Release Notes

NCP Secure Entry Client (Win32/64)

Service Release: 9.30 Build 70
Datum: Oktober 2011

1. Neue Leistungsmerkmale und Erweiterungen

In diesem Release sind folgende neue Leistungsmerkmale enthalten:

Seamless Roaming

Seamless Roaming bietet die automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium. Wird ein Laptop beispielsweise in eine Dockingstation abgelegt, so wird automatisch von einer zuvor genutzten WLAN bzw. 3G/UMTS-Verbindung auf LAN umgeschaltet. Dabei bleibt die IP-Adresse erhalten, so dass eine – über den VPN-Tunnel kommunizierende – Anwendung nicht im Betrieb gestört ist.

Wird die Internetverbindung z. B. wegen schlechten Empfangs kurzzeitig unterbrochen, so wird der VPN-Tunnel logisch gehalten. Auch in diesem Fall kann eine den VPN-Tunnel nutzende Anwendung kurzzeitige Unterbrechungen ohne Session-Verlust überstehen.

Voraussetzung ist der Einsatz eines NCP Secure Servers ab Version 8.05. Seamless Roaming wird nur für IKEv1-Verbindungen unterstützt.

Internationale Erweiterung der UMTS-Providerliste

Die Möglichkeiten einer Profil-Einstellung für GPRS- und UMTS-Verbindungen wurden um eine internationale Provider-Liste erweitert. Im Konfigurationsmodus mit Provider-Liste werden mit der Auswahl eines Landes die dortigen wichtigsten Anbieter angezeigt und mit Auswahl eines Providers die weiteren Parameter automatisch eingetragen. Die Provider-Liste ist editierbar im Installationsverzeichnis als APN.ini abgelegt. (Die Konfiguration wird in den Profil-Einstellungen unter GPRS / UMTS vorgenommen.)

Windows 7 - Mobile Broadband Unterstützung

Aufgrund der bei LTE möglichen, hohen Übertragungsraten wurde die frühere Implementierung via MS Windows virtuellen COM-Ports zum Flaschenhals. Die Kommunikation via MS Windows Mobile Broadband Schnittstelle hebt diese Beschränkung auf.

IKEv2 Unterstützung

Mit der Implementierung des Internet Key Exchange Protocol Version 2 (IKEv2), eingeschlossen der Mobility Extensions (MOBIKE), in den Client-Unterbau, verhält sich der Secure Client kompatibel zu anderen IPsec Gateways wie Microsoft Windows Server 2008 R2.
Die alternative Verwendung von IKEv2 bzw. IKEv1 wird am Entry Client in den Profil-Einstellungen unter der Rubrik „IPsec-Einstellungen / Austausch-Modus" konfiguriert.

Erweiterung des WLAN-Konfigurations-Assistenten

Wird über den WLAN-Konfigurations-Assistenten ein WLAN-Profil angelegt, so wird unmittelbar nach Abschluss der Konfiguration mit diesem WLAN die Verbindung hergestellt.

Deaktivieren der Proxy-Systemeinstellungen

Der für das System definierte Proxy-Server kann im Konfigurationsmenü unter Hotspot deaktiviert werden. Nach Ablauf eines Timeouts, sowie unmittelbar nach erfolgreichem VPN-Verbindungsaufbau, wird der Proxy-Server automatisch wieder aktiviert.

Beachten Sie, dass diese Einstellung nur mit Browsern funktioniert, die den System-Einstellungen folgen, zum Beispiel: Safari, Google Crome, Internet Explorer, Firefox.

Umbenennung von Projekt-Logo in Custom Branding Option

Die Funktionalität „Projekt-Logo" ist in dieser und künftigen Versionen für alle Sprachen in „Custom Branding Option" umbenannt.

Tests zur Internet-Verfügbarkeit

Das Hilfemenü des Client-Monitors bietet Tests an, womit die Internet-Verfügbarkeit getestet werden kann. Sie gestatten sowohl einen PING auf eine IP-Adresse im Internet auszuführen als auch die Auflösung eines Internet-Domain-Name (DNS-Request) in die entsprechende IP-Adresse zu prüfen, wobei der Domain-Name in Form von „ncp-e.com" angegeben wird.
Nach Eingabe der Adresse wird der entsprechende Test-Button gedrückt, woraufhin die Aktion ausgeführt wird.
Die Testergebnisse werden über ein Symbol angezeigt (erfolgreich: grüner Haken, erfolglos: rotes Kreuz). „Mehr Informationen" zeigt ein kleines Log in Klartext.
Die Tests sind insbesondere von Bedeutung wenn Firewall-Regeln für DNS-Request und ausgehende Internetverbindungen angelegt wurden.

Diffie Hellman Gruppen 15-18

Die Erweiterung der Diffie Hellman Gruppen wurden ausschließlich für die IKE-Richtlinien hinzugefügt.

Animation zum Verbindungsaufbau

Unmittelbar nach Druck auf den Verbinden-Button erhält der Anwender eine optische Rückmeldung neben dem Button durch ein Drehsymbol. Dieses Symbol zum Vorgang des Verbindungsaufbaus wird angezeigt, solange dieser dauert. Kann keine Verbindung hergestellt werden, verschwindet die Animation und im grafischen Feld des Client-Monitors erscheint statt eines grünen Verbindungsbalkens eine Fehlermeldung.

Automatisierte Prüfung auf eine neue Version

Wird der Menüpunkt „Auf Updates prüfen" aufgerufen, wird ein neuer Dialog angezeigt, über den der Abfragezyklus (nie, täglich, wöchentlich, monatlich) konfiguriert werden kann. Zusätzlich ist ein Button enthalten „Jetzt prüfen".

WLAN trennen wenn VPN-Tunnel beendet

Durch setzen der Option "WLAN trennen wenn VPN-Tunnel beendet" wird die Sicherheit im Hotspot-Umfeld erhöht. Dieser Parameter wurde in der Konfiguration der WLAN-Profile unter "Allgemein" hinzugefügt.

Neue Firewall-Konfiguration GUI

Die GUI der Firewall ist dahingehend überarbeitet, dass Firewall-Regeln direkt - mit einem Mausklick - aktiviert und deaktiviert werden können, sowie vordefinierte Regeln erstellt werden können. Insbesondere wird eine bessere Übersicht über das Regelwerk angeboten. Eine DENY-Regel steht immer zu Beginn des Regelsatzes. Die „offene Grundeinstellung" fällt weg.

Firewall – Neuer Parameter „FND-abhängige Aktionen starten“

Sobald der Client den Wechsel von einem bekannten zu einem unbekanntem Netzwerk (oder umgekehrt) erkennt, kann in Abhängigkeit davon eine beliebige Aktion gestartet werden. So könnte beispielsweise ein externes Programm aufgerufen werden welches die Proxy-Einstellung des Windows-Systems umschaltet.

IPv6-Fähigkeit der Firewall

In der Client Firewall können nun Regeln für IPv6 definiert werden.

Kommandozeilen-Tool "NcpClientCmd"

Alternatives Kommandozeilenprogramm zu rwscmd welches über keinerlei graphische Ausgabe verfügt.

Ausblenden gesperrter Menüpunkte

Menüpunkte in den Pulldown-Menüs des Client-Monitors, die vom Administrator für die Benutzung gesperrt werden, werden vollständig ausgeblendet, nicht mehr ausgegraut wie in früheren Versionen. Auf diese Weise werden die Pulldown-Menüs entsprechend verkürzt. Die Sperrung erfolgt über die Konfigurationssperren im Konfigurations-Menü.

2. Fehlerbehebungen

Folgender Fehler wurde in diesem Release behoben:

Änderung des WLAN-Assistenten

Wird ein offenes WLAN eingefügt, wird ein Dialog zur Hotspot-Anmeldung gezeigt. Dieser führte häufig zu Verwirrungen, da hier nur Telekom-Hotspots für Deutschland ausgewählt werden konnten.

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.

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, der Mac-Adresse des DHCP-Servers 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)
- 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