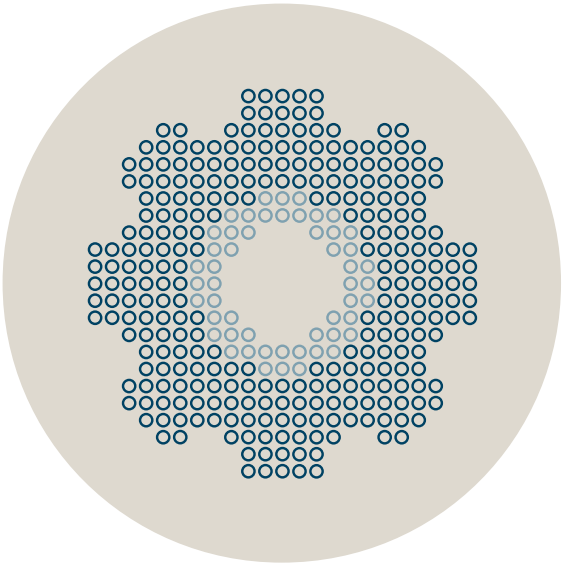

Stonesoft Security Engine

Release Notes for Version 5.5.1

Created: July 25, 2013

STONESOFT

Table of Contents

What's New

Stonesoft Security Engine 5.5 is the second major release for the new combined Stonesoft Security Engine. Version 5.5.1 is a maintenance version for the Security Engine.

This major release enhances the 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 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 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 Engines now log HTTP/XFF proxy IP addresses when a client contacts the 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 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.

Fixes

Problems described in the table below have been fixed in Stonesoft Security Engine 5.5.1. 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
Failover may not work optimally with large number of connections (#61142)	FW	Failover may not work optimally with a large number of connections between two hosts.	N/A
Firewall may add unrelated error messages to dmesg entries (#78677)	FW	In situations in which there is a large number of connections, the Firewall may add unrelated error messages to the dmesg entries.	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
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.
Connections may not match to correct rules when Logical Interfaces are used (#89889)	IPS L2FW	Connections may not match to the correct Access rules when Logical Interfaces have been defined in the rules.	N/A
IPsec VPN log messages may have incorrect or missing peer gateway information (#91189)	FW	IPsec VPN log messages may have incorrect or missing peer gateway information.	N/A
Related connection idle timeouts may not be inherited from the parent connection (#91237)	FW	Related connection idle timeouts may not be inherited from the parent connection with FTP and MSRPC protocols. Instead, fixed one-hour or two-hour idle timeouts are used.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Link Status test checks interfaces in bypass mode (#92767)	IPS	Even though an interface is in bypass mode, the Link Status test checks the status of the interface. As a result, an alert that the test failed is unnecessarily triggered.	N/A
Unnecessary "net_ratelimit: ... callbacks suppressed" messages printed to console (#92844)	FW	Unnecessary messages similar to the following may be printed to the console: "net_ratelimit: 9 callbacks suppressed"	N/A
HTTP traffic may be delayed by category-based web filtering if there is no connection to BrightCloud servers (#93211)	ALL	When category-based web filtering is used, category information for recently accessed URLs is stored in a local cache on the engine. Categories for URLs that are not found in the local cache are resolved from the BrightCloud servers. If there is no connection to the BrightCloud servers, HTTP connections to URLs that are not in the local cache are delayed for 7 seconds.	N/A
IPS stability issues on multi-core platforms with throughput-limited licenses (#93674)	IPS	There may be stability issues when IPS engines on multi-core platforms with throughput-limited licenses are under a heavy traffic load.	N/A
Sg-inspection process may create core dump files repeatedly (#93682)	IPS	In some network environments, the sg-inspection process on Security Engine version 5.4.4 or 5.5.0 may create core dump files repeatedly.	Downgrade to Security Engine version 5.4.3.
Web filtering may not use latest category information (#93882)	ALL	Web filtering may not always use the latest available category information.	N/A
Policy installation fails with proxy ARP and Physical Interfaces in Aggregated mode (#94201)	FW	Policy installation fails if the configuration for a Single Firewall engine includes proxy ARP and Physical Interfaces in Aggregated mode.	N/A
Engine may not be stable if inspection load is too high (#94371)	ALL	The engine may not be stable if the inspection load is too high.	N/A
System time changing backwards 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
Sg-inspection may generate core dump files when Deep Inspection is enabled for HTTP and HTTPS traffic (#94497)	ALL	In rare conditions, the sg-inspection process may generate core dump files when Deep Inspection is enabled for HTTP and HTTPS traffic.	N/A
HTTP_Request-Unknown Situation is logged for non-HTTP traffic (#94589)	ALL	The HTTP_Request-Unknown Situation may match non-HTTP traffic when the Access rules have the following configurations: - Log Application Information is set to Enforced in Logging options OR - Deep Inspection is enabled in a rule in which the Service is ANY OR - Protocol identification is enabled using an Application element in which the default port is ANY	In an Inspection Policy, use an Exception rule that matches the HTTP_Request-Unknown Situation to set the Log Level to None.
IPS monitoring in Management Client shows 0% CPU load (#94664)	IPS	IPS monitoring in the Management Client shows 0% CPU load even though the engine is processing traffic normally.	N/A
Opening and closing Connection Monitoring view can cause engine to crash (#94806)	ALL	Opening and closing the Connection Monitoring view several times can cause the engine to crash.	N/A

Synopsis	Role	Description	Workaround for Previous Versions
Policy installation may fail (#94828)	FW	In certain scenarios, the engine may interrupt the policy installation while the SMC is uploading the policy to the engine.	N/A
Inspection may not work with WLAN Interfaces (#95030)	FW	Inspection may not work if traffic passes through a WLAN interface on a Firewall/VPN engine.	N/A
Path MTU handling and fragmentation may not work for Route-Based VPNs (#95070)	FW	Path MTU handling and fragmentation may not work for Route-Based VPNs.	N/A
Firewall that has a dynamic interface may not use the new IP address (#95195)	FW	When the firewall has a dynamic interface, it may continue to use the old IP address even if the IP address of the dynamic interface has changed.	N/A
Proxy ARP does not work with VLAN Interfaces (#95296)	FW	Proxy ARP does not work with VLAN Interfaces. This issue affects only single node Firewall/VPN configurations.	N/A
Proxy ARP does not work for a VLAN Interface if link aggregation is in use (#95326)	FW	Proxy ARP may not work on a VLAN Interface that has been configured as part of link aggregation.	N/A
Firewall may run out of memory if 3G modem is plugged in to the engine but not in use (#95449)	FW	When a 3G modem is plugged in to the Firewall but is not in use, the Firewall may run out of memory.	Unplug the modem from the Firewall.
Using a single port to blacklist traffic does not work (#95702)	ALL	Using a single port as the matching criteria to blacklist traffic does not work.	N/A
Generating IPsec VPN certificate request for Security Gateway does not work (#95797)	FW	Generating an IPsec VPN certificate request for a Security Gateway does not work if the ID Type is set to "Distinguished Name" in some of the Security Gateway End-Points.	N/A

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 on 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.
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 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
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 5.5.1 build version is 9848.

Product Binary Checksums

sg_engine_5.5.1.9848_i386.iso
MD5SUM 124160f9d5cc72ae10c2b2868d9c729b
SHA1SUM 60b7210fd0363145fb64184d65d2fe5312dc1140

sg_engine_5.5.1.9848_i386.zip
MD5SUM 020144f32d06030a888b1c12ca37cd97
SHA1SUM 96f1b5381c73ff16daf7fd186c6e09b0f35ed3b7

sg_engine_5.5.1.9848_x86-64.iso
MD5SUM 116f197087b3d209ff77f779de552444
SHA1SUM 7803eadf158844d9c578461f8cf5e08e3dd1efaf

sg_engine_5.5.1.9848_x86-64.zip
MD5SUM e6f94cf26645d6288dd1dba58ccee60a
SHA1SUM 423104d2868cb03806b6565032aa291e0fd721f0

Compatibility

Stonesoft Security Engine version 5.5.1 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 5.5.1 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.

Known Issues

The current known issues of Stonesoft Security Engine version 5.5.1 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
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
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
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).

Synopsis	Role	Description	Workaround
Some statistics items do not show any data for IPS or Layer 2 Firewall engines (#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
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
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
HTTP Redirect and HTML Page do not work (#93699)	ALL	The responses "HTTP Redirect" and "HTML Page" do not work.	N/A

Copyright and Disclaimer

These materials, Stonesoft products, and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE INFORMATION CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-Link technology, Multi-Link VPN, and the Stonesoft clustering technology-as well as other technologies included in Stonesoft-are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.

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