About this release

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

New features

No major new features are included in this maintenance version.

Resolved issues

These issues have been resolved in Stonesoft Security Engine 5.3.11. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious code execution vulnerabilities in Bash shell (#111992)</td>
<td>The Bash shell included in the NGFW engine is subject to malicious code execution vulnerabilities described in CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277. The issue concerns engines that have a dynamic interface configuration that uses DHCP for the engine’s IP address configuration.</td>
</tr>
</tbody>
</table>

Changes

Before upgrading to this version, note the changes below that may make the existing version 5.2 configuration partly incompatible with the new version.

**Network driver in VMware virtual appliances**

The use of multicast traffic or standby clustering with multicast clustering mode with 5.3.0 or newer software version requires a vmxnet3 network driver. The vmxnet3 driver requires virtual appliance hardware version 7. If the virtual machine hardware version is not 7, the virtual machine must be reinstalled.

**Dynamic routing software**

The routing daemon included for support of some dynamic routing protocols has been changed from XORP to Quagga. Existing XORP configurations made locally on the firewall node must be manually converted to Quagga configurations. See support documentation at [https://my.stonesoft.com/support/document.do?product=StoneGate&docid=6688](https://my.stonesoft.com/support/document.do?product=StoneGate&docid=6688) for more details.
**VPNs: End of Support for Legacy UDP Encapsulation**

The 5.1 Firewall/VPN engine release is the last major version that supports StoneGate’s proprietary UDP encapsulation method for NAT traversal. If NAT traversal is required, reconfigure your VPNs to use the NAT-T encapsulation method (supported by StoneGate Firewall/VPN engines version 4.2 and higher). When you upgrade to Firewall/VPN version 5.2 or 5.3, the upgrade will automatically remove any remaining references to the legacy UDP encapsulation method from your VPN configurations.

**Different software images for 32-bit systems and 64-bit systems**

Starting from Firewall/VPN version 5.2.0, there is a new software image for the new StoneGate appliances that are capable of running 64-bit software. The 64-bit software image can also be installed on compatible third-party servers when a proper license is used. The images are named as follows:

<table>
<thead>
<tr>
<th>Image</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit remote upgrade package</td>
<td>sg_engine_version.build_i386.zip</td>
</tr>
<tr>
<td>32-bit installation CD image</td>
<td>sg_engine_version.build_i386.iso</td>
</tr>
<tr>
<td>64-bit remote upgrade package</td>
<td>sg_engine_version.build_x86-64.zip</td>
</tr>
<tr>
<td>64-bit installation CD image</td>
<td>sg_engine_version.build_x86-64.iso</td>
</tr>
</tbody>
</table>

Note that it is not possible to upgrade a 32-bit system to a 64-bit system or vice versa. A cluster must consist of nodes running the same software architecture.

**System requirements**

**Stonesoft Firewall/VPN appliances**

<table>
<thead>
<tr>
<th>Appliance model</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG-1100</td>
</tr>
<tr>
<td>SG-4000L</td>
</tr>
<tr>
<td>FW-310</td>
</tr>
<tr>
<td>FW-315</td>
</tr>
<tr>
<td>FW-1020e</td>
</tr>
<tr>
<td>FW-1030</td>
</tr>
<tr>
<td>FW-1035</td>
</tr>
<tr>
<td>FW-1050e</td>
</tr>
<tr>
<td>FW-1060</td>
</tr>
<tr>
<td>FW-1200e</td>
</tr>
<tr>
<td>FW-5000</td>
</tr>
<tr>
<td>FW-5000L</td>
</tr>
<tr>
<td>FW-5100</td>
</tr>
<tr>
<td>FW-5105</td>
</tr>
<tr>
<td>SG-1301</td>
</tr>
<tr>
<td>SG-3201</td>
</tr>
<tr>
<td>SG-3205</td>
</tr>
<tr>
<td>SG-5201</td>
</tr>
<tr>
<td>SG-5205</td>
</tr>
</tbody>
</table>

Certified Intel platforms
Stonesoft has certified specific Intel-based platforms for the Stonesoft Security Engine. The list of certified platforms can be found at www.stonesoft.com/en/products/appliances/.

We strongly recommend using certified hardware or a preinstalled Stonesoft appliance as the hardware solution for new Stonesoft Security Engine installations. If it is not possible to use a certified platform, the Stonesoft Security Engine can also run on standard Intel-based hardware that fulfills the Stonesoft hardware requirements.

Basic Security Engine hardware requirements
- Intel® Pentium 4®/Xeon®-based hardware
- IDE hard disk (IDE RAID controllers are not supported) and CD-ROM drive
- 1 GB RAM minimum (2 GB recommended if inspection is used)
- One or more certified network interfaces
- VGA-compatible display and keyboard

Requirements for Virtual Appliance
- VMware ESX Server versions 4.0 and 4.1, ESXi versions 4.0, 4.1, and 5.0
- 2 GB virtual disk minimum, 8 GB recommended
- 256 MB RAM minimum, 1 GB recommended (2 GB recommended if inspection is used)
- A minimum of one virtual network interface

The following limitations apply when a Stonesoft Firewall/VPN is run as a virtual appliance:
- Only Packet Dispatching CVI mode is supported.
- Only Standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

Build version
The Stonesoft Firewall/VPN version 5.3.11 build version is 9128.

Product Binary Checksums
sg_engine_5.3.11.9128_i386.iso
MD5SUM a710b2219f6c91b33f4e7d179f696a29
SHA1SUM 10c2c8c767611a38629be8b1ab2a8d174b3fad6d

sg_engine_5.3.11.9128_i386.zip
MD5SUM 88c73194eb12d7cb73eeeb6b8d841862
SHA1SUM d7005c67a545a19c4a51295128fb955e7035c0f2

sg_engine_5.3.11.9128_x86-64.iso
MD5SUM 980c5dd5205ec346e2b12ce7f4bd9f7
SHA1SUM 6e3db64fc21139e4c27d385dad1edc42a3d2b745

sg_engine_5.3.11.9128_x86-64.zip
MD5SUM e53f181f02953f8afedc9df878e9048d
SHA1SUM 86aac10bf53b0e3e16099533e7f62b0b6c27dd17
Compatibility

Stonesoft Firewall/VPN version 5.3.11 is recommended to be used with the following Stonesoft component versions:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum compatible version</th>
<th>Recommended version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stonesoft Management Center</td>
<td>5.3</td>
<td>Latest 5.3 or 5.4 maintenance version</td>
</tr>
<tr>
<td>Stonesoft Dynamic Update</td>
<td>393</td>
<td>Latest available</td>
</tr>
<tr>
<td>Stonesoft IPsec VPN Client</td>
<td>5.1.0</td>
<td>Latest 5.3 or 5.4 maintenance version</td>
</tr>
<tr>
<td>Stonesoft Server Pool Monitoring Agent</td>
<td>4.0.0</td>
<td>Latest 4.0 or 5.0 maintenance version</td>
</tr>
<tr>
<td>Stonesoft User Agent</td>
<td>1.1.0</td>
<td>Latest available</td>
</tr>
</tbody>
</table>

Installation instructions

The main installation steps for Stonesoft Firewall/VPN are as follows:

1. Install the Management Server, the Log Server(s), and the Management Client to the host(s) to be used as the management system. The Authentication Server and Web Portal Server(s) need to be installed if the optional Authentication Server and Stonesoft Web Portal are used.
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. If not using Stonesoft appliances, install the engines by rebooting the machines from the installation CD-ROM.
5. Make the initial connection from the engines to the Management Server and enter the one-time password provided during step 3.
6. Create and upload a policy on the engines using the Management Client.
7. Command the nodes online by right-clicking the element and selecting Commands | Go Online.

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 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

When running a StoneGate Firewall/VPN version older than 5.1.0, you must first upgrade to the latest 5.1.x or 5.2.x version following the instructions in the Release Notes for that version. Upgrading to version 5.3.10 from other versions is not supported.

Stonesoft Firewall/VPN version 5.3.11 requires an updated license if upgrading from version 5.2.x or earlier. 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 SMC if communication with Stonesoft servers is enabled and the maintenance contract is valid.

To upgrade the firewall engine, use the remote upgrade feature or reboot from the installation CD-ROM and follow the instructions. Detailed instructions can be found in the Firewall/VPN Installation Guide.

Note

Stonesoft appliances support only the software architecture version that they are pre-installed with. 32-bit versions (i386) can only be upgraded to another 32-bit version and 64-bit versions (x86-64) can only be upgraded to another 64-bit version. Clusters can only have online nodes using the same software architecture version. State synchronization between 32-bit and 64-bit versions is not supported.

Changing architecture for third-party server machines using software licenses requires full re-installation using a CD-ROM.

Prior to upgrade, check that the /data partition in the firewall node is not full: check the Data partition
Known issues

The current known issues of Stonesoft Security Engine version 5.3.11 are described in the table below.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Firewall cannot renew its dynamic IP address (#17184)        | When the firewall is configured with a dynamic IP address, the initial DHCP broadcast request is automatically allowed. However, when the lease expires and the firewall tries to renew the lease, the unicast connection to the DHCP server is discarded. A new broadcast request is sent after the renew connection has failed, which may cause the firewall to get a new IP address each time the lease expires.  
  
  Workaround: Add the following rule to the Firewall policy:
  
  Source: "$DHCP Interface 1.IP", Destination: "Any"
  
  Service: "bootps"
  
  Action: "Allow"

Only one external proxy can be contacted with SIP over UDP (#17389) | If multiple different SIP proxies are contacted simultaneously from the same source IP address (for example, an internal SIP proxy contacts different external proxies), only the connection that opens first works when static source NAT or no NAT is used and SIP protocol uses UDP transport.  
  
  Workaround: Use dynamic source NAT for the SIP over UDP when there is a need to contact multiple different proxies at the same time.

A node may go offline after policy installation if VLAN Interface with e1000 driver is used as Heartbeat Interface (#17554) | If a VLAN Interface with an e1000 driver is used as the Heartbeat Interface, one node in the cluster may go offline when a policy is installed.  
  
  Workaround: Increase the Heartbeat Failover Time to 7000 ms.

Inspection configuration contains Firewall Access rules as plain text on the engine (#22141) | Even if "Encrypt Configuration Data" is selected in the properties of the Firewall, Access rules are stored as plain text in the inspection configuration. The rest of the configuration data is still encrypted.

SIP connections are lost in failover (#23073) | SIP phones that are registered to an external SIP proxy through a particular Firewall Cluster node cannot make new calls to SIP phones inside the Firewall Cluster after that Firewall node goes offline. The external SIP phone cannot terminate an existing call if the call was established before the failover occurred. If a call is not answered when the failover occurs, the connection is lost.  
  
  Workaround: The phones inside the Firewall Cluster need to register to the SIP proxy again after the cluster failover.

Only Active Directory security groups can be used in Firewall Access rules (#41267) | Currently only Active Directory security groups can be used as User Groups in Firewall Access rules. Active Directory organizational units cannot be used.

Built-in "Domain Users" Active Directory security group cannot be used in authentication (#54814) | The built-in "Domain Users" Microsoft Active Directory security group cannot be used as a User Group in authentication.  
  
  Workaround: Create another security group and add the users there.
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.