bintec Secure IPSec Client

Release Notes V. 6.14

1 Requirements

Microsoft Windows Operating Systems - The following Microsoft Windows operating systems are supported with this release:

- Windows 11, 64 bit
- Windows 10, 64 bit

Note that version 6 of Secure Client requires a new license, even if you are upgrading from an earlier version.

2 New features and enhancements

- **New Option: „resolve DNS Domains in the tunnel“**
  The split DNS functionality can be configured with the new "Resolve DNS domains in the tunnel" / "DNS domains to be resolved in the tunnel" option. In the case of configured split tunneling, the DNS requests the configured domains are sent via the VPN tunnel. All other DNS requests bypass the VPN tunnel.

- **Support RFC 7296**
  The VPN client now supports RFC 7296 for the distribution of split tunneling configurations through the VPN gateway.

3 Improvements / Bug fixes

- **New rights structure within C:\ProgramData\NCP\**
  A user had writing permissions within the C:\ProgramData\NCP\ directory. These have now been restricted to a minimum so that, among other things, a user can no longer store CA certificates there. Likewise, the directory and rights structure has been rebuilt so that no application in the user and system context can write here. The problem has been fixed.
- **Improvements in the server-side configured split DNS**
- **Automatic Windows login**
  If the "Perform automatically with configured logon data" option was selected during login, Windows login did not work. There was also a problem related to 2-factor authentication via TOTP. This problem has been fixed.
- **Troubleshooting Seamleass Roaming and IPv6 Destination Addresses**
  VPN username from cache
- After updating a previous version, the cached VPN username was sometimes not displayed correctly in the login dialogue. This problem has been fixed.
- **Incorrect status display after profile change**

After a profile change from a certificate-based profile with successful PIN entry to a profile with pre-shared key, the PIN entered was not deleted and the PIN icon was not removed from the client's GUI. This problem has been fixed.

- **PKI error during profile change**
  When switching profiles from a certificate-based profile with *.p12 file to a profile with smart card reader, a PKI error was displayed. This problem has been fixed.
- **Update to zlib version 1.2.12**
  The zlib version used in the VPN client was raised to 1.2.12. This closed the zlib vulnerability [CVE-2018-25032].
- **OpenSSL security patch**
  Vulnerabilities [CVE-2022-0778] and [CVE-2020-1971] have been fixed in OpenSSL.
- **Changeover to TLS 1.2**
- **TLS versions 1.0 and 1.1 are no longer supported with this client version.**
- **Update to cURL-Library 7.84.0**
  The cURL version used in the VPN client was raised to 7.84.0. This solved cURL vulnerabilities [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207] and [CVE-2022-32208].
- **Compatibility with third-party gateways in connection with 2-factor authentication / token entry has been improved.**
- **Incorrect status display: chip card**
  Under certain circumstances, a profile with 2-factor authentication incorrectly displayed a chip card symbol. When switching to a profile with a chip card, an error message was displayed stating that the chip card was not initialized correctly. This problem has been fixed.
- **Troubleshooting after changing the DNS entries in the VPN bypass configuration**
- **Troubleshooting when calling up the HotSpot login**
  The HotSpot login was not called up correctly when the "Icon in system tray" autostart option was selected. This problem has been fixed.
- **Troubleshooting an incorrectly displayed PIN request**
  When using the CSP user certificate store, a PIN was often incorrectly requested. This problem has been corrected. The option to request a PIN in the case of the CSP user certificate store has also been removed in the client plug-in.
- **Improve compatibility with third-party gateways when addressing via IPv6**
- **PAP/CHAP error when establishing a connection**
  Under certain circumstances, the VPN client displays a PAP/CHAP error when establishing an IKEv2 connection. This can be resolved by the user by opening the VPN profile and confirming with "Ok". This problem has been fixed.
- **Revision of the "Establish connection before Windows login“ function**
  To prevent a possible privilege escalation, the "Connection establishment before Windows logon" function was revised. Here, a standard user, if this function was not deactivated via the configuration locks, could sneak administrator rights (e.g., via a configured CMD shell). With this change, only batch files created by the administrator in the C:\ProgramData\NCP\SecureClient\scripts\ directory can be selected.
- **Improve compatibility with Juniper SRX gateways in the case of the ReKeying phase.**
- **Support RFC 8598**
  RFC 8598 defines how to forward the split DNS configuration to the VPN client using the VPN gateway. This RFC is supported as of this client version.

- **Network connection permanently disconnected after installation**
  After installing the client, the network connection was permanently disconnected. Only after rebooting the computer was network communication possible again. This problem was solved.
- **Problem importing a previously exported profile**
  Importing an exported profile into 13 clients failed. This problem has been fixed.
- **General improvements for INI or PCF file import**
- **Improvement of compatibility with third-party gateways with regard to IP address assignment**
  If the VPN client was assigned an IP address ending with .255 during the connection setup, routing through the VPN tunnel was not possible. This problem has been fixed.
- **Troubleshooting for online activation when proxy is used and configured as DNS name**

4 Known limitations

- **Option: "Open dialogue for connection automatically".**
  Under certain circumstances, the "Automatically open dialogue for connection establishment" login option does not work.
- **Application-based VPN bypass configuration**
  Configuring a DNS within the VPN Bypass configuration renders an application-based rule contained therein ineffective.
- **PIN menu items**
  When using hardware certificates, PIN menu items "Enter/Reset/Change PIN" can be incorrectly selected despite having no function.
- **Seamless Roaming**
  Under certain circumstances, when switching from WLAN to LAN, the VPN tunnel status remains at "Keep tunnel logical" and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.
- **Home Zone and IPv6**
  If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets in the defined Home Zone network are discarded in the local network.