SOPHOS

Sophos UTM 9.2 Accelerated

Release Notes

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

May 2014

Contents

Major New Features

Advanced Threat Protection

One of the headline features for UTM 9.2 is the addition of an Advanced Threat Protection system (ATP). Using a new integration to Sophos Labs, your UTM will know about globally identified botnets and command & control sites, and can intelligently blackhole their communications with great accuracy. This avoids wasting processing time interpreting their traffic; if sites are known to be “bad” then we can ignore them. In addition, clients behind the UTM that attempt to communicate with these sites are intelligently deemed to be infected with malware or other malicious code, and will trigger alerts and warnings while having their communications to these sites blocked.

Much more will be released on this technology, but for now, note that we have new notifications for this engine, a new status widget for the WebAdmin dashboard, and new logging/reporting entries. This feature is included in the Network Protection subscription of UTM.

Intrusion Protection Performance Improvements

One of our top requests was for more performance of IPS. After consuming hundreds of development hours, the system has been heavily optimized across all products and further optimized for each UTM appliance model by tuning the engine to the appropriate hardware configuration. In addition, a new pattern-aging system has been implemented designed to increase the relevance of scanning profiles without wasting resources on older patterns that might not be relevant any longer. This functionality can be adjusted if you want to alter the default settings.

One-Time Password (OTP) / Two-Factor Authentication (2FA)

A new system has been implemented to support two-factor authentication for areas like WebAdmin, UserPortal, VPN, and more. Support has been built-in for the Google Authenticator to allow users to on-board themselves into this system (if the admin enables it) via the UserPortal.

Admins can also add users themselves by setting the initial secret code from within a new section of WebAdmin. Once setup, the user will append their password with the rolling OTP code that is generated, so a login might look like "johndoe / mypasswordXXXXXX" where "XXXXXX" is the 6 digit passcode generated by the system. Mechanisms that use hardware tokens, 3rd party services (such as Duo Security) and other applications that support (OAuth) are intended to work. Try out your favorite and let us know your results!

New GUI design for Web Protection

The Web Policy approach has been totally overhauled for UTM 9.2 with many new mechanisms.

The base policy and profile policies can be more easily applied, assigned, and edited, and policies can now be applied on a per-user basis. We have enhanced this even further by allowing for per-device authentication assignments, extending the power of the Web Protection suite by orders of magnitude.

Additional profiles have been re-designed as well. and the Web Filter Profiles menu section has been revamped with a new look and increased functionality throughout.

Transparent Mode with Transparent SSO Authentication

We are proud to say that you can now use the Web Protection in transparent mode with transparent authentication. This requires no proxy settings on the client and gives you all the same benefits as you would normally enjoy when using AD single-sign on and an explicit proxy, and thus is quite powerful. For this to work, the fully qualified domain name of the UTM must be resolvable by the clients on your network. Users will be automatically re-authenticated every five minutes (the browser should auto renew without user input). Note that non-browsers (without agents) may not handle HTTPS redirects correctly (such as certain windows downloader) and your mileage may vary with those applications of this ingenious technology.

Authentication Offloading for Web Server Protection

An entirely new authentication offloading feature has been added to Web Server Protection that supports both basic authentication and form-based authentication, allowing this system to have users authenticate against it and then represent the result to the backend server(s).

Note It is not possible to use our new Two-Factor Authentication (one-time password) with this feature using the backend authentication mode, you must use the form-based one. This is so you know what request it is, as backend authentication will cache the credentials and thus in a few seconds user requests would be invalid.

Live AV Lookups and Sandbox Execution via Sophos Labs (Catchy Name still in the Works!)

When using Web Protection with the Sophos AV scanning engine enabled, a new option has been added to use live cloud checksum lookups from Sophos Labs. Lookups that fail will still be scanned by the AV engine, and as part of the global feedback network unknown files will be sampled for execution and deep analysis by Sophos Labs to benefit the global community while allowing you to tap the knowledge gained by these events worldwide.

Fully Transparent HTTPS Filtering

The UTM can now perform URL filtering on HTTPS sites without activating the existing man-in-middle “full” HTTPS scanning engine. Using SNI, the URL (or IP if URL is absent) is extracted from the HTTPS session and checked against the URL database. Note that deep-scanning inspection (like malware for example) is not possible with this high-pass option; to look inside the HTTPS sessions and take more advanced actions you will need to use the full HTTPS inspection deployment.

SPX One-Way Message Encryption

UTM now supports one-way encryption of messages to recipients that do not have a trusted encryption system in place such as the ones already supported by UTM via PGP or S/MIME. A new section can be found in Mail Protection called “SPX Encryption”. This one-way mail encryption engine is based on Secure PDF eXchange (SPX). Users can encrypt outgoing messages which are then wrapped in an encrypted PDF that can be received and read by the recipient without them needing to have any support for this process on their end.

The recipient receives a notification email that alerts them they have been sent an encrypted message. The content is attached in a PDF. Upon opening it, they will need to enter a password to view the contents. If enabled by the administrator, a user is also able to respond to the message via a reply button integrated into the PDF. The reply portal (when enabled) listens on a default of port 10443 and can be changed. The interface(s) the reply portal listens on can also be configured.

Both the PDF and the secure message to the recipient have a default cover page that you can override with your own customizations. Many areas are customizable such as images, formats, headers and footers. In addition, the mechanics of the password creation, communication, message response times, un-retrieved message handling, and more can also be customized by the administrator to provide a seamless experience to their end-users.

Data Leakage Protection (DLP)

A new system for Data Leakage Protection has been added to mail which scans through messages and attachments for data you may not want to leave the company. You can filter by category and region/country for parameters like credit card numbers, bank routing codes, postal addresses, phone numbers, and over 200 other factors.

Minor New Features

Google Application Control

Enforcement has been added for Google apps, allowing you to limit access to these services to your company domain only. By limiting to your company domain only, users will not be able to access their personal apps any more. You will find this as “Enforce allowed domains for Google apps” in the “Edit Filter Action” dialog box when creating Web policies.

Background Active Directory Synchronization Option

Currently, when a user authenticates against AD, the UTM does a lookup against each group they are a member of. In environments with extensive groups or large organizations, this can cause a lot of load on both the UTM and the AD server, a new option has been added to fetch the mapping every 2 hours (or manually at the admins discretion) to sync their group memberships at a constant rate.

Enhanced Web Log Searching

You can now search through the web log(s) with more parameters, such as running a search for “Bill” going to “Facebook.com” and getting only those entries that match. In addition, you can filter for all the block reasons the system can trigger on.

Fully Customizable Wireless Hotspot Pages

Increased abilities for customization have been added to the user-facing pages which are served as part of the Wireless Hotspot functionality. Using these tools, customers can now implement their corporate identity in a more complete fashion.

RED Tunnel Compression

RED device configurations can now select to enable tunnel compression. This can save bandwidth if this is a the primary concern, however the compression operation will take increased CPU power, and as traffic volume scales up the CPU will then be the limiter, especially on the RED10 devices. For compression, sites with less than 10 megabits is the target use-case.

Web Protection Policy Testing Tool

Within the WebAdmin in a new section of Web Protection called “Policy Test”, the admin can enter parameters and be informed how such a request would be handled by the system. This avoids you having to manually test users on real machines. You can enter a destination or URL, time, and other parameters to match and then see a detailed output as to what the user would experience as a result.

Authentication Method by Device Type

It is now possible to specify different HTTP authentication methods for different devices! Using identification agent scanning, UTM can now detect Windows, Mac OSX, Linux, iOS, Android, Blackberry and Kindle devices, and let you have filtering profiles based on this. For example, you can apply special filtering for all iPads in a school which uses a different method than the normal windows workstations.

Local Site Reclassification Listing

It is now possible to override the reputation and/or category of a particular URL/IP/IP range. If you only override the category, reputation will still be looked up, and if you only override reputation then category will still be checked. This allows admins to specify a site with a different result, such as adding an uncategorized site into a desired classification. You can import from an existing list by pasting many entries into the import dialog, and paths are prefix matched; if www.google.com/myurl is placed, it will classify all subsequent URLs using that string.

More Detailed HTTP Logging

In addition to the changes outline in “Other” below, for every http.log transaction, there are two new significant tags added for diagnostic purposes. One is for the device type and another for the authentication type, which complements the increased functionality we have introduced around device-based authentication explained above. The number designator descriptions will be explained in detail within the online help of WebAdmin for the GA release.

Web Control Integration with Sophos Enterprise Console

Endpoints can now be managed by Sophos Enterprise console while getting their web policy (and reporting) from the UTM. Note that UTM can manage approximately 1000 deployed UTM deployed endpoints, but as Sophos Enterprise endpoints differ significantly from the endpoints deployed directly from the UTM and this feature is integrated in a way that doesn't sync the SEC endpoints to the UTM, significantly larger deployments of SEC can receive UTM Web protection. Remember that this does not let you manage all your SEC endpoint features; it only provides web filtering for your classic SEC clients using the UTM as an engine. This requires that you enable full web control in SEC and then copy the UTM information into SEC.

Potentially Unwanted Application (PUA) Blocking

Many applications are not inherently malicious, yet are considered by many to be unsuitable for business use. If enabled, applications such as hacking tools, OS admin utilities, and other potentially disruptive tools will be blocked during their download by the AV engine, and logged as reason "PUA". Note that PUA blocking is a global setting, and has also been added to the available User-facing block pages which you can customize.

HTTPS End-User Block Pages

Users will now see a proper Web "block" page when encountering a block event over HTTPS. To serve this block page, the UTM will complete the SSL handshake and send the block page inside the tunnel. In both "light" SSL scanning and deep HTTPS inspection, your client will need to trust the UTM proxy CA first (via the UserPortal or our other adoption mechanisms) to avoid seeing browser certificate errors when these events occur.

Custom Certificate for End-User Pages

Since end-user pages will be using HTTPS in 9.2, end-users without the UTM CA will see a warning in their browser about the certificate. To counter this, we now support custom over-the-counter certificates that can be used for these block pages that will be then trusted by the browser and avoid the error.

Multi-domain Active Directory user support

In UTM 9.2 the user's domain will now be considered when matching users, so that users from a second, separate domain with the same username as the first (such as "jdoe") will be treated separately and can have their own policy applied, eliminating the restriction for each user to be unique across domains.

Other Changes

- [Authentication] The UTM will now consult the SID as well as the username of authenticated users to allow for the same username to be used in two different domains.
- [Endpoint] You can now specify a parent proxy when enabling Endpoint Protection
- [Endpoint] Administrator is able to configure alerts (via Email or SNMP) for endpoint virus detections from the WebAdmin UI (Management -> Notifications -> Notifications). There should be a new section called Endpoint with one entry called Endpoint Virus Detected.

- [Endpoint] A new configurable notification has been added for when UTM deployed endpoints detect a virus. This is off by default and must be enabled.
- [General] Backup notifications have been removed from the notifications section, as they were required to be enabled to actually transmit backups when the admin enabled that functionality. They are now wholly configured via the backup section.
- [General] The version number of the UTM will now only be updated once an Up2Date package has been fully applied in all respects to avoid a rare condition where an Up2Date failed in the final stages after the version had been advanced.
- [General] During installation, SWAP file size will now be set to match the system memory (this is a change from a default of 1GB for all installations).
- [General] UTM 9.2 will by default no longer allow outgoing SSH connections when logged into the command line environment. This is to increase the security and sanctity of the system. If you require this ability, you will need to manually add a rule to the OUTPUT chain. (unsupported)
- [General] The initial setup wizard has been overhauled with new functionality and updated components to offer a better experience.
- [Intrusion Protection] Support has been added to disable file-based pattern rules.
- [Intrusion Protection] For the command-line tinkerers, a new command ‘Ipsctl’ has been added for control of the IPS engine.
- [Licensing] The license import function will now show you the parameters of the license you have selected so it can be reviewed before uploading.
- [Logging]Under Logging & Repting -> View Log Files -> Search, there will be three new fields when a user selects 'Web Filtering' from the dropdown.
    - User
    - Url
    - Action
- [Logging] Many new diagnostic factors have been added to the Web Protection log (http.log). Fields such as DNS time, authentication time, categorization time, and more can assist performance tuning and troubleshooting.
- [Logging] Like IPv4, IPv6 multicast packets will now no longer be logged by default, as they are largely useless noise and tend to create gigabytes of log files with no value to the security policy or auditing.
- [Network] The Dynamic DNS engine has been updated to allow for even more providers like OpenDNS, No-IP, and others.

- [Network] It is now possible to place the UTM in bridging mode using two separate LAG interfaces.
- [RED] RED firmware updating has been slightly tweaked to prefer the online provisioning server and only serve firmware files from the UTM directly if the provisioning server is not reachable to avoid that in environments with large amounts of deployed RED devices that the Internet connection of the HQ is saturated when trying to deliver the updates.
- [RED] Handling changes have significantly reduced the fail-over time on a RED50 when two uplinks are used and a WAN port fails or suffers downtime.
- [RED] RED50 now supports VLAN tagging on a per-port basis. You can choose from Untagged, Untagged/drop tagged, Tagged, disabled.
- [RED] The RED50 LCD screen now displays much more information, such as uptime, 3G signal strength, and firmware version. The navigation buttons can be used to page through the screens. Future versions will look to make configuration adjustment possible.
- [Reporting] Web Security reports have been enhanced with support for IPv6 addresses.
- [Reporting] Several new reports have been added.
  - Some new views have been added to Web Reports
    - Users with Categories
    - Users with URL’s
    - Domains with Categories
  - New default saved reports have been added to Web Reports
    - Virus Downloaders
    - Policy Violators
    - PUA Downloaders
- [Reporting] The executive report will now be sent weekly by default (up from daily).
- [Reporting] It is no longer necessary to press the “back” navigation button twice in Web Reporting after selecting a filter and a report to step back one level.
- [Reporting] Many filters that a user wanted to apply when navigating through the Web reporting engine have been fixed to work more consistently and effectively as the user expects:
  - User report, filter by action no longer has the same results regardless of action.

  - Domains report, if you click on a domain, click on Users and the domain filter won't apply to the Users report.
  - URLS report, click on URL, click on Users and the URL filter won't apply to the Users report
  - URLS report, click on Action, click on Users and the Action filter won't apply to the Users report
  - Overrides report, click on Users, click on Domains and the Users filter won't apply to the Domain report
  - Overrides report, click on Users, click on Sites and the Action filter won't apply to the Sites report

- [VPN] Users should no longer be disconnected when transferring large files over SSL VPN Remote Access connections.
- [VPN] Support has been added for backend groups to be used for IPSec X.509 and Cisco VPN remote access authentication.
- [Web] Browser authentication and policy override pages have been converted to HTTPS to avoid transmitting unencrypted credentials over the wire.
- [Web] URL White/Blacklisting has been overhauled to be much more intuitive and powerful, allowing for wildcards more easily and subdomain matching with ease.
- [Web] The FTP proxy will now perform scanning on PUT requests (as well as the existing GET request scanning ability). If the uploaded file contains malware an error will be sent to the FTP client.
- [Web] The “drop” option for profile mode has been removed as an action for some checks, as this caused the same behavior as “reject” and thus was redundant.
- [Web Server] The maximum file size for uploaded files via the WAF has been increased from 128MB to 1GB.
- [Web Server] The WAF engine has been updated with a new version that offers many improvements.
- [Web Server] The WAF protection rule set has a fully updated set of new patterns, more patterns to choose from, and will be updated continually via Up2Date.
- [WebAdmin] WebAdmin timeout has been increased to a default of 30 minutes (up from 5)
- [WebAdmin] The UserPortal is now reachable by internal hosts on port 443 when the Web Proxy is activated.

- [WebAdmin] WebAdmin now supports wildcard certificates and certificate chains, allowing you to replace the WebAdmin certificate with a paid alternative more easily.
- [WebAdmin] Many places in the UTM where you can pick allowed networks (e.g. Web Proxy) have had a warning and additional confirmation added if “any” is selected.
- [WebAdmin] With the introduction of the new Advanced Threat Protection system, AppAccuracy settings has moved from Web Protection >> Application Control >> Advanced to Management >> WebAdmin Settings >> Advanced.
- [Wireless] A new dynamic channel assignment logic will continually seek out the best channel for the AP’s based on the surrounding wireless landscape and adjust accordingly.
- [Wireless] New additions to the overview page show more detailed mesh-information if the AP is part of one.
- [Wireless] A button has been added to create new vouchers in the hotspot form - It is also possible to add new voucher definitions inside the hotspot form.
- [Wireless] Backend authentication is now a supported mechanism for the hotspot, allowing you to remove voucher logins to the hotspot itself and instead allow users to authenticate in a dialog box against a backend system configured on the UTM.

Coming soon

- Admins can now choose to “warn” a user on desired categories in addition to block/allow.
- Allow for fallback to an IP-based Web policy if the desired authentication fails.