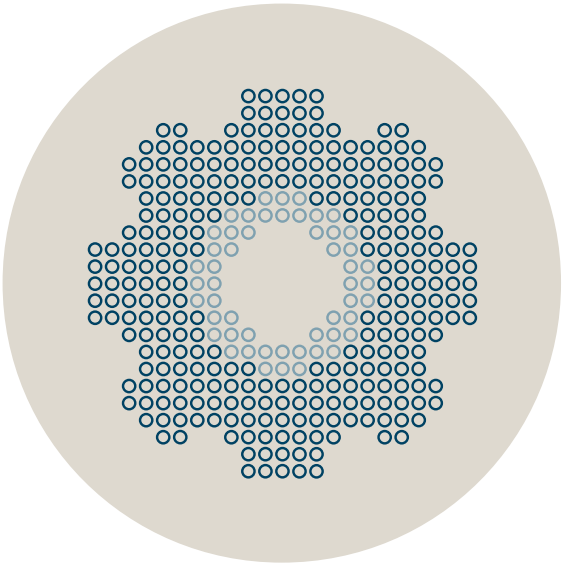

Stonesoft Security Engine

Release Notes for Version 5.5.0

Created: May 7, 2013

STONESOFT

Table of Contents

What's New

Stonesoft Security Engine 5.5.0 is a second major release for the new combined Stonesoft Security Engine.

This major release enhances Stonesoft Security Engine by adding support for virtual engines, enhanced quality of service 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 product documentation.

Feature	Description
Virtual 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. Master Engine can be a cluster too – one master can contain up to 16 cluster nodes. The virtual engines are load balanced so that they are automatically spread between master nodes. One master engine will handle all the traffic of one virtual engine at 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 also 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 previous Stonesoft Security Engine maintenance versions 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 Engine now logs HTTP/XFF proxy IP addresses when a client contacts Server address through proxies.
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 communication.
Loopback Interfaces	A Loopback IP address allows the firewall to communicate with itself. 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 also be used 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 with the Firewall role. 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.

Fixes

Problems described in the table below have been fixed in Stonesoft Security Engine 5.5.0. A workaround solution is presented for earlier versions where available.

Synopsis	Role	Description	Workaround for Previous Versions
Log entries may be stored even when Log Level is Transient or Essential (#76163)	FW	Log entries generated by Inspection rules or Access rules that use Application elements may be stored even when the Log Level is set to Transient or Essential.	N/A
New initial contact may be required after upgrade (#80172)	IPS	New initial contact is required for IPS engines after upgrade to 5.4 or upgrade to 5.4 after first downgrading to 5.2. This occurs when initial contact is made after the upgrade or downgrade.	Make new initial contact with the Management Server in the following situations: - If you made initial contact with the Management Server after upgrade to 5.4. - If you made initial contact with the Management Server after downgrade to 5.2 and then upgrade to 5.4. In other cases, refresh the policy for the IPS engine after upgrading the engine to 5.4.
Blacklisting and logging of blacklisted connections may not work correctly (#81864)	ALL	Log entries from blacklisted connections do not indicate that the connection is blacklisted. If ports are used in the blacklisting entries, invalid entries are created and connections that match the blacklist are not blacklisted.	For logging, use the rule tags in the log entries to match the blacklisted connections to the blacklist rule in the Firewall Policy. Do not use ports in blacklist entries.
Protocol Agent parameters are ignored if application identification and/or application logging is used in Access rules (#82829)	ALL	If you use a Service that contains a Protocol Agent in an Access rule and enable application identification and/or application logging in the rule, only the port information for the Protocol Agent is used in the rule. This prevents the Protocol Agent, for example, from allowing related connections.	N/A
Performance issues with SIP traffic inspection (#83896)	ALL	In some network scenarios, SIP traffic inspection may cause performance issues.	N/A
VPN traffic not handled correctly with Balancing Cluster Mode (#84793)	FW	In some cases, VPN traffic may not be handled correctly when the Firewall Cluster uses Balancing Cluster Mode. VPN traffic stops and the following message is printed to the console on the engine: "h2a_2nd_level_receive: previous 2nd level packet was not received successfully".	Change the Cluster Mode to Standby.
Destination interface Zone matching issues (#85104)	FW	Rules that contain a Zone element in the Destination cell may not match correctly when the destination interface changes after Access rule matching, for example with destination NAT, Outbound Multi-Link, or VPN.	N/A
Destination Zone not logged (#85456)	FW	The destination Zone is not included in the log entry generated when traffic matches a rule with a destination Zone.	N/A
Traffic may be routed incorrectly if destination Zone match is used in the FW policy (#85462)	FW	Packets subject to destination NAT may be routed incorrectly if the Firewall policy uses a Zone element in the Destination cell.	Do not use Zone elements in the Destination cell.

Synopsis	Role	Description	Workaround for Previous Versions
User Responses and Applications cannot be used together (#86106)	ALL	User Responses do not work if Applications are also used in the same policy.	N/A
Fast VPN client connection rate may cause resource leak in ipsecpmd process (#86255)	FW	There may be a resource leak in the ipsecpmd process when a large number of VPN client connections are negotiated in a short time. This causes the ipsecpmd process to restart.	N/A
IPv6 link-local routing issues with VLANs (#87767)	FW	IPv6 link-local packets may not be processed correctly when VLAN Interfaces are used.	N/A
Firewall may not allow returning ICMP error messages through VPN tunnel (#87862)	FW	The Firewall may not allow returning ICMP error messages through the VPN tunnel. The following message appears in the log entries for the connections: "VPN tunnel selection failed".	N/A
Wireless Interfaces in 802.11n Wireless Mode with 40 MHz Width do not work (#88290)	FW	Wireless Interfaces in 802.11n Wireless Mode with 40 MHz Width do not work.	N/A
TCP connection handling grace period does not work properly with High-Security Inspection Policy (#88409)	IPS	The TCP connection handling grace period (300 seconds) does not work properly when the IPS engine comes back online and the High-Security Inspection Policy is installed on the IPS engine. After the IPS engine comes back online, the IPS engine terminates all TCP connections that are not seen from the beginning of the connection.	To allow connections that the IPS engine does not see from the beginning during the grace period, take the following steps: 1. Before upgrading or rebooting the engine or setting the engine offline, make sure that the Failure Mode for the inline interfaces is set to Bypass. 2. Install the Medium-Security Inspection Policy on the engine. 3. After the IPS engine is back online, wait for 300 seconds (grace period). 4. Install the High-Security Inspection Policy on the engine. Note! For proper evasion protection, we recommend using the High-Security Inspection Policy. For deployment-specific instructions, see the Known Limitations section of the Release Notes.
Inspection may not work correctly if Zone elements are used in the Destination cell (#88414)	FW	Inspection may not work correctly if Zone elements are used in the Destination Cell of a rule.	N/A
blacklistd process may generate core files (#88842)	ALL	In some blacklisting configurations, the blacklistd process may generate core files.	N/A
Engine may reboot due to error in monitoring counter initialization (#88942)	ALL	The engine may reboot due to an error in the initialization of counters for monitoring. The situation is rare and is likely to occur only if VPNs is used.	N/A
Policy installation fails with large authentication configuration (#88981)	FW	Policy installation fails when the authentication configuration is large. The following error message is displayed: "Sending configuration to authd failed (error -5)".	Reduce the size of the authentication configuration by deleting any unused LDAP Domains and Authentication Methods.
Firewall may reboot itself when processing related connections under heavy load (#89524)	FW	In rare conditions, connection handling that is under a heavy load may lead to a spontaneous firewall node reboot.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Capture Interface in IPS role does not detect VLAN tags (#89758)	IPS	The Capture Interface for a Security Engine in the IPS role does not detect VLAN tags from incoming frames. If you have defined VLAN Interfaces for a Capture Interface, no traffic is seen unless the Inspect Unspecified VLANs option is enabled. Resets are sent without VLAN tagging because the source VLAN is not detected.	Enable the Inspect Unspecified VLANs option in the Physical Interface Properties dialog.
Wireless clients get disconnected when policy is refreshed (#89953)	FW	If the "Source for Authentication Requests" option is defined in the Firewall properties, wireless client devices get disconnected when the policy is refreshed even if there are no changes to the Wireless Interface configuration.	N/A
Policy installation issues with PPPoE configuration (#90103)	FW	Policy installation may not work reliably when PPPoE is used in the engine's interface configuration.	N/A
VPN tunnel selection may work incorrectly when both VPN Clients and dynamic End-Points are configured for the same VPN (#90117)	FW	The firewall may select VPN tunnel settings incorrectly during the VPN negotiation when both VPN Clients and dynamic End-Points are configured for the same VPN. As a result, the firewall may not send NAT-T notification for the VPN Client or switch from IKEv2 to IKEv1 when it should.	
Incorrect log messages when connections are restricted by concurrent connection limit (#90126)	ALL	When new connections are restricted by a concurrent connection limit, the information message shown in the log entries is incorrect.	N/A
Wireless clients cannot connect to Wireless Interfaces with 40 MHz Width and 5 GHz Band (#90267)	FW	Wireless clients cannot connect to Wireless Interfaces that use 40 MHz as the channel Width and 5 GHz as the Band. No error messages are shown during policy installation.	Use 20 MHz as the channel Width option.
Connection failover does not work correctly for UDP connections when Multi-Link is used (#90363)	FW	Connection failover between cluster nodes does not work correctly for UDP connections when Multi-Link is used.	N/A
Engine does not correctly connect to additional Authentication Server nodes (#90423)	FW	When the Authentication Server has multiple nodes, the Firewall/VPN engine does not correctly connect to the additional Authentication Server nodes.	N/A
Connections may be terminated after 72 hours (#90547)	IPS L2FW	Connections that are active for over 72 hours may be terminated. The following message is shown in the logs: "Connection timeout in state INSPECTION".	N/A
Firewalls with a dynamic control IP address may not be able to use backup control IP addresses (#90607)	FW	Firewalls with a dynamic control IP address may not be able to use the backup control IP address.	N/A
HTTP Protocol Agent with URL Logging may cause engine to reboot (#90691)	FW	In some rare cases, using the HTTP Protocol Agent without Deep Inspection but with URL Logging enabled may cause the engine to reboot.	N/A
SNMP traffic counters may not be updated for interfaces 32-bit engines (#90703)	ALL	SNMP traffic counters may not be updated for interfaces 32-bit engines.	N/A
Synchronization of blacklist entries between Firewall Cluster nodes may fail after upgrade (#90723)	FW	After a Firewall Cluster is upgraded to version 5.4, the synchronization of blacklist entries may fail between the cluster nodes.	N/A
Packets originating from the firewall may not be sent into the VPN tunnel (#90831)	FW	Packets originating from the firewall may not be sent into the VPN tunnel. A "spoofed VPN tunnel" message is shown in the logs.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Backup Control Interface not used in communication with Authentication Server (#90839)	FW	The engine's Backup Control Interface is not used in communication with the Authentication Server.	N/A
NetLink monitoring does not work if more than 20 NetLinks are used on the same firewall (#91071)	FW	NetLink monitoring does not work if the total number of NetLinks used in Outbound Multi-Link elements on the same firewall is more than 20.	N/A
Related connections for MSRPC do not work after upgrade from 5.3 version (#91240)	FW	Related connections for MSRPC are not allowed by the MSRPC Protocol Agent after upgrading from SMC version 5.3.	Refresh the policy after upgrading to SMC version 5.4 or higher.
Weakness in TCP random sequence number generation (#91336)	ALL	The Linux kernel used in Stonesoft engines has a weakness in TCP random sequence number generation. Ref: CVE-2011-3188	N/A
Engine may accept VPN configurations that are too large (#91443)	FW	The Firewall/VPN engine may accept VPN configurations that are too large for it to handle correctly.	N/A
TCP connections opened by engine may hang when Idle Timeout is reached (#91725)	ALL	TCP connections opened by the engine itself, such as connections to a DNS server, may hang when the Idle Timeout configured in a rule is reached.	N/A
Domain Names or user names may not be matched correctly in Access rules (#91813)	ALL	If you use a Domain Name or user name in an Access rule, the rule may not be matched correctly in traffic inspection if application detection is used in Access rules that are matched earlier than this rule in the policy.	N/A
Firewall/VPN node may go to initial configuration state after upgrade with large VPN configurations (#91902)	FW	If you have a very large VPN configuration when you upgrade from version 5.3 to version 5.4, the Firewall/VPN node may return to the initial configuration state after the upgrade.	Reduce the size of the VPN configuration by using fewer elements in VPN site definitions.
IPv6 neighbor discovery messages may not be sent correctly from all cluster nodes (#91941)	FW	IPv6 neighbor discovery messages may not be sent correctly from all cluster nodes. This issue affects only clusters.	N/A
Assert message writing to local serial console may slow engine down (#91966)	FW	The Firewall/VPN engine may write "H2A assertion failed ... sh_tcp_adjust_ack" messages to the local serial console so fast that normal engine operation is disturbed. This happens only in very rare cases of connection failover when the connections use a Protocol Agent that does not apply Deep Inspection.	N/A
Deep inspection of SSH traffic may hang SSH connections (#92173)	ALL	When large files are transferred over SSH connections and deep inspection is applied to the SSH traffic, the SSH connections may hang.	Do not deep inspect SSH traffic.
Deleted VLAN Interfaces may not be removed from the Firewall (#92332)	FW	In some cases, VLAN Interfaces that have been deleted from the Firewall's configuration may not be removed.	N/A
Log compression may not work on the Firewall when concurrent connection limits are used (#92555)	FW	When the concurrent connection limit defined in an Access rule is reached, the Firewall discards the matching connections but the logs are not compressed. Depending on the number of concurrent connections to be discarded, the Firewall may not function correctly.	N/A
Some interface types may not perform as well as expected (#92607)	FW	Some interface types may not perform as well as expected.	N/A
Firewall may run out of memory when SNMP counters are used (#93255)	FW	In some cases, the Firewall may run out of memory when SNMP counters are used.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Using Zone elements in the Destination cell of a rule with Action Options may cause the engine to reboot (#93502)	FW	Using Zone elements in the Destination cell of a rule with Action Options may cause the engine to reboot.	Do not use Action Options in rules that contain a Zone element in the Destination cell.

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 engine node must be able to see all the packets in the connection. In Strict TCP mode the engine also enforces the packet direction (for example, SYN and SYN-ACK packets are not allowed from the same interface). The TLS inspection and Web Filtering features use Strict TCP mode and are not supported in asymmetrically-routed networks in IPS and Layer 2 Firewall roles.
SSL/TLS Inspection and Web filtering are not supported in capture (IDS) mode.	The TLS Inspection and Web Filtering features are not supported in capture (IDS) mode.
Inline interface Disconnect Mode on IPS role.	The inline interface “Disconnect Mode” is not supported on IPS Virtual Appliance, IPS software installations or appliance models other than IPS-6xxx or modular (13xx, 32xx,52xx) appliance models on bypass NIC modules.
Virtual Engine in Layer 2 Security Engine roles is not supported	Layer 2 Firewall or IPS Security Engine roles are not supported by this version.
SYN flood protection	Situation-based SYN flood protection is not supported. Use "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
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.stonesoft.com/en/customer_care/product_life_cycle/ 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 5.5.0 build version is 9838.

Product Binary Checksums

sg_engine_5.5.0.9838_i386.iso
MD5SUM 10e7c025f387d75535da30fb9daea038
SHA1SUM ec78397d28557740a082e5639e9a69d14870e315

sg_engine_5.5.0.9838_i386.zip
MD5SUM ae24bf8d3b11874dda77c0efe87eeaf9
SHA1SUM c0d9425fd85d3096f9e77999d23f545c797bd33c

sg_engine_5.5.0.9838_x86-64.iso
MD5SUM d4d55e4f935a7a9398396ad4c85d1394
SHA1SUM ade774068b1ad4c9de162a3d3f73839bc23f2def

sg_engine_5.5.0.9838_x86-64.zip
MD5SUM 037913957a3ca83506864df544528939
SHA1SUM ab774b91f4250a067e4f440e03293895f892e147

Compatibility

Stonesoft Security Engine version 5.5.0 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* documents. 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 5.5.0 requires an updated license if upgrading from version 5.4.x or earlier. 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 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 an earlier 5.5.x version or from a 5.4.x version. If you are running an earlier version, please first upgrade to the latest 5.4.x version following the instructions in the release notes for that version.

Known Issues

The current known issues of Stonesoft Security Engine version 5.5.0 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
Non-stateful access control for ICMP in Layer 2 Firewall (#81807)	IPS L2FW	In the IPS and Layer 2 Firewall roles, matching for non-TCP or non-UDP traffic is packet-based. For this reason, incoming and outgoing ICMP traffic must be allowed separately in the Layer 2 Firewall Policy.	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
VLAN tagged Control Interface configuration does not work (#82993)	IPS L2FW	Using a VLAN tagged interface as the Control Interface does not work in the IPS or Layer 2 Firewall roles.	N/A
Zone matching fails in Inspection Exceptions (#83165)	IPS L2FW	Matching fails when the Source or Destination of an Inspection Exception rule contains a Zone element. No Actions are applied to the traffic and no logs are produced.	N/A
Zone logging done according to packet instead of connection with inspection (#83175)	FW IPS L2FW	Zone matching follows the packet instead of the connection. For example, inspection of an FTP connection may cause several logs that have alternating Destination and Source Zones, even though the logged Destination and Source addresses are always the same.	N/A
TLS Match may generate false log events when SSL/TLS Inspection is not activated (#84071)	FW IPS L2FW	The TLS_Decrypted-Domain Situation is triggered when the detected domain name does not match any domain names that are excluded from decryption. The description of the Situation is the following: "The connection will be decrypted." However, when no Client Protection Certificate Authority or Server Protection Credentials are configured for SSL/TLS Inspection, the connection is never decrypted.	N/A

Synopsis	Role	Description	Workaround
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).
Monitoring items that do not show data in Security Engine, IPS/L2FW roles (#84316)	IPS L2FW	Monitoring items that currently do not show data in IPS/L2FW roles: - Lost traffic, IPS FW IF (Bits) - Received traffic, IPS FW IF (Bits) - Allowed inspected TCP connections, IPS FW IF (Connections) - Allowed inspected UDP connections, IPS FW IF (Connections) - Allowed uninspected TCP connections, IPS FW IF (Connections) - Allowed uninspected UDP connections, IPS FW IF (Connections) - Discarded TCP connections, IPS FW IF (Connections) - Discarded UDP connections, IPS FW IF (Connections) Obsolete monitoring items for 5.4 and newer versions in IPS/L2FW roles: - Received traffic by source IP address, IPS FW IF (Bits) - Received traffic by destination IP address, IPS FW IF (Bits) - Received traffic by logical interface (Bits) - Received traffic by destination TCP port (Bits) - Received traffic by destination UDP port (Bits)	N/A
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
Destination interface Zone matching issues (#85104)	FW	Rules that contain a Zone element in the Destination cell may not match correctly when the destination interface changes after Access rule matching, for example with destination NAT, Outbound Multi-Link, or VPN.	N/A
Matches to Inspection Rules and Exceptions with Record Logging option do not produce PCAP file for traffic (#85663)	IPS L2FW FW	Matches to Inspection Rules and Exceptions with the Record Logging option do not produce a PCAP file for the matching traffic.	N/A
Inspection of tunneled traffic does not work (#85690)	IPS L2FW FW	Inspection of IP-in-IP traffic, encapsulated IPv6 traffic, and GRE traffic does not work.	N/A

Synopsis	Role	Description	Workaround
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.
TCP connection handling grace period does not work properly with High-Security Inspection Policy (#88409)	IPS	The TCP connection handling grace period (300 seconds) does not work properly when the IPS engine comes back online and the High-Security Inspection Policy is installed on the IPS engine. After the IPS engine comes back online, the IPS engine terminates all TCP connections that are not seen from the beginning of the connection.	To allow connections that the IPS engine does not see from the beginning during the grace period, take the following steps: 1. Before upgrading or rebooting the engine or setting the engine offline, make sure that the Failure Mode for the inline interfaces is set to Bypass. 2. Install the Medium-Security Inspection Policy on the engine. 3. After the IPS engine is back online, wait for 5 minute (grace period). 4. Install the High-Security Inspection Policy on the engine. Note! For proper evasion protection, we recommend using the High-Security Inspection Policy. For deployment-specific instructions, see the Known Limitations section of the Release Notes.
Inspection may not work correctly if Zone elements are used in the Destination cell (#88414)	FW	Inspection may not work correctly if Zone elements are used in the Destination Cell of a rule.	N/A
Capture Interface in IPS role does not detect VLAN tags (#89758)	IPS	The Capture Interface for a Security Engine in the IPS role does not detect VLAN tags from incoming frames. If you have defined VLAN Interfaces for a Capture Interface, no traffic is seen unless the Inspect Unspecified VLANs option is enabled. Resets are sent without VLAN tagging because the source VLAN is not detected.	Enable the Inspect Unspecified VLANs option in the Physical Interface Properties dialog.
Backwards system time change makes IPS switch to bypass mode (#94432)	IPS	If the system time on a Security Engine in the IPS role changes backwards, the engine switches to bypass mode. The engine recovers and goes back online after the same length of time by which the system time changed. For example, if the system time changes backwards by one minute, the engine recovers after one minute.	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 Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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