Release Notes

Revision A

Stonesoft Security Engine 5.5.8

Contents

About this release

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

New features

Features that have been added since Stonesoft Security Engine 5.4 are described below. For more details, refer to the product-specific documentation.

Virtual Security Engines

Virtual Security Engines are logically separate engines that run as virtual engine instances on a physical engine device. You can now use a physical Security Engine device as a Master Engine to provide resources for Virtual Security Engines. This means that the same Master Engine can simultaneously have different security policies, separate routing tables and overlapping IP addresses for different interfaces (reserved by different Virtual Security Engines).

You can configure up to 250 Virtual Firewalls per Master Engine. The Master Engine can be used as a cluster – one Master Engine can support up to 16 cluster nodes. The Virtual Security Engines are load-balanced so that they are automatically spread between master nodes. One Master Engine handles all the traffic of one Virtual Security Engine at any given time.

Virtual Security Engines do not require individual licenses. Instead, the Security Engine license for the Master Engine defines how many Virtual Resources can be created. The number of Virtual Resources limits the number of Virtual Security Engines. In this major version, Virtual Security Engines can be used in the Firewall/VPN role with some limitations to normal Firewall/VPN role features. Virtualization works across several SMC Domains. For example, the Master Engine can be in the Shared Domain and the Virtual Security Engines can be in one or several other Domains.

Enhancements

Enhancements that have been made since the previous Stonesoft Security Engine major version are described below.

Enhancements introduced in Stonesoft Security Engine 5.5

New options in QoS Policies

Multiple enhancements have been made to the current bandwidth management and traffic prioritization features. The new QoS Mode option in the properties of a Physical, VLAN, ADSL, Tunnel, or SSID Interface allows you to define in more detail how QoS is applied to the interface.

You can now read and/or write DSCP markers for traffic without configuring Access rules to apply a QoS class to the traffic. The matching is done based only on the QoS Policy.

QoS Class-based statistics items are now available even when QoS is not used for bandwidth management and traffic prioritization. The QoS class for the packet comes from the QoS Classes that are applied in the Access rules.

New Active Queue Management (AQM) features reduce the volume of dropped or retransmitted packets when there is network congestion. AQM monitors the average queue size and uses a scheduling algorithm to determine the statistical probability for dropping incoming packets.

It is now possible to assign a weight to QoS Classes so that different QoS Classes with the same priority can be assigned to the queue according to their weight when the QoS Class Guarantee is reached and traffic must be queued. This allows more granular control of traffic prioritization, but does not act as a guarantee.

VoIP support

Related connection handling for SCCP and MGCP voice-over IP protocols has been added.

SMB2 Inspection

SMB2 protocol normalization and inspection has been enhanced.

SSL/TLS AES inspection

SSL/TLS throughput performance has been improved on AES CPU accelerated appliance models.

Logging of X-Forwarded-For (XFF) proxy IP addresses

Security Engines now log HTTP/XFF proxy IP addresses when a client contacts the server address through proxies.

Policy installation process for large number of Virtual Security Engines improved

The policy installation process for a large number of Virtual Security Engines has been improved.

Traffic inspection throughput in certain network conditions with latency/packet loss improved

Traffic inspection throughput in certain network conditions with latency/packet loss has been improved.

Improved Security Strength of Management Connections

It is now possible to use 256-bit encryption for the connection between Security Engines and the Management Server. This requires both the engines and the Management Server to be version 5.5 or higher. You must also use an Internal ECDSA Certificate Authority to sign certificates for system communications.

Loopback Interfaces

It is now possible to configure any IP address that is not already used as a Cluster Virtual IP Addresses (CVI) or Node Dedicated IP Addresses (NDI) on another interface as a loopback IP address. You can add several loopback IP addresses to each Firewall. Loopback IP addresses can be used, for example, as End-Point IP addresses in policy-based VPNs and in the Route-Based VPN.

Improved packet flow

IPS and Layer 2 Firewall Security Engine roles now use the same packet flow as in the Firewall role. The new packet flow improves inspection throughput in all Security Engine roles. In addition, the Security Engine’s inspection throughput can be better optimized using Access rules.

Enhancements that have been made since the previous Stonesoft Security Engine maintenance version are described below.

Enhancements introduced in Stonesoft Security Engine 5.5.7

TLS Heartbeat Extension detection

TLS Heartbeat Extension detection has been added due to vulnerability CVE-2014-0160.

Hardware monitoring for power supply

Power supply monitoring has been improved to send a log message when the monitoring detects the power supply functioning again after a failure.

TCP SYN detection with no options set

It is now possible to detect TCP SYN packets with no options set. The Situation “TCP_Segment-SYN-No-Options” is generated when a packet is matched during inspection.

Resolved issues

These issues have been resolved in Stonesoft Security Engine 5.5.8. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Role	Description
HTTP URL Filtering Situations cannot be used for correlation (#69500)	FW L2FW IPS	HTTP URL Filtering situations cannot be used for correlation.
User authentication is accepted even with trailing whitespace (#87050)	FW	User authentication is accepted even when there is trailing whitespace in the user name. However, traffic does not match rules that contain the user name without trailing white-space.
Engine may fail to read user information (#93742)	FW L2FW IPS	The engine may occasionally fail to read the user information that is received from the User Agent. This may result in incorrect Access rule matching or no information being shown in the User field in the Logs view.
Existing Sun RPC connections may be discarded during policy installation (#95061)	FW L2FW IPS	In environments where Sun RPC is used, already established connections that use this protocol may be discarded by the engine during policy installation.
HTTP file transfers over 4 GB may not work if inspected (#96802)	FW L2FW IPS	HTTP file transfers with files over 4 GB in size may not work if the connection is inspected and the High-Security Inspection Policy is used.
Virtual Security Engines may incorrectly drop packets as spoofed packets (#100829)	FW L2FW IPS	Virtual Security Engines may incorrectly drop packets as spoofed packets after the interface configuration has been changed. The Information Message column in the logs shows a message similar to "spoofed packet. NIC index asymmetry. The packet did not come through correct NIC." Workaround: Reboot the Master Engines after making interface configuration changes.
Authentication timeouts may not be applied to connections when application detection is used (#102452)	FW	When application detection is used, the engine may not apply authentication timeouts for connections that match Access rules where a timeout value is set.
Destination Zones may not be matched correctly in Access rules when application detection is used (#102553)	FW L2FW IPS	Destination Zones may not be matched correctly in Access rules when application detection is used.
Engine may fail to initialize interfaces that have a dynamic IP address (#103040)	FW	Due to certain race conditions, the engine may fail to initialize interfaces that have a dynamic IP address. This may cause the engine to go to the wrong state during reboot.

Security Engine may incorrectly change media settings configured in sg-reconfigure (#103073)	FW L2FW IPS	The Security Engine may incorrectly change the interface media settings configured in sg-reconfigure. Workaround: Run sg-reconfigure again and set forced media settings for each interface even if the settings appear to be forced already.
Browser-based authentication may work slowly in large environments (#104598)	FW	Browser-based authentication may work slowly in large environments with a large number of users authenticating simultaneously.
Engine may reboot when using Protocol Agents (#105199)	FW L2FW IPS	Engine may reboot in rare situations when Protocol Agents are used and there are a large number of related connections to be handled.
Connections transferred to another node during failover may be in wrong connection state (#105327)	FW	When failover occurs on a Firewall Cluster, connections that are transferred from one node to the other may be in the wrong connection state.
Security Engine may lose connectivity with User Agent (#105653)	FW L2FW IPS	The Security Engine may lose connectivity with the User Agent. As a result, Access rules with Users or User Groups defined may stop working.
2nd level forwarding may not work on a standby/offline node if Heartbeat Interface has CVI address (#105659)	FW	2nd level forwarding may not work on a standby/offline node if the Heartbeat Interface has a CVI address configured. Workaround: Do not use a CVI address. Alternatively, select "Encrypt and Sign" as the Sync Security Level setting on the Advanced tab in the Firewall's settings.
"Identity for Authentication Requests" and "Source for Authentication Requests" settings sometimes ignored (#105980)	FW	Even if the "Identity for Authentication Requests" and "Source for Authentication Requests" settings are configured for a Firewall, the settings are ignored in IPsec VPN Client authentication in cases where the VPN EAP pass-through authentication method is used. This affects third-party IPsec VPN Clients that use IKEv2.
Security Engine not stable in systems that use tg3 driver (#106381)	FW L2FW IPS	The Security Engine does not work reliably in third-party hardware platforms that use a tg3 driver
Site-to-site VPN may incorrectly use RSA signature based authentication (#106721)	FW	A site-to-site VPN may incorrectly use RSA signature based authentication even if pre-shared keys are configured when the IPsec VPN client configuration is added to the VPN configuration.
Security Engine may return to initial configuration state when started if 3G modem interfaces are used (#106862)	FW	Due to an issue with modem interface detection during reboot, the Security Engine may return to the initial configuration state when started.
Security Engine may drop first data packet after TCP handshake when MSS rewrite is used (#106950)	FW L2FW IPS	The Security Engine may drop the first data packet after a TCP handshake when MSS rewrite is used. The logs may display messages like the following: "MSS Rewrite: packet dropped (invalid packet)". TCP retransmission takes care of resending the packet, so there is no actual packet loss.
Security Engine may not handle connections correctly when H.323 Protocol Agent is used (#107021)	FW	The Security Engine may not handle connections correctly when the H.323 Protocol Agent is used. Connections may get dropped with the following log message: "Illegal Logical Channel state".
Security Engine may reboot after policy installation if connection limits are set (#107055)	FW L2FW IPS	The Security Engine may reboot after policy installation if connection limits are set. Security Engine Clusters are not affected.

32-bit Security Engine may reboot when using SIP Protocol Agent with large UDP datagrams (#107081)	FW L2FW IPS	A 32-bit Security Engine may reboot when handling large UDP datagrams if the SIP Protocol Agent is used and NAT is applied.
Inspection process may restart when application detection or deep inspection is used (#107134)	FW L2FW IPS	The inspection process may restart in rare situations when application detection or deep inspection is used.
User information might be missing from log entries generated by deep inspection (#107422)	FW L2FW IPS	User information might be missing from log entries that are generated by deep inspection.

Known limitations

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 in 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.

IPS and Layer 2 Firewall roles are not supported for Virtual Security Engines

Layer 2 Firewall and IPS Security Engine roles are not supported for Virtual Security Engines in 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
FW-310	Firewall/VPN
FW-315	Firewall/VPN
MIL-320	Firewall/VPN
FW-1030	Firewall/VPN
FW-1060	Firewall/VPN
FW-1200e	Firewall/VPN
FW-5000	Firewall/VPN
FW-5000L	Firewall/VPN
FW-5100	Firewall/VPN
FW-5105	Firewall/VPN
IPS-1030	IPS and Layer 2 Firewall
IPS-1060	IPS and Layer 2 Firewall
IPS-1205	IPS and Layer 2 Firewall
IPS-6000	IPS and Layer 2 Firewall
IPS-6100	IPS and Layer 2 Firewall
IPS-6105	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 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 Stonesoft Security Engine. The list of certified platforms can be found at www.stonesoft.com/en/products/appliances/.

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 Security Engine 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://my.stonesoft.com/support/document.do?product=StoneGate&docid=7849.

Requirements for Virtual Appliance Nodes

- Intel®Core™2 / Intel® Xeon®-based hardware
- 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 5.5.8 build version is 9891.

Product Binary Checksums

sg_engine_5.5.8.9891_i386.iso
MD5SUM 4986dd42fd4e7eda7e624fe29affa662
SHA1SUM 9109431b35cca372eabdfb870b615c87e39cf5b4

sg_engine_5.5.8.9891_i386.zip
MD5SUM 597a1352483473740328d7564e58e58d
SHA1SUM 9c1003d90944c07a9ba8d8ead7ae330b8118af44

sg_engine_5.5.8.9891_x86-64.iso
MD5SUM 1bcac29ac1213317ae7a12743f0d2aec
SHA1SUM eb29df140fcbd1c13ee7f7bd45e264f6170b84b8

sg_engine_5.5.8.9891_x86-64.zip
MD5SUM ae127fbb6e9c6f3a4beb39396364fb76
SHA1SUM 4804791ed4d79497208488c01a354f879a46b7d5

Compatibility

Minimum

Stonesoft Security Engine version 5.5.8 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
- Stonesoft User Agent 1.1.0 or higher

Installation instructions

The main installation steps for the Stonesoft Security Engines are as follows:

1. Install the Management Server, the Log Server(s), and the Management Client to host(s) to be used as the management system. The Authentication Server and Web Portal Server(s) need to be installed if the optional Authentication Server and Stonesoft Web Portal are used.
2. Configure the Firewall, IPS, or Layer 2 Firewall element using the Management Client.
3. Generate an initial configuration for the engines by right-clicking the element and selecting **Save Initial Configuration**.
4. If not using Stonesoft appliances, install the engines by rebooting the machines from the installation DVD.
5. Make the initial connection from the engines to the Management Server and enter the one-time password provided during step 3.
6. Create and upload a policy on the engines using the Management Client.
7. Command the nodes online by right-clicking the element and selecting **Commands** | **Go Online**.

The detailed installation instructions can be found in the *Stonesoft Management Center Installation Guide*, *Firewall/VPN Installation Guide*, and *IPS and Layer 2 Firewall Installation Guide*. For more information on using the Stonesoft system, refer to the Management Client *Online Help* or the *Stonesoft Administrator's Guide*. For background information on how the system works, consult the *Stonesoft Management Center Reference Guide, Firewall/VPN Reference Guide*, and *IPS and Layer 2 Firewall Reference Guide*.

Upgrade instructions

Stonesoft Security Engine version 5.5.8 requires an updated license if upgrading from version 5.4.x or lower. The license upgrade can be requested at our website 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 CD.

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.

Note It is recommended to set the Cluster Mode to Standby when upgrading from version 5.5.4 or lower to version 5.5.5 or higher on clusters that process GRE or IP-IP traffic. If the upgrade is done when the cluster is in Load-Balancing Mode, tunneled traffic connections may break due to changes in load-balancing functionality.

Note If you have not changed the root password since engine version 4.x, change the root password before upgrading using the sg-reconfigure tool or the Management Client. If the upgrade is done without changing the root password, root login to the engine does not work after upgrading to 5.5.7 or higher until the password has been reset in the Management Client.

It is recommended to change root password in any case, as the salted hash of the root password is stored using a stronger hash (SHA-512) in version 5.5.5 and higher.

Known issues

The current known issues of Stonesoft Security Engine version 5.5.8 are described in the table below.

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.
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. Workaround: 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.
Activating port scan detection can decrease engine's performance (#85692)	IPS L2FW FW	Activating port scan detection can cause a high CPU load and decrease the engine's performance. Workaround: 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. Workaround: Add a rule to allow ICMPv6 Packet Too Big messages from the cluster CVI addresses.
User Responses may	ALL	When the HTTPS (with decryption) Service is used in the Service cell

not work with HTTPS (with decryption) Service (#90789)	of an Access rule with the Discard action, User Responses configured in the Action Options may not work.

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.