Release Notes

Revision B

Stonesoft Security Engine 5.5.4 build 9869.cc.2

Contents

About this release

Stonesoft Security Engine version 5.5.4 build 9869.cc.2 contains no new features compared to the previously released Stonesoft Security Engine version 5.5.4 build 9869.

This specific version (5.5.4 build 9869.cc.2, 64-bit) has been Common Criteria (CC) certified to the EAL4+ level under the Swedish CSEC scheme.

Instructions for users installing Stonesoft Security Engine in a Common Criteria certified configuration can be found from the Stonesoft Security Engine Common Criteria User's Guide available at https://www.stonesoft.com/en/customer_care/documentation/common_criteria/.

This document contains important information about the current release. We strongly recommend that you read the entire document.

Resolved issues

These issues have been resolved since version 5.5.4 build 9869. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Role	Description
Related connections may not work when traffic is allowed by certain Protocol Agents (#100481)	FW IPS L2FW	When traffic is allowed by a rule that uses the Oracle, H323, or Shell (RSH) Protocol Agent, related connections may not work in certain circumstances.
Packet size issues with inspected connections (#101337)	FW IPS L2FW	Traffic that is inspected by the engine in a mode that modifies the traffic may not honor "ICMP fragmentation needed" messages. As a result, the engine may send packets that are too large to the network and cause the connection to hang.
HTTPS access to Browser Based Authentication page does not work in cluster (#101731)	FW IPS L2FW	HTTPS-based access to the Browser Based Authentication page does not work reliably in a cluster setup due to a private key synchronization issue.
OpenSSL library update (#106380)	FW IPS L2FW	The OpenSSL library has been updated to version 1.0.1g to address the issue listed in CVE-2014-0160. The engine uses vulnerable OpenSSL routines only for its TLS management communications and cluster communications between the cluster nodes. If you use the default template from dynamic update package 575 or newer, engine exposure is limited, as connections to vulnerable TLS endpoints are allowed only from the Management Server IP address.

Known limitations

Before upgrading to this version, note the following limitations related to version 5.5 configuration.

Limitation	Description
High-Security Inspection Policy and Strict TCP mode are not supported in asymmetrically routed networks in IPS and Layer 2 Firewall roles	The High-Security Inspection Policy and Strict TCP mode are not supported in asymmetrically routed networks or in environments where a Security Engine in the IPS or Layer 2 Firewall role is directly connected to a load-balancing or high-availability network device. It is recommended to base policies on the Medium-Security Inspection Policy in such cases. In Strict TCP mode and in the High-Security Inspection Policy, the Security Engine controls the progress of a TCP connection and checks that the TCP handshake proceeds according to the TCP protocol. The same Security Engine node must be able to see all the packets in the connection. In Strict TCP mode, the Security Engine also enforces the packet direction (for example, SYN and SYN-ACK packets are not allowed from the same interface). The TLS inspection and Web Filtering features use Strict TCP mode and are not supported in asymmetrically routed networks in IPS and Layer 2 Firewall roles.
SSL/TLS Inspection and Web filtering are not supported in capture (IDS) mode	The TLS Inspection and Web Filtering features are not supported in capture (IDS) mode.
Inline Interface Disconnect Mode on IPS role	The Inline Interface “Disconnect Mode” is not supported on IPS Virtual Appliances, IPS software installations, or appliance models other than IPS-6xxx or modular (13xx, 32xx, 52xx) appliance models on bypass NIC modules.
Virtual Engine in Layer 2 Security Engine roles is not supported	Layer 2 Firewall or IPS Security Engine roles are not supported by this version.
SYN flood protection	Situation-based SYN flood protection is not supported. Use the "SYN Rate Limits" feature instead.

System requirements

Stonesoft appliances

Appliance model	Supported roles
MIL-320	Firewall/VPN
IPS-1205	IPS and Layer 2 Firewall
1035	Firewall/VPN, IPS, and Layer 2 Firewall
1065	Firewall/VPN, IPS, and Layer 2 Firewall
1301	Firewall/VPN, IPS, and Layer 2 Firewall
1302	Firewall/VPN, IPS, and Layer 2 Firewall
1402	Firewall/VPN, IPS, and Layer 2 Firewall
3201	Firewall/VPN, IPS, and Layer 2 Firewall
3202	Firewall/VPN, IPS, and Layer 2 Firewall
3205	Firewall/VPN, IPS, and Layer 2 Firewall
3206	Firewall/VPN, IPS, and Layer 2 Firewall
5201	Firewall/VPN, IPS, and Layer 2 Firewall
5205	Firewall/VPN, IPS, and Layer 2 Firewall
5206	Firewall/VPN, IPS, and Layer 2 Firewall

Some features in this release are not available for all appliance models. See http://www.mcafee.com/us/support/support-eol-next-gen-firewall.aspx and https://my.stonesoft.com/support/document.do?product=StoneGate&docid=3927 for up-to-date appliance-specific software compatibility information. Stonesoft appliances support only the software architecture version (32-bit or 64-bit) that they are shipped with.

Certified Intel platforms

Stonesoft has certified specific Intel-based platforms for the Security Engine. Tested platforms can be found from McAfee Support Knowledge Center (https://support.mcafee.com/ServicePortal/faces/knowledgecenter) under the Next Generation Firewall product.

We strongly recommend using certified hardware or a preinstalled Stonesoft appliance as the hardware solution for new Stonesoft Security Engine installations. If it is not possible to use a certified platform, the Stonesoft Security Engine can also run on standard Intel-based hardware that fulfills the Stonesoft hardware requirements.

Basic NGFW hardware requirements

- Intel®Core™2 / Intel® Xeon® based hardware
- IDE hard disk (IDE RAID controllers are not supported) and CD-ROM drive
- Memory:
    - 2 GB RAM minimum for 32-bit (i386) installation
    - 8 GB RAM minimum for 64-bit (x86-64) installation
- VGA-compatible display and keyboard
- One or more certified network interfaces for the Firewall/VPN role
- 2 or more certified network interfaces for IPS with IDS configuration
- 3 or more certified network interfaces for Inline IPS or Layer 2 Firewall

For more information on certified network interfaces, see https://kc.mcafee.com/corporate/index?page=content&id=KB78844.

Requirements for Virtual Appliance Nodes

- VMware ESXi versions 5.1 and 5.5
- 8 GB virtual disk
- 1 GB RAM minimum, 2 GB recommended if inspection is used
- A minimum of one virtual network interface for the Firewall/VPN role, three for IPS or Layer 2 Firewall roles

The following limitations apply when a Stonesoft Security Engine is run as a virtual appliance node in the Firewall/VPN role:

- Only Packet Dispatching CVI mode is supported.
- Only Standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

The following limitations apply when a Stonesoft Security Engine is run as a virtual appliance node in the IPS or Layer 2 Firewall role:

- Clustering is not supported.

Build version

The Stonesoft Security Engine version 5.5.4 build version is 9869.cc.2

Product binary checksums

sg_engine_5.5.4.9869.cc.2_x86-64.iso

SHA1SUM a0c5053a82fe1eb3d77640f050b5aaef887936bb

SHA512SUM

2dba33056e0fdb10eb1360acb4e6101b25680f3fa23abf6caa44e95419ad2bbd88197dbc24ee5fd19c34f7b897dd4dc04678088ea2569aa75dacc4668bc9630e

sg_engine_5.5.4.9869.cc.2_x86-64.zip

SHA1SUM 12198db55c734e18956fcb34e0a0b7863557ca8a

SHA512SUM

6c4c605472fe8206d1c840c56addea2e3399ee2a9ab5299823973ae24d3af4ecbd66ba8b8785598415e8b30515ab5ae1448665b5851166526d75e1efc67012f1

Compatibility

Minimum

Stonesoft Security Engine version 5.5.4 is compatible with the following component versions:

- Stonesoft Management Center 5.5.0 or higher
- Stonesoft Dynamic Update 517 or higher
- Stonesoft IPsec VPN Client 5.1.0 or higher
- Stonesoft Server Pool Monitoring Agent 4.0.0 or higher 1.1.0 or higher
- Stonesoft User Agent

Installation instructions

Note The sgadmin user is reserved for McAfee use on Linux, so it must not exist before the McAfee Security Management Center is installed for the first time.

The main installation steps for the McAfee Security Management Center (SMC) and the NGFW engines are as follows:

1. Install the Management Server, the Log Server(s), and optionally the Web Portal Server(s) and the Authentication Server(s).
2. Import the licenses for all components (you can generate licenses at https://my.stonesoft.com/managelicense.do).
3. Configure the Firewall, IPS, or Layer 2 Firewall elements with the Management Client using the Security Engine Configuration view.
4. Generate initial configurations for the engines by right-clicking each Firewall, IPS, or Layer 2 Firewall element and selecting Save Initial Configuration.
5. Make the initial connection from the engines to the Management Server and enter the one-time password provided during Step 4.
6. Create and upload a policy on the engines using the Management Client.

The detailed installation instructions can be found in the product-specific installation guides. For a more thorough explanation of using the McAfee Security Management Center, refer to the Management Client Online Help or the *McAfee SMC Administrator's Guide*. For background information on how the system works, consult the *McAfee SMC Reference Guide*. All guides are available for download at https://www.stonesoft.com/en/customer_care/documentation/current/.

Upgrade instructions

Stonesoft Security Engine version 5.5.4 requires an updated license if upgrading from version 5.4.x or lower. The license upgrade can be requested at https://my.stonesoft.com/managelicense.do. Install the new license using the Management Client before upgrading the software. The license is updated automatically by the SMC if communication with Stonesoft servers is enabled and the maintenance contract is valid.

To upgrade the engine, use the remote upgrade feature or reboot from the installation CD and follow the instructions. Detailed instructions can be found in the Firewall/VPN Installation Guide and IPS and Layer 2 Firewall Installation Guide.

Note Stonesoft appliances support only the software architecture version that they are pre-installed with. 32-bit versions (i386) can only be upgraded to another 32-bit version and 64-bit versions (x86-64) can only be upgraded to another 64-bit version. Clusters can only have online nodes using the same software architecture version. State synchronization between 32-bit and 64-bit versions is not supported. Changing architecture for third-party server machines using software licenses requires full re-installation using a DVD.

Upgrading to any 5.5.x version is only supported from a lower 5.5.x version or from a 5.4.x version. If you are running a lower version, please first upgrade to the highest 5.4.x version following the instructions in the release notes for that version.

Known issues

The current known issues of Stonesoft Security Engine version 5.5.4 are described in the table below. For a full and updated list of known issues, consult our website at http://www.stonesoft.com/en/customer_care/kb/.

Issue	Role	Description
SunRPC Protocol Agent is not supported in IPS and Layer 2 Firewall roles (#79844)	IPS L2FW	The SunRPC Protocol Agent is not supported in the IPS and Layer 2 Firewall roles.
Security Engine displays log message "State sync kernel event Setting node X failed" (#82888)	IPS L2FW	The Security Engine 5.4 in the IPS and Layer 2 Firewall roles displays the following log message: "State sync kernel event Setting node X failed". This log message requires no administrator action.
Using VLAN Interface as Control Interface does not work (#82993)	IPS L2FW	Using a VLAN Interface as the Control Interface does not work in the IPS or Layer 2 Firewall roles.
TLS Match may generate false log events when SSL/TLS Inspection is not activated (#84071)	FW IPS L2FW	The TLS_Decrypted-Domain Situation is triggered when the detected domain name does not match any domain names that are excluded from decryption. The description of the Situation is the following: "The connection will be decrypted." However, when no Client Protection Certificate Authority or Server Protection Credentials are configured for SSL/TLS Inspection, the connection is never decrypted.
DNS protocol enforcement may drop valid DNS responses (#84145)	FW IPS L2FW	DNS responses with additional response records (RRs) trigger the DNS_Server-UDP-Extra-Data Situation, even though additional response records are valid in queries as specified in "RFC 2671: Extension Mechanisms for DNS (EDNS0)". If DNS protocol enforcement has been activated in a custom DNS Service element, this also triggers the DNS_Protocol_Violation Situation, and the response is terminated. Disable DNS protocol enforcement from the custom DNS Service element (it is disabled by default).
SNMP IP-MIB: ipInReceives counter does not work correctly (#84964)	IPS L2FW	The IP-MIB ipInReceives counter included in the SNMP IP-MIB does not provide the total number of input datagrams received from interfaces.
Matches to Inspection Rules and Exceptions with Record Logging option do not produce PCAP file for traffic (#85663)	FW IPS L2FW	Matches to Inspection Rules and Exceptions with the Record Logging option do not produce a PCAP file for the matching traffic.
Activating port scan detection can decrease engine's performance (#85692)	FW IPS L2FW	Activating port scan detection can cause a high CPU load and decrease the engine's performance. Remove the following Situations from the Inspection Rules to disable port scan detection: - TCP_Stealth_Scan_Started - TCP_SYN_Scan_Started - Aggressive_TCP_Scan_Started
IPv6 ICMP Packet Too Big messages not allowed by default (#87542)	FW	ICMPv6 Packet Too Big messages generated for VPN path MTU discovery originate from cluster CVI addresses instead of NDI addresses. By default, these messages are not allowed from cluster CVI addresses. Add a rule to allow ICMPv6 Packet Too Big messages from the cluster CVI addresses.
User Responses may not work with HTTPS (with decryption) Service (#90789)	FW IPS L2FW	When the HTTPS (with decryption) Service is used in the Service cell of an Access rule with the Discard action, User Responses configured in the Action Options may not work.

Configuration created on additional Management Server may not work (#97865)	FW IPS L2FW	In environments where there is more than one Management Server, the following engine features may not work if the elements used in the configuration are created on an additional Management Server: - QoS Classes (all engine versions) - NetLink configuration (all engine versions) - VPN with ESP DSCP Match/Mark rules in the QoS policy (engine 5.5 and newer) Create elements only on the primary Management Server.

Find product documentation

Stonesoft provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the online Knowledge Base. Information about Stonesoft and the Stonesoft Management Center can still be found at www.stonesoft.com.

To access...	Do this...
User documentation	Go to https://www.stonesoft.com/en/customer_care/documentation/
Knowledge Base	Go to the Stonesoft Knowledge Base: http://www.stonesoft.com/en/customer_care/kb/. The known issues database and the release notes can be found on the website. Go to the McAfee Knowledge Center: https://support.mcafee.com/ServicePortal/faces/knowledgecenter New material will be published under the Next Generation Firewall product.