Release Notes
bintec Secure IPSec Client
Version 4.10

Inhalt

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10 32/64 Bit (bis einschließlich Version 1803)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Unterstützung für Windows Vista entfällt ab dieser Version

1 Neue Leistungsmerkmale und Erweiterungen

1.1 Biometrische Authentisierung

(z. B. Fingerabdruck- oder Gesichtserkennung) vor VPN-Verbindungsaufbau

Zur Absicherung vor einem VPN-Verbindungsaufbau durch nicht autorisierte Dritte wurde im bintec Secure IPSec Client eine optionale biometrische Authentisierung vor der VPN-Einwahl integriert. Die Konfiguration dieser Option findet sich unter **Profil-Einstellungen ➔ Erweiterte Authentisierung ➔ Authentisierung vor VPN ➔ Fingerabdrucksensor / biometrische Authentisierung**. Bei gesetzter Option erfolgt direkt nach dem Klick auf den Verbinden-Button in der Client-GUI die Aufforderung zur Benutzerauthentisierung. Der VPN-Verbindungsaufbau wird daraufhin erst nach positiver Authentisierung gestartet. Voraussetzung für die biometrische Authentisierung ist die Windows Hello-Funktionalität ab Windows 8.1 oder neuer. Für ältere Betriebssysteme oder nicht vorhandene biometrische Hardware wird bei gesetzter Konfigurationsoption eine alternative Benutzerauthentisierung, z. B. das Passwort, abgefragt. Diese Option steht nur für die Verbindungsmodi *manuell* und *wechselnd* zur Verfügung.

1.2 Modernisierte Client-GUI

Die Client-GUI und das aus der Taskleiste gestartete Tray Popup-Fenster wurde an das aktuelle Windows 10-Design angepasst.

1.3 Komplette 64 Bit Umsetzung des bintec Secure IPSec Clients

Ab dieser Version sind alle Komponenten des bintec Secure IPSec Clients in 64 Bit-Ausführung enthalten.

1.4 Neue GUI des Credential Providers inkl. HotSpot-Anmeldefunktionalität

Ist der bintec Secure IPSec Client für den VPN-Tunnelaufbau vor der Benutzeranmeldung am Windows System konfiguriert, so erscheint die Client-GUI in reduzierter Funktionalität im Vergleich zum Standard-Betrieb. Des Weiteren ist es nun möglich bereits vor der Benutzerauthentisierung am Windows System eine HotSpot-Anmeldung durchzuführen. Diese geschieht analog zur bereits bekannten

HotSpot-Anmeldung des Clients. Die Icons des Credential Providers zeigen durch Ihre rote oder grüne Einfärbung den VPN-Tunnelstatus an.

2 Verbesserungen / Fehlerbehebungen

2.1 Konfiguration des VPN-Tunnelendpunkt

Ab dieser Version können mehrere VPN-Tunnelendpunkte mit Ihrem Domainnamen konfiguriert werden.

2.2 Optimierung der DPD-Funktionalität

FIPS-Inside

Innerhalb der Installationsroutine kann bei Neu-Installation oder bei Ändern der Installation der FIPS-Modus ein- oder ausgeschaltet werden. Über die Kommandozeile kann der FIPS-Modus wie folgt konfiguriert werden:

Hinzufügen: ADDLOCAL=FipsMode; Entfernen: REMOVE=FipsMode

2.3 Erweiterung der Darstellung der Verbindungsinformationen

Auch IPv6-Adressen des Tunnel Endpoints werden nun in den Verbindungsinformationen dargestellt.

2.4 Erweiterung des Client Info Centers

Ein neuer Abschnitt mit Treiber-Informationen zeigt im Client Info Center folgende direkt von der Registry übernommene Werte: Name, Version, IfType, InfPath, MtU, NetCfgInstanceId. Für ein Windows 10 Betriebssystem wird nun zusätzlich die Version und der Build im Client Info Center mit angezeigt.

2.5 Verbesserung der HotSpot-Funktionalität

Die Kompatibilität zu HotSpot-Anmeldeseiten wurde weiter ausgebaut. Das während der Anmeldung am HotSpot erscheinende Browserfenster wird nach dem in der NCPMON.INI konfigurierbaren Timeout ([HOTSPOTBROWSER] Timeout=300; Standardwert) automatisch geschlossen. Einhergehend wird die Proxy-Konfiguration im Betriebssystem wieder aktiv, die dynamischen Firewall-Regeln zur HotSpot-Anmeldung gelöscht und ggf. die WLAN-Verbindung abgebaut.

2.6 Erweiterung der Prüfung auf vorhandene Client Software Updates

Die Funktionalität **Software-Update** unterstützt ab dieser Version den Abgleich mit der zentralen Definitionsdatei über das HTTPS-Protokoll. Des Weiteren muss diese Definitionsdatei ab dieser Version zwingend signiert sein, so dass die Information über etwaige vorhandene Updates fälschungssicher an den Client gelangt. Auf diesem Wege zur Verfügung gestellte Installationsdateien werden vom Client ebenso mit der in der Definitionsdatei genannten Signatur verglichen.

3 Bekannte Einschränkungen

3.1 Demo-Benutzerzertifikate

Die **Demo-Benutzerzertifikate**, die mit bisherigen Client-Versionen installiert wurden, verlieren ihre Gültigkeit am 9. Oktober 2018. Damit werden existierende Test-Profile, z. B. zum DemoServer "vpntest.ncp-e.com", ab diesem Zeitpunkt nicht mehr funktionieren. Ab dieser Clientversion steht bei Neuinstallationen die automatische Einrichtung dieser Test-Profile mit Zertifikat nicht mehr zur Verfügung. Es existiert ausschließlich die Möglichkeit, Test-Profile mit der VPN-Konfiguration **Pre-shared key** zu erstellen.

Neue Zertifikate mit verlängerter Gültigkeit befinden sich nach der Installation im Unterverzeichnis *certs*. Bisher waren sie immer direkt im Installationsverzeichnis abgelegt.

4 Leistungsmerkmale

4.1 Betriebssysteme

Beachten Sie dazu die **Voraussetzungen** auf Seite 1.

4.2 Security Features

Unterstützung aller IPsec-Standards nach RFC

Virtual Private Networking

- RFC-konformes IPsec (Layer 3 Tunneling)
  - IPsec-Tunnel Mode
  - IPsec-Proposals können via das IPsec-Gateway (IKE, IPsec Phase 2) determiniert werden
  - Kommunikation nur im Tunnel oder Split Tunneling konfigurierbar
  - Message Transfer Unit (MTU) Size Fragmentation und Re-assembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)
  - Anti-Replay Protection

Authentisierung

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
  - Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA Signatures (und entsprechende Public Key Infrastructure)

- Extended Authentication Protocol (EAP) – (Benutzername und Passwort für ClientAuthentisierung gegenüber Gateway; Zertifikat zur Server-Authentisierung gegenüber Client)
  - EAP unterstützt: PAP, MD5, MS-CHAP v2, TLS (ausgewählt durch Responder/Gateway)
  - IKEv2 Mobility und Multihoming Protokoll (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
- Benutzer-Authentisierung:
  - Benutzer-Authentisierung über GINA/Credential Management
    - Windows Logon über VPN-Verbindung
  - XAUTH (IKEv1) für erweiterte Benutzer-Authentisierung
    - One-Time-Passwörter und Challenge Response Systeme
    - Zugangsdaten aus Zertifikaten (PKI)
- Unterstützung von Zertifikaten in einer PKI:
  - Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless Rekeying
- PAP, CHAP, MS-CHAP v2
- HTTP Authentisierung vor VPN
- IEEE 802.1x:
  - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (MS-CHAPv2): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten mit IKEv2 (Layer 2)
- Hotspot Anmeldung mit HTTP oder EAP
- RSA SecurID Ready

Verschlüsselung (Encryption)

Symmetrisch: AES-GCM 128, 256 bits (nur IKEv2 & IPsec); AES-CTR 128, 192, 256 bits (nur IKEv2 und IPsec); AES (CBC) 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits Asymmetrisch: RSA bis 2048 bits, für dynamischen Schlüsselaustausch

Hash / Message Authentisierungs-Algorithmen

- SHA-1, SHA-256, SHA-384, SHA-512, MD5.
- Diffie Hellman Gruppen 1, 2, 5, 14, 15-18, 19-21, 25, 26 für asymmetrischen Schlüsselaustausch und PFS.
- Diffie Hellman Gruppen 19 - 21, 25, 26 mit Algorithmus elliptischer Kurven (nur unter IKEv2).

Public Key Infrastructure (PKI) - Starke Authentisierung

- X.509 v.3 Standard
- Entrust Ready
- Zertifikats-Unterstützung in einer PKI
  - Smart Cards und USB Tokens
    - PKCS#11-Schnittstelle für Verschlüsselungs-Tokens (USB und Smart Cards)
    - Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0
  - Smart Card Reader-Schnittstellen
    - PC/SC, CT-API
  - Soft-Zertifikate
    - PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- PIN Richtlinien: Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Certificate Service Provider (CSP) zur Verwendung von Benutzerzertifikaten im WindowsZertifikatsspeicher
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL vormals CRL)
  - Certification Authority Revocation List, (CARL vormals ARL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Management Protocol (CMP)

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines FND-Servers)
  - FND-abhängige Aktionen starten
- Sicheres Hotspot Anmeldung
- Anwendung starten vor oder nach VPN-Verbindungsaufbau
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports, Applikationen und IP-Adressen
  - Schutz des LAN Adapter
- Schutz des VMware Gastsystems
- IPv4- und IPv6-Fähigkeit
- Option: **ausgehenden Verkehr mit Reject** quittieren oder ohne Rückmeldung verwerfen

4.3 Networking Features

Sichere Netzwerk Schnittstelle

- LAN Emulation
  - Ethernet-Adapter mit NDIS-Schnittstelle
  - Volle Unterstützung von Wireless Local Area Network (WLAN)
  - Volle Unterstützung von Wireless Wide Area Network (WWAN)

Netzwerk Protokoll

- IPv4-Protokoll
  - IPv4 für Tunnelaufbau und Datenverkehr innerhalb des VPN-Tunnels;
- IPv6-Protokoll
  - IPv6 für Tunnelaufbau von Client zu Server-Komponenten (Secure Enterprise VPN-Server);
  - zur Datenübertragung innerhalb des VPN-Tunnels wird IPv4 genutzt

Verbindungs-Medien

- LAN
- WLAN
- Mobiles Netzwerk, GSM - LTE
  - Ab Windows 7 – Mobile-Broadband-Fähigkeit
- xDSL (PPPoE)
- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)
- Externer Dialer
- Seamless Roaming (LAN / Wi-Fi / Mobiles Netzwerk)

Dialers

- Secure Dialer
- Microsoft RAS Dialer (für ISP Einwahl mit Einwahl-Script)

Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- WLAN Roaming (handover)
- Modi des Verbindungsaufbaus
  - manuell
  - immer
  - automatisch (Datenverkehr initiiert VPN-Verbindung)
  - wechselnd (automatischen Modus manuell starten)
  - wechselnd (Immer-Modus manuell starten)
- Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)
- Short Hold Mode
- Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert
- Budget Manager
  - Eigenes Management für WLAN, Mobilfunk, xDSL, ISDN und Modem-Verbindungen
  - Budgets nach Verbindungsdauer oder Volumen
  - Management der Roaming-Kosten (Mobilfunk)
  - Eigenes Management verschiedener WLAN-Zugriffspunkte

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS): Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server

VPN Path Finder

- Path Finder Technologie
- Fallback auf HTTPS (port 443) wenn IPsec-Port 500 bzw. UDP Encapsulation nicht möglich ist

Datenkompression

- IPsec Kompression

Link Firewall

- Stateful Packet Inspection

Weitere Features

- VoIP Priorisierung
- UDP Encapsulation
- IPsec Roaming
- WLAN Roaming
- WISPr-Unterstützung (T-Mobile Hotspots)

Point-to-Point Protokolle

- PPP über Ethernet
- PPP über GSM,
- PPP über ISDN,
- PPP über PSTN,
  - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

4.4 Unterstützte Standards

Internet Society RFCs und Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer (DPD)
  - Negotiation of NAT-Traversal in the IKE (RFC 3947)
- Internet Key Exchange Protocol v2 (IKEv2) (RFC 4306, 5996)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)
- UDP encapsulation of IPsec Packets (RFC 3948),

Extended Key Usages:

- id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) nach RFC 4945
- anyExtendedKeyUsage (2.5.29.37.0) nach RFC 4945
- IKEIntermediate (1.3.6.1.5.5.8.2.2) nach draft-ietf-ipsec-pki-req-03

FIPS Inside

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt wird:

- Diffie Hellman Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit)
- Hash Algorithmen: SHA1, SHA 256, SHA 384, oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192, 256 Bit oder Triple DES

4.5 Benutzerfreundliche Features

APN von SIM-Karte

Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen. Das erleichtert die Nutzung von günstigen lokalen Providern im Ausland.

4.6 Secure Client Monitor

Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch, Spanisch)
  - Monitor & Setup: en, de, fr, es
  - Online Hilfe und Lizenz en, de
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – Übersicht über:
  - Allgemeine Informationen - Version, MAC-Adresse etc.
  - Verbindung – aktueller Status
  - Services/Applications – Prozess-Status
  - Zertifikats-Konfiguration – eingesetzte Zertifikate etc.
- Konfiguration, Verbindungsstatus, Logbuch (mit Farbmarkierungen und Copy&Paste-Funktion)
- Unterstützung von Mobilfunk-Hardware
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool für Fehlerdiagnose
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden
- Hotkey Support für Verbindungsauf- und -abbau.
- Custom Branding Option
- Tests zur Internet-Verfügbarkeit
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)