StoneGate Firewall/VPN

Release Notes for Version 5.3.6

Created: July 10, 2012
# Table of Contents

What's New ............................................................................................................................... 3
Features ..................................................................................................................................... 3
Enhancements ............................................................................................................................. 3
Fixes .......................................................................................................................................... 3
Changes ..................................................................................................................................... 4

System Requirements ............................................................................................................... 5
Stonesoft StoneGate Firewall/VPN Appliances ...................................................................... 5
Certified Intel Platforms ........................................................................................................... 5
Basic Hardware Requirements ................................................................................................. 5
Requirements for Virtual Node ................................................................................................. 6

Build Version ............................................................................................................................. 6
Product Binary Checksums ....................................................................................................... 6
Compatibility .............................................................................................................................. 6

Installation Instructions ............................................................................................................ 7
Upgrade Instructions .................................................................................................................. 7
Known Issues .............................................................................................................................. 8
What’s New

Features

No major new features are included in this maintenance version.

Enhancements

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply hardware monitoring</td>
<td>Stonesoft appliances that have two power supplies have now an appliance hardware monitoring item for power supplies.</td>
</tr>
<tr>
<td>Dynamic routing logs</td>
<td>Log messages from the Quagga routing suite are now delivered with firewall logs to the Log Server.</td>
</tr>
</tbody>
</table>

Fixes

Problems described in the table below have been fixed since StoneGate Firewall/VPN version 5.3.5. A workaround solution is presented for earlier versions where available.

<table>
<thead>
<tr>
<th>Synopsis</th>
<th>Description</th>
<th>Workaround for Previous Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall may incorrectly report lack of connectivity to BrightCloud servers (#61138)</td>
<td>In certain situations, the firewall may incorrectly report a lack of connectivity to BrightCloud servers. In such cases, the following logs can be seen: &quot;HTTP_BrightCloud-Service-Down&quot;</td>
<td>N/A</td>
</tr>
<tr>
<td>Anti-Spam processing errors with blacklists (#74189)</td>
<td>Automatic blacklisting and blacklist rules may lead to Anti-Spam processing errors. DNS blacklist filtering is not affected by this issue.</td>
<td>N/A</td>
</tr>
<tr>
<td>Policy installation may fail when Deep Inspection is enabled in a large policy (#77503)</td>
<td>Installation of a large policy may fail with a timeout when Deep Inspection is enabled in the policy.</td>
<td>Increase the &quot;Contact Node Timeout&quot; on the Advanced tab in the Firewall properties.</td>
</tr>
<tr>
<td>Some supported 3G modems may not always be detected (#79047)</td>
<td>Some supported 3G modems may not always be detected.</td>
<td>N/A</td>
</tr>
<tr>
<td>Connections dropped by session limiting in Inspection rules may be logged incorrectly (#80056)</td>
<td>When using session limiting in Inspection rules, connections that are dropped due to session limiting may be incorrectly logged with a &quot;Refused by inspection&quot; message.</td>
<td>N/A</td>
</tr>
<tr>
<td>Session limiting may incorrectly prevent connections (#80057)</td>
<td>In certain situations, the Firewall may keep already closed connections in the session limit buffer, causing new connections to be dropped.</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP POST/PUT request may be silently discarded when divided into several TCP packets (#81201)</td>
<td>An HTTP POST/PUT request may be silently discarded when the request is divided into several TCP packets.</td>
<td>N/A</td>
</tr>
<tr>
<td>Network traffic may get cut during policy installation when aggregated interfaces are used (#81630)</td>
<td>The Firewall may unnecessarily set aggregated interfaces down during policy installation when the network configuration is modified. Depending on the surrounding network, traffic may get cut before the links are negotiated up again.</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP connections may slow down when Application detection is used (#82222)</td>
<td>In certain situations, HTTP connections may slow down when Application detection is used.</td>
<td>N/A</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.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network driver in VMware virtual appliances</td>
<td>The use of multicast traffic or standby clustering with multicast clustering mode with version 5.3.0 or newer requires a vmxnet3 network driver. The vmxnet3 driver requires virtual appliance hardware version 7. If the virtual machine hardware version is something other than 7, the virtual machine must be reinstalled.</td>
</tr>
<tr>
<td>Dynamic routing software</td>
<td>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 <a href="https://my.stonesoft.com/support/document.do?product=StoneGate&amp;docid=6688">https://my.stonesoft.com/support/document.do?product=StoneGate&amp;docid=6688</a> for more details.</td>
</tr>
<tr>
<td>VPNs: End of Support for Legacy UDP Encapsulation</td>
<td>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 automatically removes any remaining references to the legacy UDP encapsulation method from your VPN configurations.</td>
</tr>
</tbody>
</table>
| 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 proper license is used. The images are named as follows:  
| 32-bit remote upgrade package | sg_engine_version.build_i386.zip |
| 32-bit installation CD image | sg_engine_version.build_i386.iso |
| 64-bit remote upgrade package | sg_engine_version.build_x86-64.zip |
| 64-bit installation CD image | sg_engine_version.build_x86-64.iso |

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 StoneGate Firewall/VPN Appliances

At the time of release, this software version is supported on the following Stonesoft appliances:

- SG-1100
- SG-4000L
- FW-310
- FW-315
- FW-1020e
- FW-1030
- FW-1050e
- FW-1060
- FW-1200e
- FW-5000
- FW-5000L
- FW-5100
- FW-5105
- SG-1301
- SG-3201
- SG-3205
- SG-5201
- SG-5205


StoneGate appliances support only the software architecture version (32-bit or 64-bit) that they are shipped with.

Certified Intel Platforms

Stonesoft has certified specific Intel-based platforms for the StoneGate Firewall/VPN gateway. The list of certified platforms can be found at http://www.stonesoft.com/en/products/fw/Software_Solutions.

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

Basic 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 (http://www.stonesoft.com/en/products/fw/Software_Solutions/certified_nics.html)
- VGA-compatible display and keyboard
Requirements for Virtual Node

- 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 StoneGate Firewall/VPN is run as a virtual node:

- Only Packet Dispatching CVI mode is supported.
- Only Standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

Build Version

The StoneGate Firewall/VPN version 5.3.6 build version is 9095.

Product Binary Checksums

sg_engine_5.3.6.9095_i386.iso
MD5SUM 105f8c229daa1328231acc5c40201aa9
SHA1SUM 9674bf376095baca5515caf5a6187cbda45e75c

sg_engine_5.3.6.9095_i386.zip
MD5SUM ef906d7dd869fc2bb475dd98fd1f3055
SHA1SUM 95f02c9ad19aac4a3a444109b5e069b2a32da779

sg_engine_5.3.6.9095_x86-64.iso
MD5SUM f7444cee63529cfbd3edeb83e182d8a6f
SHA1SUM d752dcd98a80f33454a2aec8d9d6ecbb5a672045

sg_engine_5.3.6.9095_x86-64.zip
MD5SUM b4234c0e7660d2e3ebc7212693f71081
SHA1SUM 5c9c594e7ec0f2bd1d939aab0266ea13ec6294f2

Compatibility

StoneGate Firewall/VPN version 5.3.6 is recommended to be used with the following StoneGate component versions:

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

The main installation steps for StoneGate Firewall/VPN 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. The Authentication Server and Web Portal Server(s) need to be installed if the optional Authentication Server and StoneGate 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** from the menu that opens.

4. If not using Stonesoft firewall appliances, install the firewall 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 firewall and selecting **Commands → Go Online** from the menu that opens.

The detailed installation instructions can be found in the *Management Center Installation Guide* and *Firewall/VPN Installation Guide*. For more information on using StoneGate, refer to the Online Help system or *StoneGate Administrator's Guide*. For background information on how the system works, consult the *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 5.3.6 is not supported from other versions.

StoneGate Firewall/VPN version 5.3.6 requires an updated license if upgrading from version 5.2.x or earlier. The license upgrade can be requested at our Web site at [https://my.stonesoft.com/managelicense.do](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** – StoneGate 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 under File Systems on the Firewall’s Appliance Status tab in the System Status view. If partition usage is over 95%, remove unnecessary files before upgrading. Disk usage can also be checked locally from the engine console with the command “df –h”.

# Known Issues

The current known issues of StoneGate Firewall/VPN version 5.3.6 are described in the table below. For an updated list of known issues, consult our Web site at [http://www.stonesoft.com/support/StoneGate/Known_Issues/](http://www.stonesoft.com/support/StoneGate/Known_Issues/).

<table>
<thead>
<tr>
<th>Synopsis</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall cannot renew its dynamic IP address (#17184)</td>
<td>When the firewall is configured with a dynamic IP address, the initial DHCP broadcast request is allowed implicitly. However, when the lease expires and the firewall tries to renew the lease, the unicast connection to the DHCP server is discarded. This may cause the firewall to get a new IP address every time when the lease expires because a new broadcast request is sent after the renew connection has failed.</td>
<td>Add the following rule to the firewall policy: Source: &quot;$DHCP Interface 1.IP&quot;, Destination: &quot;Any&quot;, Service: &quot;bootps&quot;, Action: &quot;Allow&quot;</td>
</tr>
<tr>
<td>Only one external proxy can be contacted with SIP over UDP (#17389)</td>
<td>If multiple different SIP proxies are contacted simultaneously from the same source IP address (e.g., an internal SIP proxy contacts different external proxies), only the first call works when static source NAT or no NAT is used and SIP protocol uses UDP transport.</td>
<td>Use dynamic source NAT for the SIP over UDP when there is a need to contact multiple different proxies at the same time.</td>
</tr>
<tr>
<td>A node with VLAN heartbeat may go offline after policy installation (#17554)</td>
<td>If the heartbeat is configured using a VLAN interface and an e1000 driver, one node of the cluster goes offline when a policy is installed.</td>
<td>Increase the heartbeat failover time to 7000 ms.</td>
</tr>
<tr>
<td>Inspection configuration contains firewall access rules as plain text on the engine (#22141)</td>
<td>Even if the &quot;Encrypt configuration data&quot; is checked in the firewall's properties, the access rules are stored as plain text with the inspection configuration. The rest of the configuration data is still encrypted.</td>
<td>N/A</td>
</tr>
<tr>
<td>SIP connections are lost in failover (#23073)</td>
<td>A SIP phone located outside the firewall cluster cannot make new calls to the internal SIP phones after a firewall node goes offline if the phones were registered to an external SIP proxy through that firewall node. Also, the external SIP phone cannot terminate an existing call either if the call was established before the failover occurred. Furthermore, if someone was making a call that had not been answered yet when the failover happened, the connection is lost.</td>
<td>The internal phones need to register to the SIP proxy again after the cluster failover.</td>
</tr>
<tr>
<td>Only Active Directory security groups can be used in firewall Access rules (#41267)</td>
<td>Currently only Active Directory security groups can be used as groups in Access rules. Active Directory organizational units cannot be used.</td>
<td>N/A</td>
</tr>
<tr>
<td>VPN monitoring for client-to-gateway VPNs shows status as unknown (#44991)</td>
<td>When there are no VPN client users connected, VPN monitoring for client-to-gateway VPNs shows the status as 'Unknown'.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Copyright and Disclaimer

© 2000—2012 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 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 StoneGate clustering technology—as well as other technologies included in StoneGate—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.