STORMSHIELD NETWORK SECURITY
STORMSHIELD VPN CLIENT

RELEASE NOTES VERSION 6.30

English version

20 november 2015

Version

This Release Note details the features, improvements and fixes of the Stormshield Network VPN Client.

6.30 build 002	Features	Improvements	Bug fixing	
6.30 build 001	Features	Improvements	Bug fixing	
6.21 build 002			Bug fixing	
6.21 build 001		Improvements	Bug fixing	
6.20 build 006			Bug fixing	
6.20 build 005	Features	Improvements	Bug fixing	
6.20 build 001	Features	Improvements	Bug fixing	
6.12 build 001		Improvements	Bug fixing	
6.11 build 003		Improvements	Bug fixing	
6.10 build 014		Improvements	Bug fixing	
6.10 build 011	Features	Improvements	Bug fixing	Known issues
6.10 build 010	Features			
6.10 build 009	Features	Improvements	Bug fixing	Known issues
6.10 build 008			Bug fixing	Known issues
6.10 build 006	Features	Improvements	Bug fixing	Known issues
6.08 build 003			Bug fixing	
6.07 build 001			Bug fixing	
6.05 build 001	Features		Bug fixing	
6.04 build 001	Features		Bug fixing	
6.02 build 001	Features	Improvements	Bug fixing	Known issues
5.51 build 003		Improvements		
5.51 build 001	Features	Improvements	Bug fixing	Known issues
5.13 build 001		Improvements	Bug fixing	Known issues
5.10 build 009	Features	Improvements	Bug fixing	Known issues
5.06 build 004		Improvements	Bug fixing	
5.03 build 002		Improvements	Bug fixing	Known issues
5.00 build 025	Features	Improvements	Bug fixing	Known issues
4.71 build 001		Improvements	Bug fixing	
4.70 build 001	Features	Improvements	Bug fixing	

Stormshield Network VPN Client 6.30 build 002

Features, improvements and fixes since release 6.30.001

Features

- Ability to hide the activation window which normally appears at the end of a subscription period

Improvements

- DPD mechanism improvement
- Ercom smartcard management improved with SSL
- Improvement of the .ovpn files conversion (OpenVPN configuration)
- Security of the tunnel opening is improved : when the gateway CA is unknown, the tunnel doesn't open.

Bug Fixing

- SSL error "TLS handshake failure: No CA" fixed by improving the management of CA check.
- IKEv1 erratic freeze fixed
- Systray popup message for SSL tunnel fixed

Stormshield Network VPN Client 6.30 build 001

Features, improvements and fixes since release 6.21.002

Features

- Windows 10 full compatibility
- New Token interoperability with Feitian epass2003 and gemalto/axalto .net
- New Ercom CryptoSmart Micro SD support for IKEv1, IKEv2 and SSL
- New Xiring Pinpad support for IKEv2 and SSL.
- After a 1st installation, a tip is displayed over the taskbar icon in order to show the user how to use the VPN Client.
- Logs can now be enabled from the Console.

Improvements

- IKEv1 - DPD mechanism improvement: tunnel correctly closes on DPD failure and gateway renegotiation, DPD keeps on on network disconnection, DPD timers management is tuned.
- When a VPN Configuration is created with the Wizard, the default parameters are: DH Group = Auto and Aggressive Mode = TRUE (set)
- Smartcard management improvement

- Debug/Trace mode can be activated from any window/panel of the VPN Client (Configuration panel, connection panel or Console).
- Tunnel opening or closing process is stopped on IKE reset
- Compatibility between tunnel configured with VPN 5.5 and tunnel configured with VPN 6.2
- Integration of security update for OpenSSL (CVE-2015-0204, FREAK vulnerability fix)
- Windows IKEEXT cohabitation is correctly managed on Windows 8 / Windows 6.1 upgrade.

Bug Fixing

- Compatibility with 3rd party software such as firewall, anti-malware or antivirus
- BSOD/Conflict with 3rd party software
- Log files names are correctly updated on date changing.
- Launched in silent mode, the setup ended with a crash if a password greater than 15 characters was set in the command line. This bug is fixed.
- For a 2-DNS tunnel, the management of the second DNS is fixed.

Stormshield Network VPN Client 6.21 build 002

Features, improvements and fixes of release 6.21.001

Bug Fixing

- The wizard works when Client use only one protocol.

Stormshield Network VPN Client 6.21 build 001

Features, improvements and fixes of release 6.20.006

Improvements

- IKE tunnel closes more quickly on network disconnection.
- During a software update, the software activation can be processed within a VPN tunnel.
- Possibility to create a VPN configuration with multiple auth + EAP + certificate.
- (IKEv1) Phase1 closes (and can be re-open) as soon as the tunnel is closed by the gateway.
- VPN Client can open tunnels even if the Internet connection appears after it starts.
- (IKEv2) Local and Remote ID now display explicit "E-mail" instead "ID_RFC822_ADDRESS".

Bug Fixing

- (IKEv1) "Initial contact" is not sent anymore upon tunnel renegociation.
- Correct management of certificates containing an OID in the subject.

- Tunnel opening on traffic detection might not work after a restart of the VPN Client software.
- Cannot open an IKEv1 tunnel when switching from a network to another while VPN Client is running (on a workstation with two NICs)

Stormshield Network VPN Client 6.20 build 006

Features, improvements and fixes of release 6.20.005

Bug Fixing

- With Mode Config on IKEv1, Phase 2 establishment could fail.

Stormshield Network VPN Client 6.20 build 005

Features, improvements and fixes of release 6.20.001

Features

- New Certificate's OIDs supported.
- Support of nested tunnels between different protocols
- New Configuration Wizards for IKEv2 and SSL tunnels
- Support of the Ingenico "Leo" Pinpad
- Possibility of certificate injection via a command line option (online certificate injection)
- Support of Freebox compatibility

Improvements

- Dynamic display of Config Payload Mode informations for IKEV2/IPV6.
- IKEv2: Support of several Child SA per Initial SA.
- Improvement of token access speed.
- IKEv1: When the PIN code entry is canceled, the tunnel opening process is aborted.

Bug fixing

- DPD still working when "split tunneling" is enabled.
- IKEv1 "Automatic" mode works for Phase1 encryption when gateway reports AES.
- Modification of IKE port and NAT port (IKEv1 parameters) is fixed.
- Improvement of Token removal detection.

Stormshield Network VPN Client 6.20 build 001

Features, improvements and fixes of release 6.12.001

Features

- Smartcard roaming support for IKEv2.
- Handle IKEV2 multi-proposals in order to simplify tunnel setup.
- [SSL] Support of TCP mode for the transport.
- [IKEv2] Automatic switch to PKCS#11 when middleware doesn't work in CSP mode.

Improvements

- Allow to use a self-signed Root Certificate from Windows Certificate Store.
- USB Mode Confirmation popup only appears when required.

Bug fixing

- [IKEv2] Import certificate with "DC" RDN from Windows Store fixed.
- [IKEv2] VPN tunnel properly opens when Certificate received from the VPN gateway is the same as the user Certificate.
- [IKEv2] VPN tunnel properly opens even if no Remote Id has been specified in the VPN Client.
- Windows firewall configuration correctly restored on uninstall.
- [IKEv2] Gemalto PKCS#11 middleware now available.
- VPNConf synchro issue when using USB Mode and autostart tunnel.
- Autostart USB tunnel error "No thread found to handle IKE version 1 packet" fixed.
- [DualToken] Fix on multiple partition token (automatic extraction detection)

Stormshield Network VPN Client 6.12 build 001

Features, improvements and fixes of release 6.11.003

Improvements

- Support of TLS connection without user certificate.
- Prevent broadcast transfers to remote network.

Bug fixing

- Import or export VPN Configuration to or from a mapped drive fails.
- Packets with a payload smaller than 24 bytes are dropped in IPv6 VPN tunnel, causing issues for FTP.

- Incoming packets ending with .255 on port 4500 are not handled properly.
- 'TSocket message data type 0 could not be sent' error message preventing an IKEv1 VPN tunnel to open using an IPv6 IP address.
- VPN tunnel fails to open due to unknown OID from the Certificate (i.e. Object Identifier). Need to add 'GN' label for OID (i.e. Given Name).

Stormshield Network VPN Client 6.11 build 003

Features, improvements and fixes of release 6.10.014

Improvements

- Support of all 3 addressing modes i.e. host, subnet and IP address range with IKEv2 VPN tunnels.
- Certificate Authority (CA) might or might not be specified when importing a P12 certificate within an IKEv2 VPN tunnel configuration.
- IKEv2 VPN tunnel supports an empty Remote ID and it is considered as 'Accept any ID from remote' as it does in IKEv1 VPN tunnels.
- New default Algorithms for Auto selections.

Bug fixing

- Pre Shared Key can be saved with shortcut 'Crtl+S' without checking against the 'Confirm' field.

Stormshield Network VPN Client 6.10 build 014

Features, improvements and fixes of release 6.10.011

Improvements

- Various text strings and user interface improvements.

Bug fixing

- Error "disagreement on PFS" when configured with 'Auto' for PFS in IKEv1 Phase2 (gateway specific).

Stormshield Network VPN Client 6.10 build 011

Features, improvements and fixes of release 6.10.010

Features

- Disable SHA-384 choice, SSL and IPsec IKEv2 VPN tunnel.

Improvements

- Various user interface improvements.
- VPN tunnel opens faster when using a certificate on a PKCS#11 Smartcard or Token.
- All settings in the 'Security' tab are set to 'Auto' mode when creating a new SSL VPN tunnel.

Bug fixing

- The VPN Client might crash if import a VPN configuration file modified with wrong parameters for a VPN tunnel configured using IKEv1.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- A new network interface is not detected when it becomes up.

Known issues

Here is the list of known issues in this release. This replaces previous list of known issues for this major release. We are doing our utmost to fix them as soon as possible.

- The VPN Client virtual network interface appears in 'Unidentified network' list in Windows Control Panel (Network).
- Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- DPD continues after tunnel failure (IKEv1 only).

Stormshield Network VPN Client 6.10 build 010

Features, improvements and fixes of release 6.10.009

Improvements

- User interface improvement for IPsec IKEv2 & IKEv1 VPN configuration:
  - Root tree strings "IKE V1 Configuration" &"IKE V2 Configuration" might be truncated.

Stormshield Network VPN Client 6.10 build 009

Features, improvements and fixes of release 6.10.008

Features

- IP address can change during renegotiation with VPN tunnel using IKEv2.
- SSL disabled.

Improvements

- VPN tunnel IKEv2 and IPV6, replace mask with prefix length in the Child SA.
- New menu strings to create a Phase1 and Phase2 consistent between IKEv1 and IKEv2 now called 'New VPN Gateway' and 'New VPN Connection' accordingly.

Bug fixing

- VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv6 VPN tunnel is not opening properly.
- VPN tunnel configured with IKEv2 and IPv6 toward a VPN gateway configured with IPv4 VPN tunnel is not opening properly.
- 'View Certificate' button is not working properly with VPN tunnel using IKEv2, after saving the VPN configuration.
- 'New Phase1' and 'Paste Phase1' menu from root tree not working properly.
- VPN configuration with IKEv2 can be saved although Remote Gateway field is empty.
- IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration.
- VPN tunnel with IKEv2 CHILD SA negotiation in IKE AUTH exchange with Diffie-Hellman.
- VPN tunnel with IKEv2, user must click twice on EAP button to have password enabled.
- VPN tunnel with IKEv2, Pre Share Key is empty after saving the VPN Configuration.
- VPN tunnel with IKEv2, the local/remote ID type of ID set to null is not working properly.
- VPN tunnel with IKEv1, Auto for Phase 1 doesn't work.
- VPN tunnel with IKEv1, X-Auth login/password popup is not working properly.
- Change in configuration from IPv6 to IPv4 in VPN tunnel within IKEv2 Child SA is not detected.

- VPN tunnel configured with IKEv1 and IPv4 toward a VPN gateway configured with IPv4, has no traffic if PFS=None and without NAT-T in Phase 1.
- VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv4, has no traffic if PFS=None.
- New buttons in the Configuration Panel root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.
- Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- Config Payload information in VPN tunnel configured with IKEv2 not displayed properly when tunnel opens or closes.
- Timeout of 30sec to monitor VPN tunnel opening might too short in some circumstances like using USB Token with a certificate protected by PIN, or large number of packet rejections.
- Word 'Static' appears in the Configuration Panel tree root IKEv1, IKEv2 and SSL.
- Texts of protocol description displayed in the Configuration Panel tree for each protocol (i.e. SSL, IPsec IKEv1, IKEv2) are not corrects.
- New buttons in the Configuration Panel root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.

Known issues

- The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- DPD continues after tunnel failure (IKEv1 only).
- A new network interface is not detected when it becomes up. Workaround: quit and start the software.

Stormshield Network VPN Client 6.10 build 008

Features, improvements and fixes of release 6.10.006

Bug fixing

- VPN tunnel using IKEv2 opens only once when LocalId is not filled in with certificate subject.
- The type IKEV2_ID_FQDN as remote ID Type is not yet supported.
- Several text typos in Configuration Panel 'Child SA' or Phase2 tabs.
- Phase renegotiation, on VPN tunnel with IKEv1, uses port 500 again instead of port 4500.
- Shortcut Crtl+S doesn't save the remote sharing and Certificate store settings.
- Feature blocking traffic outside VPN Tunnel (i.e. Split tunneling) with IKEv2 and SSL VPN tunnels is not yet available.
- Notification FAILED_CP_REQUIRED with IKEv2 VPN tunnels received from the gateway closes the VPN tunnel unexpectedly.
- The 'Initial Contact' mechanism is not yet supported with IKEv2 VPN tunnels.
- VPN Configuration with IKEv2 and SSL is lost after transferring IPsec IKEv1 configuration to USB mode.
- Remote ID ID_DER_ASN1_DN received from the gateway is not checked properly.
- Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- SHA2 in 'Child SA' tab is not available yet with IKEv2 VPN tunnels.
- DNS/WINS manual setup is not yet supported with IKEv2 VPN tunnels.

Known issues

- The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- VPN tunnel with IKEv1 using SHA512 doesn't open properly.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).

- DPD continues after tunnel failure (IKEv1 only).
- Texts of protocol description displayed in the Configuration Panel tree for each protocol (i.e. SSL, IPsec IKEv1, IKEv2) are not corrects.
- Word 'Static' appears in the Configuration Panel tree root IKEv1, IKEv2 and SSL.
- New buttons in the Configuration Panel root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.

Stormshield Network VPN Client 6.10 build 006

Features, improvements and fixes of release 6.08.003

Features

- Support of IPv4 and IPv6 simultaneously
  - Ability to handle heterogeneous IPv4 and IPv6 networks on the LAN and WAN sides, either on corporate or user home networks. The feature 'Auto' (for IPv4/IPv6) enables to support those complex environments with IPsec (IKEv1/v2) or SSL VPN tunnels.
  - Ability to detect IPv4 or IPv6 network automatically for both IPsec and SSL VPN tunnels.
  - Ability to send IPv4 and IPv6 within the same tunnel.
- Support of IPsec and SSL/TLS simultaneously
  - Ability to open multiple SSL VPN tunnels with any VPN gateways supporting OpenVPN.
  - Introduction of two new user authentication mechanisms specific to SSL i.e. Mode TLS-Auth and Extra Login/Password.
  - Auto adaptive capabilities to adapt to the SSL gateway settings automatically, assuming the gateway support multi proposal mechanism. The IT manager can disable this feature and force his own settings.
  - Ability to define a redundant SSL gateway in case of unavailability of the primary SSL gateway.
  - Ability to open SSL VPN tunnel on detection of traffic to the remote network.
  - Ability to start automation via scripts before/after tunnel opens or closes.
  - Ability to start a desktop sharing session with a machine on remote network in one click.
  - Ability to add traffic compression.
  - Inherits all IPsec encryption and hash algorithms from TheGreenBow IPsec VPN client (e.g. SHA1, SHA2, ..).
- Support of IPsec with IKEv1 and IKEv2 simultaneously
  - Ability to open IKEv1 and IKEv2 VPN tunnels simultaneously.
  - Ability to define a redundant gateway in case of unavailability of the primary gateway.
  - IKEv2 introduces a new user authentication mechanism called EAP similar to X-Auth. The new user authentication mechanism EAP can be combined with Certificate (i.e. select multiple Auth support in your VPN tunnel configuration > 'IKEv2 Auth' > 'IKE SA' tab. EAP replaces X-Auth when using IKEv2 VPN tunnel.

  - Auto adaptive capabilities to adapt to the gateway settings automatically, assuming the gateway support multi proposal mechanism. The IT manager can disable this feature and force his own settings.
- Supported OS: Windows Server 2003 32-bit, Server 2008 32/64-bit, Server 2012 32/64-bit, Vista 32/64-bit, Seven 32/64-bit, Windows 8/8.1 32/64-bit. Stormshield Network VPN Client 6.0 and further do not support Windows XP.
- Supported languages (25 languages). Arabic, Chinese simplified, Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai and Turkish.

Improvements

- All logs are now tagged by protocol (i.e. IPsec vs SSL) with a new 'Facility' field.
- Ability to select a specific network interface by its name (i.e. as displayed in 'Control Panel' > 'Network and Internet' > 'Network Connections') instead of an IP address.
- All traces from console are now available in a text file with other logs when Trace/Debug mode is activated (i.e. Ctrl+Alt+D).
- Several improvements on the reliability.
- Names of virtual interface has been changed to be more meaningful (i.e. as displayed in the 'Control Panel' > 'Network and Internet' > 'Network Connections').

Bug fixing

- MiniPort driver uninstallation failure (i.e. error x023c) might occur when multiple upgrades from old releases.

Known issues

- The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- DNS/WINS manual setup is not yet supported with IKEv2 VPN tunnels. Work around would be to enter IP address of the target machine or use Config Payload mode (i.e. equivalent to Config Mode in IKEv1).
- Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2 vs. SSL).
- Split tunneling can not be disabled with IKEv2 and SSL VPN tunnels. All internet traffic remains authorized. However, a work around would be forcing all traffic in the tunnel via a VPN config (i.e. 0.0.0.0 in remote network address).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.

- Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels. Work around: set up a long time (e.g. 1 day) for 'IKE AUTH' and 'Child SA' Lifetime.
- IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration. Work around: Select your IP type for IDs (e.g. IP_IPv6_ADDR or IP_IPv4_ADDR) in 'IKE Advanced' tab > 'Identity' section and keep the value empty. For Config Payload mode, please proceed as follow in 'Child SA' tab:
  - Uncheck 'Request configuration from gateway'
  - Set VPN Client address to '0.0.0.0' (or '::' for IPv6)
  - Set Remote LAN Address to '0.0.0.0' (or '::' for IPv6)
  - Set Subnet Mask to '255.255.255.255' (or 'FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF' for IPv6)
  - Check 'Request configuration from gateway'
- SHA2 in 'Child SA' tab is not available yet with IKEv2 VPN tunnels.
- The type IKEV2_ID_FQDN as remote ID Type is not yet supported.
- The 'Initial Contact' mechanism is not yet supported with IKEv2 VPN tunnels.
- The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.

Stormshield Network VPN Client 6.08 build 003

Features, improvements and fixes of release 6.07.001

Bug fixing

- Reception of fragmented packets in reverse order is not working properly.
- Bad DPD handling when DPD reply from the gateway is lost, and the VPN Client resend a new DPD sequence.

Stormshield Network VPN Client 6.07 build 001

Features, improvements and fixes of release 6.05.001

Bug fixing

- IKE process (TgbIke) might crash when the IP address is changing.
- Packets with DF flag (i.e. Don't Fragment) are not handled properly in some specific circumstances.

Stormshield Network VPN Client 6.05 build 001

Features, improvements and fixes of release 6.04.001

Features

- Support of Windows 8.1 32/64-bit.

Bug fixing

- The button 'Add WINS' server stays enabled after VPN tunnel opens in Mode-Config.
- Alternate WINS server addresses are not applied to the Virtual Interface, and not showed in the VPN Client > 'Phase2 IPsec' > 'Advanced' tab after the VPN tunnel opens in Mode-Config.
- Wrong DNS server IP address format displayed after the VPN tunnel opens in Mode-Config.

Stormshield Network VPN Client 6.04 build 001

Features, improvements and fixes of release 6.02.001

Features

- Ability to enter a machine name instead of an IP address when adding a Remote Sharing entry (i.e. 'Phase2' > 'Remote Sharing').

Bug fixing

- One of the log files is not created. This log file is used by our tech support for debug (OEM partners specific).
- No connectivity to the DNS server when setting up an Alternative DNS in some very rare Windows configuration.
- Crash when using 'easyVPN' module in some circumstances. 'easyVPN' module allows to fetch a VPN Configuration on a VPN configuration server making VPN configuration update very easy for IT managers and users.
- License agreement is displayed in Spanish when choosing Italian during setup.

Stormshield Network VPN Client 6.02 build 001

Features, improvements and fixes of release 5.52.001

Features

- Support of IPv4 and IPv6 protocols.
- Support of Diffie-Hellman Group 15 (3072-bit), Group 16 (4096-bit), Group 17 (6144-bit), Group 18 (8192-bit).
- Support of 2 new SHA2 algorithm: SHA2-384, SHA2-512. The IPsec VPN Client now supports SHA256-96, SHA256-128, SHA2-384, SHA2-512.
- Support of multiple DNS servers (2) per VPN Tunnel. They can be configured manually or, received from the VPN gateway in Mode Config.
- Ability to add a DNS suffix to DNS server addresses.
- Ability to open a tunnel within another tunnel. This allows access your company network with a first gateway, and then access a second secured network within your company with a second gateway. Restriction: Mode Transport, and force all traffic in tunnel are not supported.
- Support of Windows Server 2008 32/64-bit, Windows Server 2012 32/64-bit, Windows Vista 32/64-bit, Windows Seven 32/64-bit, Windows 8 32/64-bit. Note: Windows XP is no longer supported, please download the previous release for Windows XP support.
- Support of 25 languages including English, Arabic, Chinese simplified, Czech, Danish, Dutch, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, Turkish.

Improvements

- Log files generated when user activate the Trace mode (Ctrl+Alt+D) are now deleted automatically if older than 10 days. Those files could become fairly big fairly quickly.
- More debug logs when user activates the Trace mode (Ctrl+Alt+D).
- Remove both buttons 'Apply' and 'Save' from the Configuration Panel. Save can be found in the menu 'Configuration' > 'Save', or Ctrl+S. Apply is automatic when the user clicks on 'Open tunnel'.
- When trying to upgrade to the latest release without Update Option, or if Update Option has expired (i.e. license to update to the latest release), the upgrade was previously blocked. Now, the user can choose to proceed or not (knowing that software activation might fail right after installation).

Bug fixing

- IKE port and NAT ports not updated correctly upon VPN Configuration changes by user.
- Unable to open tunnel (Phase 2 not completed) when forcing NAT-T in Transport Mode in the VPN Configuration.
- DIR command (FTP protocol) doesn't work when trying to access a FTP server within a VPN tunnel, in some network circumstances.

- No systray icon (taskbar) when Windows starts or after sleep mode, in some Windows configurations.
- Multiple Phase1 with the same remote gateway addresses would not work properly.
- 'Invalid Cookie' error message wrongfully displayed when SA expires during Phase1 renegotiation.
- VPN tunnel may not re-open right after closing when the VPN Gateway is originating the closing (originator of the last DELETE payload).
- Display of 'X-Auth warning' error message instead of 'Virtual Interface problem' when virtual interface issues detected.
- VPN tunnel may not open properly when the VPN gateway rejects the request with a NO_PROPOSAL_CHOSEN error (e.g. possible reasons are encryption algorithm not supported, ..).
- The icon 'tunnel opened' in the Configuration Panel tree might be displayed although VPN tunnel could not open in some cases where the computer opens the VPN tunnel really fast.
- Old value for SHA2 header size for compatibility with some gateways.
- Alternate DNS/WINS server addresses received via Mode Config are not immediately applied when opening tunnel in some circumstances.
- The PKI Options parameter called KeyUsage is not taken into account by the Setup option.
- Upgrade using silent install and setup installation options while the software is running might not complete properly.
- Tunnel closes unexpectingly after wakeup from Windows sleep.
- VPN tunnel does not open when Certificate received from the VPN Gateway contains a multi-valued subjectAltName field.
- Selecting 'Any' interface (Configuration Panel > 'Phase1' > 'Interface') doesn't choose the correct network interface in some Windows configuration with other applications using network interfaces.
- No VPN traffic when two Phase2 have the same IP address. Both VPN tunnel may have been configured this way or, when a VPN tunnel opens using Mode Config, then the VPN Client receives an IP address 10.10.10.100 (example) from the router while another VPN tunnel has been configured with the exact same IP address.
- No VPN traffic when opening a VPN tunnel on a network interface with multiple IP addresses.
- USB Token might not be detected if plugged in after the software started and the token was not used to create the VPN Configuration, even though the PKI option 'Use the first Token found on this computer' is checked.
- VPN tunnel is not closing automatically when a Gemalto Dual .NET Token configured in the VPN Configuration is unplugged.
- Crash when trying to import a localization file (i.e. strings in your language) if the file name is too long.
- Unable to open tunnel when configuring 8 VPN tunnels with virtual IP address all set to 0.0.0.0.

Known issues

- The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).

- In VPN Configuration with two VPN Tunnels with the same virtual IP address, DNS/WINS server address of the first VPN tunnel only is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.

Stormshield Network VPN Client 5.51 build 003

Features, improvements and fixes of release 5.51.001

Improvements

- Russian, Chinese language strings updated.

Stormshield Network VPN Client 5.51 build 001

Features, improvements and fixes of release 5.13.002

Features

- Support of Windows 8 32-64bit.
- Gina Mode supported on Windows Vista 32-64bit, Windows 7 32-64bit and Windows 8 32-64bit.
- Support of new Token ePass3003.
- Added a password confirmation field when exporting a VPN Configuration.
- ESP anti-replay service supported i.e. RFC 2401/4303.
- Added several command lines (and setup init file) to better choose Certificates from Token or SmartCard in VPN Configuration. They are called PKI Options. For more details, look at our deployment guide on our website. 'KeyUsage' allows limiting access only to 'Authentication' certificates from the Token or SmartCard. 'SmartCardRoaming' allows setting the rule used to fetch a Certificate from the Token or SmartCard. 'Pkcs11Only' allows limiting access only to 'PKCS#11' certificates from the Token or SmartCard. 'NoCaCertReq' allows using Certificate with different Certificate Authority the VPN Gateway is using. 'PKICheck' allows to force the VPN Client to check the Certificate Root Authority when receiving a Certification from the VPN gateway.
- The PKI Options are also manageable through the user interface via a new tab in the 'Tools' > 'Option…' window.
- Enable the IT manager to disable the Configuration Panel via registry key. When the specific registry key is set, the user cannot access the Configuration Panel.
- Exclusion of DHCP protocol from network filter to allow DHCP mechanism when network configuration forces everything in tunnel (0.0.0.0/0.0.0.0).
- Algorithms SHA2 is supported to sign with a CSP smart card.
- Remove 'buy' button.
- Korean and Farsi are now embedded as new languages, bringing to 25 the total number of languages.

- Ability to open the current User Certificate Store when selecting a Certificate in the configuration Panel, instead of the local machine Certificate Store.
- Gemalto .NET with CSP middleware supported on Windows Vista & Seven.
- Use VendorID (IKE) to restrict usage of the VPN Client to a specific gateway.
- Enable auto import of VPN configuration if a specific configuration file name is available in the installation folder.

Improvements

- New order to move the focus from one field to another with the tab key in the Configuration Panel > IPsec Phase 2 tab.
- Enable Russian for the user interface of the 'easyVPN' module.
- Do not display systray popup on Phase1/Phase2 renegotiation.
- Extended the size of SmartCard PIN code field to be able to enter longer PIN code.
- Ability to activate the software on Windows machine where system folders like MyDocuments or ProgramData might or might not be available.
- Ability to connect to Wifi hotspot with VPN Configuration forcing all traffic in the tunnel (i.e. subnet mask 0.0.0.0).
- The 'Lock Access to Config Panel' password popup doesn't have focus.
- Ctrl+Alt+T is now the shortcut for Trace mode.
- Minor cosmetic.

Bug fixing

- The 'easyVPN' module does not support windows 8.
- Once tunnel opened using Mode-Config, WINS value might be overwritten by DNS value.
- Unselect PKICheck might not be taken into account in some circumstances.
- A specific and large number of tunnel Phase 1 may crash the VPN Client in some circumstances.
- Error initializing IKE service.
- The online support and license purchase links does not work.
- Activated License quota is not reset after software uninstallation.
- BSOD when Windows is coming back from sleep mode (Windows XP only).
- Gina Mode (open tunnel before windows logon) not working.
- Finnish and Danish language typo in the Software Activation window.
- VPN tunnel might not open when another IPsec service is enabled on the machine, as port 500 and/or 4500 are used.
- VPN tunnel re-connection fails with some gateways because INITIAL-CONTACT was not sent.
- Debug log generation fails if software installation folder is changed by user during install.
- Phase1 Renegotiation fails when initiated by a StrongSwan gateway type.
- Silent uninstallation doesn't launch upgrade.
- VPN Client 'Start Mode' should be 'Manual' instead of 'After Windows logon' in Windows Seven 64bit.

- The VPN Client cannot open a tunnel when using a Certificate with Unicode or UTF8 characters like Japanese characters.
- PKCS#11 middleware used instead of CSP middleware when SmartCardRoaming Option is set to either 2, 3, 4 or 5.
- No wrong PIN code popup when using Smart Card with CSP middleware.
- Alternate DNS/WINS are not applied if tunnel open when enabling 'Auto open this tunnel on traffic detection'.
- In Gina mode and 'Open tunnel' with Alternate DNS/WINS, the DNS/WINS are applied to Local Interface instead of Virtual Interface.
- Packet fragmentation not properly performed when modifying MTU size (some values) on Windows XP.
- Software upgrade fails when using silent mode "/S".
- Impossible to open with certificate when user does not have admin right.
- VPN Client not responding after received Key renewal from router.
- Wrong Finnish translation in Software Activation window.
- No tunnel when using SHA2 algorithm and Windows Certificate Store.
- Another tunnel does not open properly after unplugging a smartcard with some smartcard models.
- Crash IKE in some network circumstances when coming out of sleep mode, or when tunnel fails to open on 'Wrong Remote Address' followed by 'Save' VPN Configuration.
- Remote Config feature creates logs in the wrong directory.
- Activation not properly working in some circumstances like multiple user levels on the same machine.
- Accept the Section ID in VPN Configuration file coming from the VPN Gateway when virtual IP address is set to 0.0.0.0.
- Support VPN configuration coming from the VPN gateway containing '-' in the tunnel names and also when using configuration with certificates.
- IKE crash when Phase name is too long. Phase names now limited to 49 chars.
- The feature VPN "Peer to Peer" might fail when there is a router with NAT-T in between, in some network configuration.
- VPN tunnel might not open when configured with a Certificate selected from the User Certificate Store.
- The VPN tunnel opens properly but no traffic goes through when using X-Auth based configuration and VPN Client address is 0.0.0.0.
- VPN Client stops responding for a while after received Key Renewal from the VPN Router in some VPN Configuration circumstances.
- IP address renewal with DHCP server does not working properly with VPN Configuration forcing all traffic in the tunnel (i.e. subnet mask 0.0.0.0).
- Import of VPN Configuration not working properly when the Certificate has a local ID type DER_ASN1_DN_ID containing a subject with chars like spaces and "/".
- 'Phase2' > 'Advanced' > 'Alternate Server' > IP addresses cannot be reset to 0.0.0.0.
- Cannot create a VPN Configuration via the Configuration Panel.

Known issues

- Several Certificates with same Subject added to the Windows Certificate Store might prevent a tunnel to open in some circumstances.
- The VPN Client might be able to open tunnel under RDP sessions in some circumstances.
- Windows might not recognize setup software signature when installing the software for the first time although signature is provided, Windows Vista only.
- The VPN Client virtual network interface appears in "Unidentfied network" list in Windows Control Panel (Network).

Stormshield Network VPN Client 5.13 build 001

Features, improvements and fixes of release 5.10.009

Improvements

- Clarification of the rules to select which Certificates to take into account when available via Token, Smartcard Reader.
- Speedup display of systray menu when 100+ VPN tunnels configured.
- Log file name format changed to include date/time. This allows smaller file size when sending logs to techsupport.
- Gina/Credential Provider (i.e. Open VPN tunnel before Windows logon) now customized.

Bug fixing

- VPN tunnel send Certificate Request with DN from a specific Certificate Authority only. However some VPN Gateway might use other CA.
- VPN Client can now send INITIAL-CONTACT message during IKE negotiation.
- Console stops displaying logs after clicking on menu Tools > Reset IKE.
- Some 3G USB drives from Orange (e.g. 3G Business Everywhere) are changing routing settings preventing VPN traffic to go through especially when configuring the VPN Client to force all traffic in VPN tunnel.
- A second VPN Client popup show up when coming back from sleep prior to Windows login if Gina mode (i.e. opening VPN tunnel before Windows logon) has been configured.
- Wrong IKE timestamp format in console.
- VPN tunnel might not re-open properly when using 3G connexion especially if a new IP address is re-assigned by the mobile network.
- When a tunnel is using Config Mode, Phase 2 renegotiation does not use the settings sent by the gateway, but the parameters from the configuration file, therefore preventing from opening the VPN tunnel.
- VPN tunnel might not open properly when using PKCS#11 Certificate and multiple certificate with the same subject on a single smart card.
- VPN tunnel might not open properly when importing a VPN Configuration containing a smart card. The message "conf_x509_subject_set: error while using PKCS#11 middleware" displays.
- Payload CERT_REQ not send properly in some circumstances.

- VPN tunnel might not open properly when coming back from windows sleep mode.
- VPN tunnel configured with IP Address Range might not open properly.
- DNS/WINS addresses might not be restored properly when using Gina Mode (i.e. opening VPN tunnel before Windows logon).
- DNS/WINS addresses might not be configured properly when VPN Client Address (remote IP address is configured to 0.0.0.0).
- Computer freeze in rare case of VPN Configuration using Certificates i.e. Windows Seven 64-bit on some Dell machines.
- Traffic remains blocked when "Disable Split Tunneling" is selected and the VPN Client IP address (i.e. remote IP address of the computer) selected already exists on the computer.
- Traffic might be slower when all traffic forced into tunnel (remote mask is 0.0.0.0) and using IE or Firefox.
- The tunnel might not open properly, when the remote gateway is sending a large Certificate (e.g. key size of 2048-bit).
- MTU modification might not be taken in account (Windows XP 32-bit only).
- VPN tunnel doesn't open with 'Error 307' when the remote network mask contains specific values (e.g. 255.255.254.0, 255.255.252.0,...).
- No smartcard PIN code popup when a special sequence of events occurs, like plugging in the smartcard, then VPN tunnel fails to open (e.g. router not responding), then plugging in again the smartcard.
- VPN Configuration Wizard does not start when software starts and VPN Configuration is empty.
- Remove menu "Close All Tunnels".

Known issues

Here is the list of known issues in this release. This replaces previous list of known issues for this major release. We are doing our utmost to fix them asap.

- No Gina (aka. Open tunnel before Windows logon) on Windows 64-bit (Vista and Seven). Gina connection panel (before Windows logon) may appear with 5-8sec delay on Windows XP.
- Wireshark must be installed after the VPN Client software to be able to scan its interfaces.
- Exporting a VPN configuration to a mapped drive is not possible. No error message but the file is not exported. A work around would be to export to the local disk, and then copy to the mapped drive.

Stormshield Network VPN Client 5.10 build 009

Features, improvements and fixes of release 5.06.004

Features

- Ability to support SIP/VoIP traffic in VPN Tunnel (Window Vista and Seven).
- Ability to open a Windows RDP session in one click from systray menu. This allows the user to open a remote desktop sharing with any machine on the remote network. Multiple desktop sharing sessions per VPN tunnel can be defined, and the right VPN tunnel opens automatically when a desktop sharing session is requested.

- Ability to execute a silent un- installation when the software was installed with silent installation configuration.
- Ability to set a specific MTU per IPSEC tunnels.
- Added a checkbox to run the IPsec VPN Client after software installation.

Improvements

- Ability to install the software without rebooting Windows operating system.
- Ability to disable the systray popup window that shows up when opening or closing VPN tunnel.
- Ability to close all tunnels in one click. New menu item in the Configuration Panel.
- Show a little USB Icon in Configuration Panel whenever an USB drive is plugged in and the software is in USB Mode (i.e. expecting the USB drive to hold the VPN configuration).
- Each VPN tunnel Phase1 & Phase2 names now appear in the systray menu.
- All VPN tunnel names are sorted by alphabetical order in the systray menu.
- The stability of the IP address change detection has been significantly improved.
- The stability of the DNS/WINS management has been significantly improved.
- The time to quit has been significantly improved.
- The management of Token insertion and extraction has been significantly improved. Upon insertion or extraction, all VPN tunnels are opened or closed accordingly.
- Ctrl+Alt+D starts the debug logs, and now also add an icon with a link to the log folder.
- IKE logs are now timestamps with daily span to reduce log files sent to techsupport.
- More help added for Hybrid Mode. Hybrid Mode requires a Certificate and X-Auth to be set to function properly.
- Warning info when using an USB drive VPN configuration in case the USB drive was not supposed to be plugged in.
- A 'Don't warn me anymore' checkbox added in warning popup when the VPN Client address belongs to the remote network configured in 'Remote LAN Address'.
- 'Block non-ciphered connections' has been replaced by 'Disable Split tunneling'.
- Support of Token containing multiple certificates with the same certificate subject.
- Added Certificate validity date check before opening a tunnel. If multiple Certificates, the VPN Client only uses the Certificate with a valid date. If no certificate with valid date can be found, the tunnel does not open, and an error message 'no suitable certificate' displays in the console.

Bug fixing

- All VPN tunnel Phase2 do not close when unplugging the smartcard used to authenticate.
- VPN tunnel cannot be opened coming back from Windows Sleep mode.
- Too many errors shown in systray popup window when opening VPN tunnel in some network circumstances.
- Once in USB Mode, the sub-menu 'Move to USB drive' is still enabled.
- OSAport not supported in vpnconf.ini
- Error message when launching help using 'F1'.

- Software crashes when entering into the USB Mode for the first time in some Windows configurations.
- All leds are green although the IPsec VPN Client is 'giving up' after several attempts to open a VPN tunnel.
- Export of a VPN Configuration can be empty in USB Mode (i.e. VPN configuration has been moved to the USB drive).
- A message 'INVALID COOKIE' received while the VPN tunnel is open might make the systray popup window to show up with orange led instead of green.
- A special icon is displayed in the Configuration Panel tree when 'Auto open on traffic detection' is selected.
- The char '\' should not be allowed in PreShared Key confirmation field.
- Remote LAN address and subnet field are empty after importing a configuration with 'Remote LAN Address' and 'subnet' 0.0.0.0/0.
- Manual activation fails with an Activation error message: 0 in some circumstances.
- Software crashes when numerous clicks on 'Apply' button.
- Tunnel with certificates cannot be opened when using Phase 1 ID with FQDN.
- Setup command option "--GuiDefs" not working properly.
- Silent installation not working properly when used with options "--license", "--activmail", "--noactiv", "--autoactiv", "--guidefs".
- Software crashes when copy&paste an existing VPN tunnel, and then trying to delete it in Configuration Panel.
- Wrong activation code file might be used if multiple users try to activate the IPsec VPN Client on the same machine.
- TgbIke crash when using with smartcard while debug logs are activated and a connection error occurs.

Known issues

Here is the list of known issues in this release. This replaces previous list of known issues for this major release. We are doing our utmost to fix them asap.

- After a Windows session lock/unlock, it may be impossible to open a tunnel, save or apply configuration. A work around is to restart the VPN Client software.
- No Gina (aka. Open tunnel before Windows logon) on Windows 64-bit (Vista and Seven).
- After a Windows session logoff/logon with Gina, Internet connection might be impossible due to DNS/WINS address not restored properly. Switching from one user to another may cause the IPsec VPN client not to function properly. A work around is to restart the VPN Client software.
- System error when coming back from Windows sleep mode. A work around is to restart the VPN Client software.
- Wireshark must be installed after the VPN Client software to be able to scan its interfaces.
- Exporting a VPN configuration to a mapped drive is not possible. No error message but the file is not exported. A work around would be to export to the local disk, and then copy to the mapped drive.

Stormshield Network VPN Client 5.06 build 004

Features, improvements and fixes of release 5.03.002

Improvements

- Login X-Auth accepts more than 31 characters.
- Removed restriction on SHA2 256 & DH14 for one of our partners.
- Ability to increase hash from 96bit to 128bit when using SHA-256.
- For RFC compliancy, SHA2-256 becomes SHA-256.

Bug fixing

- Combination of SHA2 & DES or 3DES is not working.
- Access denied error when launching the IPsec VPN Client through an RDP remote connection.
- 'Open' tunnel button & menu stays disabled even if tunnel failed to open when user enter wrong X-Auth login/password in popup.
- X-Auth popup cannot be saved until the user erases login/password fields.
- Tunnel negotiation fails with error "exchange_validate failed" when 'Remote LAN Address' and 'Mask' are 0.0.0.0/0.
- IKE service crash when coming back from Windows Hibernate or Sleep mode.
- TgbStarter.exe might crash when updating the VPN Configuration in some circumstances.

Stormshield Network VPN Client 5.03 build 002

Features, improvements and fixes of release 5.00.025

Improvements

- Support of 3G modem Sony Ericsson MD300, Huawei E1756 and E1553.
- Compliance release number of one of our partners.

Bug fixing

- Version of tgbgina.dll not found in the 'About' window.
- Alternate DNS & WINS not working on 3G connection using 3G Huawei E1756 and E1553 on Windows 7 or XP.
- Proxy configuration feature for software activation not available following an activation timeout (i.e. activation server or network not available).
- The option 'Start VPN Client after Windows logon' cannot be disabled on Windows 64-bit editions.
- Link to more info on error 33 not working properly when Software Activation after evaluation period expiration.
- Software un-installation might leave the 'IPsec VPN Client' un-install shortcut.

- 'Activation Error 70, Can't activate software' due to various naming of the 'Application Data' folder mainly in Windows XP but not only.
- Script before closing tunnel might not be executed, and DNS/WINS might not be restored properly in a complex scenario where alternate DNS/WINS have been configured (no Mode-Config), tunnels have been opened triggering some scripts, and the user is plugging in an USB drive containing another VPN Configuration.
- Activation Wizard in '?' menu doesn't become disabled after software activation.
- The VPN Configuration is not loaded from an USB Drive if already plugged in before the IPsec VPN Client software started.
- Phase 2 Advanced option "Automatically open this tunnel when USB stick is inserted" might not work in some Windows configuration because USB drive not detected.
- Importing VPN Configurations with Certificates in IPsec VPN Client 5.0 from a VPN Client 4.7 might prevent from opening a tunnel. The field 'Name' is not properly parsed.
- Keyboard stroke 'Del' (Delete) is not supported in the new language translator editor.
- Windows IP stack may crash when forcing high fragmentation of IP packets beyond 10 fragments. Now, max number of fragments supported.
- In case the local IP address retrieved from an imported VPN Configuration does not exist the local machine, the field 'Interface' is not forced to 'Any'.

Known issues

- Here is the list of known issues in this release. This replaces previous list of known issues for this major release. We are doing our utmost to fix them asap.
- Some setup command line options may not work correctly during a silent install.
- After a Windows session lock/unlock, it may be impossible to open a tunnel, save or apply configuration. A work around is to restart the VPN Client software.
- No Gina (aka. Open tunnel before Windows logon) on Windows 64-bit (Vista and Seven). Gina connection panel (before Windows logon) may appear with 5-8sec delay on Windows XP. The Gina connection panel does not display when computer is 'locked' on Windows Seven only.
- Changing from a 'left to right' language to a 'right to left' language (or vice-versa) might not take effect. A work around would be to quit the software and restart.
- Exporting a VPN configuration to a mapped drive is not possible. No error message but the file is not exported.
- In USB Mode, exporting a protected VPN Configuration creates a wrong configuration file.

Note: Debug mode (Ctrl+Alt+D) creates fairly large trace logs, fairly quickly. Don't forget to disable the debug mode or to regularly delete logfiles.

Stormshield Network VPN Client 5.00 build 025

Features, improvements and fixes of release 4.70.001

Features

- New graphical user interface to provide easier user experience. Among major changes are a simpler top menu, smaller and clearer Connection Panel, less buttons and more tabs in

Configuration Panel. Install this new release and give us feedback.

- Language can be changed on the fly, and all the strings can be modified from the software. This allows our partners to localize any strings and see the changes in one click.
- Support of 2 new languages Hungarian and Norwegian for a total of 23 languages.
- Automatically sort VPN tunnels by name.
- Display virtual IP address sent by gateway when "Mode-Config" feature is set.
- Add "Purchase licenses online" link under '?' menu.
- Command line option /pwd (password) must be specified when using command line option /export.
- New setup option --reboot=1 to reboot automatically after silent installation.
- DNS/WINS server addresses received from remote gateway are now displayed in 'Phase2' > 'Advanced'. In case Mode-Config feature is enabled, both fields are disabled to prevent manual settings but DNS/WINS server addresses are displayed anyway.
- Display the amount of data encrypted per VPN tunnel in Connection Panel.
- DPD can now be disabled with a checkbox added in 'Global Parameters' > 'DPD'.

Improvements

- 'Phase1' > 'Certificate' tab now shows all Tokens/SmartCard Readers configured, not those plugged in. And a warning message pops up when the certificate cannot be read on the Token/SmartCard Reader (not plugged in, card not in the reader,..).
- No more need to be administrator user to activate IPsec VPN Client software.
- Single field to enter the license number whether it is 20 or 24 digits long.
- VPN Client virtual IP address and DNS/WINS fields are disabled when 'Mode-Config' is selected.
- Script fields are now disabled when 'Enable before Windows login' is selected.
- More information and clearer messages on Software Activation errors.
- If a VPN tunnel closes because the computer has changed its IP address, the VPN tunnel does not re-open automatically once the network is available again (unplug IP cable, wireless network IP@ changes,..).
- X-Auth Authentication Type 'OTP' now supported (i.e. http://tools.ietf.org/html/draft-beaulieu-ike-xauth-02, section 6.3). If VPN gateway supports it and requests it, the IPsec VPN Client will ask the user for X-Auth authentication for each key renegotiation (timeout).
- X-Auth Authentication Type 'CHAP' now supported (i.e. http://tools.ietf.org/html/draft-beaulieu-ike-xauth-02, section 6.3). Used by the VPN Gateway, if supported, to pass through the X-Auth login/password to AAA Authentication server (Radius,..).
- Software is getting 25% smaller.

Bug fixing

- CHAP Radius X-Auth doesn't work when login & password are embedded in configuration file.
- X509 Certificate parser assumes that serial number in Certificate is mandatory and rejects certificates without serial number (e.g. coming from USB Tokens). X509 standard ETSI TS 102 280 doesn't specifies that the serial number field is mandatory in Certificates.

- IPsec VPN Client Mode-Config feature does not take into account mask value provided by the VPN gateway but uses a default mask (i.e. RFC2408 A.4 ISAKMP Identification Type Values).
- X-Auth Authentication Type in a reply to the VPN Gateway is not identical to the X-Auth Authentication Type received in the request from the VPN gateway. It must be identical.
- DNS Windows network setting is set back to static when VPN tunnel closes, although it was set to dynamic before opening the VPN tunnel. This may occurs on some Windows versions as the inet_addr system function used doesn't have the same behavior on all Windows versions.
- Software un-installation might not remove NDIS filter drivers properly which might disable network adapters.
- 'Phase2' > IP addresses were a mandatory fields even when 'Mode-Config' was selected.
- Un-installation deletes all program shortcuts, if different installation path than Program File (system folder). From techsupport feedback [TGB#10005492]
- Entering a 20 digits license number in Windows XP is not working anymore.
- DNS address not restored properly after closing a VPN tunnel as a consequence of un-plugging the USB drive with VPN configuration on it (aka USB Mode) while that VPN tunnel was opened.
- VPN Client stops working after entering smartcard PIN code larger than 10 digits. From techsupport feedback [TGB#1068241].
- Opening a tunnel triggers some systray popup messages about another VPN tunnel when using multiple VPN tunnels configuration. From techsupport feedback [TGB#1074282] [TGB#1078470] [TGB#1078665]
- Receiving a message with unknown SA may trigger a systray popup message repeatedly.
- Impossible to import VPN Configuration file from a network drive on some Windows network configuration. From techsupport feedback [TGB#1078968].
- Command line option "/export" doesn't export if the VPN Client software is already running.
- VPN tunnel status in Configuration Panel (led in configuration tree) might not be updated to 'Tunnel opened' in some circumstances. The Connection Panel tunnel status are properly updated.
- The feature 'Launch this script after the tunnel is closed' might launch the script too early in case the user quits the software, which in turn forces all opened tunnels to close.
- The feature that prohibits users to access the Configuration Panel (menu 'Options' > 'Configuration' > enter a password) should also prohibit the ability to import via command line using 'vpnconf.exe /import', or '/replace'. From techsupport feedback [TGB#1065029].
- Selecting the 'Desktop' folder in the Windows 'browse' panel (e.g. when trying to import a configuration file) might cause an error, on Windows Vista.
- Execution of command line options vpnconf.exe /close:tunnel1 and /open:tunnel1 opens the Configuration Panel. Configuration will remain closed, only systray popup messages will appear.
- Upon response from gateway of failure to authenticate the user, the IPsec VPN retries automatically several times. Auto retry upon wrong parameter has been disabled, and popup to the user to enter his credential again.

- TheGreenBow Gina library (i.e. Connection Panel windows before logon) does not find all necessary system resources which might prevent user from login, which may forces the user to login in safe mode. Problem occurs, on all Windows XP in some VMware (without VMware 'Tools'), and some strip down versions of Windows XP (not up to date with all service packs) and only if a tunnel feature 'Windows before logon' have been selected.
- Phase1' > 'Certificate' contains a string called 'TheGreenBow Configuration File'.

Known issues

Here is the list of known issues in this release. We are doing our utmost to fix them asap.

- Click on 'Save' before click on 'Quit' software, in case of VPN configuration has been modified. If not done so, connections with IKE module might be possible next time the software starts.
- Click on 'Save' while tunnels are opened might prevent DNS/WINS server address to be restored properly. A work around would be to close all tunnels before saving the VPN Configuration.
- No Gina connection panel (aka. Open tunnel before Windows logon) on Windows 64-bit (Vista and Seven). Gina connection panel may appear with 5-8sec delay on Windows XP. The Gina connection panel does not display when computer is 'locked' on Windows Seven only. Gina Connection Panel displays only 1 tunnel (if multiple configured in Configuration Panel).
- Importing VPN Configurations with Certificates in IPsec VPN Client 5.0 from a VPN Client 4.7 might prevent from opening a tunnel. A work around would be to only import the Certificates itself in IPsec VPN Client 5.0.
- Changing from a 'left to right' language to a 'right to left' language (or vice-versa) might not take effect. A work around would be to quit the software and restart.
- The Phase 2 Advanced option "Automatically open this tunnel when USB stick is inserted" might not work in some Windows configuration because USB drive not detected.
- Exporting a VPN configuration to a mapped drive is not possible. No error message but the file is not exported.
- Keyboard stroke 'Del' (Delete) is not supported in the new language translator editor.
- Note: Debug mode (Ctrl+Alt+D) creates fairly large trace logs, fairly quickly. Don't forget to disable the debug mode.

Stormshield Network VPN Client 4.71 build 001

Features, improvements and fixes since release 4.70.001

Improvements

- Display more info from Mode-Config feature (DNS, WINS) in the Console.

Bug fixing

- Initial DNS, WINS server addresses might not be restored in some circumstances like unplugging LAN cable with an opened VPN tunnel using Mode-Config.

- Secondary DNS, WINS server addresses provided by the gateway Mode-Config feature might disable IPsec VPN Client Mode-Config feature, especially if those DNS, WINS server addresses are empty. They are now ignored.

Stormshield Network VPN Client 4.70 build 001

Features, improvements and fixes since release 4.65.003

Features

- Support 2 new languages Czech and Danish for a total of 21 languages. Czech and Danish now embedded in the software setup.
- Support of new WWAN driver model for 3G/4G devices on Windows 7 (Windows Seven 32/64bit). With this new software release any WWAN compatible adapter should be working fine. WWAN stands for Wireless Wide Area Network or Wireless WAN, and is now supported by several 3G/4G wireless modem/adapter manufacturers. All manufactures must support “Mobile Broadband Driver Model Specification” for Windows 7 based on NDIS6.20 miniport driver model. Among those adapters, we do support now Atheros Wireless Adapter, Dell Wireless 5530 HSDPA Mini-Card, Dell Wireless 5600 EVDO-HSPA Mini-Card, Huawei 3G modem, Qualcomm Gobi 2000, Sierra wireless MC8781 HSPDA.
- Windows firewall rules auto setup extended to 'public' and 'domain' profiles.
- Configuration file now encrypted during software upgrade. If ‘GUI Access’ password has been setup, or a password is set in setup command line, they will be used (i.e. ‘View’ > ‘Configuration’ > ‘GUI Access’ or see Deployment Guide).

Improvements

- Ability to copy&paste the license number from the ‘About..’ windows, so it can be sent easily to our techsupport.
- Change in user interface of the Phase2 panel around the “Certificates Management..” button.
- Temporary installation folder for drivers in Windows 7 64-bit shall not had restricted access rights. It doesn’t matter now.
- RFC defines port 4500 UDP for key renegotiation. Port 500 now is allowed.
- Command line /export and /exportonce always requires /pwd:[password] now to export VPN Configuration.

Bug fixing

- Embedded pre-configured VPN Configuration file into the setup might not work properly (see Deployment Guide section ‘How to embed a specific VPN configuration into the VPN Client Setup?’).
- No retransmit of Phase2 request when the remote gateway does not answer.
- When a remote gateway is not responding, the IPsec VPN Client does not switch to a redundant gateway. This does not occur if another tunnel is opened.
- IKE engine might not be listening anymore in some cases of message exchanges with the VPN gateway e.g. timeout on no response (or lost) from the VPN Gateway.

- Default mask in VPN Configuration Wizard shall be set to class C.
- DNS/WINS server address not removed from Windows network settings on Windows 7 Ultimate using WiFi connection.
- Multiple Mode-Config messages received with DNS/WINS server addresses to be updated might not work properly.
- Phase2 ESP mode might still be 'Tunnel' mode although 'Transport' mode has been selected with some VPN gateways.
- Command line to replace a configuration file protected with password (e.g. /replace:c:\test.tgb /pwd:test) might erase current configuration if wrong password. Command lines to /add or /importonce are not affected.
- Command lines ("vpnconf.exe /import:[filename]") might not be executed properly.
- Events not logged in 'Console' when opening/closing tunnel before Windows logon (for Gina mode go to 'Phase2 Advanced' > 'Enable before Windows logon')
- Software activation may not work properly in case Windows default temporary folder is restricted to the user.
- Bluescreen when leaving sleep mode in Windows 7 64-bit.
- Special characters in Phase1 or Phase2 names could crash when software starts.
- Popup shows continuously "Remaining tunnel" after tunnel closed, due to erroneous cookie in 'INVALID COOKIE' notification message (i.e. RFC2522)
- Limitation in length of all parameters to avoid buffer overflow. Retrofit of old patch.
- 'Open Tunnel' button disabled while network interfaces become available or unavailable to avoid crash. Especially wireless network interfaces (e.g. 3G, WiFi,..).
- IKE service might crash if user open and close the tunnel multiple times rapidly while a redundant gateway as been set.
- Support for numerical OID in certificate subject may lead to inability to open tunnel.
- Sound ('Ding') when using 'Tab' keyboard key in X-Auth Authentication popup.
- Password limiting access to some features ('View' > 'Configuration') might be asked even when not set.
- "Don't start VPN Client when I start Windows" is not working on Windows 7 64-bit. The IPsec VPN Client always starts.
- Bluescreen on Sony VAIO VGN-FW51MF with 3G option, Windows Seven 64-bit (Wind 7) and a VPN Configuration using Certificates.
- When local and remote network are on the same subnet, access to remote network would not work properly if the 'Auto open tunnel on traffic detection' feature has not been selected.
- Bad version IKE daemon.

STORMSHIELD