Release Notes

Revision A

Stonesoft Security Engine 5.5.12

Contents

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

New features

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

Virtual Security Engines

Virtual Security Engines are logically separate engines that run as virtual engine instances on a physical engine device. You can now use a physical Security Engine device as a Master Engine to provide resources for Virtual Security Engines. This means that the same Master Engine can simultaneously have different security policies, separate routing tables and overlapping IP addresses for different interfaces (reserved by different Virtual Security Engines).

You can configure up to 250 Virtual Firewalls per Master Engine. The Master Engine can be used as a cluster – one Master Engine can support up to 16 cluster nodes. The Virtual Security Engines are load-balanced so that they are automatically spread between master nodes. One Master Engine handles all the traffic of one Virtual Security Engine at any given time.

Virtual Security Engines do not require individual licenses. Instead, the Security Engine license for the Master Engine defines how many Virtual Resources can be created. The number of Virtual Resources limits the number of Virtual Security Engines. In this major version, Virtual Security Engines can be used in the Firewall/VPN role with some limitations to normal Firewall/VPN role features. Virtualization works across several SMC Domains. For example, the Master Engine can be in the Shared Domain and the Virtual Security Engines can be in one or several other Domains.

Enhancements

Enhancements that have been made since the previous Stonesoft Security Engine major version are described below.

Enhancements introduced in Stonesoft Security Engine 5.5

New options in QoS Policies

Multiple enhancements have been made to the current bandwidth management and traffic prioritization features. The new QoS Mode option in the properties of a Physical, VLAN, ADSL, Tunnel, or SSID Interface allows you to define in more detail how QoS is applied to the interface.

You can now read and/or write DSCP markers for traffic without configuring Access rules to apply a QoS class to the traffic. The matching is done based only on the QoS Policy.

QoS Class-based statistics items are now available even when QoS is not used for bandwidth management and traffic prioritization. The QoS class for the packet comes from the QoS Classes that are applied in the Access rules.

New Active Queue Management (AQM) features reduce the volume of dropped or retransmitted packets when there is network congestion. AQM monitors the average queue size and uses a scheduling algorithm to determine the statistical probability for dropping incoming packets.

It is now possible to assign a weight to QoS Classes so that different QoS Classes with the same priority can be assigned to the queue according to their weight when the QoS Class Guarantee is reached and traffic must be queued. This allows more granular control of traffic prioritization, but does not act as a guarantee.

VoIP support

Related connection handling for SCCP and MGCP voice over IP protocols has been added.

SMB2 Inspection

SMB2 protocol normalization and inspection has been enhanced.

SSL/TLS AES inspection

SSL/TLS throughput performance has been improved on AES CPU accelerated appliance models.

Logging of X-Forwarded-For (XFF) proxy IP addresses

Security Engines now log HTTP/XFF proxy IP addresses when a client contacts the server address through proxies.

Policy installation process for large number of Virtual Security Engines improved

The policy installation process for a large number of Virtual Security Engines has been improved.

Traffic inspection throughput in certain network conditions with latency/packet loss improved

Traffic inspection throughput in certain network conditions with latency/packet loss has been improved.

Improved Security Strength of Management Connections

It is now possible to use 256-bit encryption for the connection between Security Engines and the Management Server. This requires both the engines and the Management Server to be version 5.5 or higher. You must also use an Internal ECDSA Certificate Authority to sign certificates for system communications.

Loopback Interfaces

It is now possible to configure any IP address that is not already used as a Cluster Virtual IP Addresses (CVI) or Node Dedicated IP Addresses (NDI) on another interface as a loopback IP address. You can add several loopback IP addresses to each Firewall. Loopback IP addresses can be used, for example, as End-Point IP addresses in policy-based VPNs and in the Route-Based VPN.

Improved packet flow

IPS and Layer 2 Firewall Security Engine roles now use the same packet flow as in the Firewall role. The new packet flow improves inspection throughput in all Security Engine roles. In addition, the Security Engine’s inspection throughput can be better optimized using Access rules.

Enhancements introduced in Stonesoft Security Engine 5.5.12

SIP protocol handling improved

SIP protocol handling has been improved.

glibc library upgrade in regards CVE-2015-0235

This release updates NGFW engine to use glibc library that is not vulnerable to GHOST vulnerability. Note: Only hostnames that NGFW engine may look up come as part of the configuration from the administrator, so there exists no attack vector for other entities than NGFW administrator themselves.

Resolved issues

These issues have been resolved in Stonesoft Security Engine 5.5.12. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Role	Description
IPv6 ICMP Packet Too Big messages not allowed by default (#87542)	FW	ICMPv6 Packet Too Big messages generated for VPN path MTU discovery originate from cluster CVI addresses instead of NDI addresses. By default, these messages are not allowed from cluster CVI addresses. Workaround: Add a rule to allow ICMPv6 Packet Too Big messages from the cluster CVI addresses.
Inspection process might restart (#90139)	FW L2FW IPS	The inspection process might restart when some types of HTTP traffic are inspected.
Link Status test fails after configuring new interface for new Virtual Resource (#101522)	FW L2FW IPS	After adding an interface to a new Virtual Resource and installing the policy, the Link Status test fails and one of the nodes in the Master Engine Cluster goes offline. If the Virtual Resource is not associated with a Virtual Security Engine, the interface is not up. However, the Link Status Test is active if the Link Status test is set to run on all interfaces. Workaround: Install the policy only after adding the new Virtual Resource and Virtual Security Engine to the configuration.
Using anti-virus and TLS inspection might cause inspection process to restart (#108533)	FW	Using anti-virus and TLS inspection at the same time might cause the inspection process to restart.
Support for using interfaces with loopback IP addresses as VPN endpoints (#109928)	FW	It is now possible to use Firewall interfaces that have loopback IP addresses as VPN endpoints.
Static route configuration might fail with large number of Tunnel Interfaces (#110024)	FW	When the Firewall engine configuration contains a large number of Tunnel Interfaces, some static routes through these interfaces might not be configured when the policy is uploaded.
Policy installation may fail on engines that have interfaces with dynamic IP addresses (#110165)	FW	Policy installation may fail on Single Firewall engines that have interfaces with dynamic IP addresses.
Using Refuse action in Access rules might cause engine to hang or reboot (#110230)	FW L2FW IPS	Using the Refuse action in Access rules might cause the engine to hang or reboot.
sg-reconfigure may not work correctly on Master Engines (#110240)	FW	When using the sg-reconfigure tool on the command line of a Master Engine that has Virtual Security Engines configured, the tool may not start correctly. Instead, a "Waiting for stonegate kernel module to unload..." message is shown, and a process named "sgcfg" may generate core files. Workaround: Contact McAfee Support for a workaround.

Engines may not report SNMP interface data correctly in logs (#110594)	FW L2FW IPS	Engines may report data related to SNMP interfaces incorrectly in the Logs view. The affected SNMP log fields are "SNMP Return Src IF" and "SNMP Src IF."
Applying QoS configuration might cause engine to reboot (#110788)	FW L2FW IPS	In rare cases, refreshing the policy when QoS is configured might cause the engine to reboot.
Hardware monitoring might stop working (#110990)	FW L2FW IPS	In rare cases, hardware monitoring might stop working. This causes operations that depend on hardware monitoring, such as sgInfo collection, to stop.
Communication between User Agent and NGFW might not work (#111018)	FW L2FW IPS	The User Agent might stop forwarding user information to the engine if the connectivity between the User Agent and the engine is not working reliably.
MTU setting for VLAN trunk might be incorrectly configured (#111078)	FW L2FW IPS	The MTU setting for the VLAN trunk might be incorrectly set in some configurations.
Problems with application detection accuracy when using Firewall license (#111179)	FW	When you use application detection on a Firewall that has a Firewall license, application detection can only identify a subset of applications compared to a Firewall that has a Security Engine license.
Authentication timeout setting in Access rules affects VPN client connections (#111721)	FW	When the VPN client connection matches an Access rule that has an authentication timeout defined, the mobile VPN user authentication inherits the timeout setting. This can lead to a situation where a mobile VPN user is not able to access internal resources because authentication has timed out, but the VPN tunnel is still up. Workaround: Adjust the authentication timeout in the matching Access rules to match the IKE SA lifetime setting in the VPN Profile.
IPsec NAT-T keepalive packets might be dropped (111736)	FW	In some cluster configurations, IPsec NAT-T keepalive packets might be incorrectly treated as spoofed packets.
Traffic that matches Ethernet rules using MAC addresses is not inspected (#111836)	L2FW IPS	If traffic matches an Ethernet rule that specifies MAC addresses, the traffic might not be sent for deep inspection, even if deep inspection is enabled in the policy. Workaround: Edit the Ethernet rule so that MAC addresses are not used for matching.
Inspected connections might fail when dynamic source NAT is applied (#111873)	FW	Inspected connections might fail when dynamic source NAT is applied.
VLAN tagged traffic passing through Inline Interfaces might be dropped (#111880)	IPS	On IPS-6x00 appliance models, VLAN tagged traffic might be dropped if it is passing through Inline Interfaces. Workaround: Contact McAfee Support for a workaround.
Route-Based VPN packets might be dropped on Firewall Clusters (#112070)	FW	Route-Based VPN packets might be dropped as spoofed on Firewall Clusters.
SunRPC connections might fail (#112105)	FW	SunRCP connections through the engine might fail.
IPv6 traffic over IPsec VPN with IPv4 endpoints does not work (#112164)	FW	IPv6 traffic over an IPsec VPN with IPv4 endpoints does not work. The IPsec tunnel is negotiated but traffic is not sent into the tunnel.
Processing NATed ICMPv6 packets can cause engine to restart (#112266)	FW	Processing NATed ICMPv6 packets can cause the engine to restart.

Virtual Engines might not send NAT-T keepalive packets correctly (112294)	FW	Virtual Security Engines might not send NAT-T keepalive packets correctly when Virtual Security Engines are in use. Instead, the NAT-T keepalive packets are sent from the Master Engine.
RPC connections can cause engine to restart (#112312)	FW	If RPC connections originated from a node are allowed in a rule using the RPC protocol agent, the engine might restart. Workaround: Allow connections with a rule that uses a service element without the protocol agent.
Inspecting tunneled traffic can lead to a memory leak (#112397)	L2FW IPS	Inspecting tunneled traffic can cause a memory leak.
Engine might use wrong certificate fingerprint in SMC connection verification (#112422)	FW L2FW IPS	If the management CA is changed from RSA to ECDSA or from ECDSA to RSA, and the Management Server certificate fingerprint has been defined in the engine, the engine tries to verify the management connection using the previous fingerprint. Workaround: Remove the certificate fingerprint using sg-reconfigure.
Logs related to inspected GRE traffic might be missing information (#112463)	L2FW IPS	Some information might be missing from logs related to inspected GRE tunneled traffic.
Decryption of POP3S or IMAPS traffic might not work (#112480)	FW L2FW IPS	Decryption of POP3S or IMAPS traffic might not work.
Engine might reboot when refreshing the policy (#112481)	FW	Using dynamic routing can cause the engine to reboot when refreshing the policy.
VPN-related information missing from logs with applications (#112526)	FW	Application logs might not contain all VPN-related information.
Master Engine might restart when deleting a Virtual Security Engine (#112783)	FW	The Master Engine might restart when you delete a Virtual Security Engine that still has a Virtual Resource attached to it. Workaround: Delete the Virtual Resource first in the Virtual Engine Properties and then the Virtual Security Engine element itself.
Master Engine might reboot (#113059)	FW	The Master Engine might reboot when it is processing connections that use the H323, Oracle, or RSH Protocol Agents, and NAT is applied to the connections.
Engine might not answer SNMP queries sent to Interfaces with dynamic IP addresses (#113074)	FW	The engine might not answer SNMP queries that are sent to interfaces that have dynamic IP addresses.
PPTP might not work if Tunnel Rematching is in use (#113079)	L2FW IPS	The Security Engine may not handle PPTP connections correctly if Tunneled Traffic Rematching is in use.
Master Engine may not handle traffic correctly when MAC addresses are used for CVIs (#113281)	FW L2FW IPS	Master Engines may not handle traffic correctly when MAC addresses are used for CVIs on the Virtual Firewalls. Workaround: Do not configure MAC addresses for CVIs in the Master Engine interface properties. This way the MAC addresses of the Physical Interfaces will be used instead.
Policy installation can fail when browser-based authentication is in use (#113287)	FW	Policy installation can fail when browser-based authentication is in use.
Engine can become unresponsive when NAT is used together with loose connection tracking (#113302)	FW	In rare situations where there is static source and destination NAT for the same IP addresses, and the same connections use loose connection tracking, the engine can become unresponsive.

Backslash cannot be used in user names with RADIUS authentication (#113372)	FW	The engine prevents using the backslash character in user names when querying a RADIUS server. As a result, authentication using a user name that contains the "\" character fails when using RADIUS authentication. The log message is: "Login is not valid (test\user)".
Policy installation can fail on engine with dynamic interfaces (#113459)	FW	Policy installation can fail on an engine if it has dynamic interfaces configured and destination NAT configured on those interfaces.
Engine can take a long time to recover from ADSL network issues (#113614)	FW	The engine can take a long time to start processing traffic in situations where the ADSL interface has recovered from a network problem.
Authentication process can restart (#113661)	FW	The authentication process can restart, causing authentication to fail on the engine.
Master Engine might not handle correctly traffic if link aggregation is in use (#113858)	FW	Master Engines might not correctly handle traffic assigned to Virtual Security Engines if link aggregation is in use. The connections are dropped as spoofed.

Known limitations

High-Security Inspection Policy and Strict TCP mode are not supported in asymmetrically routed networks in IPS and Layer 2 Firewall roles

The High-Security Inspection Policy and Strict TCP mode are not supported in asymmetrically routed networks or in environments where a Security Engine in the IPS or Layer 2 Firewall role is directly connected to a load-balancing or High Availability network device. It is recommended to base policies on the Medium-Security Inspection Policy in such cases.

In Strict TCP mode and in the High-Security Inspection Policy, the Security Engine controls the progress of a TCP connection and checks that the TCP handshake proceeds according to the TCP protocol. The same Security Engine node must be able to see all the packets in the connection. In Strict TCP mode, the Security Engine also enforces the packet direction (for example, SYN and SYN-ACK packets are not allowed from the same interface).

The TLS inspection and Web Filtering features use Strict TCP mode and are not supported in asymmetrically routed networks in IPS and Layer 2 Firewall roles.

SSL/TLS Inspection and Web filtering are not supported in capture (IDS) mode

The TLS Inspection and Web Filtering features are not supported in capture (IDS) mode.

Inline Interface Disconnect Mode in IPS role

The Inline Interface "Disconnect Mode" is not supported on IPS Virtual Appliances, IPS software installations, or appliance models other than IPS-6xxx or modular (13xx, 32xx, 52xx) appliance models on bypass NIC modules.

IPS and Layer 2 Firewall roles are not supported for Virtual Security Engines

Layer 2 Firewall and IPS Security Engine roles are not supported for Virtual Security Engines in this version.

SYN flood protection

Situation-based SYN flood protection is not supported. Use the "SYN Rate Limits" feature instead.

System requirements

Stonesoft appliances

Appliance model	Supported roles
FW-310	Firewall/VPN
FW-315	Firewall/VPN
320X (MIL-320)	Firewall/VPN
FW-1030	Firewall/VPN
FW-1060	Firewall/VPN
FW-1200e	Firewall/VPN
FW-5000	Firewall/VPN
FW-5000L	Firewall/VPN
FW-5100	Firewall/VPN
FW-5105	Firewall/VPN
IPS-1030	IPS and Layer 2 Firewall
IPS-1060	IPS and Layer 2 Firewall
IPS-1205	IPS and Layer 2 Firewall
IPS-6000	IPS and Layer 2 Firewall
IPS-6100	IPS and Layer 2 Firewall
IPS-6105	IPS and Layer 2 Firewall
1035	Firewall/VPN, IPS, and Layer 2 Firewall
1065	Firewall/VPN, IPS, and Layer 2 Firewall
1301	Firewall/VPN, IPS, and Layer 2 Firewall
1302	Firewall/VPN, IPS, and Layer 2 Firewall

1402	Firewall/VPN, IPS, and Layer 2 Firewall
3201	Firewall/VPN, IPS, and Layer 2 Firewall
3202	Firewall/VPN, IPS, and Layer 2 Firewall
3205	Firewall/VPN, IPS, and Layer 2 Firewall
3206	Firewall/VPN, IPS, and Layer 2 Firewall
5201	Firewall/VPN, IPS, and Layer 2 Firewall
5205	Firewall/VPN, IPS, and Layer 2 Firewall
5206	Firewall/VPN, IPS, and Layer 2 Firewall

Some features in this release are not available for all appliance models. See https://my.stonesoft.com/support/document.do?product=StoneGate&docid=3927 for up-to-date appliance-specific software compatibility information. Stonesoft appliances support only the software architecture version (32-bit or 64-bit) that they are shipped with.

Certified Intel platforms

Stonesoft has certified specific Intel-based platforms for the Stonesoft Security Engine. The list of certified platforms can be found at www.stonesoft.com/en/products/appliances/.

We strongly recommend using certified hardware or a preinstalled Stonesoft appliance as the hardware solution for new Stonesoft Security Engine installations. If it is not possible to use a certified platform, the Stonesoft Security Engine can also run on standard Intel-based hardware that fulfills the Stonesoft hardware requirements.

Basic Security Engine hardware requirements

- Intel®Core™2 / Intel® Xeon® based hardware
- IDE hard disk (IDE RAID controllers are not supported) and CD-ROM drive
- Memory:
  - 2 GB RAM minimum for 32-bit (i386) installation
  - 8 GB RAM minimum for 64-bit (x86-64) installation
- VGA-compatible display and keyboard
- One or more certified network interfaces for the Firewall/VPN role
- 2 or more certified network interfaces for IPS with IDS configuration
- 3 or more certified network interfaces for Inline IPS or Layer 2 Firewall

For more information on certified network interfaces, see https://my.stonesoft.com/support/document.do?product=StoneGate&docid=7849.

Requirements for Virtual Appliance Nodes

- Intel®Core™2 / Intel® Xeon®-based hardware
- VMware ESXi versions 5.1 and 5.5
- 8 GB virtual disk
- 1 GB RAM minimum, 2 GB recommended if inspection is used
- A minimum of one virtual network interface for the Firewall/VPN role, three for IPS or Layer 2 Firewall roles

The following limitations apply when a Stonesoft Security Engine is run as a virtual appliance node in the Firewall/VPN role:

- Only Packet Dispatching CVI mode is supported.
- Only Standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

The following limitations apply when a Stonesoft Security Engine is run as a virtual appliance node in the IPS or Layer 2 Firewall role:

- Clustering is not supported.

Build version

The Stonesoft Security Engine version 5.5.12 build version is 9912.

Product Binary Checksums

sg_engine_5.5.12.9912_i386.iso
MD5SUM b3c11fc8567be02a1058a28fd9163819
SHA1SUM 48b04a5b894167d5ff209bd742a164b9dbe86b6c

sg_engine_5.5.12.9912_i386.zip
MD5SUM 252b00b13bcc3d7e93bca43b443b6513
SHA1SUM ed2055ea26974c2500fe01c5602f93361b713a3b

sg_engine_5.5.12.9912_x86-64.iso
MD5SUM 838a5ac65853c01afb15af70ca92818a
SHA1SUM 86d2dbd7d0560a9013c391a1afbc1a59b8956440

sg_engine_5.5.12.9912_x86-64.zip
MD5SUM a6ddec6799cc02acbd4c6426e4877117
SHA1SUM 0144619dd031fb4bc3eda2a7d8cd70115f0cb616

Compatibility

Minimum

Stonesoft Security Engine version 5.5.12 is compatible with the following component versions:

- Stonesoft Management Center 5.5.0 or higher
- Stonesoft Dynamic Update 517 or higher
- Stonesoft IPsec VPN Client 5.1.0 or higher
- Stonesoft Server Pool Monitoring Agent 4.0.0 or higher
- Stonesoft User Agent 1.1.0 or higher

Installation instructions

The main installation steps for the Stonesoft Security Engines are as follows:

1. Install the Management Server, the Log Server(s), and the Management Client to host(s) to be used as the management system. The Authentication Server and Web Portal Server(s) need to be installed if the optional Authentication Server and Stonesoft Web Portal are used.
2. Configure the Firewall, IPS, or Layer 2 Firewall element using the Management Client.
3. Generate an initial configuration for the engines by right-clicking the element and selecting **Save Initial Configuration**.
4. If not using Stonesoft appliances, install the engines by rebooting the machines from the installation DVD.
5. Make the initial connection from the engines to the Management Server and enter the one-time password provided during step 3.
6. Create and upload a policy on the engines using the Management Client.
7. Command the nodes online by right-clicking the element and selecting **Commands** | **Go Online**.

The detailed installation instructions can be found in the *Stonesoft Management Center Installation Guide*, *Firewall/VPN Installation Guide*, and *IPS and Layer 2 Firewall Installation Guide*. For more information on using the Stonesoft system, refer to the Management Client *Online Help* or the *Stonesoft Administrator's Guide*. For background information on how the system works, consult the *Stonesoft Management Center Reference Guide, Firewall/VPN Reference Guide*, and *IPS and Layer 2 Firewall Reference Guide*.

Upgrade instructions

Stonesoft Security Engine version 5.5.12 requires an updated license if upgrading from version 5.4.x or lower. The license upgrade can be requested at our website at https://my.stonesoft.com/managelicense.do. Install the new license using the Management Client before upgrading the software. The license is updated automatically by the SMC if communication with Stonesoft servers is enabled and the maintenance contract is valid.

To upgrade the engine, use the remote upgrade feature or reboot from the installation CD and follow the instructions. Detailed instructions can be found in the *Firewall/VPN Installation Guide* and *IPS and Layer 2 Firewall Installation Guide*.

Note Stonesoft appliances support only the software architecture version that they are pre-installed with. 32-bit versions (i386) can only be upgraded to another 32-bit version and 64-bit versions (x86-64) can only be upgraded to another 64-bit version. Clusters can only have online nodes using the same software architecture version. State synchronization between 32-bit and 64-bit versions is not supported. Changing architecture for third-party server machines using software licenses requires full re-installation using a CD.

Upgrading to any 5.5.x version is only supported from a lower 5.5.x version or from a 5.4.x version. If you are running a lower version, please first upgrade to the highest 5.4.x version following the instructions in the release notes for that version.

Note It is recommended to set the Cluster Mode to Standby when upgrading from version 5.5.4 or lower to version 5.5.5 or higher on clusters that process GRE or IP-IP traffic. If the upgrade is done when the cluster is in Load-Balancing Mode, tunneled traffic connections may break due to changes in load-balancing functionality.

Note If you have not changed the root password since engine version 4.x, change the root password before upgrading using the sg-reconfigure tool or the Management Client. If the upgrade is done without changing the root password, root login to the engine does not work after upgrading to 5.5.7 or higher until the password has been reset in the Management Client.

It is recommended to change root password in any case, as the salted hash of the root password is stored using a stronger hash (SHA-512) in version 5.5.5 and higher.

Known issues

The current known issues of Stonesoft Security Engine version 5.5.12 are described in the table below.

Issue	Role	Description
SunRPC Protocol Agent is not supported in IPS and Layer 2 Firewall roles (#79844)	IPS L2FW	The SunRPC Protocol Agent is not supported in the IPS and Layer 2 Firewall roles.
Security Engine displays log message "State sync kernel event Setting node X failed" (#82888)	IPS L2FW	The Security Engine 5.4 in the IPS and Layer 2 Firewall roles displays the following log message: "State sync kernel event Setting node X failed". This log message requires no administrator action.
DNS protocol enforcement may drop valid DNS responses (#84145)	FW IPS L2FW	DNS responses with additional response records (RRs) trigger the DNS_Server-UDP-Extra-Data Situation, even though additional response records are valid in queries as specified in "RFC 2671: Extension Mechanisms for DNS (EDNS0)". If DNS protocol enforcement has been activated in a custom DNS Service element, this also triggers the DNS_Protocol_Violation Situation, and the response is terminated. Workaround: Disable DNS protocol enforcement from the custom DNS Service element (it is disabled by default).
SNMP IP-MIB: ipInReceives counter does not work correctly (#84964)	IPS L2FW	The IP-MIB ipInReceives counter included in the SNMP IP-MIB does not provide the total number of input datagrams received from interfaces.

Activating port scan detection can decrease engine's performance (#85692)	IPS L2FW FW	Activating port scan detection can cause a high CPU load and decrease the engine's performance. Workaround: Remove the following Situations from the Inspection Rules to disable port scan detection: - TCP_Stealth_Scan_Started - TCP_SYN_Scan_Started - Aggressive_TCP_Scan_Started
User Responses may not work with HTTPS (with decryption) Service (#90789)	FW IPS L2FW	When the HTTPS (with decryption) Service is used in the Service cell of an Access rule with the Discard action, User Responses configured in the Action Options may not work.

Find product documentation

Stonesoft provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the online Knowledge Base. Information about Stonesoft and the Stonesoft Management Center can still be found at www.stonesoft.com.

To access...	Do this...
User documentation	Go to https://www.stonesoft.com/en/customer_care/documentation/
Knowledge Base	Go to the Stonesoft Knowledge Base: http://www.stonesoft.com/en/customer_care/kb/. The known issues database and the release notes can be found on the website. Go to the McAfee Knowledge Center: https://support.mcafee.com/ServicePortal/faces/knowledgecenter New material will be published under the Next Generation Firewall product.

00-A