Release Notes

NCP Secure Entry Client (Win32/64)

Service Release: 9.24 Build 84
Datum: Juli 2011

1. Neue Leistungsmerkmale und Erweiterungen

In diesem Release sind folgende neue Leistungsmerkmale enthalten:

Implementierung von IKEv2

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 Client in den Profil-Einstellungen unter der Rubrik „IPsec-Einstellungen / Austausch-Modus" konfiguriert. In diesem Pulldown-Menü können folgende Einstellungen vorgenommen werden:
– Main Mode (IKEv1) [dies ist der Standardwert bei der Profilerstellung]
– Aggressive Mode (IKEv1)
– IKEv2
Wird das Internet Key Exchange Protocol Version 2 (IKEv2) eingesetzt, so wird als Authentisierungsprotokoll Microsoft CHAP Version 2 (MS-CHAPv2) verwendet.

Auswertung der übertragenen Sub CA-Zertifikate in der IKE-Verhandlung

Werden in der IKE-Verhandlung CA-Zertifikate übertragen, so werden diese in der Zertifikats-Überprüfung mit verwendet. D.h. diese CA-Zertifikate müssen nicht mehr im Installationsverzeichnis des Clients unter CACerts gespeichert sein. Das Root-Zertifikat muss sich immer am Client befinden.

Auswertung der Extended Key Usages

Bei einer IKE-Verhandlung werden jetzt zusätzliche Ext. Key Usages akzeptiert:
– id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) RFC 4945
– anyExtendedKeyUsage (2.5.29.37.0) RFC 4945
– IKEIntermediate (1.3.6.1.5.5.8.2.2) entsprechend zu draft-ietf-ipsec-pki-req-03

Toleranzverhalten bei instabilen Verbindungen

Wird eine Internet-Verbindung über drahtlose Medien (UMTS, WLAN) gestört oder für eine gewisse Zeit unterbrochen, so bleibt der VPN-Tunnel bis zum nächsten Wiederaufbau der physikalischen Verbindung erhalten. Dies wird durch einen gelben Tunnelstatus im grafischen Feld des Client-Monitors angezeigt.
Eine Unterbrechung der physikalischen Verbindung darf maximal so lange dauern wie die für das DPD-Intervall am Gateway eingestellte Zeitspanne.
Wird im Client-Profil unter „Erweiterte IPsec-Optionen" die DPD-Funktionalität deaktiviert, schickt auch das Gateway keine DPD-Pakete mehr, sodass auch das am Gateway eingestellte Intervall keinen Einfluss mehr hat.

Verbindungsaufbau über Hotkey

Über den Hotkey [Alt] + [v] (englisch [Alt] + [c]) kann die Verbindung auf- und wieder abgebaut werden.

2. Fehlerbehebungen

Folgende Fehler wurden behoben:

"Eingefrorener" VPN Client nach StandBy-Modus

Ist der Rechner aus dem StandBy-Zustand erwacht, so war der NCP VPN Client „eingefroren“ – es kam zu einer Dead-Lock-Situation. Aufgrund der Konfiguration „wechselnder Verbindungsaufbau“ versuchte der Client direkt nach dem Aufwachen eine Verbindung aufzubauen, was die Erkennung der UMTS-Hardware im Windows Gerätemanager verhinderte.
Die Behebung des Problems ließ sich durch eine Verzögerung des Verbindungsaufbaus im Client für den Konfigurationsfall automatischer bzw. wechselnder Verbindungsmodus umsetzen.

Modem nicht gefunden (kein aufgebauter VPN-Tunnel)

Ist der Rechner aus dem StandBy-Zustand erwacht, so meldete der NCP VPN Client bei Verwendung von UMTS-Hardware „Modem nicht gefunden“. Nach Änderungen am Unterbau des NCP VPN Clients wurde auch die neue UMTS-Hardware unterstützt. Da die Aushandlung des APNs bereits beim Einwahlvorgang in das UMTS-Netz des Providers geschieht, konnte eine wiederholte Aushandlung des APNs beim Aufbau des UMTS-Links weggelassen werden. Die Einwahl in ein UMTS-Netz geschieht nun um einige Sekunden schneller.

DNS Request auf falschen DNS-Server

Für die ordnungsgemäße Funktion des NCP VPN Clients ist es notwendig, dass der NCP Netzwerkadapter als erstes an den TCP/IP-Stack des Windows Vista Betriebssystems gebunden ist. Der NCP VPN Client prüft nach jedem Start des Rechners die Bindung des NCP-Adapters an den TCP/IP-Stack und setzt den NCP-Adapter ggf. an erste Stelle. Diese Prüfung erfolgt allerdings nicht nach einem Beenden des StandBy-Zustandes. Aus diesem Grunde konnte es vorkommen, dass trotz deaktiviertem Split-Tunneling ein DNS-Request am VPN-Tunnel vorbei erfolgte.

Fehlfunktion von Split Tunneling, Automatische Medienerkennung und UMTS

Bei Profilen mit automatischer Medienerkennung und UMTS-Option konnte Split Tunneling nicht korrekt ausgeführt werden, insoweit alle Pakete über den Tunnel gesendet wurden.

Falsche Statusanzeigen bei aufgebauter VPN-Verbindung

Die GUI des Clients zeigt im Client Monitor den Verbindungsaufbau mittels einer animierten Darstellung an. Ebenso wird der Verbindungsstatus über ein zugehöriges Tray-Icon angezeigt. Obwohl bereits eine VPN-Verbindung bestand, zeigte die Animation eine gelbe, dünne Linie und das Tray-Icon eine rote Ampel an. Dieses Fehlverhalten erfolgte, wenn vor dem Verbindungsaufbau ein VPN-Profil mit ISDN-Link ausgewählt wurde. Die Darstellung wurde korrigiert. Ursache war die im System nicht vorhandene CAPI-Schnittstelle.

Fehlfunktion bei NAS-Authentisierung

Wurde am Client ein NAS-Passwort von mehr als 19 Zeichen konfiguriert, ist die NAS-Authentisierung fehlgeschlagen. Die Verschlüsselungsfunktion wurde angepasst und um eine Konvertierungsfunktion erweitert.

BSOD in WIN7

Wurde im Service-Teil der Registry der Name eines Dienstes eingetragen, der länger als 64 Zeichen war, verursachte dies infolge des Scan-Vorgangs durch den NCP-Treiber einen Bluescreen.

Folgende Fehler bei der Zertifikatsverwendung wurden behoben

Wurde im Zertifikatsdialog nach den P11-Modulen gesucht und der Assistent hatte ein P11-Modul ohne Hersteller gefunden, konnte dieser nicht selektiert werden.

VPN-Tunneling bei gesperrter Grundeinstellung der Firewall

Bei gesperrter Grundeinstellung der Firewall (Standard-Einstellung) sollte auf komfortable Weise die Firewall ausschließlich für VPN-Tunneling geöffnet werden. In der Firewall-Konfiguration wurde dafür unter „Optionen" ein Schalter eingebaut, der den Datenverkehr über IPsec oder VPN Path Finder global zulässt (oder sperrt). Die dabei automatisch im Hintergrund aktivierte Regel gestattete aber auch anderen Tools (Browser, Mail-Programm) über Port 443 zu kommunizieren. Diese Regel wurde dahingehend modifiziert, dass dies nicht mehr möglich ist.

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 (PFS)
- 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
Seamless Rekeying (Perfect Forward Secrecy)

Hash / Message Authentisierungs-Algorithmen

- SHA-1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman Gruppen 1, 2, 5, 14 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)
- 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

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

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

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

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