Release Notes

Revision B

Stonesoft Firewall/VPN Express 5.5.16

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 5.5.16 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 5.5.16. A workaround solution is presented for earlier versions where available.

Issue	Description
First policy installation after initial configuration might fail (#111797)	The first policy installation after an engine's initial configuration might fail. This problem is likely to occur when an ADSL Interface is used as the management interface. Workaround: Disable the Policy Handshake option in the engine properties, then install the first policy. After the installation, reboot the engine.
Installing policy on engine with Wireless Interface might cause unexpected reboot (#112905)	The engine might unexpectedly reboot when you install a policy on an engine that has a Wireless Interface defined but no SSIDs configured, or when install a policy with a wireless configuration on an engine that uses the initial policy.
Engine might leak memory when MSRPC Protocol Agent is used (#113571)	The engine might leak memory when the MSRPC Protocol Agent is used.
Engine might not clear old SIP dialogs when SIP Protocol Agent is used (#114252)	When the SIP Protocol Agent is used, the engine might not clear old SIP dialogs if the established SIP call is not terminated with a BYE message.
Policy refresh operation might stop working when VPN configuration is changed (#114275)	The policy refresh operation might stop working if the policy contains changes to the VPN configuration. As a result, VPN processing also stops working.
Load balancing and NAT might not be applied to IPv6 ICMP packets correctly (#114455)	On Firewall Clusters, load balancing and NAT might not be applied to IPv6 ICMP packets correctly.

Issue	Description
Engine might log SIP_Message-No-Transaction Situations unnecessarily (#114771)	The engine might produce unnecessary log entries for SIP_Message-No-Transaction Situations. Call handling on the engine is not affected.
Manually created blacklists might not work (#114839)	Blacklists created manually in the Management Client might not match if the source or destination contains networks.
NAT issues with SIP Protocol Agent (#114881)	The SIP Protocol Agent might apply NAT incorrectly to some SIP messages.
Route-Based VPN endpoints might not be updated (#115364)	If you change the endpoints of a Route-Based VPN, the endpoints might not be updated on the engine when you refresh the engine's policy. Workaround: Reboot the engine to update the IP addresses of the Route-Based VPN endpoints.
Log flooding if modem is disconnected (#115549)	The engine can flood the logs with the message "Failed to open /dev/gsm0: No such file or directory" if a modem is disconnected from the engine while it is in use.
Policy installation can fail if WLAN interface has more than one SSID configured (#115619)	Policy installation can fail on the engine if the WLAN interface has more than one SSID configured.
Route-based VPN tunnels are re-negotiated after each policy install (#115792)	Route-based VPN tunnels are re-negotiated after each policy install, even if no changes are applied to them. This can result in latency in the traffic using the VPN tunnel.
Remote engine upgrade might fail occasionally (#116237)	Remote engine upgrade might fail occasionally with the following error messages: "Read failed" or "Invalid checksum of uploaded software image".

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 5.5.16 build version is 9927.

Product Binary Checksums

sg_engine_5.5.16.9927_express.zip
MD5SUM cfc4bb12ecc9fbe9e28c4f97cdb1a26a
SHA1SUM 239cf2912a9850073cc1870f3de7ab1e90ac2db0

Compatibility

Minimum

Stonesoft Firewall/VPN Express version 5.5.16 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 Servers, and the Management Client to the hosts to be used as the management system. Optionally, you can install the Authentication Server and Web Portal Servers.
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 5.5.16 requires an updated license if upgrading from version 5.4.x. The license upgrade can be requested at our website at https://ngfwlicenses.mcafee.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, 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 5.5.16 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

McAfee 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 Center.

1. Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.
2. Enter a product name, select a version, then click **Search** to display a list of documents.