Trustwave®

Smart security on demand

Secure Web Gateway 11.8 Release Notes

Trustwave is pleased to announce the release of Secure Web Gateway version 11.8.

August 2016

Contents

New Features

Socks Server

SWG can now act as a SOCKS Server responsible for relaying data between application client and application server. The SWG Console enables you to define rules that specify the Socks commands applied to specific or a range of source and destination IPs, and specific or a range of source and destination ports.

AV Update Alerts

An SNMP or email security alert will be triggered if the antivirus program has not received an update for a set number of days.

Trustwave Anti-Virus

A no-cost, licensed Trustwave anti-virus option is added to the available third party Anti-Virus scanners.

Explicit and Transparent Proxy

In previous SWG versions, the proxy machine operated in either Explicit or Transparent mode, via port 8080.

In SWG 11.8, HTTP and HTTPS ports can be configured as Transparent, Explicit, or Both Transparent and Explicit. By default, the proxy listens to port 8080 and/or 8443 for Explicit mode and 8081 and/or 8444 for Transparent mode, and behaves differently according to the ingress traffic port.

Nested AD Domains

SWG now provides Parent-Child domain support for nested Active Directory domains. Where a user group in a main directory has sub groups from other domains, the users from the other domains are included in the group when adding the main group to the LDAP tree, and the appropriate policy is assigned to them.

SHA2 Support

By default, SWG 11.8 supports SHA2 (Secure Hash Algorithm 2), used to generate unique hash values. SHA2 works in the same way as SHA1 but is stronger and generates a longer hash.

Streamlined Security Engine Configuration

The Security Levels for the Malware Entrapment Profile and Binary VAD rules are now set at a default Medium level and can no longer be configured by users using a slider. Existing Entrapper and Binary VAD rules that have a level other than Medium are automatically reset to the Medium security level.

Hyper-V Support

SWG now supports Hyper-V Server 2012 appliances. On installation using the iso image, select "vm" to install on the Hyper-V virtual machine.

Filter HTTPS sites by SNI

When a client browses to a URL in Transparent mode, the proxy receives an IP address instead of the server URL. As a result, SWG cannot perform a block using the URL. To resolve this, SWG now uses the Server Name Indication (SNI) as the server name on which to perform URLList and URLCat.

New Bypass Card Support

SWG now supports inline deployment with a bypass card in environments with a single scanning server. SWG versions 11.5, 11.6, 11.7, and 11.8 currently support Bypass card model Silicom CI0532-86M Silicom PEG2BPi-RoHS 2 port bypass.

Coach by Category

The Coach feature has been improved.

Other

- The Entrapper engine has been upgraded.
- SWG 11.8 now supports Microsoft Windows 10. Microsoft Edge browser is not supported by MSC.
- SWG 11.8 is released simultaneously with Mobile Security Client 2.4.
- SSL processes have been improved and made more stable. In addition, the ability to revoke certificates via OCSP has been added and the method of AIA handling has been changed.
- Support for SSL v2 has been removed. SSL v3 is now disabled by default.
- The User Approval action for HTTPS policy rules has been improved. Note that where browser options are configured to remove stored cookies on exit, all cookies, including cookies used by User Approval will be deleted when the browser session is closed.
- An SNMP trap is now sent when all SSL_Middleware processes are down. In addition, a trap will be sent if an instance is down for longer than a set number of seconds. This value is currently set for WASP to 3600 (1 hour).

Limitations and Known Issues

- 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.
- 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.
- 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.
- 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:

- SWG 3000/NG5000-S2 (IBM Model 3550 M4)
- TS-250 SWG
- SWG 5000 (IBM Model X3550 M4)
- TS-500 SWG
- SWG 7100/NG8100-S1 (IBM Model HS23 7875)
- SWG 7080/NG8080-S1 (IBM Model HS23 7875)

The following appliances are capable of running SWG 11.8, but will not receive full support after they have reached their End of Life:

- SWG 5000 (IBM Model X3550 M3) *
- SWG 3000/NG5000-S2 (IBM Model 3250 M3)
- SWG 7100/NG8100-S1 (IBM Model HS22 7870)
- SWG 7080/NG8080-S1 (IBM Model HS22 7870)

Note: SWG 11.8 requires a minimum of 8GB RAM. Appliances marked with an asterisk * in the above list were shipped originally with less. 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 *SWG 11.8 Setup Guide.*

Note:

SWG Installation Utility VSInstaller version 1.9.1-01 is required.

Legal Notice

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.