Release Notes

Revision A

Stonesoft Firewall/VPN Express 5.5.12

Contents

About this release

Stonesoft Firewall/VPN Express version 5.5.12 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 5.5.12. A workaround solution is presented for earlier versions where available.

Issue	Description
IPv6 ICMP Packet Too Big messages not allowed by default (#87542)	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.
Support for using interfaces with loopback IP addresses as VPN endpoints (#109928)	It is now possible to use Firewall interfaces that have loopback IP addresses as VPN endpoints.
Policy installation may fail on engines that have interfaces with dynamic IP addresses (#110165)	Policy installation may fail on Single Firewall engines that have interfaces with dynamic IP addresses.
MTU setting for VLAN trunk might be incorrectly configured (#111078)	The MTU setting for the VLAN trunk might be incorrectly set in some configurations.
IPv6 traffic over IPsec VPN with IPv4 endpoints does not work (#112164)	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)	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.

Issue	Description
Policy installation can fail when browser-based authentication is in use (#113287)	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)	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)	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)	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)	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)	The authentication process can restart, causing authentication to fail on the engine.

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 5.5.12 build version is 9912.

Product Binary Checksums

sg_engine_5.5.12.9912_express.zip
MD5SUM 400662c1331ade09b13c6769aabad6ab
SHA1SUM 3357562e088ea085f2d84c6fdb95cd31c78ed616

Compatibility

Minimum

Stonesoft Firewall/VPN Express version 5.5.12 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 5.5.12 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, 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 5.5.12 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.