Release Notes

Revision B

Stonesoft Security Engine 5.5.16

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.

Resolved issues

These issues have been resolved in Stonesoft Security Engine 5.5.16. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Role	Description
Interface settings for Master Engines might not be applied on Virtual Security Engines (#98731)	FW	When a cluster MAC address is modified in the properties of a Master Engine interface, the changes might not be applied to the VLAN Interfaces defined for the Virtual Security Engines that are hosted by the Master Engine.
Inspection logs might not show destination interface ID correctly (#109563)	FW L2FW IPS	Inspection logs might not show the destination interface ID correctly for connections that have been opened to the engine.
Domain Name elements might not work correctly in Inspection Exception rules (#110940)	FW L2FW IPS	When a Domain Name element is used in the Source field of an Inspection Exception rule and logging is not enabled in the rule, the engine might interpret the Domain Name element as ANY.
First policy installation after initial configuration might fail (#111797)	FW	The first policy installation after an engine's initial configuration might fail. This problem is likely to occur when an ADSL Interface is used as the management interface. Workaround: Disable the Policy Handshake option in the engine properties, then install the first policy. After the installation, reboot the engine.
Engine might not log connections correctly when application detection is used (#112005)	FW L2FW IPS	When Application elements are used in Access rules and the Action is set to Discard or Refuse, the engine drops the connection correctly but does not remove it from the connection state table. As a result, traffic counters for the connection might not be shown correctly, and the engine might generate a log entry with a Connection Closed message even if the connection was dropped.
Installing policy on engine with Wireless Interface might cause unexpected reboot (#112905)	FW	The engine might unexpectedly reboot when you install a policy on an engine that has a Wireless Interface defined but no SSIDs configured, or when install a policy with a wireless configuration on an engine that uses the initial policy.
Virtual Security Engines might incorrectly close connections (#113194)	L2FW	Virtual Security Engines might incorrectly remove connections from the connection state table, which causes the connections to fail. Workaround: Reboot the Master Engine node. In the case of a cluster, reboot both nodes simultaneously.
Dynamic routes might not show in Routing Monitoring view (#113305)	FW	The Firewall engine might not send information about dynamic routes correctly, so dynamic routes might not be visible in the Route Monitoring view of the Management Client.
Engine might leak memory when MSRPC Protocol Agent is used (#113571)	FW L2FW IPS	The engine might leak memory when MSRPC Protocol Agent is used.
Engine might not clear old SIP dialogs when SIP Protocol Agent is used (#114252)	FW	When the SIP Protocol Agent is used, the engine might not clear old SIP dialogs if the established SIP call is not terminated with a BYE message.
Policy refresh operation might stop working when VPN configuration is changed (#114275)	FW	The policy refresh operation might stop working if the policy contains changes to the VPN configuration. As a result, VPN processing also stops working.

Cluster MAC Address for Master Engine cannot be set for an Aggregated Link interface that has VLAN Interfaces for Virtual Security Engines under it (#114414)	FW	The Cluster MAC Address cannot be set for an Aggregated Link Interface on a Master Engine if the interface has VLAN Interfaces that are associated with Virtual Resources under it.
Load balancing and NAT might not be applied to IPv6 ICMP packets correctly (#114455)	FW	On Firewall Clusters, load balancing and NAT might not be applied to IPv6 ICMP packets correctly.
Monitoring might show an engine load value that is too high (#114618)	FW L2FW IPS	In some environments, monitoring might show an engine load value that is higher than the actual load due to the calculation method used.
Engine might log SIP_Message-No-Transaction Situations unnecessarily (#114771)	FW L2FW IPS	The engine might produce unnecessary log entries for SIP_Message-No-Transaction Situations. Call handling on the engine is not affected.
Manually created blacklists might not work (#114839)	FW L2FW IPS	Blacklists created manually in the Management Client might not match if the source or destination contains networks.
NAT issues with SIP Protocol Agent (#114881)	FW	The SIP Protocol Agent might apply NAT incorrectly to some SIP messages.
Locking issues when same traffic seen by multiple Capture Interfaces (#114902)	L2FW IPS	The engine might have locking issues when the same traffic is seen by multiple Capture Interfaces within the same Logical Interface. The symptoms include messages like "BUG: soft lockup" on the engine console.
First policy upload after configuring Virtual Security Engines might fail (#115334)	FW L2FW IPS	The first policy upload after configuring Virtual Security Engines might fail. The policy is uploaded on the Master Engine, but the upload fails on the first Virtual Security Engine. The following error message is shown: "FATAL: could not acquire lock by file: (errno=11). Another sgcfg running?".
Route-Based VPN endpoints might not be updated (#115364)	FW	If you change the endpoints of a Route-Based VPN, the endpoints might not be updated on the engine when you refresh the engine's policy. Workaround: Reboot the engine to update the IP addresses of the Route-Based VPN endpoints.
Engine might not terminate VPN negotiations with IPsec VPN Clients correctly in error situations (#115412)	FW	In environments where the IPsec VPN Clients have been configured to use IKEv2, the engine might not terminate the VPN negotiations correctly if the connection to the the DHCP server times out. As a result, the previous negotiation is not cleared on the engine and the following connection attempts from the same IPsec VPN Client fail. Workaround: Use IKEv1 with IPsec VPN Clients.
Log flooding if modem is disconnected (#115549)	FW	The engine can flood the logs with the message "Failed to open /dev/gsm0: No such file or directory" if a modem is disconnected from the engine while it is in use.
Policy installation can fail if WLAN interface has more than one SSID configured (#115619)	FW	Policy installation can fail on the engine if the WLAN interface has more than one SSID configured.
Route-based VPN tunnels are re-negotiated after each policy install (#115792)	FW	Route-based VPN tunnels are re-negotiated after each policy install, even if no changes are applied to them. This can result in latency in the traffic using the VPN tunnel.

Inspection process might restart when handling SIP traffic	FW	The inspection process might restart when handling SIP traffic on Firewall Clusters if the nodes are running different versions. Nodes can be running different versions, for example, during an upgrade of the cluster.
Engine can incorrectly log blacklisting failures (#115968)	FW L2FW IPS	Due to internal timing issues, the engine might report blacklisting failures even if the blacklisting entries have been created successfully. The following log entry can be seen: "Could not create a blacklisting entry to terminate the connection".
Remote engine upgrade might fail occasionally (#116237)	FW L2FW IPS	Remote engine upgrade might fail occasionally with the following error messages: "Read failed" or "Invalid checksum of uploaded software image".
Engine might not apply NAT correctly to related connections for FTP (#116313)	FW	The engine might not apply NAT correctly to related connections for FTP if the connections also use Server Pool load balancing.
Engine might not handle GRE traffic correctly (#116495)	L2FW IPS	The engine might drop GRE traffic when GRE keepalives are used.
Rules with logical interfaces might not be matched correctly (#116496)	L2FW IPS	Rules with logical interfaces might not be matched correctly when the "Inspect Unspecified VLANs" setting is selected in the properties of the physical interface.

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
320X (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 http://www.mcafee.com/us/support/support-eol-next-gen-firewall.aspx and https://kc.mcafee.com/corporate/index?page=content&id=KB78906 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. Search for the list of certified platforms at the McAfee Knowledge Center: https://support.mcafee.com/ServicePortal/faces/knowledgecenter.

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://kc.mcafee.com/corporate/index?page=content&id=KB78844.

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 5.5.16 build version is 9927.

Product Binary Checksums

sg_engine_5.5.16.9927_i386.iso
MD5SUM 652815a8d435e075ffe21e6b99f17f66
SHA1SUM 55dc4ddbb5bb95e13340af3460da0fe404e71ee6

sg_engine_5.5.16.9927_i386.zip
MD5SUM 1821bf78b4eacbddd820e483621b58f1
SHA1SUM 1b5276b9790702d1c159c900e6299303c4da9c98

sg_engine_5.5.16.9927_x86-64.iso
MD5SUM 78c2433e8edddc0971b9fa7398820d47
SHA1SUM d4b549c8594dc7078b2845252c71b5d45329468b

sg_engine_5.5.16.9927_x86-64.zip
MD5SUM 1af93abd21f5dbafd9f2c1fc3f158c4a
SHA1SUM 75dbf3ff62eba132882e661e7ad7466e4a3877a3

Compatibility

Minimum

Stonesoft Security Engine version 5.5.16 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 5.5.16 requires an updated license if upgrading from version 5.4.x or lower. The license upgrade can be requested at our website at https://ngfwlicenses.mcafee.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 5.5.16 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
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

McAfee 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 Center.

1. Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.
2. Enter a product name, select a version, then click **Search** to display a list of documents.