



# **Stonesoft Firewall/VPN Express**

## **Release Notes for Version 5.5.5**

Created: January 28, 2014

# Table of Contents

<b>What's New .....</b>	<b>3</b>
Enhancements.....	3
Fixes .....	3
<b>System Requirements .....</b>	<b>4</b>
Stonesoft Firewall/VPN Appliances .....	4
<b>Build Version .....</b>	<b>4</b>
<b>Product Binary Checksums .....</b>	<b>4</b>
<b>Compatibility.....</b>	<b>4</b>
<b>Installation Instructions.....</b>	<b>5</b>
<b>Upgrade Instructions .....</b>	<b>5</b>
<b>Known Issues .....</b>	<b>5</b>

# What's New

Stonesoft Firewall/VPN Express version 5.5.5 is a maintenance version for the Stonesoft Firewall/VPN Express appliance series.

## Enhancements

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

Enhancement	Description
DHCP logging enhanced	Security Engines in the Firewall role now log DHCP lease activation and expiration.

## Fixes

Problems described in the table below have been fixed in Stonesoft Firewall/VPN Express version 5.5.5. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
Engine may reboot during policy installation (#46654)	If the SYN packet that initiates the TCP connection has been sent through Multi-Link and the Firewall policy is refreshed before the SYN-ACK packet is received from the server, the Firewall engine may reboot.	N/A
Connection issues with Protocol Agent for Sun RPC protocol (#55153)	When the Protocol Agent for the Sun RPC protocol is used, RPC queries may be blocked or dropped by the Firewall engine if the Portmapper is unreachable.	N/A
Related connections may not work when traffic is allowed by certain Protocol Agents (#100481)	When traffic is allowed by a rule that uses the Oracle, H323, or Shell (RSH) Protocol Agent, related connections may not work in certain circumstances.	N/A
Switching DHCP mode may cause reboot (#101053)	When switching between DHCP Relay and DHCP Server modes, the node may reboot at policy installation.	1. Select "Disabled" as the DHCP Mode. 2. Refresh the policy. 3. Select the DHCP Mode.
Modem PIN status detection does not always work (#101524)	Modem PIN status detection may not work with some modems.	N/A
Established HTTP connections may be dropped at policy installation (#101557)	Established HTTP connections are dropped at policy installation if the connection matches an Access rule with default system HTTP as the Service. If URL logging, CIS redirection, or deep inspection is used in the rule, policy refresh works correctly.	N/A
Initial contact may not always work when using dynamic management interface (#101623)	A node with a dynamic control IP address may attempt an initial contact connection before it receives a usable IP address. As a result, the connection fails.	Initiate initial contact again using the Engine Configuration Wizard or the sg-contact-mgmt command.
Unknown SPI value does not work with IKEv2 (#101819)	When IKEv2 is used for IPsec, the engine may not send notification to a peer VPN gateway if the engine receives an IPsec packet with an unknown SPI value. As a result, VPN tunnels may not recover as quickly.	N/A

Synopsis	Description	Workaround for Previous Versions
OpenSSL library update (#102392)	The OpenSSL library has been updated to version 1.0.1f in order to address issues listed in CVE-2013-6449 and in CVE-2013-4353. The engine uses vulnerable OpenSSL routines only for its internal TLS management communication.	N/A
Change in Route-Based VPN encryption mode may not be applied at policy installation (#102414)	If you change the Route-Based VPN encryption mode from Tunnel Mode to No Encryption, or from No Encryption to Tunnel Mode, the new encryption mode may not be applied at policy installation.	N/A

## 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 5.5.5 build version is 9877.

## Product Binary Checksums

sg\_engine\_5.5.5.9877\_express.zip

MD5SUM e1a37aa6149dc46582d95f6c1772a890

SHA1SUM f8cbd2381e054e1f8f59f08d75834f34a279d0de

## Compatibility

Stonesoft Firewall/VPN Express version 5.5.5 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 element 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 element 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 the *Firewall/VPN Reference Guide*.

## Upgrade Instructions

Stonesoft Firewall/VPN Express version 5.5.5 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.

## Known Issues

The current known issues of Stonesoft Firewall/VPN Express version 5.5.5 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/](http://www.stonesoft.com/en/customer_care/kb/).

No open known issues.

## Copyright and Disclaimer

© 2000—2014 Stonesoft Corporation. All rights reserved.

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