Release Notes

Revision A

Stonesoft Firewall/VPN Express 5.5.8

Contents

- *About this release*
- *Resolved issues*
- *System requirements*
- *Build version*
- *Compatibility*
- *Installation instructions*
- *Upgrade instructions*
- *Known issues*
- *Find product documentation*

About this release

Stonesoft Firewall/VPN Express version 5.5.8 is a maintenance version for the Stonesoft Firewall/VPN Express appliance series.

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

Resolved issues

Problems described in the table below have been fixed in Stonesoft Firewall/VPN Express version 5.5.8. A workaround solution is presented for earlier versions where available.

Issue	Description
User authentication is accepted even with trailing whitespace (#87050)	User authentication is accepted even when there is trailing whitespace in the user name. However, traffic does not match rules that contain the user name without trailing white-space.
Engine may fail to initialize interfaces that have a dynamic IP address (#103040)	Due to certain race conditions, the engine may fail to initialize interfaces that have a dynamic IP address. This may cause the engine to go to the wrong state during reboot.
Security Engine may incorrectly change media settings configured in sg-reconfigure (#103073)	The Security Engine may incorrectly change the interface media settings configured in sg-reconfigure. Workaround: Run sg-reconfigure again and set forced media settings for each interface even if the settings appear to be forced already.
Security Engine may return to initial configuration state when started if 3G modem interfaces are used (#106862)	Due to an issue with modem interface detection during reboot, the Security Engine may return to the initial configuration state when started.
Security Engine may drop first data packet after TCP handshake when MSS rewrite is used (#106950)	The Security Engine may drop the first data packet after a TCP handshake when MSS rewrite is used. The logs may display messages like the following: "MSS Rewrite: packet dropped (invalid packet)". TCP retransmission takes care of resending the packet, so there is no actual packet loss.

Issue	Description
Security Engine may not handle connections correctly when H.323 Protocol Agent is used (#107021)	The Security Engine may not handle connections correctly when the H.323 Protocol Agent is used. Connections may get dropped with the following log message: "Illegal Logical Channel state."
Security Engine may reboot after policy installation if connection limits are set (#107055)	The Security Engine may reboot after policy installation if connection limits are set.
32-bit Security Engine may reboot when using SIP Protocol Agent with large UDP datagrams (#107081)	A 32-bit Security Engine may reboot when handling large UDP datagrams if the SIP Protocol Agent is used and NAT is applied.

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 5.5.8 build version is 9891.

Product Binary Checksums

sg_engine_5.5.8.9891_express.zip
MD5SUM 90bdedf6b4b0905ff5b9fb4d335528bf
SHA1SUM daf44614c50163223cad62621e7826ef1ef90a32

Compatibility

Minimum

Stonesoft Firewall/VPN Express version 5.5.8 is recommended to be used with the following Stonesoft component versions:

- Stonesoft Management Center 5.5.0 or higher
- Stonesoft Dynamic Update 517 or higher

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**.

Refer to the *Stonesoft FW-105 Series Appliance Installation Guide* for alternative methods for the initial configuration of the engines.

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 5.5.8 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 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 Firewall/VPN Express version 5.5.8 are described 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.

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.