Release Notes

Revision A

Stonesoft Security Engine 5.5.10

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 5.5.10

Application detection for TLS traffic improved
Application detection for TLS traffic has been improved.

Resolved issues

These issues have been resolved in Stonesoft Security Engine 5.5.10. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Role	Description
Using connection monitoring for Security Engine may lead to large number of logs (#82962)	FW L2FW IPS	Using connection monitoring for a Security Engine when diagnostics is enabled causes the Security Engine to produce a large amount of log data.
Incomplete information in Connection Monitoring view (#83716)	FW L2FW IPS	No information is shown in the Src Zone, Dst Zone, and User field in the Connection Monitoring view. The Netlink link field incorrectly shows 0.
NetLink selection based on DSCP matching does not work (#84761)	FW	Selecting NetLinks in Multi-Link based on DSCP matching does not work.
Engine can drop connections to itself when VPN and deep inspection are used (#93364)	FW	The engine can drop connections to itself in scenarios where these connections come through a VPN tunnel and deep inspection is in use with the High-Security Inspection Policy. The related situation seen is TCP_Checksum-Mismatch. Workaround: Permit the TCP_Checksum-Mismatch situation for the traffic involved in inspection exception rules, or use the Medium-Security Inspection policy, where this situation is permitted by default.
Policy installation can hang the engine (#105066)	FW	In rare situations, the policy installation can hang the engine, halting all network traffic processing. Workaround: Reboot the engine from the physical console.
Packet fragmentation does not work in Route-Based VPNs (#105647)	FW	Packet fragmentation does not work properly in Route-Based VPNs.
Usage of VPN TCP encapsulation breaks VPNs on Virtual Engines (#105987)	FW	Using VPN TCP encapsulation breaks VPNs on Virtual Engines.
Engine can drop HTTPS connections when deep inspection or application detection is in use (#106157)	FW L2FW IPS	In setups where an HTTPS connection uses the unauthenticated Diffie-Hellman key exchange protocol and TLS decryption is not enabled on the engine, the engine can drop the connection when deep inspection or application detection is in use. The situation seen in the logs is TLS_Unrecoverable-Error.
Browser-Based User Authentication can fail (#107745)	FW	Browser-Based User Authentication can fail in large environments.
"View Interface as One LAN" option does not work (#107890)	L2FW IPS	The "View Interface as One LAN" option in the Logical Interface Properties does not work.
Engine may not detect 3G modem (#107998)	FW	The engine may fail to detect the 3G modem. Workaround: Reboot the engine.
User and VPN information missing from some log entries generated by deep inspection (#108014)	FW L2FW IPS	Some log entries that are generated by deep inspection may not show any User or VPN information.

Next Generation Firewall 3206 appliances can map 8-port interface modules incorrectly (#108016)	FW L2FW IPS	McAfee Next Generation Firewall 3206 appliances can map 8-port interface modules incorrectly. If, for example, the interface module is inserted in slot 2, new network interfaces are numbered eth3_x. This only affects revision 2 of the appliance.
Low-level interface settings can be lost after disconnecting and reconnecting a cable (#108156)	FW L2FW IPS	If a cable is disconnected and reconnected while the appliance is turned on, low-level interface settings can be lost, which can affect throughput. This affects only network interfaces that use igb or ixgbe drivers. Workaround: Reboot the appliance after reconnecting the cable.
sg-inspection process may restart (#108315)	FW L2FW IPS	The sg-inspection process may restart. This causes established connections to hang.
Connection Tracking mode Loose does not work with specific NAT configurations (#108751)	FW	The Connection Tracking mode Loose does not work with specific NAT configurations. As a result, the engine may hang.
Policy install that removes VLAN may cause traffic interruption (#108849)	FW L2FW IPS	Policy install that removes VLAN may cause traffic interruption up to five seconds.
User-based Access Rules may not work (#108916)	FW L2FW IPS	User-based Access Rules may not work on the engine in certain situations. A high load on the engine may also be reported in these situations.
Fragmented traffic may cause engine to reboot (#109169)	FW L2FW IPS	When the engine sees the same incoming fragmented traffic on several interfaces, the engine may reboot.
Incorrect source port logged (#109339)	FW L2FW IPS	In certain situations, the incorrect source port may be logged.
IGMP Proxy might not work (#109420)	FW	In some very specific configurations, the IGMP Proxy might not work in IGMPv2 mode.
Monitoring SYN Rate Limit feature does not work (#109599)	FW L2FW IPS	Monitoring the SYN Rate Limit feature does not work. SMC counter items such as "SYN rate dropped traffic by interface" do not provide data.
Engine may run out of memory when overloaded (#109632)	IPS	When overloaded and bypassing some traffic, the engine may run out of memory if in an inline serial cluster.
Engine might not handle TFTP connections correctly (#109642)	FW L2FW IPS	If a TFTP server communicates back to the client from source port 69, the engine might not handle TFTP-related connections correctly.
Engine may stop processing traffic after reboot with certain run-at-boot script (#109700)	FW	If the workaround in https://my.stonesoft.com/support/document.do?product=StoneGate&docid=1088463 has been set into run-at-boot script, the engine may stop processing traffic after reboot. Workaround: Remove the run-at-boot script after upgrading to version 5.4.3.
PXE protocol might not work through VPN (#109863)	FW	The PXE protocol might not work through site-to-site VPN in some situations.
Engine may reboot when Connection Tracking Mode is set to Loose (#109924)	FW L2FW IPS	In very rare situations, the engine may reboot when the Connection Tracking Mode is set to Loose and the connection receives packets with specific timing.
Handling of RTP UDP connections might cause engine to reboot (#110084)	FW L2FW IPS	In rare situations, the handling of RTP UDP connections may cause the engine to reboot.

Engine might hang when Concurrent Connection Limit is reached (#110137)	L2FW IPS	The engine might hang when the Concurrent Connection Limit is reached in a configuration that uses GRE or IPIP tunnels.
Server Pool load balancing might hang with Virtual Security Engines (#110196)	FW	When Server Pool load balancing is used with Virtual Security Engines, the engine might hang when synchronizing state information in the cluster.
Using Refuse action in Access rules might cause engine to hang or reboot (#110230)	FW L2FW IPS	Using the Refuse action in Access rules might cause the engine to hang or reboot.
QoS class set with Continue rule does not work if Application matches are used in Access rules (#110438)	FW L2FW IPS	A QoS class set with a Continue rule does not work correctly if Application matches are used in Access rules.
SSL/TLS inspection may not work with VLAN interfaces (#110645)	FW L2FW IPS	In configurations where SSL/TLS inspection is applied to the traffic that passes through VLAN interfaces, some connections might hang.

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 5.5.10 build version is 9901.

Product Binary Checksums

sg_engine_5.5.10.9901_i386.iso
MD5SUM   6f95057c3d0045683c3fe55257176767
SHA1SUM   25ec15907df42b075af9d5f73e6e383b58c11d39

sg_engine_5.5.10. 9901_i386.zip
MD5SUM   ad6f203c367d62df3a4bd5ecc24f63e6
SHA1SUM   88e4c31158a81c026ccfa238d42700ed54d74584

sg_engine_5.5.10. 9901_x86-64.iso
MD5SUM   6d53af9c273fef873c8babac7bf81284
SHA1SUM   b854ae1dd98e20a371f5d620b809bb333d830715

sg_engine_5.5.10. 9901_x86-64.zip
MD5SUM   458dccf0ca587ac6f4c35e83e542d12a
SHA1SUM   f0dd009532713dd6a592d8bfa7a11cb9b1979b84

Compatibility

Minimum

Stonesoft Security Engine version 5.5.10 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 5.5.10 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 5.5.10 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.
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 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.

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.

00-A