Release Notes
bintec Secure IPSec Client
Version 5.2

Prerequisites

Operating System Support:

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 Bit (up to and including version 20H2)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

1 New Features and Enhancements

1.1 New configuration option: DNS entry for VPN bypass

This new configuration option ensures that for external VPN bypass destinations, name resolution through the VPN tunnel is only carried out by the two configured DNS servers. For this purpose, a primary and a secondary DNS can be entered in the VPN bypass configuration, optionally as an IPv4 or IPv6 address. In this release, the configured DNS servers are only effective for configured web domains. Configured applications within the VPN bypass functionality are currently not taken into account.

1.2 Screen sharing over Wi-Fi is no longer blocked by the client firewall

Screen sharing via Wi-Fi, e.g., for presentation via projector with Miracast protocol, is no longer blocked by the client firewall and is now possible.

2 Improvements / Problems Solved

2.1 Troubleshoot reverse DNS requests

Fixed a problem with reverse DNS (PTR) requests by the operating system.

2.2 Update to OpenSSL version 1.0.2u-8

The OpenSSL version used in the IPSec Client has been increased to 1.0.2u-8. This closed the OpenSSL vulnerability CVE-2020-1971.

2.3 Blue screen after updating IPSec Client

In rare cases the user computer crashed during the first restart after an update of the IPSec Client. This problem only occurred with Windows 10 and has been resolved.

2.4 FND detection fails with Hyper-V installed

If Hyper-V is installed on the user computer and a virtual switch is active, the IPSec Client's FND functionality is not working correctly. This problem has been fixed.

2.5 Problems related to multiple IPv6 addresses on the adapter

If several IPv6 addresses were assigned to the IPSec network adapter, the establishment of the VPN connection or the data transfer through the VPN tunnel could be disturbed in certain cases. This problem has been fixed.

2.6 No data transport through the VPN tunnel at Juniper SRX remote station

In rare cases, no data can be transported through the VPN tunnel in connection with a Juniper SRX remote station. This manifests itself in an incorrectly assigned IPv4 address on the IPSec adapter. This problem has been fixed.

2.7 DNS error

Under certain circumstances, DNS requests were not properly resolved through the VPN tunnel or returned an error. The reason was an incorrectly assigned metric on the IPSec network adapter. This problem has been fixed.

2.8 Support assistant

The output path for storing the ZIP file with the collected log files was ignored. This problem has been fixed.

2.9 Compatibility with CISCO ASA Gateway

The connection to the CISCO ASA Gateways was not established correctly in rare cases. This problem has been fixed.

2.10 No data throughput in the VPN tunnel

In rare cases, when seamless roaming was used, no data could be transported through the VPN tunnel after the media change. The reason was that the DHCP negotiation for the IPSec network adapter ran into a timeout and the IP address was not assigned correctly. This problem has been fixed.

2.11 Bugfix in the area of the VPN bypass functionality

There have been general improvements made to this function.

3 Known Issues

3.1 Network connection remains disconnected after installation / update

After the installation / update process of the IPSec Client, the network connection remains inactive and can only be used after restarting the computer.

3.2 Silent Installation on Windows 7

Since the software signature was changed from SHA-1 to SHA-256 within Windows 7, two Windows security dialogs are generally displayed to confirm driver installation during client installation. This does not occur in Windows 8.x or Windows 10.

3.3 Option: "Automatically Open Connection Setup Dialog“

Under certain circumstances, the Logon option "Automatically Open Connection Dialog" does not work.