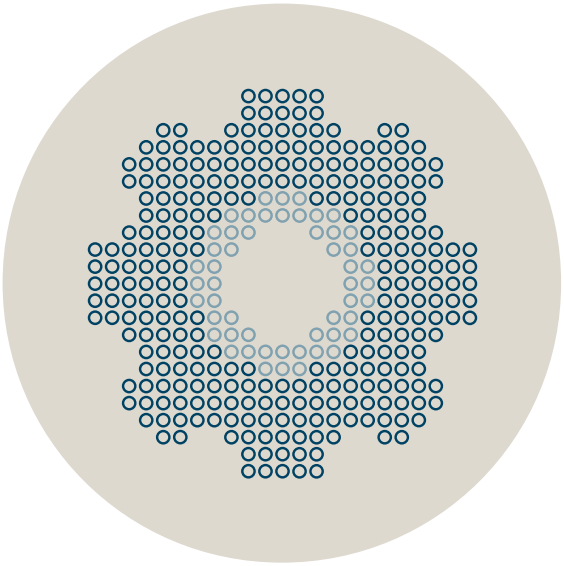

Stonesoft Security Engine

Release Notes for Version 5.5.7

Created: April 9, 2014

STONESOFT
A McAfee Group Company

Table of Contents

What's New

Stonesoft Security Engine 5.5 is the second major release for the new combined Stonesoft Security Engine. Version 5.5.7 is a maintenance version for the Security Engine.

This major release enhances the Stonesoft Security Engine by adding support for Virtual Security Engines, enhanced Quality of Service (QoS) controls, additional voice-over IP protocol support, and other enhancements.

New Features

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

Feature	Description
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 in the table below.

Enhancement	Description
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 amount of Virtual Security Engines improved	The policy installation process for large numbers 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 in the table below.

Enhancement	Description
TLS 1.2 support in TLS inspection	TLS protocol version 1.2 is now supported in TLS inspection for client protection and server protection.

Fixes

Problems described in the table below have been fixed in Stonesoft Security Engine 5.5.7. A workaround solution is presented for earlier versions where available.

In the table below, the following abbreviations are used for the engine roles:

- FW: Firewall/VPN
- IPS: Intrusion Prevention System
- L2FW: Layer 2 Firewall

Synopsis	Role	Description	Workaround for Previous Versions
SIP Protocol Agent may leak memory with some traffic patterns (#75652)	FW L2FW IPS	The SIP Protocol Agent may leak memory with some traffic patterns, which leads to the sg-inspection process restarting.	N/A
IP protocol validity checks and TCP Situations not logged (#85657)	L2FW IPS	The following IP protocol validity checks and TCP Situations are not logged: Please refer to the known issue in the knowledge base for a complete list.	N/A
Blacklist entry with Duration of zero does not terminate connections (#87460)	IPS	A Blacklist entry with a Duration of 0 (zero) seconds does not terminate the current connection from the specified IP addresses and ports when the engine does not use a High-Security Inspection Policy.	Use a High-Security Inspection Policy.
FW-315 appliance interface mapping incorrect (#94292)	FW	After a factory reset, the mapping of ADSL and WLAN Interfaces in the FW-315 appliance is incorrect.	Use the sg-reconfigure wizard to map the interfaces as explained in the Appliance Installation Guide.
Engine may drop NAT-T packets sent by itself (#95390)	FW	When the local VPN endpoint address is excluded from antispoofing (for example, when the same address is used as a NAT address and proxy ARP is enabled), the engine may drop NAT-T packets sent by itself.	N/A
Configuration created on additional Management Server may not work (#97865)	FW L2FW IPS	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 higher)	Create elements only on the primary Management Server.
HTTP application caching issues (#97912)	FW L2FW IPS	In some cases, Application detection has been activated even though the configuration does not require Application detection. For some connections, the engine has also reported the wrong application.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Incorrect IP addresses in related connection log entries (#98580)	FW	Log entries that are generated for related connections when deep inspection is enabled may have incorrect IP addresses and ports if NAT is applied to the connection.	N/A
NAT destination address not displayed as translated in logs (#98582)	FW	The translated NAT destination address may not be displayed as translated in the logs. Instead, the untranslated destination IP address is shown in the "NAT Dst" log field.	N/A
H.323 protocol parsing may not work correctly in some situations (#98625)	FW	H.323 protocol parsing may not work correctly in some situations, which may lead to the engine rebooting.	N/A
Engine may reboot when blacklisting is enabled (#99524)	FW L2FW IPS	In certain scenarios, the engine may reboot when blacklisting is enabled. In the Firewall/VPN role, this issue only affects Single Firewalls. In other roles, this issue affects both single engines and clusters.	N/A
Oracle Protocol Agent may work incorrectly (#100312)	FW	The Oracle Protocol Agent may work incorrectly and may cause the engine to reboot when used.	N/A
WLAN logs do not report failed authorizations (#101103)	FW	Logs from the WLAN access point do not report failed authorizations.	N/A
Incorrect engine status shown in SMC due to hardware monitoring (#101302)	IPS	The SMC may display an incorrect status for the engine due to hardware monitoring.	N/A
IPv6 deep inspection may not work correctly (#101384)	FW L2FW IPS	Deep inspection of IPv6 traffic may not always work correctly. This may cause the sg-inspection process restart.	N/A
Policy installation may fail when User Agent is used (#101440)	FW	Policy installation may fail when the User Agent is used.	N/A
Multi-Link VPN may not update link statuses in cluster (#101514)	FW	Under certain circumstances, cluster nodes may disagree on the link statuses of Multi-Link VPN members.	N/A
POP3 e-mail traffic only partially inspected by anti-virus (#101944)	FW	POP3 e-mail traffic is only partially inspected by anti-virus.	N/A
SSID Interface Security Mode setting does not persist (#102221)	FW	Setting the Security Mode of an SSID Interface to Disabled does not persist. After uploading the policy or rebooting, a specific Security Mode may be enabled for the SSID Interface.	N/A
Engine may fail to detect a broken link with Multi-Link VPN if dynamic end-points configured (#102516)	FW	When Multi-Link VPN is in use and the engine has dynamic end-points configured, the engine may fail to detect broken links after rebooting.	N/A
sg-inspection process may restart with large policy (#102725)	FW L2FW IPS	The sg-inspection process may restart when the policy includes a large number of Access rules and Deep Inspection is enabled.	Reduce the number of Access rules in the policy.
Network configuration is slow at policy installation (#102731)	FW	When changing the network configuration during a policy installation, traffic is stopped for an unnecessarily long time, particularly with large routing tables.	N/A
Engine may report duplicate VPN end-points with SNMP monitoring (#102894)	FW	The engine may report a VPN end-point more than once, for example, when making SNMP queries for the Firewall.	N/A
Engine may reboot when anti-virus is enabled (#102932)	FW	In certain scenarios, the engine may reboot when anti-virus is enabled.	N/A
Connections to the engine may break when engine is set to offline (#103208)	FW	Connections to the engine may be broken when the engine is set to offline and source NAT is applied to the connections.	Make sure that the connections to the engine do not match any NAT rules.

Synopsis	Role	Description	Workaround for Previous Versions
Node ID conflict with two clusters sharing same heartbeat network (#103213)	FW L2FW IPS	If two or more clusters share the same heartbeat network, node ID conflicts may occur, even if different multicast addresses are configured. This results in extra logging and performance issues.	N/A
Installing large policies takes a long time (#103260)	FW L2FW IPS	Installing a large policy may take a long time.	N/A
Engine may become unresponsive when VPN is configured (#103387)	FW	In very rare situations when a VPN is configured, the engine may become unresponsive. Messages similar to the following may be shown in the console: "BUG: soft lockup - CPU#0 stuck for 22s! [sg_vpn/0/0:5003]"	N/A
Using an alias in engine DNS configuration may lead to policy installation failure (#103443)	FW	Using the alias "$$ DHCP Interface 1.dns" in the engine DNS configuration may cause a policy installation to fail. You may receive an error message similar to "FATAL: syntax error in policy configuration: DHCP parameter lookup failure near line 29".	N/A
Reset response in IDS configuration does not work correctly (#103483)	IPS	A Reset response sent by an engine in the IPS role and in an IDS configuration does not work correctly. The packet is sent with the wrong sequence number.	N/A
Engine may not log dropping of SYN-ACKs if connections use smaller MSS than defined on engine (#103623)	FW L2FW IPS	In situations where connections have smaller MSS values than configured on the engine, the engine may not create any log entries when dropping the SYN-ACK packets for these connections.	N/A
Engine may not restore primary control connection to Management Server if dynamic control IP addresses in use (#103721)	FW	In situations where the engine has two control interfaces with dynamic IP addresses and the secondary interface is used as the control connection to the Management Server, the primary control connection may not be restored, even after connectivity through the primary interface is working.	N/A
HTTP and TCP monitoring of Server Pool members may not work (#103757)	FW	HTTP and TCP monitoring of Server Pool members may not work if the expected response is 1-3 characters long.	N/A
Policy installation may fail when using PPPoE (#103907)	FW	The engine may not request DNS information from the peer when using PPPoE. If the policy to be applied requires DNS information (for example, domain names are used in the policy), the policy installation will fail.	Do not use elements that need DNS information in the policy.
"No Policy Installed" shown in System Status view, even if policy is installed (#104147)	FW	The System Status view may display "No Policy Installed" for a Firewall, even if a policy has been installed. This may occur when the Firewall has a dynamic control IP address configured. The problem arises when the monitoring process does not send the configuration name or dynamic update name to the Management Server after a successful policy upload to the Firewall. You cannot refresh the policy because the SMC is not aware of the policy installed on the Firewall. You must install the policy instead.	Run the "sg-status" command on the engine command line to verify the latest policy installation time and dynamic update package number, and install the policy again.
Inline Interface pairs on IPS do not work after network configuration changes (#104255)	L2FW IPS	When a policy is installed on an IPS engine that uses Inline Interface pairs, the interfaces may not work if the network configuration changes.	N/A
TLS inspection may cause sg-inspection process to restart (#104469)	FW L2FW IPS	In some cases, enabling TLS inspection may cause the sg-inspection process to restart.	N/A
Packets may become corrupted if 10 Gbps interfaces used with 32-bit engines (#104574)	FW	Packets may become corrupted if 10 Gbps interfaces are used with 32-bit engines.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Rule counter results may not be shown (#104802)	FW L2FW IPS	Rule counter results may not be shown in the Management Client if the policy contains more than approximately 6000 rules. You may receive the error message "No rule counters found".	N/A
Number of blacklist entries is limited to 65535 (#104982)	FW L2FW IPS	The number of blacklist entries is limited to 65535.	N/A
Ipsecpmd process may restart (#105171)	FW	The Ipsecpmd process may restart.	N/A
Engine may suddenly reboot after running sg-reconfigure command (#105326)	FW L2FW IPS	The engine may suddenly reboot after you run the sg-reconfigure command locally from the console.	Reboot the engine after running the sg-reconfigure command locally from the console.
User information not always added to DHCP request (#105467)	FW	User information is not added to the DHCP request for the IPsec VPN Client user's virtual IP address in cases where the VPN EAP pass-through authentication method is used. This affects third-party IPsec VPN Clients that use IKEv2.	N/A
Large number of interfaces on engine may result in memory corruption messages (#105738)	FW L2FW IPS	A large number of interfaces on an engine may result in several diagnostic messages being sent to the local console. If diagnostic messages similar to the following appear, do not add more interfaces or VLANs. Otherwise engine may become unstable. Messages indicating this issue: "__h2a_memcheck:Memory corrupted (invalid end magic 0xcdcdfffd size=36)" "__h2a_memcheck:Memory corrupted (invalid begin magic 0xabababab" "upd_loop:1454:h2a_memcheck(trans_info.cur.need_upd=ffff88005786e808)"	N/A
BGP routing may stop working if there are slow BGP peers (#105754)	FW	The BGP routing protocol may stop working on an engine if there are BGP peers that read BGP messages very slowly.	N/A
Related connections that use TCP ECN are not properly handled (#105801)	FW	Related connections that enable TCP Explicit Congestion Notification (ECN) are not properly handled.	N/A
OpenSSL library update (#106380)	FW L2FW IPS	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 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 of 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 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

- VMware ESXi versions 5.0 and 5.1
- 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 5.5.7 build version is 9887.

Product Binary Checksums

sg_engine_5.5.7.9887_i386.iso
MD5SUM a61fd6de04d4b26bcd337b93c4c3f218
SHA1SUM e36be2840e1f1405987f56c5390912b292d2507e

sg_engine_5.5.7.9887_i386.zip
MD5SUM 9baaa1a286ac8c583d75977658df6363
SHA1SUM 3bdcf34f95a0ae55d7d2aedbd5c6895ce133d613

sg_engine_5.5.7.9887_x86-64.iso
MD5SUM 07ae6c223173c97fcd4aef8d477a5567
SHA1SUM a625e95ebc21583b96a0896f93f2b00c09cf6008

sg_engine_5.5.7.9887_x86-64.zip
MD5SUM e54baacb8b0c85a7f5f916a9c94a1f7e
SHA1SUM 459db17da07ed9e32446ad7d718f53e3c226eb56

Compatibility

Stonesoft Security Engine version 5.5.7 is recommended to be used with the following Stonesoft component versions:

Component	Minimum Compatible Version	Recommended Version
Stonesoft Management Center	5.5.0	Latest 5.5 maintenance version
Stonesoft Dynamic Update	517	Latest available
Stonesoft IPsec VPN Client	5.1.0	Latest 5.4 maintenance version
Stonesoft Server Pool Monitoring Agent	4.0.0	Latest 4.0 or 5.0 maintenance version
Stonesoft User Agent	1.1.0	Latest available

Installation Instructions

The main installation steps for Stonesoft Security Engine 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 5.5.7 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 a higher version 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 5.5.7 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/.

In the table below, the following abbreviations are used for the engine roles:

- FW: Firewall/VPN
- IPS: Intrusion Prevention System
- L2FW: Layer 2 Firewall

Synopsis	Role	Description	Workaround
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.	N/A
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.	N/A
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.	N/A
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.	N/A
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.	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)	ALL	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.	N/A

Copyright and Disclaimer

Trademarks and Patents

Stonesoft Corporation

Itälahdenkatu 22A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

STONESOFT
A McAfee Group Company

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131