

   - **FTP Server:** The *File Transfer Protocol* (FTP) method needs the following parameters to be set:
     - **Host:** Host definition of the FTP server.
     - **Service:** TCP port the server is listening on.
     - **Username:** Username for the FTP server account.

- **Password:** Password for the FTP server account.
- **Path:** Remote (relative) path where the log files are stored.

- **SMB (CIFS) Share:** The SMB method needs the following parameters to be set:
  - **Host:** Host definition of the SMB server.
  - **Username:** Username for the SMB account.
  - **Password:** Password for the SMB account.

    Security Note – The password will be saved plain-text in the configuration file. It is therefore advisable to create a user/password combination uniquely for this logging purpose.

  - **Share:** SMB share name. Enter the path or the network share information where the log files are to be transferred to, e.g. `/logs/log_file_archive`.
  - **Workgroup/Domain:** Enter the workgroup or domain the log file archive is part of.
- **Secure Copy (SSH Server):** To use the SCP method, it is necessary that you add the public SSH DSA key to the authorized keys of your SCP server. On a Linux system, you can simply cut and paste the SSH DSA key and add it to the `~/.ssh/authorized_keys` file of the configured user account. During the installation, Sophos UTM creates a new SSHDSA key. For security reasons, this SSH DSA key is not included in backups. After a new installation or the installation of a backup, you must therefore store the new SSH DSA key on the remote server to be able to securely copy your log file archives to the SCP server.
  The SCP method requires the following settings:
  - **Host:** Host definition for the SCP server.
  - **Username:** Username for the SCP server account.
  - **Path:** Remote (full) path where the log files should be stored.
  - **Public DSA key:** On the remote storage host, add the provided public DSA key to the list of authorized keys.
- **Send by email:** To have the log file archive sent by email, enter a valid email address.

3. **Click *Apply*.**
   Your settings will be saved.

If the transfer fails, the archive will remain on UTM. During each run of the log cleaning process, UTM tries to deliver all remaining archives.

17.12 Reporting Settings

In the *Logging & Reporting* > *Reporting Settings* menu you can make settings for the reporting functions such as enabling/disabling certain features of reporting, setting time frames and amounts for keeping data. Additionally, you can anonymize data to enhance privacy protection.

17.12.1 Settings

The *Settings* tab allows you to define reporting actions and the time period reporting data will be kept on the system before it is automatically deleted. The following report topics can be set:

- Application Control
- Authentication
- Email Protection
- Firewall
- IPS
- Network Usage
- Remote Access
- Web Protection
- Webserver Protection

Use the checkboxes on the left side to enable or disable reporting for a certain report topic. By default, all report topics are enabled.

Use the drop-down lists on the right to determine how long reporting data is kept.

Note – Disabling needless reports will lower the base load of your machine and can reduce performance bottlenecks. Try to keep time frames as short as possible since high amounts of

stored data result in a higher base load and decreased responsiveness on the dynamical reporting pages.

The settings on this tab do not affect the log file archives.

Web Protection Reporting Detail Level

In this section you can define the detail level of Web Protection reporting. Note that a higher detail level results in a perceptible increase in memory usage and system load, so unless necessary, it is recommended to keep the detail level low.

The following detail levels are available:

- **Domain only:** Reports display the top-level domain and second-level domain of a URL, e.g. `example.com`. Third-level domains will be also displayed if they are enforced, such as `example.co.uk`.
- **Full domain:** Reports display the full domains, e.g. `www.example.com` or `shop.example.com`
- **1 level of URL:** Reports display additionally the first (virtual) directory of a URL, e.g. `www.example.com/en/`.
- **2 levels of URL:** Reports display additionally the first two (virtual) directories of a URL, e.g. `www.example.com/en/products/`.
- **3 levels of URL:** Reports display additionally the first three (virtual) directories of a URL, e.g. `www.example.com/en/products/new/`.

Executive Report Settings

In this area you can define respectively the number of executive reports to keep:

- Daily reports: 60 at maximum
- Weekly reports: 52 at maximum
- Monthly reports: 12 at maximum

Click *Apply* to save your settings.

For more information on the executive report and its options, see *Logging & Reporting* > *Executive Report*.

PDF Paper Settings

The default paper format for the PDF executive report is A4. Using the drop-down list you can alternatively select *Letter* or *Legal*. Click *Apply* to save your settings.

Remote Access Accounting

Here you can enable or disable accounting for remote access connections. If enabled, data about remote access connections is stored and displayed on the *Logging & Reporting > Remote Access > Session* tab in the *Down* and *Up* columns. If disabled, accounting is stopped. Note that if enabled, this feature may increase the system load.

CSV Delimiter Settings

Here you can define which delimiter is used when exporting reporting data to CSV format. Please note that with Windows operating systems the delimiter should match the regional settings of your system to make sure that the exported data will be displayed correctly in a spreadsheet program like e.g., Excel.

IPFIX Accounting

By means of IPFIX you can export IPv4 flow data of UTM to a provider for e.g. monitoring, reporting, accounting, or billing purposes.

Internet Protocol Flow Information Export (IPFIX) is a message-based protocol for exporting accounting information in a universal way. The accounting information is collected by an *exporter* and sent to a *collector*. A typical set of accounting information for an IPv4 flow consists of *source address, destination address, source port, destination port, bytes, packets, and network traffic classification data*.

If enabled, UTM serves as exporter: It exports IPFIX accounting data. The collector generally is located at a provider's site where the accounting data of one or more of your UTMs is aggregated and analyzed. During the system setup at your provider, you will be given the hostname and you have to define a unique Observation Domain ID (OID) per exporter, i.e., UTM. Enter this data into the corresponding fields.

Data is exported on UDP port 4739. A single network connection uses two IPFIX flows–one for the export direction, one for the reply.

Security Note – Be aware that with IPFIX the accounting data will be transmitted unencrypted. It is therefore recommended to send the data via private network only.

Click *Apply* to save your settings.

17.12.2 Exceptions

The *Reporting Settings* > *Exceptions* tab allows you to exclude certain domains and addresses from reporting, which affects the Executive Report as well as the affected *Logging & Reporting* pages and the affected statistics overview pages.

Note – The effect will not be immediately visible on today's statistics pages because the information on these pages is updated every 10 to 15 minutes only. Note also the import function with which you can define multiple items at once.

Reporting Exceptions: Web

In this section you can define domains to be excluded from all web protection reports. The domain names have to be entered exactly as they are listed in the *Domains* report on the *Logging & Reporting* > *Web Protection* > *Web Usage Report* tab. Click *Apply* to save your settings.

Reporting Exceptions: Mail

In these two sections you can define domains and mail addresses to be excluded from all email protection reports.

Use the *Domains* box to exclude all email addresses of a particular domain. Just enter the domain part of the email address e.g. `sophos.com`. Use the *Addresses* box to enter particular email addresses to exclude from the reports. Click *Apply* to save your settings.

Emails having the specified domain names or addresses as sender or recipient will be excluded from all email protection reports.

Reporting Exceptions: Network Protection

In this section you can define IPv4 and IPv6 addresses to be excluded from all network protection reports. Click *Apply* to save your settings.

Reporting Exceptions: Network Accounting

In this section you can define IPv4 and IPv6 addresses to be excluded from all network usage reports. Click *Apply* to save your settings.

17.12.3 Anonymizing

The *Reporting Settings* > *Anonymizing* tab allows to anonymize reporting data based on the four-eyes principle. That means that deanonymization can only take place when two different people agree on that procedure. Anonymization ensures that user data is kept secret when viewing reporting data, and therefore actions (such as web-surfing habits) cannot be traced back to a specific person.

To use anonymization, proceed as follows:

1. **On the *Anonymizing* tab enable anonymization.**
   Click the toggle switch.

   The toggle switch turns amber and the *Anonymizing Settings* area becomes editable.
2. **Enter two security passwords.**
   The four-eyes principle is only allowed for when two different people enter a password unknown to each other.
3. **Click *Apply*.**
   Your settings will be saved.

To disable anonymization (globally) again, both passwords are necessary.

1. **On the *Anonymizing* tab click the toggle switch.**
   The toggle switch turns amber and the *Anonymizing Settings* area becomes editable.
2. **Enter both passwords.**
   Enter the first and the second password that have been provided to enable anonymization.
3. **Click *Apply*.**
   Your settings will be saved.

If necessary, anonymization can be disabled for single users, see *Logging & Reporting* > *Web Protection* and *Logging & Reporting* > *Email Protection*.

18 Support

This chapter describes the support tools available for Sophos UTM.

The pages of the *Support* menu contain many customer support related features ranging from various web links, through contact information, to the output of useful network tools that are used to determine important network properties without the need to access UTM's command-line interface.

The following topics are included in this chapter:

- Documentation
- Printable Configuration
- Contact Support
- Tools
- Advanced

In addition, the main page of the *Support* menu contains web links to the following information resources:

- **Knowledgebase** (KB): Official knowledgebase of Sophos NSG contains numerous information on configuring Sophos UTM.
- **Known Issues List** (KIL): The list of known problems that cannot be fixed or for which a workaround is available.
- **Hardware Compatibility List** (HCL): The list of hardware that is compatible to Sophos UTM Software.
- **Up2Date Information:** Sophos NSG Up2Date blog, which informs about product improvements and firmware updates.

18.1 Documentation

Online Help

This section gives a description of how to open and use the online help.

Manual Download

You can download the current Administration Guide in PDF format. Select the language of the guide and click *Start download*. Note that you need a special reader to open PDF documents such as Adobe's Reader or Xpdf.

Cross Reference – Administration Guides from former UTM versions and other documentation can be downloaded from the Sophos Knowledgebase.

18.2 Printable Configuration

On the *Support > Printable Configuration* page you can create a detailed report of the current WebAdmin configuration.

Note – The printable configuration is opened in a new window. Depending on your browser it may be necessary to allow pop-up windows for WebAdmin.

The structure of the printable configuration matches the WebAdmin menu structure to facilitate finding the corresponding configuration options in WebAdmin.

The printable configuration browser page consists of an overview page, called *index*, and several subpages. Links to subpages are highlighted blue. Subpages give detailed information to the respective topic. You can always return from a subpage to the index by clicking the *Back to the index* link at the bottom of the subpage.

There are two more viewing options for the printable configuration:

- WebAdmin format
- Confd format

You can find the links to these viewing options at the bottom of the index page.

18.3 Contact Support

Sophos offers a comprehensive range of customer support services for its security solutions. Based on the support/maintenance level, you have various levels of access and committed response time by the Sophos service department and/or Sophos NSG Certified Partners.

All support cases concerning Sophos UTM are processed via the MyUTM Portal. You may open a support case via a web form by clicking *Open Support Ticket in New Window*. For more information see the MyUTM User Guide.

18.4 Tools

The tabs of the *Support* > *Tools* menu display the output of useful network tools that can be used to determine important network properties without the need to access UTM's command-line interface. The output of the following tools can be viewed:

- Ping
- Traceroute
- DNS Lookup

18.4.1 Ping Check

The program *ping* is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP *echo request* packets to the target host and listening for ICMP *echo response* replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

To make a ping check, proceed as follows:

1. **Select the ping host.**
   Select the host you want to ping. In the *Ping Host* box, you can select a host for which a host definition exists. Alternatively, you can also select *Custom hostname/IP address* and enter a custom hostname or IP address into the textbox below.
2. **Select the IP version** (only available if IPv6 is globally enabled).
   From the *IP version* drop-down list, select *IPv4* or *IPv6*.
3. **Click *Apply*.**
   The output of the ping check will be displayed in the *Ping Check Result* area.

18.4.2 Traceroute

The program *traceroute* is a computer network tool used to determine the route taken by packets across an IP network. It lists the IP addresses of the routers that were involved in transporting the packet. If the packet's route cannot be determined within a certain time frame,

traceroute will report an asterisk (*) instead of the IP address. After a certain number of failures, the check will end. An interruption of the check can have many causes, but most likely it is caused by a firewall along the network path that blocks traceroute packets.

To trace a route, proceed as follows:

1. **Specify the traceroute host.**
   Select the host you want to trace the route to. In the *Traceroute host* box, you can select a host for which a host definition exists. Alternatively, you can also select *Custom host-name/IP address* and enter a custom hostname or IP address into the textbox below.
2. **Select the IP version** (only available if IPv6 is globally enabled).
   In the *IP version* drop-down list, select *IPv4* or *IPv6*.
3. **Print hop addresses numerically rather than symbolically and numerically** (optional).
   Selecting this option saves a nameserver address-to-name lookup for each gateway found on the path.
4. **Click *Apply*.**
   The output of traceroute will be displayed in the *Traceroute Result* area.

18.4.3 DNS Lookup

The program *host* is a network tool for interrogating DNS name servers. It performs DNS look-ups and displays the answers that are returned from the name server(s) that were queried.

To make a DNS lookup, proceed as follows:

1. **Specify the hostname/IP address.**
   Enter the hostname or IP address of the host for which you want to determine DNS information.
2. **Select *Enable verbose output*** (optional).
   Select this option to generate lengthy output showing more information.
3. **Click *Apply*.**
   The output of dig will be displayed in the *DNS Lookup Result* area.

18.5 Advanced

The *Support > Advanced* menu displays even more information on your UTM and gives access to advanced features. It gives overview of running processes and local network connections and you can view the routing table and the interfaces table. Additionally, you can download a support package for debugging and recovery purposes and find background information about internally used configuration references which you may encounter in log files.

18.5.1 Process List

The program *ps* displays a header line followed by lines containing information about your processes that have controlling terminals. This information is sorted by controlling terminal, then by process ID.

18.5.2 LAN Connections

The program *netstat* (short for *Network Statistics*) is a network tool that displays a list of the active Internet connections a computer currently has, both incoming and outgoing.

18.5.3 Routes Table

The program *ip* is a network tool for controlling TCP/IP networking and traffic control. Invoked with the parameter `route show table all` it displays the contents of all routing tables of UTM.

18.5.4 Interfaces Table

The table shows all configured interfaces of Sophos UTM, both network interface cards and virtual interfaces. The program *ip* invoked with parameter `addr` displays interfaces and their properties.

18.5.5 Config Dump

For debugging or recovery purposes it is useful to gather as many information as possible about your installation of Sophos UTM. The support package that can be downloaded from the

Support > *Advanced* > *Config Dump* tab provides exactly this. The `zip` file contains the following items:

- The entire dump of UTM's configuration (`storage.abf`). Note that this is no genuine backup file—it does not contain any passwords, among other things—and can be used for debugging purposes only.
- Information on the hardware present in the system (`hwinfo`).
- Information on the software packages installed on the system (`swinfo`).

18.5.6 Resolve REF

For debugging purposes you can resolve configuration references internally used by the system. If you encounter a reference somewhere in the logs, you can paste the reference string here (e.g., `REF_DefaultSuperAdmin`). The tab will then display an excerpt of the configuration daemon's data structure.

19 Log Off

You can log out of UTM by clicking the *Log Off* menu entry. If you do not log out properly or if you close the web browser inadvertently, you might not be able to log in again for approximately 30 seconds.

Note – You will be logged out if you visit a different website during a session. In this case, you will have to log in again.

20 User Portal

This chapter provides information on how the User Portal works and which services it provides for end-users.

The User Portal of Sophos UTM is a browser-based application providing among others personalized email and remote access services to authorized users. It can be accessed by browsing to the URL of Sophos UTM, for example, `https://192.168.2.100` (note the HTTPS protocol).

On the login page, users can select a language from the drop-down list located on the right side of the header bar.

Depending which services and features have been activated in WebAdmin by the administrator, users can have access to the following services:

- Mail Quarantine
- Mail Log
- POP3 Accounts
- Sender Whitelist
- Sender Blacklist
- Hotspots
- Client Authentication
- OTP Tokens
- Remote Access
- HTML5 VPN Portal
- Change Password
- HTTPS Proxy

If the one-time password feature is enabled, a login page with one or more QR codes is displayed after the login attempt under some conditions. The login page is displayed only when the *Auto-create OPT tokens for users* feature is enabled, and the user logged in with his user-specific password only (not appending a one-time password), and an unused OTP token is available for the user. The page shows instructions on how to configure a mobile device to generate one-time passwords. After configuring the mobile device, the user can log in again, now using

the UTM password, directly followed by the one-time password. Example: If your UTM password is `1z58.xa` and the one-time password is `123456`, just enter the password `1z58.xa123456` to log in.

20.1 User Portal: Mail Quarantine

On this tab, end-users can view and release messages held in quarantine.

Note – The *Mail Quarantine* tab is available if either POP3 or SMTP has been activated in WebAdmin and the user has been configured to use these services. If the user should receive emails both via SMTP and POP3, the emails will be organized into two tabs *POP3 Quarantine* and *SMTP Quarantine*, both providing a similar functionality.

The *Mail Quarantine* tab shows an overview of all emails addressed to the user but blocked and quarantined by Sophos UTM. For POP3 quarantine emails to be listed the user has to enter their POP3 credentials on the *POP3 Accounts* tab.

Sort and Filter Quarantined Emails

By default, all emails are shown. If the list contains more than twenty emails, it is split into several chunks which can be browsed with Next (>) and Previous (<) buttons.

Users can influence which items are displayed:

Sort by: By default, the list is sorted by time of arrival. Messages can be sorted by date, subject line, sender address, and message size.

and show: The checkbox allows to display 20, 50, 100, 250, 500, 1000, or all messages per page. Note that showing all messages may take a lot of time.

Several elements on the page let users filter their emails:

- **# messages quarantined:** On top of the page, several checkboxes allow to show or hide emails by the reason why they were quarantined (malware, spam, expression match, file extension, MIME type, unscannable, others).
- **Addresses** or **Accounts:** Allows to filter the messages according to the recipient address (SMTP) or account (POP3).

- **Sender/Rcpt/Subject substring:** Here users can enter a sender, recipient (only with POP3), or subject to search for in the quarantined messages.
- **Received date:** To only show messages processed during a certain time frame, users can enter a date or select a date from the Calendar icon.

Manage Quarantined Emails

Users can apply actions on a message using the drop-down list in front of the message. An action can also be applied to several selected messages. Use the checkbox in front of each message or click a message to select it. Then select one of the actions available in the drop-down list below the table. The following actions are available:

- **View** (only available for an individual message): Opens a window with the contents of the email.
- **Download:** Selected messages will be downloaded in EML format.
- **Delete:** Selected messages will be deleted irrevocably.
- **Whitelist Sender** (only available for an individual message): Moves the email to your inbox and adds the sender to your whitelist (*Sender Whitelist* tab). Successive emails of this sender will not be quarantined. Note, that mails containing malicious content will always be quarantined, even if the sender is on the whitelist.
- **Release:** Selected messages will be released from quarantine.
- **Release and report as false positive:** Selected messages will be released from quarantine and reported as false positive to the spam scan engine.

Note – The allowed actions depend on the reason why the email was quarantined, and on the WebAdmin settings. Users can only release messages they are explicitly allowed to. Only the administrator can release *all* messages held in quarantine.

Select global cleanup action: Here you find several deletion options that will be applied on messages globally, that is, regardless whether they are selected and/or displayed or not.

20.2 User Portal: Mail Log

On this tab, end-users can view a log of their email traffic sent via SMTP.

Note – The *Mail Log* tab is only for email address belonging to the domain monitored by the SMTP proxy of Sophos UTM, and only available for users whom the administrator gave access rights to this feature. If both SMTP and POP3 have been activated for a certain user, the tab is called *SMTP Log*.

The *Mail Log* tab shows log entries of all email traffic of the user's email addresses. Log entries of undelivered emails contain the information about why they have not been delivered. Double-clicking a log entry opens a window with more log information.

By default, all emails are shown. If the list contains more than twenty emails, it is split into several chunks which can be browsed with Next (>) and Previous (<) buttons.

Users can influence which items are displayed:

Sort by: By default, the list is sorted by time of arrival. Messages can be sorted by date, subject line, sender address, and message size.

and show: The checkbox allows to display 20, 50, 100, 250, 500, 1000, or all messages per page. Note that showing all messages may take a lot of time.

Several elements on the page let users filter their emails:

- **# log events on file:** On top of the page, several checkboxes allow to show or hide emails according to their status.
- **Addresses:** Allows to filter the emails according to the sender address.
- **Sender/Subject substring:** Here users can enter a sender or subject to search for in the quarantined messages.
- **Received date:** To only show messages processed during a certain time frame, users can enter a date or select a date from the Calendar icon.

20.3 User Portal: POP3 Accounts

On this tab, end-users can identify themselves to be able to view and release their POP3 quarantine emails and receive quarantine reports.

Note – The *POP3 Accounts* tab is only available if the administrator enabled POP3 and added a POP3 server.

On the page, users need to enter the credentials of the POP3 accounts they use. Only those spam emails will appear in the User Portal for which POP3 account credentials are given. A user for whom POP3 account credentials are stored will receive an individual quarantine report for each email address.

20.4 User Portal: Sender Whitelist

On this tab, end-users can whitelist senders, so that messages from them are never regarded as spam. However, emails with viruses or unscannable emails will still be quarantined.

Note – The *Sender Whitelist* tab is only available if the user's email address belongs to the network or domain monitored by Sophos UTM, and the administrator assigned them access rights to the feature.

Whitelisted senders can be specified by clicking the Plus icon, entering the address and clicking the Tick icon to save it. Users can either enter valid email addresses (e.g., `jdoe@example.com`) or all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`). Sender whitelist and sender blacklist can be used in combination: The user can for example blacklist an entire domain (e.g., *@hotmail.com) but whitelist specific email addresses belonging to this domain (e.g., `mycolleague@hotmail.com`). This also works the other way round. If the exact email address is listed on both, whitelist and blacklist, the address is blacklisted.

20.5 User Portal: Sender Blacklist

On this tab, end-users can blacklist email senders, so that messages from them are always regarded as spam.

Note – The *Sender Blacklist* tab is only available if the user's email address belongs to the network or domain monitored by Sophos UTM, and the administrator assigned them access rights to the feature.

The blacklist is applied to both SMTP and POP3 email, if these are in use on the system. Blacklisted senders can be specified by clicking the Plus icon, entering the address and clicking the Tick icon to save it. Users can either enter valid email addresses (e.g., `jdoe@example.com`) or

all email addresses of a specific domain using an asterisk as wildcard (e.g., `*@example.com`). Sender whitelist and sender blacklist can be used in combination: The user can for example blacklist an entire domain (e.g., *@hotmail.com) but whitelist specific email addresses belonging to this domain (e.g., `mycolleague@hotmail.com`). This also works the other way round. If the exact email address is listed on both, whitelist and blacklist, the address is blacklisted.

20.6 User Portal: Hotspots

The Hotspot feature allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests.

Note – The *Hotspots* tab of the User Portal is only visible for users if the administrator created a hotspot of one of the types *Password* or *Voucher*, and added the user to the allowed users.

On this tab, users can distribute the hotspot access information to wireless network guests. What they can do on the tab depends on the type of the selected hotspot: they can either distribute a general password or generate and distribute vouchers.

Hotspot type: Password of the day

In the *Password* field, the current password is displayed. It changes automatically once a day. However, users can change the password manually. The former password will immediately become invalid and active sessions will be terminated.

To change the password, users need to proceed as follows:

1. **In the User Portal, they need to select the *Hotspots* tab.**
2. **They need to select the hotspot for which they want to manage the access information.**
   From the *Hotspot* drop-down list, they need to select the hotspot for which they want to change the password.
3. **They need to define a new password.**
   They need to enter the new password in the *Password* field or automatically create a new password by clicking the *Generate* button.
4. **If users want to send the new password per email, they need to select the *Send Mail* checkbox.**

The password will be sent to the email recipients specified by the administrator. If the administrator did not specify any email addresses, the checkbox is not available.

5. **They click *Save*.**
   The password will be changed immediately.

Hotspot type: Voucher

Users can create vouchers, each with a unique code. The vouchers can be printed and given to guests. A list of created vouchers gives an overview about their usage and helps to manage them.

To create vouchers, users need to proceed as follows:

1. **In the User Portal, they need to select the *Hotspots* tab.**
2. **They need to make the following settings:**
   Hotspot: They need to select the hotspot for which they want to create a voucher.

   Voucher Definition: The available voucher types are defined by the administrator. Which type to use for what purpose has to be defined within the company.

   Amount: Users need to enter the amount of vouchers of this type to be created.

   Comment: Optionally, they can enter a comment. The comment will be displayed in the user's vouchers list.

   Print: If users directly want to print the vouchers, they need to select this option.

   Page Size: They need to select the page size they want to print.

   Vouchers Per Page: They select how many vouchers will be printed onto one page. UTM automatically adjusts the vouchers on the page.

   Add QR Code: Users can request that in addition to the voucher text data, the printed voucher should also contain a QR code. A QR code is a square image containing encoded data. It can be scanned by a mobile device in order to access the hotspot login page, where the fields are pre-populated with the necessary data.
3. **They need to click the *Create Vouchers* button.**
   The vouchers are generated. Each voucher will immediately be displayed as a new line in the voucher list below. If specified, they will be printed directly. Each voucher has a unique code.

Note – Contents, size, and layout of the vouchers are determined by the administrator.

In the voucher list users can manage vouchers. They can sort and filter the list, they can enter or change the comment and they can print, delete, or export selected vouchers.

- To sort the list, users need to select the desired sorting criterion in the *Sort by* drop-down list. With the drop-down list to the right, they can determine the number of displayed vouchers per page.
- To filter the list, users need to use one of the fields *Status*, *Code*, or *Comment*. they need to select or enter, respectively, the desired attribute. The list will be filtered directly while typing. To reset the filter, they need to select the status entry *All* and delete all text from the *Code* and/or *Comment* text field.
- To enter or change a comment, users need to click the Notepad icon in the *Comment* column of the respective voucher. An edit field is displayed. Users can enter or edit text and press the Enter key or click the checkmark to save changes.
- To print or delete vouchers, users need to select the checkbox in front of the desired vouchers, then click the appropriate button on the bottom.

  Note – Vouchers can automatically be deleted after a specified time, which can be configured by the administrator.

- To export vouchers, users need to proceed as follows: They need to select the checkbox in front of the desired vouchers, then click the *Export CSV* button on the bottom. A window appears where they can decide to save or to directly open the CSV file. The selected vouchers will be saved in one CSV file. When opening the file users need to take care to select the correct character for column separation.

20.7 User Portal: Client Authentication

On this tab, end-users can download the setup file of the Sophos Authentication Agent (SAA). The SAA can be used as authentication mode for the Web Filter.

Note – The *Client Authentication* tab is only available if client authentication is enabled by the administrator.

20.8 User Portal: OTP Tokens

On this tab, end-users have access to the QR codes and data to install the OTP configuration on their mobile device.

Configure OTP Token With Google Authenticator

1. **Install Google Authenticator on your mobile device.**
2. **Scan the QR code.**
3. **Open the app.**
   It shows you the one-time password that changes every 30 seconds.
4. **Open the facility which you have to use the one-time password for.**
   The administrator configured the services for which you need to enter the one-time password, for example for connecting via remote access, for the web application firewall, or for the User Portal itself.
5. **Enter your username and your UTM password, directly followed by the current one-time password. Then click the *Login* button.**
   Now you have access to the facility.

Using Other Software

1. **Install the software on your mobile device.**
2. **Open the app.**
3. **Configure the app using the data beside the QR code.**
   The app now produces the one-time passwords.
4. **Open the facility which you have to use the one-time password for.**
   The administrator configured the services for which you need to enter the one-time password, for example for connecting via remote access, for the web application firewall or for the User Portal itself.
5. **Enter your username and your UTM password, directly followed by the current one-time password. Then click the *Login* button.**
   Now you have access to the facility.

20.9 User Portal: Remote Access

On this tab, end-users can download remote access client software and configuration files automatically generated and provided for them according to the WebAdmin settings made by the administrator.

Note – The *Remote Access* tab is only available if at least one remote access mode has been enabled for a user.

Only the remote access data is available that corresponds to the connection types the administrator enabled for a user, e.g., if a users has been enabled to use SSL VPN remote access, they will find an *SSL VPN* section.

Each connection type is displayed in a separate section. Depending on the connection type, information and/or buttons to download the respective software are available. Where appropriate, on top of the sections, users find an *Open installation instructions in new window* link which opens a detailed installation documentation.

20.10 User Portal: HTML5 VPN Portal

The HTML5 VPN Portal feature allows users from external sources to access internal resources via pre-configured connection types, using only a browser as a client.

Note – The *HTML5 VPN Portal* tab is only available for users for whom the administrator created VPN connections and added them to the allowed users.

Note – The user's browser has to be HTML5-compliant. The following browsers support the HTML5 VPN feature: Firefox 6.0 onwards, Internet Explorer 10 onwards, Chrome, Safari 5 onwards (on MAC only).

On the *HTML5 VPN Portal* tab the allowed connections are listed. The icons give a hint about the type of connection.

To use a connection, users need to proceed as follows:

1. **Clicking the respective *Connect* button.**
   A new browser window opens. Contents and layout depend on the connection type, e.g., it contains a website if the user opened a HTTP or HTTPS connection, whereas it contains a command-line interface for SSH connections.
2. **Working in the new VPN window.**
   For some tasks, the VPN window provides a connection-type-specific menu bar which fades in when the cursor is moved to the window top:
   - **Using function keys or key combinations:** If users want to use special commands like function keys or `CTRL-ALT-DEL`, they need to select the respective entry in the *Keyboard* menu.
   - **Copy & paste from the local host into the VPN window:** On the local machine, users need to copy the respective text into the clipboard. In the connection window, they need to select the *Clipboard* menu. With `CTRL-V`, they paste the text into the text box. After that they need to click the *Send to Server* button: With SSH or Telnet connections, the text will then be directly pasted at the cursor position. With RDP or VNC connections, the text will be sent to the clipboard of the server and can then be pasted as usual.

     Note – Copy & paste does not work with Webapp connections.

   - **Copy & paste from the VPN window into another window:** With SSH and Telnet connections, users can just copy and paste text like they would in local windows. With RDP or VNC connections, in the VPN window, users need to copy the respective text to their clipboard. Then they select the *Clipboard* menu. The copied text is displayed in the text box. Users need to mark the text and press `CTRL-C`. Now it is in the local clipboard and can be pasted as usual.
   - **Changing keyboard layout in a Remote Desktop connection:** For Remote Desktop connections with a Windows host, users can change the keyboard language settings of the VPN window. Especially for the Windows login the selected language should match the Windows language settings to ensure that users type the password correctly. Users need to select the appropriate language from the *Keyboard* > *Keyboard Layout* menu. The selected keyboard layout is saved in a cookie.
   - **Go back to the Start page in a Webapp connection:** To return to the default page in a Webapp connection, select the *Navigation* > *Home* menu.

3. **Closing the connection after having finished their work.**
   - To finally terminate the connection, users need to select the *Stop Session* command from the *Connection* menu or close the browser window by clicking the X icon in the title bar. They can start a new session using the *Connect* button again.
   - To disconnect the session, users need to select the *Suspend Session* command from the *Connection* menu. The status of the session will be saved for five minutes. When they connect again during this time interval, users can continue the previous session.

20.11 User Portal: Change Password

On this tab, end-users can change their password for access to the User Portal and, if available, remote access over PPTP.

20.12 User Portal: HTTPS Proxy

On this tab, end-users can import the HTTP/S Proxy CA certificate to get rid of error messages when visiting secure websites.

Note – The *HTTPS Proxy* tab of the User Portal is only available if the administrator globally provided an HTTP/S Proxy certificate.

After clicking *Import Proxy CA Certificate*, users will be prompted by their browser to trust the CA for various purposes.

Glossary

3

3DES
Triple Data Encryption Standard

A

ACC
Astaro Command Center

ACPI
Advanced Conguration and Power Interface

AD
Active Directory

Address Resolution Protocol
Used to determine the Ethernet MAC address of a host when only its IP address is known.

ADSL
Asymmetric Digital Subscriber Line

Advanced Configuration and Power Interface
The ACPI specification is a power management standard that allows the operating system to control the amount of power distributed to the computer's devices.

Advanced Programmable Interrupt Controller
Architecture for dealing with interrupts in multi-processor computer systems.

AES
Advanced Encryption Standard

AFC
Astaro Flow Classifier

AH
Authentication Header

AMG
Astaro Mail Gateway

APIC
Advanced Programmable Interrupt Controller

ARP
Address Resolution Protocol

AS
Autonomous System

ASCII
American Standard Code for Information Interchange

ASG
Astaro Security Gateway

Astaro Command Center
Software for monitoring and administering multiple Astaro gateway units by means of a single interface. Starting with version 4, the software was renamed Sophos UTM Manager (SUM).

Astaro Security Gateway
Software for unified threat management, including mail and web security. Starting with version 9, the software

was renamed Unified Threat Management (UTM).

Authentication Header
IPsec protocol that provides for anti-replay and verifies that the contents of the packet have not been modified in transit.

Autonomous System
Collection of IP networks and routers under the control of one entity that presents a common routing policy to the Internet.

AWG
Astaro Web Gateway

AWS
Amazon Web Services

B

BATV
Bounce Address Tag Validation

BGP
Border Gateway Protocol

Bounce Address Tag Validation
Name of a method designed for determining whether the return address specified in an email message is valid. It is designed to reject bounce messages to forged return addresses.

Broadcast
The address used by a computer to send a message to all other computers on the network at the same time. For example, a network with IP address 192.168.2.0 and network mask 255.255.255.0 would have a broadcast address of 192.168.2.255.

C

CA
Certificate Authority

CBC
Cipher Block Chaining

CDMA
Code Division Multiple Access

Certificate Authority
Entity or organization that issues digital certificates for use by other parties.

CHAP
Challenge-Handshake Authentication Protocol

Cipher Block Chaining
Refers in cryptography to a mode of operation where each block of plaintext is "XORed" with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to that point.

Cluster
Group of linked computers, working together closely so that in many respects they form a single computer.

CMS
Content Management System

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSS
Cascading Style Sheets

D

DC
Domain Controller

DCC
Direct Client Connection

DDoS
Distributed Denial of Service

DER
Distinguished Encoding Rules

Destination Network Address Translation
Special case of NAT where the destination addresses of data packets are rewritten.

Device tree
Located below the main menu. Grants access to all gateway units registered with the SUM.

DHCP
Dynamic Host Configuration Protocol

Digital Signature Algorithm
Standard propagated by the United States Federal Government (FIPS) for digital signatures.

Digital Subscriber Line
Family of technologies that provides digital data transmission over the wires of a local telephone network.

Distinguished Encoding Rules
Method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified.

DKIM
Domain Keys Identified Mail

DMZ
Demilitarized Zone

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name Service

DOI
Domain of Interpretation

Domain Name Service
Translates the underlying IP addresses of computers connected through the Internet into more human-friendly names or aliases.

DoS
Denial of Service

DSA
Digital Signature Algorithm

DSCP
Differentiated Services Code Point

DSL
Digital Subscriber Line

DUID
DHCP Unique Identifier

Dynamic Host Configuration Protocol
Protocol used by networked devices to obtain IP addresses.

E

ECN
Explicit Congestion Notification

Encapsulating Security Payload
IPsec protocol that provides data confidentiality (encryption), anti-replay, and authentication.

ESP
Encapsulating Security Payload

Explicit Congestion Notification
Explicit Congestion Notification (ECN) is an extension to the Internet Protocol and allows end-to-end notifications of network congestion without dropping packets. ECN only works if both endpoints of a connection successfully negotiate to use it.

F

FAT
File Allocation Table

File Transfer Protocol
Protocol for exchanging files over packet-swichted networks.

FQHN
Fully Qualified HostName

FTP
File Transfer Protocol

G

Generic Routing Encapsulation
Tunneling protocol designed for encapsulation of arbitrary kinds of network layer packets inside arbitrary kinds of network layer packets.

GeoIP
Technique to locate devices worldwide by means of satellite imagery.

GRE
Generic Routing Encapsulation

GSM
Global System for Mobile Communications

H

H.323
Protocol providing audio-visual communication sessions on packet-switched networks.

HA
High Availability

HCL
Hardware Compatibility List

HELO
A command in the Simple Mail Transfer Protocol (SMTP) with which the client

responds to the initial greeting of the server.

High Availability
System design protocol that ensures a certain absolute degree of operational continuity.

HIPS
Host-based Intrusion Prevention System

HMAC
Hash-based Message Authentication Code

HTML
Hypertext Transfer Markup Language

HTTP
Hypertext Transfer Protocol

HTTP/S
Hypertext Transfer Protocol Secure

HTTPS
Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol
Protocol for the transfer of information on the Internet.

Hypertext Transfer Protocol over Secure Socket Layer
Protocol to allow more secure HTTP communication.

I

IANA
Internet Assigned Numbers Authority

ICMP
Internet Control Message Protocol

ID
Identity

IDE
Intelligent Drive Electronics

IDENT
Standard protocol that helps identify the user of a particular TCP connection.

IDN
International Domain Name

IE
Internet Explorer

IKE
Internet Key Exchange

IM
Instant Messaging

Internet Control Message Protocol
Special kind of IP protocol used to send and receive information about the network's status and other control information.

Internet Protocol
Data-oriented protocol used for communicating data across a packet-switched network.

Internet Relay Chat
Open protocol enabling the instant communication over the Internet.

Internet service provider
Business or organization that sells to consumers access to the Internet and related services.

IP
Internet Protocol

IP Address
Unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard.

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

IRC
Internet Relay Chat

ISP
Internet Service Provider

L

L2TP
Layer Two (2) Tunneling Protocol

LAG
Link Aggregation Group

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

Link-state advertisement
Basic communication means of the OSPF routing protocol for IP.

LSA
Link-state advertisement

LTE
3GPP Long Term Evolution

M

MAC
Media Access Control

MAC Address
Unique code assigned to most forms of networking hardware.

Managed Security Service Provider
Provides security services for companies.

Management Information Base
Type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.

Masquerading
Technology based on NAT that allows an entire LAN to use one public IP address to communicate with the rest of the Internet.

MD5
Message-Digest algorithm 5

Message-Digest algorithm 5
Cryptographic hash function with a 128-bit hash value.

MIB
Management Information Base

MIME
Multipurpose Internet Mail Extensions

MPLS
Multiprotocol Label Switching

MPPE
Microsoft Point-to-Point Encryption

MSCHAP
Microsoft Challenge Handshake Authentication Protocol

MSCHAPv2
Microsoft Challenge Handshake Authentication Protocol Version 2

MSP
Managed Service Provider

MSSP
Managed Security Service Provider

MTU
Maximum Tansmission Unit

Multipurpose Internet Mail Extensions
Internet Standard that extends the format of email to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets.

MX record
Type of resource record in the Domain Name System (DNS) specifying how emails should be routed through the Internet.

N

NAS
Network Access Server

NAT
Network Address Translation

NAT-T
NAT Traversal

Network Address Translation
System for reusing IP addresses.

Network Time Protocol
Protocol for synchronizing the clocks of computer systems over packet-switched networks.

NIC
Network Interface Card

Not-so-stubby area
In the OSPF protocol, a type of stub area that can import autonomous system (AS) external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas.

NSSA
Not-so-stubby area

NTLM
NT LAN Manager (Microsoft Windows)

NTP
Network Time Protocol

O

Open Shortest Path First
Link-state, hierarchical interior gateway protocol (IGP) for network routing.

OpenPGP
Protocol combining strong public-key and symmetric cryptography to provide security services for electronic communications and data storage.

OSI
Open Source Initiative

OSPF
Open Shortest Path First

OU
Organisational Unit

P

PAC
Proxy Auto Configuration

PAP
Password Authentication Protocol

PCI
Peripheral Component Interconnect

PEM
Privacy Enhanced Mail

PGP
Pretty Good Privacy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PMTU
Path Maximum Transmission Unit

POP3
Post Office Protocol version 3

Port
Virtual data connection that can be used by programs to exchange data directly. More specifically, a port is an additional identifier—in the cases of TCP and UDP, a number between 0 and 65535 – that allows a computer to distinguish between multiple concurrent connections between the same two computers.

Portscan
Action of searching a network host for open ports.

Post Office Protocol version 3
Protocol for delivery of emails across packet-switched networks.

PPP
Point-to-Point Protocol

PPPoA
PPP over ATM Protocol

PPTP
Point to Point Tunneling Protocol

Privacy Enhanced Mail
Early IETF proposal for securing email using public key cryptography.

Protocol
Well-defined and standardized set of rules that controls or enables the connection, communication, and data transfer between two computing endpoints.

Proxy
Computer that offers a computer network service to allow clients to make indirect network connections to other network services.

PSK
Preshared Key

Q

QoS
Quality of Service

R

RADIUS
Remote Authentication Dial In User Service

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Remote Access Server

RBL
Realtime Blackhole List

RDN
Relative Distinguished Name

RDNS
Reverse Domain Name Service

RDP
Remote Desktop Protocol

Real-time Blackhole List
Means by which an Internet site may publish a list of IP addresses linked to spamming. Most mail transport agent (mail server) software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. For webservers as well it is possible to reject clients listed on an RBL.

RED
Random Early Detection

Redundant Array of Independent Disks
Refers to a data storage scheme using multiple hard drives to share or replicate data among the drives.

Remote Authentication Dial In User Service
Protocol designed to allow network devices such as routers to authenticate users against a central database.

RFC
Request for Comment

Router
Network device that is designed to forward packets to their destination along the most efficient path.

RPS
RED Provisioning Service

RSA
Rivest, Shamir, & Adleman (public key encryption technology)

S

S/MIME
Secure/Multipurpose Internet Mail Extensions

SA
Security Associations

SAA
Sophos Authentication Agent

SCP
Secure Copy (from the SSH suite of computer applications for secure communication)

SCSI
Small Computer System Interface

Secure Shell
Protocol that allows establishing a secure channel between a local and a remote computer across packet-switched networks.

Secure Sockets Layer
Cryptographic protocol that provides secure communications on the Internet, predecessor of the Transport LayerSecurity (TLS).

Secure/Multipurpose Internet Mail Extensions
Standard for public key encryption and signing of email encapsulated in MIME.

Security Parameter Index
Identification tag added to the header while using IPsec for tunneling the IP traffic.

Sender Policy Framework
Extension to the Simple Mail Transfer Protocol (SMTP). SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM (Return-Path), a typical annoyance of email spam.

Session Initiation Protocol
Signalization protocol for the setup, modification and termination of sessions between two or several communication partners. The text-oriented protocol is based on HTTP and can transmit signalization data through TCP or UDP via IP networks. Thus, it is the base among others for Voice-over-IP videotelephony (VoIP) and multimedia services in real time.

SFQ
Stochastic Fairness Queuing

Shared Secret
Password or passphrase shared between two entities for secure communication.

SIM
Subscriber Identification Module

Simple Mail Transfer Protocol
Protocol used to send and receive email across packet-switched networks.

Single sign-on
Form of authentication that enables a user to authenticate once and gain access to multiple applications and systems using a single password.

SIP
Session Initiation Protocol

SLAAC
Stateless Address Autoconfiguration

SMB
Server Message Block

SMP
Symmetric Multiprocessing

SMTP
Simple Mail Transfer Protocol

SNAT
Source Network Address Translation

SNMP
Simple Network Message Protocol

SOCKetS
Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS, often called the Firewall Traversal Protocol, is currently at version 5 and must be implemented in the client-side program in order to function correctly.

SOCKS
SOCKetS

Sophos UTM Manager
Software for monitoring and administering multiple UTM units by means of a single interface. Formerly known as Astaro Command Center.

Source Network Address Translation
Special case of NAT. With SNAT, the IP address of the computer which initiated the connection is rewritten.

Spanning Tree Protocol
Network protocol to detect and prevent bridge loops

SPF
Sender Policy Framework

SPI
Security Parameter Index

SPX
Secure PDF Exchange

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single sign-on

STP
Spanning Tree Protocol

SUA
Sophos User Authentication

Subnet mask
The subnet mask (also called netmask) of a network, together with the network address, defines which addresses are part of the local network and which are not. Individual computers will be assigned to a network on the basis of the definition.

SUM
Sophos UTM Manager

Symmetric Multiprocessing
The use of more than one CPU.

SYN
Synchronous

T

TACACS
Terminal Access Controller Access Control System

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

Time-to-live
8-bit field in the Internet Protocol (IP) header stating the maximum amount of time a packet is allowed to propagate through the network before it is discarded.

TKIP
Temporal Key Integrity Protocol

TLS
Transport Layer Security

TOS
Type of Service

Transmission Control Protocol
Protocol of the Internet protocol suite allowing applications on networked computers to create connections to one another. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

Transport Layer Security
Cryptographic protocol that provides secure communications on the Internet, successor of the Secure Sockets Layer (SSL).

TTL
Time-to-live

U

UDP
User Datagram Protocol

UMTS
Universal Mobile Telecommunications System

Unified Threat Management
Software for unified threat management, including mail and web security. Formerly known as Astaro Security Gateway.

Uniform Resource Locator
String that specifies the location of a resource on the Internet.

Uninterruptible power supply
Device which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available.

Up2Date
Service that allows downloading relevant update packages from the Sophos server.

UPS
Uninterruptible Power Supply

URL
Uniform Resource Locator

USB
Universal Serial Bus

User Datagram Protocol
Protocol allowing applications on networked computers to send short messages sometimes known as datagrams to one another.

UTC
Coordinated Universal Time

UTM
Unified Threat Management

V

VDSL
Very High Speed Digital Subscriber Line

Virtual Private Network
Private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol such as PPTP or IPsec.

VLAN
Virtual LAN

VNC
Virtual Network Computing

Voice over IP
Routing of voice conversations over the Internet or through any other IP-based network.

VoIP
Voice over IP

VPC
Virtual Private Cloud

VPN
Virtual Private Network

W

WAF
Web Application Firewall

WAN
Wide Area Network

W-CDMA
Wideband Code Division Multiple Access

WebAdmin
Web-based graphical user interface of Sophos/Astaro products such as UTM, SUM, ACC, ASG, AWG, and AMG.

WEP
Wired Equivalent Privacy

Windows Internet Naming Service
Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows, a name server and service for NetBIOS computer names.

WINS
Windows Internet Naming Service

WLAN
Wireless Local Area Network

WPA
Wi-Fi Protected Access

X

X.509
Specification for digital certificates published by the ITU-T (International Telecommunications Union – Telecommunication). It specifies information and attributes required for the identification of a person or a computer system.

XSS
Cross-site scripting

List of Figures

Index

D

Q

R

V

W