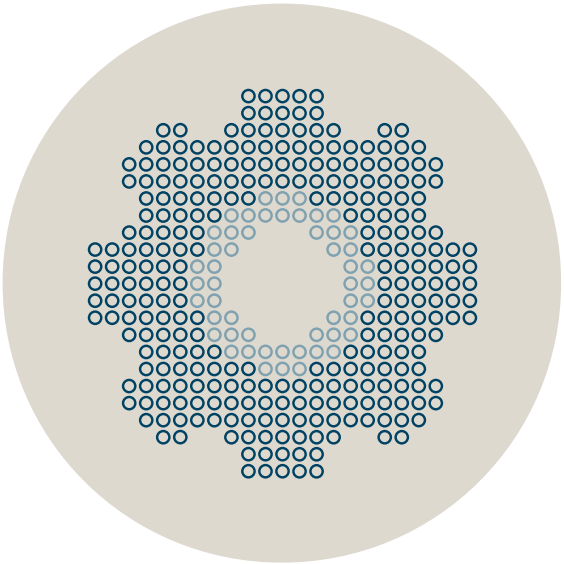

Stonesoft Firewall/VPN Express

Release Notes for Version 5.5.7

Created: April 9, 2014

STONESOFT
A McAfee Group Company

Table of Contents

What's New **3**

Fixes 3

System Requirements **5**

Stonesoft Firewall/VPN Appliances 5

Build Version **5**

Product Binary Checksums **5**

Compatibility **5**

Installation Instructions **6**

Upgrade Instructions **6**

Known Issues **7**

What's New

Stonesoft Firewall/VPN Express version 5.5.7 is a maintenance version for the Stonesoft Firewall/VPN Express appliance series.

Fixes

Problems described in the table below have been fixed in Stonesoft Firewall/VPN Express version 5.5.7. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
SIP Protocol Agent may leak memory with some traffic patterns (#75652)	The SIP Protocol Agent may leak memory with some traffic patterns, which leads to the sg-inspection process restarting.	N/A
Engine may drop NAT-T packets sent by itself (#95390)	When the local VPN endpoint address is excluded from antispoofing (for example, when the same address is used as a NAT address and proxy ARP is enabled), the engine may drop NAT-T packets sent by itself.	N/A
Configuration created on additional Management Server may not work (#97865)	In environments where there is more than one Management Server, the following engine features may not work if the elements used in the configuration are created on an additional Management Server: - QoS Classes (all engine versions) - NetLink configuration (all engine versions) - VPN with ESP DSCP Match/Mark rules in the QoS Policy (engine 5.5 and higher)	Create elements only on the primary Management Server.
NAT destination address not displayed as translated in logs (#98582)	The translated NAT destination address may not be displayed as translated in the logs. Instead, the untranslated destination IP address is shown in the "NAT Dst" log field.	N/A
Oracle Protocol Agent may work incorrectly (#100312)	The Oracle Protocol Agent may work incorrectly and may cause the engine to reboot when used.	N/A
WLAN logs do not report failed authorizations (#101103)	Logs from the WLAN access point do not report failed authorizations.	N/A
SSID Interface Security Mode setting does not persist (#102221)	Setting the Security Mode of an SSID Interface to Disabled does not persist. After uploading the policy or rebooting, a specific Security Mode may be enabled for the SSID Interface.	N/A
Engine may fail to detect a broken link with Multi-Link VPN if dynamic end-points configured (#102516)	When Multi-Link VPN is in use and the engine has dynamic end-points configured, the engine may fail to detect broken links after rebooting.	N/A
Network configuration is slow at policy installation (#102731)	When changing the network configuration during a policy installation, traffic is stopped for an unnecessarily long time, particularly with large routing tables.	N/A
Installing large policies takes a long time (#103260)	Installing a large policy may take a long time.	N/A
Using an alias in engine DNS configuration may lead to policy installation failure (#103443)	In very rare situations when a VPN is configured, the engine may become unresponsive. Messages similar to the following may be shown in the console: "BUG: soft lockup - CPU#0 stuck for 22s! [sg_vpn/0/0:5003]"	N/A

Synopsis	Description	Workaround for Previous Versions
Engine may not log dropping of SYN-ACKs if connections use smaller MSS than defined on engine (#103623)	In situations where connections have smaller MSS values than configured on the engine, the engine may not create any log entries when dropping the SYN-ACK packets for these connections.	N/A
Engine may not restore primary control connection to Management Server if dynamic control IP addresses in use (#103721)	In situations where the engine has two control interfaces with dynamic IP addresses and the secondary interface is used as the control connection to the Management Server, the primary control connection may not be restored, even after connectivity through the primary interface is working.	N/A
"No Policy Installed" shown in System Status view, even if policy is installed (#104147)	The System Status view may display "No Policy Installed" for a Firewall, even if a policy has been installed. This may occur when the Firewall has a dynamic control IP address configured. The problem arises when the monitoring process does not send the configuration name or dynamic update name to the Management Server after a successful policy upload to the Firewall. You cannot refresh the policy because the SMC is not aware of the policy installed on the Firewall. You must install the policy instead.	Run the "sg-status" command on the engine command line to verify the latest policy installation time and dynamic update package number, and install the policy again.
Rule counter results may not be shown (#104802)	Rule counter results may not be shown in the Management Client if the policy contains more than approximately 6000 rules. You may receive the error message "No rule counters found".	N/A
Ipsecpmd process may restart (#105171)	The Ipsecpmd process may restart.	N/A
Engine may suddenly reboot after running sg-reconfigure command (#105326)	The engine may suddenly reboot after you run the sg-reconfigure command locally from the console.	Reboot the engine after running the sg-reconfigure command locally from the console.
Related connections that use TCP ECN are not properly handled (#105801)	Related connections that enable TCP Explicit Congestion Notification (ECN) are not properly handled.	N/A
OpenSSL library update (#106380)	The OpenSSL library has been updated to version 1.0.1g to address the issue listed in CVE-2014-0160. The engine uses vulnerable OpenSSL routines only for its TLS management communications and cluster communications between the cluster nodes.	If you use the default template from dynamic update package 575 or newer, engine exposure is limited, as connections to vulnerable TLS endpoints are allowed only from the Management Server IP address.

System Requirements

Stonesoft Firewall/VPN Appliances

This software version is supported on Stonesoft Express FW-105 FW/VPN appliances only.

Build Version

Stonesoft Firewall/VPN Express version 5.5.7 build version is 9887.

Product Binary Checksums

sg_engine_5.5.7.9887_express.zip
MD5SUM ed2c2f1e29b5bdc11a4d6a8208fb6347
SHA1SUM 74443ffc887335d70475dd137fd73c6f27f586ec

Compatibility

Stonesoft Firewall/VPN Express version 5.5.7 is recommended to be used with the following Stonesoft component versions:

Component	Minimum Compatible Version	Recommended Version
Stonesoft Management Center	5.5.0	Latest 5.5 maintenance version
Stonesoft Dynamic Update	517	Latest available

Installation Instructions

The main installation steps for Stonesoft Firewall/VPN Express 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. Optionally, you can install the Authentication Server and Web Portal Server(s).
2. Configure the Firewall element using the Management Client.
3. Generate an initial configuration for the engines by right-clicking the firewall and selecting **Save Initial Configuration**.
4. Make the initial connection from the engines to the Management Server and enter the one-time password provided during step 3.
5. Create and upload a policy on the engines using the Management Client.
6. Command the nodes online by right-clicking the firewall and selecting **Commands → Go Online**.

There are alternative methods for the initial configuration of the engines. Please refer to the *Stonesoft FW-105 Series Appliance Installation Guide*.

The detailed installation instructions can be found in the *Stonesoft Management Center Installation Guide* and *Firewall/VPN 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* and *Firewall/VPN Reference Guide*.

Upgrade Instructions

Stonesoft Firewall/VPN Express version 5.5.7 requires an updated license if upgrading from version 5.4.x. 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 Management Server if communication with Stonesoft servers is enabled and the maintenance contract is valid.

To upgrade the engine, use the remote upgrade feature in the Management Client. Detailed instructions can be found in the *Firewall/VPN Installation Guide*.

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

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

Known Issues

The current known issues of Stonesoft Firewall/VPN Express version 5.5.7 are described in the table below. For a full and updated list of known issues, consult our website at http://www.stonesoft.com/en/customer_care/kb/.

No known open issues.

Copyright and Disclaimer

Trademarks and Patents

Stonesoft Corporation

Itälahdenkatu 22A
FI-00210 Helsinki
Finland

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

STONESOFT
A McAfee Group Company

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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