Table of Contents

What’s New ........................................................................................................................................ 3
System Requirements .......................................................................................................................... 4
Build Version ................................................................................................................................ 4
Product Binary Checksums ............................................................................................................... 4
Compatibility .................................................................................................................................. 4
IPsec Compliance ............................................................................................................................. 4
Installation and Upgrade Instructions .............................................................................................. 5
Known Issues .................................................................................................................................. 5
What’s New

Features

StoneGate IPsec VPN Client v4.2.3 contains no new features compared to v4.2.2. If you are upgrading from an earlier major version, consult the Release Notes for StoneGate IPsec VPN Client version 4.2.0 for important information on new features and changes since previous versions.

Enhancements

Enhancements that have been made since StoneGate IPsec VPN Client v4.2.2 are described in the table below.

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address used with virtual adapter is saved (#39638)</td>
<td>When VPN Client requests IP address for virtual adapter, it sends the MAC address of the interface that is used for VPN connection to the FW/VPN gateway. This MAC address is now saved to Windows registry first time the VPN connection is established and the same MAC address is used in future connections regardless of used interface in VPN Client machine. There is also a tool sgvmac.exe that can be used to change the selected address if needed.</td>
</tr>
</tbody>
</table>

Fixes

Problems described in the table below have been fixed since StoneGate IPsec VPN Client v4.2.2. 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>GUI may stop working (#39998)</td>
<td>IPSec VPN Client GUI may stop working when it handles long log messages.</td>
<td>Restart the GUI from Windows program menu item &quot;StoneGate IPsec VPN&quot;.</td>
</tr>
<tr>
<td>IPSec VPN Client 4.2 filters ARP packets with multicast MAC addresses (#40466)</td>
<td>IPSec VPN Client 4.2 filters ARP packets with multicast MAC addresses. Therefore any machine having IPSec VPN Client installed cannot communicate with or through those devices in local network that use multicast MAC address.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Changes Introduced in Previous Major Version

This section lists major changes that were introduced in StoneGate IPsec VPN Client v4.2.0 that may affect you if you are upgrading from a version prior to v4.2.0. This is not a full listing; see the Release Notes of each version for more details.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only software-based certificates can be used</td>
<td>The new version only supports user certificates that are loaded from files.</td>
</tr>
<tr>
<td>Client firewall is not included</td>
<td>Standard Windows firewall features must be enabled or a third party firewall product must be used to secure the client.</td>
</tr>
<tr>
<td>Windows domain logon is not supported</td>
<td>This version does not support integration with the Windows domain logon process.</td>
</tr>
<tr>
<td>Proprietary UDP encapsulation is replaced with NAT-T standard</td>
<td>When the VPN Client communicates through NAT devices, port 4500/UDP must be opened in addition to 500/UDP. Custom ports used by older StoneGate VPN Clients (2535/TCP and 2746/UDP) are not used by the VPN Client version 4.2.0 and newer.</td>
</tr>
<tr>
<td>Authentication Client is not included</td>
<td>The new VPN Client does not include the Authentication Client feature that was bundled with the older VPN Client. If the Authentication Client is needed, VPN Client version 2.6.2 can be installed on the same host if only the Authentication Client is installed.</td>
</tr>
<tr>
<td>DNS redirection feature is not included</td>
<td>DNS domain and name server information on the VPN Client Configuration tab of the VPN site properties is not used with the VPN Client version 4.2.0 and newer. Use the Virtual Adapter configuration to enable the client to use internal DNS servers automatically.</td>
</tr>
</tbody>
</table>
System Requirements

General Requirements

- Processor: Pentium 4 processor or higher recommended
- Hard disk space: 300 MB of free disk space
- Memory: 512 MB
- Mouse or other pointing device
- SVGA (800x600) display or higher
- IPv4 TCP/IP installed and configured

Operating Systems

- Windows XP 32-bit Professional or Home with Service Pack 2 or Service Pack 3
- Windows Vista 32-bit Enterprise, Business or Ultimate, no Service Pack or Service Pack 1

Build Version

The StoneGate IPsec VPN Client v4.2.3 build version is 1038.

Product Binary Checksums

<table>
<thead>
<tr>
<th>File Name</th>
<th>MD5SUM</th>
<th>SHA1SUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>StoneGate_IPsec_VPN_4.2.3.1038.exe</td>
<td>5e42996e71cbd88b90ee40965a1496d6</td>
<td>8531b17e5fb58c0725f2f2342d720ff96047a57b</td>
</tr>
<tr>
<td>StoneGate_IPsec_VPN_4.2.3.1038_with_NET2.0.exe</td>
<td>825c831f40bc03b7c0492c48b1ef31f4</td>
<td>ca0b624eacff6ba6f23f8b2c4846ee9a2a107b2c</td>
</tr>
</tbody>
</table>

Compatibility

StoneGate IPsec VPN Client v4.2.3 is compatible with StoneGate Firewall/VPN version 4.2.0 and later. StoneGate Management Center (SMC) version 4.2.1 or later is required.

IPsec Compliance

StoneGate IPsec VPN Client is compliant with the IPsec and IKEv1 standards. StoneGate IPsec VPN Client can only be used with a StoneGate Firewall/VPN gateway because of the proprietary automatic configuration methods.
Installation and Upgrade Instructions

The main installation steps for the StoneGate IPsec VPN Client are as follows:

1. If you are running a StoneGate VPN Client older than 4.2.0, uninstall that version.

2. Ensure you have administrator privileges (or on Vista, that UAC is enabled) and start the installation by running the setup file.
   - If you are installing on a Windows XP system that does not have the Microsoft .NET Framework version 2.0 or newer installed, select the installation package that also contains the .NET framework.
   - If the StoneGate IPsec VPN Client must be installed in silent mode, start the installer from the command line and add the options /s /v"/qn" to the command line.

3. Follow the on-screen instructions to complete the installation.

4. Connect to a gateway to get the configuration settings for the VPN Client.

The detailed installation instructions can be found in the StoneGate IPsec VPN Client User’s Guide. For more information on using StoneGate, refer to the Online Help system or the StoneGate Administrator’s Guide. For background information on how the StoneGate system works, consult the Reference Guide.

Known Issues

Currently there are no known issues in StoneGate IPsec VPN Client.
Copyright and Disclaimer

© 2000—2008 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.