Sophos UTM 9.1 Connected

Release Notes

The formal release announcement and accompanying link to these release notes can always be found at http://www.astaro.com/blog/up2date/UTM91

The following pages will take you through the additions and enhancements which have been introduced in this version.

June 2013
Gold Version
Angelo Comazzetto
Sr. Product Manager

Contents

Major New Features

Web Protection for UTM Endpoints

You are now able to enforce Web policy in the UTM Endpoint client, via an extensive new feature tirelessly crafted by our UTM endpoint wizards. This allows you to enforce the exact same web surfing policy on clients running our UTM Endpoint no matter where they are in the world or when they temporarily step out of the office and from behind the protection provided by the UTM itself.

All client Web activity will be logged separately on the UTM in a new Web Endpoint log, and as well, all reports on the UTM will be correlated to reflect Endpoint client usage. You will notice a small increase in traffic on your UTM from our Liveconnect service in order to gather the logs and activity from your outside users. The Endpoint Liveconnect service allows us to offer you a true aggregated view for your users, and we have engineered it so that UTM Web Endpoint clients on the network will not be double-filtered when surfing behind the UTM in the office; it will automatically recognize traffic from clients running UTM Endpoint with Web enabled and save resources by bypassing the (identical) protection on the gateway. You still however have the ability to double-AV scan traffic using separate engines by scanning with the Avira engine on the UTM (or dual-scan) and the Sophos AV agent which is used on the UTM Endpoints; this happens automatically, no special configuration is needed.

If you have not yet deployed our UTM Endpoint offering, an entitlement for a small number of seats is included with every device for you to sample.

Unified IP-Management System

Our core definition system has undergone the first of a few planned enhancements towards completely unifying objects for their use throughout the configuration. UTM 9.100 integrates the DHCP static-mapping assignments and DNS assignments directly into host objects while allowing for MAC addresses to be added as well (see below). With these enhancements, there is no longer the margin for error by having a statically assigned IP which then differs from an object definition. For example, if you have 192.168.0.5 assigned to Joe's laptop via static DHCP (and/or a corresponding DNS name with a DNS assignment), in the past you could have a definition that was 192.168.0.10 by mistake, creating the possibility that your configuration didn't match your assignments (or vice versa) which was time-consuming to audit. This has all been unified into the host object now, reducing the need to check the configuration of same thing in different areas of the WebAdmin. Filters have been added to the object definitions list that allow you to filter for clients with/without static mappings as well to more easily make adjustments, and where possible some intelligent conversion has been done on your existing mappings as part of the Up2Date process.

Support for MAC Addresses

It is now possible to add MAC address information to object definitions for use with the Firewall, NAT and Wireless areas of the configuration (like static mappings above). A new tab in the object definitions area will allow you to create lists of MAC addresses which can be used in some areas of the configuration, such as the new RED security features (see the RED changes later in this document). Object definitions can be created without an IP address using a MAC-only, and thus you can for example create firewall rules based solely on MAC address.

SSL VPN for iOS and Android

Using the newly-released SSL VPN client from OpenVPN (free in both the Android and iOS app stores) you can connect to your network via SSL tunnel from your mobile.

You should install the OpenVPN SSL client on your mobile first; from there, both the configuration of your UTM and the installation of the profile on your mobile client is simple. Setup SSL VPN (if you have not done so) and login to the UTM UserPortal from your mobile device. Choose the new IOS/Android option “install” button under the SSL VPN section which will trigger a configuration-less profile import. There is no need for extended methods such as using iTunes to sync the package files; that will be automatically done via import magic from the UserPortal, as long as you visit the UserPortal from your mobile. For Apple users, you require iOS 6 or greater.

Offline-Provisioned Deployment for RED devices

We have again advanced our unmatched Remote Office Device product to support markets with networks that are completely private with no Internet access (both for RED devices and the UTM itself), or for example as a way to provide RED-managed access using 3G/4G communications as a backup to MPLS connections, which is a popular use-case for Automated Bank Machine networks. You can now deploy RED in these privately-managed environments using a configuration download option that removes the need for the UTM AND the RED device to be able to see our cloud-based provisioning server.*

To use this feature, go to the RED Client section of WebAdmin and when deploying a RED you will find a new provisioning mode option under the “advanced” section for each device. Change this to “Offline via USB Stick” and you will be able to download the configuration for the RED to your PC. Place the corresponding .RED file on the root of a blank USB thumb-drive and then boot your RED device. The configuration will be loaded to the RED and it will then configure itself. A more detailed explanation of the steps is below.

*Note about RED firmware: Later in 2013, as our factories update newly-produced RED appliances to ship with the latest firmware version no additional steps will be needed. During this transition period, for existing RED devices without the latest firmware developed for UTM 9.1 you will need to first update them so your RED “knows” about the new offline mode. A summary for configuration of Offline RED is as follows:

1. Register your RED normally to a UTM running 9.100+ Your RED will contact the provisioning server and connect to the UTM you registered it to. It will be flashed with the latest firmware, and you are then ready to use Offline Provisioning Mode.

   Tech tip: Starting in UTM 9.1, (to accommodate for the Offline mode) firmware updates are delivered from the UTM and not the provisioning server.

2. Now that you have a RED with the latest firmware, record the unlock code (via email or WebAdmin of the current UTM).

3. On the UTM which you want to use for Offline RED deployment, deploy the RED via the [Server] Client Management tab (as this is an advanced deployment mode, it will not be supported via the Deployment Helper).

4. Configure the parameters as desired; for the UTM Hostname(s), you can use a private/non-routable IP address(es) of the UTM interface(s) the RED will be able to communicate with, depending on how your private/offline/MPLS network is structured.

5. After configuring the deployment parameters, click the '+Advanced' section and change the Device Deployment to 'Manually via USB Stick', and hit 'Save'.

6. Now from the '[Server] Client Management tab', for each RED you deploy in this manner there will be a 'Download' button next to 'Download Provisioning File'. Save the resulting xxxxx.RED file to the root of a blank USB thumb-drive.

7. Boot your RED device (which you upgraded in step 1 to the latest available firmware) with the USB drive containing the .RED file; it will load the new configuration and connect to the private IP you specified for your UTM hostname in Step 4.

Your RED device is now deployed in offline mode, and neither it nor the UTM needs Internet connectivity to function! You can manually download UTM Up2Dates and apply them via WebAdmin. As now RED firmware is included with UTM Up2Date packages, when new firmware for RED is released the UTM will deploy it directly to the connected REDs without the need for them to contact provisioning server in any way.

Tech Tip: If you make an error in your configuration or the offline UTM is unreachable by the RED, it is normal for the RED to attempt to contact our online provisioning server as a fallback (you may see traffic attempts as a result).

Wireless Repeating and Bridging for AP50

The AP50 can act as a network bridge and/or repeater using a new meshed-configuration option. Bridged setups allow the wireless radio to be used as a link back to another AP50 while using the Ethernet port to connect a wired device not easily reachable with a cable (like a roof-mounted projector). Repeating configurations can extend your wireless coverage to blanket areas where an Ethernet jack is not available (only a power outlet). It is possible to combine both these features as well, by creating repeater bridges that both link back to another AP50 for the control connection and repeat the SSID's on the bridged AP.

Mesh-network setup is largely automated; the AP50's will build a private, hidden network that they communicate on, and you can even chain meshed access points to extend their reach (at the cost of throughput). For example, you can wire in AP50 "A" and place "B" a certain distance away, while then placing "C" even farther where it cannot reach "A". "C" will then talk to "B" which will backhaul traffic to "A". Such setups have communication overhead and will reduce your transmit speeds. You can have a mix of wired "root" AP50's and bridged AP50's in your mesh, such as anchoring 3 units with ethernet cables and spreading 6 more bridged units around your company.

Minor New Features

Amazon Cloud features

Our unmatched Amazon VPC connector now supports the new Amazon single-tunnel IPSec connection option. However, the “dynamic” option from VPC VPN which creates dual tunnels and automatically configures BGP balancing and failover remains much more powerful and (being totally automated) is just as easy to configure.

Amazon Cloud instances of UTM can now have their initial interface edited (such as to rename them from the default "Internal"). You will receive a warning if trying to change Interface parameters which would render the instance un-reachable.

Download Throttling for QoS

There is a new *Download Throttling* tab in the Quality of Service section. In the past, while powerful, the QoS system required an understanding of how traffic shaping could be configured by exacting control over how interfaces “upload” traffic, such as FROM the internal interface to the LAN to limit traffic in an effort to control a download by a user. We have re-designed this functionality entirely and located it in a dedicated QoS section. Downloads can now be easily controlled and we have added a new button to the live Flow Monitor named “Throttle” (in addition to the Shape button for Upload traffic) to allow you to instantly create rules based on traffic which is actively transferring. We will likely rename these two buttons in a future Up2Date for clarity.

Country blocking enhancements

Our wildly-popular country blocking ability has been further enhanced at your request to allow you to separate incoming and outgoing traffic decisions. This means you can allow outgoing traffic like email TO a country while blocking all incoming communications (like penetration attempts) FROM it.

In addition, the country blocking system has had support for exceptions added which allows you to create the same granular exclusions as is already possible in many areas of UTM.

IPv6 additions

IPv6 Support has been further enhanced, and is now available for the POP3 proxy, server load balancing, and more! We have also taken the opportunity to further-extend our comprehensive IPv6 feature offering by adding support for IPv6 to our portscan detection system and upgrading the engine to allow for automatic IPv6 renumbering and prefix delegation.

RED improvements

Our ingenious RED technology is further bolstered by some new security options. Admins can now choose to de-authorized RED devices if they are offline for a configurable time period to protect against concerns of RED’s being transported off-site.

RED devices now also support White and Black lists for MAC addresses on a Per-RED Basis for an optional additional security layer. You can use this to either only allow certain devices or disallow unwanted devices from being able to traverse down the tunnel to the home network.

As part of sweeping architectural improvements to support “Offline” mode and deployment of large amounts of REDs, firmware is now retrieved from the UTM they are connected to as part of UTM Up2Dates.

RED appliances now support many more 3G/UMTS devices in various regions globally, while a select amount of 4G/LTE USB sticks will work as well. We are actively working to further expand the driver set for this much-demanded area. Try devices out and let us know in the RED forum at www.astaro.org how they work!

View of “automatic” firewall rules*

You can now choose to view the firewall rules which have been automatically created based on your use of this option in various configuration sections. You will find a new option to toggle the display of these rules for auditing/troubleshooting purposes in the firewall rules section. This allows you to make use of “automatic firewall rule” option in areas like NAT & VPN while being able to view them on the main firewall rules screen.

*Note that system created rules like those for areas around the HTTP proxy and other sub-components cannot be shown in WebAdmin with this option due to their complexity and how they are used by the underlying middleware.

Remote access profiles for SSL VPN

SSL VPN Profiles have been added! You can now offer varying levels of access using SSL VPN by creating (or cloning) access configurations within the remote access section. While in the past everyone had to share the same set of parameters (that could be controlled via the firewall rules only), you can now create different profiles for users or groups.

IPSec Tunnel Binding

A powerful option for IPSEC Tunnels has been added; you can bind them to their local interface using a check box when creating an IPSEC VPN connection. Tunnels can then be used with multipath rules AND fail to other tunnels as needed automatically. This enables automatic balancing and redundancy while you take precise control over how you want traffic in your network to use multiple links, and does not require selectively “layering” of subnets or the use of BGP routing.

Sticky WAN balancing rules

Multipath rules can now be made 'sticky', ensuring the traffic is not part of the fail-over behaviour and will always be routed over the desired connection, even if the link is down.

Outlook Anywhere protocol handling for Web Server Protection

Web Server Protection (WAF) can now accommodate Outlook Anywhere traffic. You will find a new button to enable this in Protection Profiles.

Customization of Web Protection block pages

We have totally re-designed the Block-Page customization section from the ground up to give you control of precisely informing your users why they are receiving a block from the Web Protection. This system can clearly communicate for example that the page they are trying to visit doesn't exist without leaving them with the impression that the UTM has blocked the site and causing them to ask the administrator erroneously.

Other Changes and Enhancements

- [Auth] The Sophos Authentication Agent (SAA) is now available for Mac OSX and lets you track user activity with precision by associating them to their current IP address(es). This lets our Apple users enjoy the same enhanced reporting and policy control that Windows users have already had access to. SAA is great for environments that do not have a central authentication system but wish to have a degree of control on a per-user basis.
- [Auth] A new WebAdmin role has been created that allows for management of the Mail Quarantine only.
- [General] When importing the WebAdmin CA into Internet Explorer, Jedi-mind trickery has been applied so that IE actually remembers this now.
- [GUI] You no longer need to enter passwords twice when performing many operations in WebAdmin. Fingers=saved.
- [GUI] Backup Files can be deleted using multi-select check boxes or all at once using a select all option at the bottom of your list of backups.
- [GUI] Flash has been replaced in charts. They now use JavaScript magic and work on mobiles, while becoming faster overall and saving you flash headaches in general.
- [GUI] On/Off "traffic lights" have been replaced with a new toggle-switch design.
- [GUI] Throughput figures in many outputs will properly scale their units intelligently based on the data, removing the need for you to always translate kilobits to megabits.
- [GUI] Time-events can now be created which span Midnight, making it easy to define "after-work" periods.
- [GUI] UserPortal will no longer display HTML5 VPN section as a choice if the logged-in user isn't configured for any connections.
- [GUI] SSH Access now has a lockout option like WebAdmin to assist in preventing repeated attempts
- [Mail] The POP3 proxy now supports encrypted SSL connections.
- [Network] Support has been added for many USB Ethernet network adapters

- [Network] Multi-link PPP support has been added to bundle multiple PPP connections into one logical one (one IP address instead of multiple). Support depends on the provider.
- [Network] Support for VDSL VLAN tagging has been added.
- [Network] You can now choose (AES + GCM) or (AES + CTR) as encryption algorithms in addition to the existing (AES + HMAC) ciphers. (AES + GCM) measurably increases performance on Intel processors.
- [Notifications] Notifications have been added to alert you when a VPN tunnel goes down/comes up again. This includes RED devices. The notification is WARN-726 and located in the notifications section.
- [Reporting] In-line and Executive reports will show host names where available before resorting to display of IP address.
- [Reporting] In-line and Executive reports now show user / definition names instead of IP's throughout
- [System] The logging daemon has been updated to a multi-core version. Logging and Network-accounting performance on multi-core systems will increase dramatically, up to a factor of 20x on bigger systems (to use a conservative estimate)
- [System] Database inline calls have been heavily optimized and will yield much faster reporting across many areas.
- [System] When configuring HA, the initial database synchronization will be much faster as many performance optimizations have been made.
- [System] Many improvements and optimizations have been made to the entire database system to significantly increase overall performance
- [Warcraft] Onyxia has had her deep-breath ability altered.
- [Web] Several Sophos Services (like Endpoint Updates) have Application Control patterns now.
- [Web] The way the Web proxy handles temporary files has been redesigned to offer a significant performance increase throughout.
- [Web] A new option "Force Caching of Sophos Endpoints" in the Web Protection advanced settings allows the UTM Web Cache (when enabled, see below) to cache Endpoint updates to save Internet bandwidth
- [Web] You can now specify a max file download size for Web Proxy users. (This pairs nicely with the option to restrict AV scanning to files no larger than "X")
- [Web] Web-Caching is disabled by default on new installations (This disables Endpoint Update caching abilities above).

- [Web Server] New behaviour choices for handling of unscannable archives in Web Server Protection (Web Server Protection >> Web Application Firewall >> Firewall Profiles)

- [Web Server] Exceptions created for Web Server Protection can now have their state toggled on/off.

- [Wireless] AP10's in some regions should offer stronger and more reliable signal.

Considerations

- If you are not already part of our feedback program, the “Help Make Sophos UTM Better?” dialog box will re-prompt you after the installation of 9.100. This is normal, as we benefit greatly from understanding how you make use of your UTM that we might best allocate our development and enhancement of features. If you are already opted-in, you will not see this dialog box, and we thank you for sharing high-level usage information so we can build a better product for you!

- The lockout mechanism of UTM has been extended to cover more areas (previously only possible for WebAdmin login attempts). As a result, this functionality tab (and previous WebAdmin security lockout feature) has been overhauled and moved to *"Definitions & Users->Authentication Servers--->Advanced".*

- Anti-Virus detection positives (Sophos AV Engine only) are now reported to Sophos Labs as part of the UTM Feedback Program (see above) in order to help ongoing research and protection efforts.

Upgrade and Installation Information

System Requirements

Hardware

The official minimum hardware requirements for UTM 9.1 are:

- Intel™ Core2 Processors @1.5 GHz, 1 GB RAM, and a 40 GB hard disk drive.

Best performance results are experienced when using recommended hardware specifications. While using 1GB of memory is possible, 2GB+ is heavily recommended for UTM 9.1. We recommend:

- Intel™ Dual/Quad-Core CPUs at 2GHz+, 2GB+ RAM, and 80GB+ 7200rpm or Solid-State disk.

For hardware recommendations when building your own appliance, please check our UTM 9 Hardware Compatibility List (HCL) at: http://astarosupport.org/hcl/

UTM 9.1 can also be installed within virtual environments, such as VMWare ESX, Citrix XENServer, Microsoft Hyper-V, and KVM (to name a few). Virtual appliances provide the same functionality as the standard UTM hardware platform. Other virtualization platforms should work flawlessly with UTM, and their use is not inhibited by Sophos. However as they are not officially supported, compatibility issues may arise in areas of networking and time-keeping.

Browsers

Sophos UTM WebAdmin supports the majority of modern browsers, and is optimized for (and developed within) Mozilla Firefox. The latest available versions of Google Chrome, Internet Explorer, and Safari are also fully supported. Take care to use the latest stable/official release of these products; older (or bleeding-edge) versions of browsers can experience compatibility issues due to the nature of browser evolution.

Upgrading to UTM 9.1 from Astaro Security Gateway (ASG) V8.3

Existing customers running legacy ASG V8.306 or greater on a hardware appliance can one-touch migrate to UTM 9.000 directly from within WebAdmin (provided that you have a compatible appliance). Once landed on 9.000, Up2Date to the latest version.

To ensure the performance of UTM 9 and the experience of using the product and its features for the installation size it was designed for, UTM V9 will **only** operate (via upgrade or re-install) on certain legacy models that meet appropriate specficiations. The following chart shows which appliance models are fully supported, which models will run UTM 9 (but will have difficulty enabling new features, particularly if already close to their performance limit) and which are not supported.

ASG/UTM Appliance models supported by UTM 9

Model	Revision	Not supported	Supported *	Recommended and Fully supported
110/120	Rev.0, Rev.1, Rev.2**	🔴		
	Rev.3, Rev.4		🟡	
	Rev.5 or greater			🟢
220	Rev.1, Rev.2	🔴		
	Rev.3, Rev.4		🟡	
	Rev.5 or greater			🟢
320	Rev.1	🔴		
	Rev.2, Rev.3		🟡	
	Rev.4, Rev.5 or greater			🟢
42x	420, 425	🔴		
	425a rev.1, rev.2, 425 rev.3		🟡	
	425 rev.4, rev.5 or greater			🟢
525	525/525F Rev.1, Rev.2	🔴		
	Rev.3		🟡	
	Rev.4 or greater			🟢
625	all revisions			🟢

This unit is **supported for running Sophos UTM version 9. However **performance may be limited** if features that were added or enhanced in UTM 9 are enabled.*

*** Rev.2 units that had a memory upgrade to Rev.3 will be recognized as a Rev.3 appliance*

Appliances pre-dating the above listed ones can continue to run ASG V8 and will receive security patches and updates until declared end-of-life. If you would like to inquire about how to replace your older appliance with a new one capable of running UTM 9 via our hardware refresh program, contact your partner or Sophos sales.

Once running UTM V9, any available Up2dates will be downloaded for you automatically, so that you can bring your installation to the latest version.

Upgrading from ASG V8 to UTM 9.100 can be done via:

Install with new configuration

1. Install a fresh UTM 9.100 firmware on your appliance.
2. Use the Setup Wizard (recommended) to kick-start your new configuration for UTM 9.100
3. Apply your ASG V8/UTM 9.100 on-demand style license (older licenses must be upgraded from within MyAstaro).

Install with import of earlier UTM/ASG configuration

1. Install a fresh UTM 9.100 firmware on your appliance and apply an exported UTM 9.000 or Astaro Security Gateway V8 backup file to have your configuration imported.

Install on a UTM appliance via a Sophos Smart Installer (SUSI)

1. Install a fresh UTM 9.100 firmware on your appliance and convert the existing V8 configuration into the new version via the restore of a configuration backup file. (See above)

Automatic ASG V8 to UTM 9.100 upgrade (qualifying Appliances only)

1. On your ASG V8 Appliance, upgrade the firmware to at least Version 8.306
2. Valid appliances (see above) can then select the “Upgrade to UTM 9” button in the Up2Date Section. All log files and reports of your V8 installation will be reset during migration. All other configuration will be retained.
3. Up2date to the latest version of UTM 9.xxx once on the UTM platform

Backup Converter Notes

All configuration will be restored from a UTM 9 backup file into UTM 9.100. Since log files and reporting data are not part of the backup file, these will begin anew as part of the re-installation process. If log files are important to you and you are doing a fresh install, first download all your logs via the WebAdmin logging section for archiving purposes!

Software Download

This new version, past releases, Up2Dates, and other software is available on our official download servers directly:

- ftp://ftp.astaro.de/pub/UTM/v9/
- ftp://ftp.astaro.com/pub/UTM/v9/
- http://download.astaro.com

Supporting Applications

Sophos UTM Manager (SUM) - Previously Astaro Command Center (ACC)

UTM 9.1 is only supported by the new Sophos UTM Manager 4. Older versions of Astaro Command Center will communicate with UTM 9, however any new functionality regarding UTM 9 will not be accessible unless you use SUM 4.x.

Known Issues

The actual UTM V9 Known Issues List (KIL) can always be found at http://www.astarosupport.org/kil

**

**While we make every effort to include all changes in our patch notes, occasionally some assorted cool things sneak in and are unintentionally omitted as a result. If you see something we failed to mention, let us know!*