StoneGate IPsec VPN Client

Release Notes for Version 5.0.0

Created: April 30, 2009
# 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 v5.0.0 contains the new features listed in the table below.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client security checks</td>
<td>IPSec VPN client can now perform a local security check based on the status of basic security software (as reported by Windows) and disallow the user from opening a VPN connection if basic security requirements are not met on the client computer.</td>
</tr>
<tr>
<td>Smartcard authentication</td>
<td>VPN client user can authenticate to a gateway using a certificate from external tokens such as smart cards.</td>
</tr>
<tr>
<td>Domain logon</td>
<td>On Windows Vista systems, users can establish a VPN connection before continuing their Windows logon sequence.</td>
</tr>
<tr>
<td>Additional supported algorithms</td>
<td>IPSec VPN client now supports the following additional settings: AES-GCM, AES XCBC-MAC, SHA-2, and Deflate compression.</td>
</tr>
<tr>
<td>Better configurability</td>
<td>Several additional configuration options have been added directly to the IPsec VPN client's Properties dialog (Advanced tab).</td>
</tr>
<tr>
<td>Reauthentication feature</td>
<td>The user can now check a timer that indicates the time when the user needs to reauthenticate and can manually launch reauthentication prematurely if the next authentication seems to be at an inconvenient time.</td>
</tr>
</tbody>
</table>

Fixes

Problems described in the table below have been fixed since StoneGate IPsec VPN client version 4.3.2. 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>VPN negotiation not automatically triggered when all traffic goes through VPN (#45923)</td>
<td>If the IPsec VPN client has a full tunnel configuration (the protected site is ANY network), VPN negotiation is not triggered automatically.</td>
<td>Connect to the VPN manually through the StoneGate IPsec VPN icon in the Windows taskbar.</td>
</tr>
<tr>
<td>IPv6 traffic does not work if VPN client is not in Disabled state (#47348)</td>
<td>With 4.3.1 and 4.3.2 VPN client versions, IPv6 traffic only works if the VPN client is in Disabled state. With older versions, IPv6 traffic does not work at all.</td>
<td>N/A</td>
</tr>
<tr>
<td>Full tunnel configuration does not work if default route metric is 1 (#48028)</td>
<td>Full tunnel configuration with virtual IP address for the VPN client does not work if the default route metric through the physical network adapter is 1. Some dialup adapters use metric 1 as the default value.</td>
<td>Increase the metric value for the problematic physical adapter or do not use full tunnel configuration.</td>
</tr>
<tr>
<td>Enabling virtual interface IP may fail if client machine has overlapping IP networks (#49888)</td>
<td>Enabling virtual interface IP may fail if the client machine has overlapping IP networks, for example, some virtual adapter's network overlaps with the physical NIC IP network.</td>
<td>N/A</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 32/64-bit versions, no Service Pack or Service Pack 1

Build Version

The StoneGate IPsec VPN client v5.0.0 build version is 2013.

Product Binary Checksums

<table>
<thead>
<tr>
<th>Product Name</th>
<th>MD5SUM</th>
<th>SHA1SUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>StoneGate_IPsec_VPN.msi</td>
<td>34f9c0b67419ceb02b0aefad4d298032</td>
<td>a6162ed93ec5ca655e14f289ca137c6ce0e3c340</td>
</tr>
<tr>
<td>StoneGate_IPsec_VPN_5.0.0.2013.exe</td>
<td>4c18fb78126e0a9311bfa1619c939fa4</td>
<td>feb31a3cc09a93cfae9eaa949d9ab6caca3a6e57</td>
</tr>
<tr>
<td>StoneGate_IPsec_VPN_5.0.0.2013_with_NET2.0.exe</td>
<td>0d89ca3f3ea3b6aad400c17d0f634</td>
<td>3d4a32b55093810e8f725f330b0daeeaaac6b360</td>
</tr>
</tbody>
</table>

Compatibility

StoneGate IPsec VPN client v5.0.0 is compatible with StoneGate Firewall/VPN version 4.2.0 and later. New algorithms are supported only with Firewall/VPN version 5.0.0 or newer. StoneGate Management Center (SMC) version 4.3.0 or later is required. SMC 5.0.0 or later is required when using client security checks.

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 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 Management Center Reference Guide and Firewall/VPN Reference Guide.

There have been reports that in some pre-installed Windows Vista systems the junctions to the C:\ProgramData folder have been set up erroneously. StoneGate IPsec VPN client must not be installed on these machines before correcting the junctions to point to the correct folder (C:\ProgramData).

Known Issues

There are currently no known issues for the StoneGate IPsec VPN client.
Copyright and Disclaimer

© 2000—2009 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.