Release Notes

NCP Secure Entry Client (Win32/64)

Service Release: 9.30 Build 102
Datum: Februar 2012

1. Neue Leistungsmerkmale und Erweiterungen

In dieser Version sind folgende neue Leistungsmerkmale enthalten:

Optische Rückmeldung beim logischen Halten des Tunnels

Wenn die Verbindung über das jeweilige Verbindungsmedium eines VPN-Profils unterbrochen wird, bleibt der VPN-Tunnel weiterhin bestehen. D. h. der VPN-Tunnel wird über einen beliebig langen Zeitraum bis zum Wiederaufbau der physikalischen Verbindung über das jeweilige Medium logisch gehalten.

Während der Haltedauer der logischen Verbindung wird der grüne Balken der VPN-Verbindung im Client-Monitor in gestrichelter Form dargestellt. Während dieser Zeitspanne leuchtet das Ampellicht im Systemtray gleichzeitig grün und gelb bis die physikalische Verbindung wieder hergestellt ist (grünes Licht).

Verliert der Client die Internet-Verbindung und der Tunnel wird logisch gehalten, wird dieser Status mit einem Ballon über dem Tray-Icon angezeigt. Somit wird der Benutzer auch darüber informiert, wenn der Monitor minimiert ist.

Erweiterungen von Online-Hilfe und Tipps

Die Hilfetexte wurden der aktuellsten Version des Clients angepasst. Der Dialog für die Profil-Gruppen wurde um einen Hilfe-Button erweitert. Alle Hilfetexte können wie üblich über einen Hilfe-Button oder kontextsensitiv mit der F1-Taste aufgerufen werden. Die Tipps wurden der aktuellen Version des Clients angepasst.

Erweiterung des UMTS-Panels

Das Panel für GPRS / UMTS, das bei Einsatz eines Profils mit einer dieser Verbindungsarten oder LTE im Client-Monitor erscheint, wurde entsprechend des neuen LTE-Standards um die LTE-Anzeige erweitert. Je nachdem welches drahtlose Netz der Provider zur Verfügung stellt, wird dessen Name und Feldstärke angezeigt. Dies gilt auch für das UMTS-Panel der NCP GINA.

Externe Anwendungen

Die Funktion zum Starten externer Anwendungen (Logon Optionen / Ext. Anwendungen) wurde dahin gehend erweitert, dass auch Skripte gestartet werden können, die mit der Extension *.vbs verknüpft sind.

Import von Konfigurationssperren

Für den Import der Konfigurationssperren wurden Ergänzungen in den Dateien Import-de.txt und Import-en.txt eingefügt. Folgende Optionen sind dadurch möglich:

- Profile dürfen exportiert werden
- Profile dürfen importiert werden.

WLAN-Konfigurations-Assistent

Der WLAN-Konfigurations-Assistent bietet bei der Konfiguration eines offenen, ungeschützten WLANs die Hotspot-Anmeldung jetzt nur noch an, sofern es sich um die bekannte SSID eines Hotspot-Anbieters handelt.

2. Fehlerbehebungen

Folgender Fehler wurde in diesem Release behoben:

Blockierter Monitor

Wurde eine PKI-Fehlermeldung über die Callback-Funktion angezeigt, bevor der Monitor aufgebaut war und der Monitor minimierte sich beim Start, konnte die Fehlermeldung nicht angezeigt werden und der Monitor war blockiert.

Fehler beim Aufbau der Routing-Tabelle

Der Client überwacht DHCP Requests an alle Netzwerk-Adapter, um IP-Informationen über jeden Adapter zu erhalten. In bestimmten Situationen ist es erforderlich, dass der Client einen DHCP-Austausch mit einem RENEW-Kommando anstößt. Wird dieses RENEW-Kommando für einen Adapter ohne IP-Adresse oder ohne Verbindungsstatus ausgeführt, so konnte die Routing-Tabelle für einige Minuten nicht aufgebaut werden.

Fehler beim Setzen der Routen im Split-Tunneling

In bestimmten Fällen wurden die Routen bei Verwendung von Split-Tunneling nicht korrekt gesetzt.

Fehlerhafte Export-Datei auf Netzlaufwerk

Bisher konnten die Profil-Einstellungen eines Clients nicht direkt in eine Datei auf einem Netzlaufwerk exportiert werden, da Passwörter und Pre-shared Key in diesem Fall nicht übertragen wurden.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Entry Client (Win32/64)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
http://www.ncp-e.com/de/downloads.html

Weitere Unterstützung bei Fragen zum Enterprise, erhalten Sie über die Mail-Adressen auf folgender Seite:
http://www.ncp-e.com/de/ueber-uns/kontakt.html

mailto:support@ncp-e.com?subject=A: NCP Secure Entry Client - Helpdesk message

5. Leistungsmerkmale

Betriebssysteme

Microsoft Windows (32 & 64 bit): Windows 7, Windows Vista, Windows XP

Security Features

Unterstützung aller IPsec-Standards nach RFC.

Virtual Private Networking

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

Authentisierung

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - IKEv2
  - 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)
- Benutzer-Authentisierung:
  - User Authentisierung über GINA/Credential Management
    - Windows Logon über VPN-Verbindung
  - XAUTH 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-CHAPv2
- 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 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 für asymmetrischen Schlüsselaustausch und PFS

Public Key Infrastructure (PKI) - Starke Authentisierung

- X.509 v.3 Standard
- 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 Status Protocol (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
  - Certification Authority Revocation List, (CARL vormals ARL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Management Protocol (CMP) [i]

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 NCP FND-Servers)
  - FND-abhängige Aktionen starten
- Sicheres Hotspot Anmeldung
- Anwendung starten vor oder nach VPN-Verbindungsausbau
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports, Applikationen und Adressen
  - Schutz des LAN adapter
- Schutz des VMware Gastsysteme
- IPv4 und IPv6 fähigkeit

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

- IP

Verbindungs-Medien

- LAN
- WLAN
- GPRS / 3G (UMTS, HSDPA), GSM (einschl. HSCSD)
  - Windows 7 - Mobile Broadband Unterstützung
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / GPRS / 3G)

Dialers

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

Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- Short Hold Mode
- Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)
- Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert
- WLAN Roaming (handover)
- Budget Manager
  - Eigenes Management für WLAN, GPRS/UMTS, xDSL, PPTP, ISDN und Modem-Verbindungen
  - Budgets nach Verbindungsdauer oder Volumen
  - Management der Roaming-Kosten (GPRS/UMTS)
  - Eigenes Management verschiedener WLAN-Zugriffspunkte
- Seamless Roaming

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

- NCP Path Finder Technology
  - Fallback auf HTTPS (port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist [ii]

Datenkompression

- IPsec Compression: LZS, deflate

Link Firewall

Stateful Packet Inspection

Weitere Features

- VoIP Prioritization
- UDP Encapsulation
- IPsec Roaming [ii]
- WLAN Roaming [ii]
- WISPr support (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

Unterstützte Standards

Internet Society RFCs und Drafts

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

- Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406),
- Negotiation of NAT-Traversal in the IKE (RFC 3947),
- UDP encapsulation of IPsec Packets (RFC 3948),
- IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
- zusätzliche Extended Key Usages, id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) und anyExtendedKeyUsage (2.5.29.37.0) nach RFC 4945, IKEIntermediate (1.3.6.1.5.5.8.2.2) entsprechend zu 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 werden:

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

Client Monitor

Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch)
  - Monitor & Setup: en, de, fr
  - 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 Farbmarlierungen und Copy&Paste-Funktion)
- Unterstützung von 3G-Karten (PCMCIA, embedded) integriert
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool fur Fehlerdiagnose
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden
- Tipp des Tages
- Hotkey Support für Verbindungsauf- und -abbau.
- Custom Branding Option
- Tests zur Internet-Verfügbarkeit

Hinweise

i NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden:
http://www.ncp-e.com/de/downloads/software.html

ii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später

Weitere Informationen zum NCP Secure Entry Client (Win32/64) finden Sie hier:
http://www.ncp-e.com/de/produkte/ipsec-client.html

Testen Sie 30 Tage kostenlos die uneingeschränkt nutzbare Vollversion des NCP Secure Entry Clients (Win32/64):
http://www.ncp-e.com/de/downloads/software.html