Secure Web Gateway 12.0 Release Notes

Trustwave is pleased to announce the release of Secure Web Gateway version 12.0.

September 2018

Contents

New Features

- New cloud-based Malware Analysis Sandbox add-on service.
- Behavioral Java analysis provided by Jentrapper can be enabled. Jentrapper is a proprietary, behavior-based dynamic analysis engine for scanning Java Applets.
- BinaryVAD functionality has been extended with a new engine to improve binary inspection capability.
- The WebSocket protocol is now supported.
- Secure ICAP is now supported. Scanners can connect to other systems using ICAP through a secure tunnel. The default port for secure ICAP is automatically changed from 1344 to 11344.
- Multiple ICAP servers and ICAP pipelining to multiple services in sequential order is now supported.
- SafeSearch can be enabled in policy rules to filter adult material and offensive content in Bing, Google, and Yahoo search results.
- Scanner access (SSH) for administrator accounts can now be allowed or disabled.
- Individualized keywords can now be defined and assigned to URL categories and URL lists. Access is blocked when defined keywords or phrases appear in a search engine query.
- The Kaspersky Anti-Virus SDK has been upgraded to a newer version.
- The enhanced certificate validation policy will validate static certificate pinning. In addition, we validate SHA1 signatures.
- Removed support for the Diffie-Hellman Key exchange algorithm because it is considered weak.
- Individual Microsoft Outlook pst file types can now be selected to create FileType rules.

Limitations and Known Issues

- Using SOCKS versions 4a or 5, if the client asks for domain name resolution (DNS) on the server side, the client should provide the hostname as a FQDN, and not the IP address. Otherwise, the request will not be blocked based on the hostname.
- Jentrapper scanning instance start-ups can be a heavy load on the CPU, with each upstream proxy having to be assigned to an instance of Jentrapper. Running Jentrapper in environments where multiple upstream proxies are defined can result in start-up failure due to the expiry of the start-up timer timeout period.
- On a clean installation, the administrator logs into the SWG UI with the default password and is required to replace the password with a new one. However, until the license is applied, the new password will not be synced with the Limited Shell.
  Until the license is applied, the default password must be used in the Limited Shell.
- Content on sites using Brotli compression as site content-encoding is not scanned by SWG.
- Some WebSocket functions may still be operational in Tunneling mode when the "Allow WebSocket" option is unchecked in the UI.
- Websocket does not interoperate with Squid caching.
- Non-secure WebSocket will only work with Microsoft Internet Explorer and Edge in Tunneling mode.
- Policy Server HA does not support IPv6.
- WCCP with Generic Routing Encapsulation (GRE) is not supported with IPv6.
- CSRs generated on HSM-enabled SWG can be signed only on Windows 2008 R2 servers or later. Earlier Windows versions will get an "Invalid algorithm" error.
- Uncommitted changes to setup settings for a device made by the administrator of one group are automatically committed when the administrator of another group performs a Commit Change action.
- Coach actions for pages containing automatically generated links to other pages that are not Coach categories will result in Block actions that are unseen by the end user.
- SWG support for NTLM is limited - some features in newer versions of NTLM are not supported.

  When using SWG Authentication mode "Negotiate" with NTLM (Negotiate NTLM, not the regular raw NTLM), this causes the client to halt the authentication process before completion if the LMCompatibilityLevel parameter in the client is set to 3 (the default value for Win7, Win2008SRV, and newer Windows versions).

  Workaround: Do not use Authentication mode "Negotiate" if planning to use NTLM. The authentication process will work in the same way as in version 11.0. If Negotiate mode is required and there are some appliances that do not support Kerberos, they will authenticate using NTLM, so the LMCompatibilityLevel parameter must be set (manually or by group policy) to LM=2 on these appliances.
- To decrease false positive results, it is recommended to add the "Web Pages" option to the File Extensions condition for Coach Rules in the customer policy.

- Where browser options are configured to remove stored cookies on exit, all cookies, including cookies used by Coaching, will be deleted when the browser session is closed. As a result, the user will be asked in each new session to coach pages even if they were coached in the previous session. Some browsers, such as Internet Explorer 11, may have the option to remove stored cookies selected by default.
- Because Coach actions work with URL Categorization on requests only, Coach actions cannot be used with dynamic URL Categorization.
  Avoid using Coaching for "Web Based Email", "Financial Institution", "Sports", and "News" URL filtering categories when dynamic categorization is enabled.
  In addition, using Coaching for category Other may have unexpected consequences.

Supported Appliances

The following SWG appliances are supported:

- TS-5000 SWG BladeCenter
- TS-250 SWG
- TS-250 SWG (Revision B)
- TS-500 SWG
- TS-500 SWG (Revision B)
- SWG 7100/NG8100-S1 (IBM Model HS23 7875)
- SWG 7080/NG8080-S1 (IBM Model HS23 7875)

Note: SWG 12.0 requires a minimum of 8GB RAM. 16GB RAM is recommended. To purchase additional memory, contact your Trustwave Channel Partner/Account Manager.

Note about Ethernet ports in the 1Gb version of the TS-5000 SWG BladeCenter: In the default configuration, the chassis is delivered with 3 switches; A 10GB switch connected to ETH0 of each blade server, a 1GB switch connected to ETH1, and another 1GB switch connected to ETH2. If the relevant chassis does not include the 10GB switch, ETH1 (and not ETH0) will be configured as the main port.

How to Install This Release

To install this release, refer to the Downloads/Documentation section of the Trustwave website for the current *SWG Setup Guide.*

Note:

SWG Installation Utility VSInstaller version 1.9.1-02 is required.

Legal Notice

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: tac@trustwave.com

Trademarks

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than 2.7 million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is a privately held company, headquartered in Chicago, with customers in 96 countries.

For more information, visit https://www.trustwave.com.