NCP Secure Entry Client (Win32/64)

Major Release: **10.10 r29061**
Datum: **April 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Neue Lizenzschlüssel ab Version 10.10

Software Update und Lizenzschlüssel

Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.

Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.

Neue Installation und Lizenzschlüssel

Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme" (vorher „Programme (x86)") installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Windows 10 Update 1511 (Threshold 2/Build 10586) führt zu Problemen mit installiertem NCP Secure Client

Das November-Update von Microsoft für Windows 10 ist weit mehr als nur die Sammlung einiger Patches oder Erweiterungen sondern prinzipiell eine runderneuerte Version von Windows 10. Im Zuge des Updates werden Bereiche der Registrierungsdatenbank umgeschrieben und einige für den NCP Secure Client wichtige Einträge gehen während dieses Vorgangs verloren.

Um dieses Problem zu beheben und die nicht übernommenen Schlüssel und zugehörigen Werte neu zu schreiben, ist eine Deinstallation und nach einem anschließenden obligatorischen Neustart des Systems erneute Installation des NCP Secure Clients notwendig. (Bestätigen Sie bei der Deinstallation **nicht** die Option „Alle Dateien löschen").

Dabei bleibt die Konfiguration komplett erhalten, jedoch müssen die Lizenzinformationen erneut eingegeben werden. Nach diesem Vorgang ist der NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

1. Neue Leistungsmerkmale und Erweiterungen

Neue Hotspot-Anmeldung

Innerhalb der neuen Hotspot-Anmeldung entfällt die zugehörige Konfiguration. Der Client erkennt potenziell verfügbare Hotspots und bietet dem Anwender in der Client GUI die Anmeldung daran an. Startet der Anwender die Hotspot-Anmeldung, so erscheint der NCP WLAN-Manager, womit der Anwender das gewünschte WLAN-Netz auswählen und die Anmeldung daran starten kann. Sobald die WLAN-Verbindung aufgebaut ist prüft der Client periodisch diese Verbindung auf Zugriff ins Internet. Ist kein Internetzugang verfügbar, startet der Client einen funktionsreduzierten Webbrowser ohne

Adressleiste. Hat sich der Anwender erfolgreich am Eingangsportal des Hotspot-Betreibers angemeldet, wird der Aufbau des VPN-Tunnels automatisch gestartet, sobald der Zugang ins Internet möglich ist.

Erhöhung der Kompatibilität zu Gateways anderer Hersteller

Der Secure Client unterstützt IKEv2 Redirect (RFC 5685). Damit können Load Balancing-Funktionen anderer Hersteller genutzt werden.

Überwachung des Filtertreibers durch den Secure Client

Erkennt der Client eine Fehlfunktion des Filtertreibers, so wird diese selbsttätig behoben und der Anwender aufgefordert einen Neustart durchzuführen.

Verwendung von Half-Routes und Default Gateways unter Windows 10

Die Client Software verwendet in der Standardeinstellung für den virtuellen Netzwerkadapter „Half-Routes". Durch einen Registry-Eintrag kann auf die Verwendung von „Default Gateways" umgestellt werden. Der Registry Key hierfür lautet:
Pfad:
`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt]`
Schlüssel:
`EnableDefGw = 1`
Type:
`REG_DWORD`

Ist der Registry-Eintrag `EnableDefGw` nicht vorhanden oder `EnableDefGw=0` gesetzt, werden Half-Routes verwendet.

2. Verbesserungen / Fehlerbehebungen

Stabilitätsverbesserungen

Die Stabilität des NCPRWSNT-Dienstes und des Update-Clients wurde verbessert.

Erweiterungen der Log-Meldungen

Die Log-Ausgaben für das PKI-Umfeld und den ncpsec-Dienst wurden erweitert.

Funktionsfähigkeit des WLAN-Moduls

Bei einer großen Anzahl von WLAN-Profilen (über 56) war die Funktion des WLAN-Adapters beeinträchtigt und der Adapter wurde im WLAN-Management nicht mehr angezeigt. Dieser Fehler ist behoben.

Windows Pre-Logon

Die Windows Pre-Logon-Funktionalität (Credential Provider) wurde für Windows 10 angepasst.

3. Bekannte Einschränkungen

Keine

Service Release: **10.04 Revision 26745**
Datum: **November 2015**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Windows 10 Update 1511 (Threshold 2/Build 10586) führt zu Problemen mit installiertem NCP Secure Client

Das November-Update von Microsoft für Windows 10 ist weit mehr als nur die Sammlung einiger Patches oder Erweiterungen sondern prinzipiell eine runderneuerte Version von Windows 10. Im Zuge des Updates werden Bereiche der Registrierungsdatenbank umgeschrieben und einige für den NCP Secure Client wichtige Einträge gehen während dieses Vorgangs verloren.

Um dieses Problem zu beheben und die nicht übernommenen Schlüssel und zugehörigen Werte neu zu schreiben, ist eine Deinstallation und nach einem anschließenden obligatorischen Neustart des Systems erneute Installation des NCP Secure Clients notwendig. (Bestätigen Sie bei der Deinstallation **nicht** die Option „Alle Dateien löschen").

Dabei bleibt die Konfiguration komplett erhalten, jedoch müssen die Lizenzinformationen erneut eingegeben werden. Nach diesem Vorgang ist der NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Korrekturen zur Installation

Es konnte bei der Installation des Clients zu einem Rollback während der Einrichtung des Filtertreibers kommen. Dies wurde durch Anpassung der Setup-Informationen korrigiert.

Windows Pre-Logon

Korrektur bei der Weiterverarbeitung des manuell eingegebenen Benutzernamens und Passworts bei der Windows-Anmeldung via Credential Provider.

Firewall

Es wurde ein Fehler im Bereich der Applikationserkennung der NCP-Firewall behoben.

Automatische Medienerkennung

Es wurde ein Fehler im Bereich der automatischen Medienerkennung in Verbindung mit PPPoE behoben.

WLAN-Adapter bei gestecktem LAN-Kabel deaktivieren

Verbesserung der Kompatibilität dieser Funktionalität zu verschiedenen Windows-Betriebssystemen.

Split Tunneling

Fehlerbehebung im Bereich Split Tunneling sofern das Remote Netzwerk denselben IP-Adressbereich hatte wie das lokale Netzwerk des Anwenders. So wurde nach einem VPN-Profilwechsel die Route in das lokale Netzwerk gelöscht.

Profilimport

Der Verbindungsmodus ConnMode=2, der den Verbindungsmodus „wechselnd" (automatischen Modus manuell starten) bezeichnet, wurde beim Profilimport nicht importiert. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Credential Provider auf Windows 10

Wird der Credential Provider des NCP Secure Clients auf einem Windows 10 Betriebssystem verwendet kann es zu fehlerhaftem Verhalten während der Benutzeranmeldung kommen.

Service Release: **10.02 Build 25056**
Datum: **August 2015**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Korrekturen zur Installation

Es konnte bei der Installation des Clients zu einem Rollback während der Einrichtung des Filtertreibers kommen.

Dies wurde durch Anpassung der Setup-Informationen korrigiert.

3. Bekannte Einschränkungen

Keine

Service Release: **10.02 Build 24934**
Datum: **Juli 2015**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Hinweis zum Betrieb des Secure Clients unter Windows 10

Zum Betrieb des Clients ist ein Produktschlüssel der Version 10.x nötig.

Hinweis zu einem Betriebssystem-Update auf Windows 10

Bei einem Update des Betriebssystems Windows 7, Windows 8 oder Windows 8.1 auf die Version Windows 10 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird.

Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern.

Erst nachdem das Update auf Windows 10 abgeschlossen wurde, sollte die neueste Version der NCP Secure Clients (10.02 oder höher) installiert werden.

1. Neue Leistungsmerkmale und Erweiterungen

Erweiterungen innerhalb der Log-Protokollierung

Für die Auswertung des Log-Textes wurden zwei Funktionen implementiert, die das Auffinden von Suchbegriffen im Log-Protokoll erleichtern. Diese Funktionen werden im Fenster der Log-Anzeige durch Klick auf „Suche einblenden" mit den Eingabefeldern „Suche" und „Filter" geöffnet.

Skalierung des Monitors für Touch-Bedienung

Damit auf Tablets die Touch-Bedienung des Client-Monitors komfortabel erfolgen kann, ist die Monitor-Oberfläche nun skalierbar.

Ein Skalierungsgrad von 150 % ist voreingestellt und kann durch Druck auf das NCP-Logo aktiviert oder wieder deaktiviert werden.

Über das Hauptmenü des Monitors unter „Ansicht / GUI-Skalierung" kann die Darstellungsgröße in Stufen von 100, 125, 150, 175 und 200 % eingestellt werden. Eine dynamische Änderung der Skalierung ist mit der Tastenkombination [Strg] [+] oder [Strg] [+] möglich.

Auf bekannte Netze periodisch prüfen

Die periodische Prüfung sollte dann aktiviert werden, wenn der Zustand des Netzwerk-Adapters, zum Beispiel beim Ziehen des LAN-Kabels, unverändert bleibt. Dies kann die Folge sein, wenn der Client in einer virtuellen Umgebung betrieben wird.

Im eingestellten Intervall wird geprüft, ob sich der Client noch in einem bekannten Netz befindet. Sobald das Friendly Net nicht mehr zur Verfügung steht, wird diese Statusänderung im Monitor als rotes Firewall-Symbol dargestellt.
Die Konfiguration erfolgt über das Konfigurationsmenü des Monitors unter „Firewall / Bekannte Netze / Automatisch", sofern die IP-Adresse nicht automatisch über DHCP bezogen wird.

VPN-Profil mit IKEv2 erhält für die PFS-Gruppe Diffie-Hellman 14

Beim Anlegen eines neuen VPN-Profils mit IPsec-Protokoll und IKEv2 ist die Diffie-Hellman-Gruppe 14 als Standardwert für das Schlüsselaustauschverfahren in der IPsec-Richtlinie voreingestellt. Diese Einstellung erfolgt unter „PFS-Gruppe" und kann dort auch verändert werden.

Umstellung des Passwort-Eingabe-Dialogs auf nicht-modal

Da modale Dialoge (z.B. PIN-Eingabe, Passwort-Abfrage) die Statusanzeigen des Clients (z.B. FND-Anzeige im System Tray) stoppen, wurden die modalen Dialoge auf nicht-modale Dialoge umgestellt.

Automatischer VPN-Tunnelaufbau vor der Windows-Anmeldung ohne Benutzereingaben

Der NCP Secure Entry Client stellt unmittelbar nach dem Systemstart einen VPN-Tunnel her, ohne dass sich der Benutzer am Windows-System angemeldet hat.

Voraussetzungen:

Der Client nutzt zur erweiterten Authentisierung ausschließlich ein Hardware-Zertifikat, und das automatisch zu verwendende VPN-Profil (in den Grundeinstellungen festgelegt als Standard-Profil nach jedem Neustart) hat folgende Konfigurationseinstellungen:

- Verbindungssteuerung / Verbindungsaufbau „immer": regt einen ständigen Verbindungsaufbau unabhängig von anstehendem Datenverkehr und Benutzereingaben an.

Kundenspezifische Anpassung für OTP-Feldbezeichner

Um in gemischten Architekturen die Felder für gleiche Eingabewerte auch mit gleichen Feldbezeichnungen versehen zu können, kann die Datei NCPMON.INI editiert werden.

Beispiel: Im Dialog für die OTP-Anmeldung gibt es die Feldbezeichner „PIN" und „Einmalpasswort". Soll in das PIN-Feld der Wert des Windows-Kennworts und in das Feld für das Einmalpasswort der Wert eines Tokens eingetragen werden, so kann demgemäß der jeweilige Feldbezeichner geändert werden. Dies erfolgt über das Client-Plugin des SEM unter der neuen Rubrik "Erweiterte Optionen".

Alternativ kann auch die NCPMON.INI modifiziert werden:

Nach dem Öffnen der Datei suchen Sie den Konfigurationsabschnitt [OTP]. Anschließend ändern Sie die Feldbezeichner rechts neben dem Gleichheitszeichen:

```
[OTP]
Caption_User = Benutzername:
Caption_Pin = Windows-Kennwort:
Caption_Pw = Token:
```

Sollen die Bezeichner mehrsprachig geändert werden, muss als Postfix zusätzlich das Kürzel der Sprache hinzugefügt werden. Existiert zur Sprache der GUI kein Eintrag, wird der Eintrag ohne Postfix verwendet.

```
[OTP]
Caption_Pin_de = Windows-Kennwort:
Caption_Pin_en = Windows Password:
Caption_Pin_fr = Windows Mot de passe:
Caption_Pin_es = Windows Contraseña:
Caption_Pw_de = Token:
Caption_Pw_en = Token:
Caption_Pw_fr = Token:
Caption_Pw_es = Token:
```

WLAN-Adapter bei gestecktem LAN-Kabel deaktivieren

Mit Hilfe der Funktion „WLAN-Adapter bei gestecktem LAN-Kabel deaktivieren" wird mobilen Teleworkern ein manuelles Umschalten erspart. Sobald ein Teleworker, der über WLAN mit dem

Firmennetz verbunden ist, inhouse das LAN-Kabel in sein Notebook steckt, wird der WLAN-Adapter deaktiviert und die LAN-Verbindung ins Firmennetz genutzt. Dies erfolgt unabhängig davon, ob er den NCP WLAN-Manager oder den eines fremden Herstellers benutzt. Wird das LAN-Kabel wieder gezogen, wird auch der WLAN-Adapter wieder aktiviert.

Die Funktion findet sich in der Monitor-Konfiguration für die WLAN-Einstellungen unter „Optionen". Sie ist nur sichtbar mit einem Lizenzschlüssel >= 10.00.

2. Verbesserungen / Fehlerbehebungen

Verbesserung der Friendly Net Detection

Damit führt der Entry Client die Zertifikatsüberprüfung des eingehenden FND-Serverzertifikats korrekt aus.

3. Bekannte Einschränkungen

Keine

Service Release: **10.00 build 21521**
Datum: **Januar 2015**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Verbesserung beim Update-Prozess

Bei einem Update-Prozess werden die Lizenzdaten der Vorgängerversion ohne erneute Eingabe von Lizenzschlüssel und Seriennummer übernommen und im Hilfemenü unter „Lizenzinfo und Aktivierung" angezeigt. Nach der Aktualisierung müssen diese Lizenzdaten durch eine erneute (Online-)Aktivierung von der Lizenzierungsinstanz erneut bestätigt werden.

Verbesserung im Bereich starker Authentisierung mittels OTP

Ein Fehler, der sich dann einstellte, wenn der Verbindungsmodus „immer" eingestellt war und das Einmalpasswort (OTP) falsche eingegeben wurde, ist behoben.

3. Bekannte Einschränkungen

Keine

Major Release: **10.00 build 21336**
Datum: **Januar 2015**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

1. Neue Leistungsmerkmale und Erweiterungen

MSI-Installer – Update auf die NCP Secure Entry Client Version 10.0

Der NCP Secure Entry Client wird ab Version 10.00 im Microsoft-Format MSI ausgeliefert. Die Einführung des neuen Formats erfordert folgendes Vorgehen:

- NCP Secure Entry Clients einer früheren Version als 10.x müssen deinstalliert werden. Anschließend kann die Neu-Installation mit dem MSI-Packet auf dem Endgerät erfolgen. Im Weiteren können neue Versionen via MSI-Update-Funktionalität eingespielt werden.

Modi des Verbindungsaufbaus

Die Auswahl für die Voreinstellungen des VPN-Verbindungsaufbaus wurde um zwei Modi erweitert. Zusätzlich wurden die Auswahlmöglichkeiten detaillierter benannt. Folgende Optionen für den Verbindungsaufbau stehen nun zur Verfügung:

manuell / (Standardeinstellung des Verbindungsmodus)

Unter dieser Einstellung muss die VPN-Verbindung vom Anwender über den Schalter in der Benutzeroberfläche manuell hergestellt werden. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout. Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, muss die Verbindung manuell getrennt werden.

automatisch (Datenverkehr initiiert VPN-Verbindung)

Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt sobald ein Datentransfer ansteht. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen des Profils.

immer

Mit dieser Einstellung wird unmittelbar nach dem Start des Clients ständig der VPN-Verbindungsaufbau angeregt. Dies erfolgt unabhängig vom Betätigen des Verbinden-Buttons, unabhängig von anstehendem Datenverkehr und unabhängig von der Darstellung des Monitors, die unter Autostart eingestellt werden kann.

wechselnd (automatischen Modus manuell starten)

Wird dieser Modus gewählt, muss zunächst die Verbindung "manuell" aufgebaut werden. Danach wechselt der Modus je nach Art des Verbindungsabbaus:

– Wird die Verbindung mit Timeout also automatisch beendet, so wird die Verbindung für den nächsten Datentransfer wieder automatisch hergestellt;

– wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

Wichtig: Sollten Sie den Verbindungsaufbau auf "manuell" umschalten, so sollten Sie den Timeout aktivieren und auf einen anderen Wert als null (0) setzen, um den Verbindungsabbau zu automatisieren.

wechselnd (Immer-Modus manuell starten)

Ist dieser Modus eingestellt, wird mit dem einmaligen Betätigen des Verbinden-Buttons der beständige Verbindungsaufbau "immer" angeregt. Dies erfolgt für die gesamte Betriebszeit des Monitors bis zu dessen Beenden.

Erweiterte Log-Einstellungen

In den erweiterten Log-Einstellungen, unter „Hilfe / Erweiterte Log-Einstellungen" im Monitormenü, kann der Zyklus bzw. die maximale Anzahl der gespeicherten Log-Dateien verändert werden.

Die Aufrufe der Kommandozeilen-Tools RWSCMD und NcpClientCmd inklusive der eingesetzten Parameter können in eine Logdatei geschrieben werden. Dazu müssen diese Anwendungen in den erweiterten Log-Einstellungen aktiviert werden. Alternativ kann dies auch über die NCPMON.INI mit der Zeile "[RWSCMD]Logs=1" angeregt werden. Die Logausgabe erfolgt als "RwscmdLog.txt" in das Log-Verzeichnis.

Erweiterung des Support-Assistenten

Der Support-Assistent wurde erweitert, damit jetzt auch die Log-Dateien von Microsoft für die Treiber-Installation hinzugefügt werden können.
Folgende Dateien werden dann hinzugefügt falls sie verhanden sind:
WINDOWSDIR\inf\setupapi.dev.log
WINDOWSDIR\inf\setupapi.app.log
WINDOWSDIR\inf\setupapi.setup.log

Optimierte IKEv2-Konfiguration

Der Client-Monitor bietet in den IPsec-Einstellungen (unter „Konfiguration") die Möglichkeit für IKEv2 eigene Richtlinien anzulegen. Nach diesen Richtlinien erfolgt der IKEv2-Schlüsselaustausch.

Die weitere IKEv2-Konfiguration befindet sich in der Standard-Profilkonfiguration. Hier kann die zugehörige Authentisierung – Zertifikat, Pre-shared Key oder EAP – konfiguriert werden.

Entsprechend der gewählten Authentisierungsmethode werden Eingabefelder für VPN-Benutzername und Passwort bzw. die IKE-ID ein- oder ausgeblendet.

In den Profil-Einstellungen unter „IPsec" wird die gewünschte IKEv2-Richtlinie selektiert, sofern nicht der automatische Modus gewählt wird. Zusätzlich können Diffie-Helman- und PFS-Gruppen bestimmt werden, welche für den IKEv2-Schlüsselaustausch elliptische Kurven verwenden (ECP mit DH-Gruppen: 19, 20, 21, 25, 26).

Über den Editor-Button kann von der IPsec-Konfiguration der Profil-Einstellungen direkt zur Konfiguration der Richtlinien gewechselt werden.

Unterstützung von elliptischen Kurven in Zertifikaten und Schlüsselaustauschverfahren (ECC, Elliptic Curve Cryptography)

Um Zertifikate mit elliptischen Kurven einsetzen zu können, wird auf verschiedene Speichermedien bzw. –Orte zugegriffen. Sie können aus PKCS#12-Dateien gelesen bzw. über die PKCS#11- oder PC/SC-Schnittstelle via Smartcard-Leser ausgewertet werden. Ebenso ist der Zugriff auf sie über den Windows CSP bzw. CNG möglich.
Die Verifizierung der Signatur, erstellt nach dem Prinzip der elliptischen Kurven, ist nur für IKEv2 spezifiziert. Neuere Smartcards wie die TCOS 3.0 V2, welche nur noch die Verschlüsselungsmethode der elliptischen Kurven verwenden, können daher nur bei IKEv2-Übertragungen eingesetzt werden.

Prüfung auf Datendurchsatz im Tunnel

Unter schwierigen Mobilfunk-Empfangsverhältnissen kann es vorkommen, dass trotz eines grün angezeigten VPN-Tunnels im Client-Monitor keine Daten durch den VPN-Tunnel transportiert werden können. Um auch in solchen Situationen dem Anwender eine korrekte Rückmeldung zu geben, lässt sich in der Client-Konfiguration unter „Verbindungen" ein automatischer Ping auf eine beliebige

Zieladresse im Remote-Netzwerk konfigurieren. Wird der Ping nicht beantwortet, so wird der VPN-Tunnelstatus entsprechend gesetzt.

AES_GCM - Galois/Counter Mode

Der Galois/Counter Mode (GCM) bietet einen authentifizierten Verschlüsselungsmodus, d.h. dieser Betriebsmodus kombiniert Verschlüsselung und Integritätsschutz. Desweiteren wurde dieser Verschlüsselungsmodus aufgrund seiner Eignung bei hohem Datendurchsatz und seiner Performance implementiert.

AES_GCM 128 oder 256 kann als Verschlüsselungsalgorithmus in der Konfiguration der IKEv2-Richtlinien und der IPsec-Richtlinie eingesetzt werden, wobei ein zusätzlicher Integritätsalgorithmus entfallen kann.

Neue Konfigurationsmöglichkeit in der Firewall

Wird in der Konfiguration der Firewall unter „Optionen" der Schalter „ausgehenden Verkehr mit Reject quittieren" gesetzt, so werden blockierte Datenpakete nicht verworfen, sondern der blockierte ausgehende Datenverkehr wird mit einem Reject quittiert.

Die Verbindungsmedien xDSL (PPP over Capi) und PPTP werden nicht mehr unterstützt

Das Tunnelprotokoll IPsec over L2TP wird nicht mehr unterstützt

MSI-Installer – NCP spezifische Funktionen

Beim Installieren eine CNF-Datei hinzufügen

Bei der Installation des MSI-Pakets kann weiterhin eine CNF-Datei mit installiert werden. Musste beim früheren Setup die CNF-Datei in das Disk1-Verzeichnis kopiert werden, kopiert der Installer die CNF-Datei nun selbständig in das Installationsverzeichnis, sobald er sie in dem Verzeichnis findet, in dem auch das MSI-Paket oder der Installer als EXE-Datei liegt. Der Rückgabewert beim Kopieren wird nicht berücksichtigt. Bei einem Fehler bricht die Installation nicht ab.

Beim Installieren zusätzliche Dateien hinzufügen

Zusätzliche Dateien können zum Beispiel eigene Zertifikate oder Dateien für ein kundenspezifisches Projekt-Logo (CBO) sein, welche mit dem Setup installiert werden sollen.

Früher wurde im Disk1-Verzeichnis ein Unterverzeichnis **ncple** angelegt, woraus alle Dateien inklusive Unterverzeichnisse entnommen und in das Installationsverzeichnis mit installiert wurden.

Dies erfolgt jetzt anders. Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet das Verzeichnis **IMPORTDIR**, werden aus diesem Verzeichnis alle Dateien rekursiv, inklusive aller Unterverzeichnisse, ins Installationsverzeichnis mit installiert. Der Rückgabewert beim Kopieren wird nicht berücksichtigt. Bei einem Fehler bricht die Installation nicht ab. Da diese Dateien der Installer nicht kennt werden diese weder aktualisiert noch deinstalliert.

Eine weitere Möglichkeit Dateien, Icons, Registry-Einträge, usw. einer Installation hinzufügen ist der Weg über eine Transform-Datei. Hierfür kann über Admin-Tools diverser Hersteller (z.B. InstallShield, SuperOrca) das MSI-Paket geöffnet werden, beliebige Features, Komponenten, Dateien usw. hinzufügt werden und eine Transform-Datei erstellt wird, welche bei der Installation übergeben wird.

msiexec /i myproduct.msi TRANSFORM=mytransfom.mst

Dies ist der offizielle Weg, ein bestehendes MSI-Paket zu ergänzen. Vorteil ist, dass diese Ergänzungen dem Installer bekannt sind und er diese aktualisieren und deinstallieren kann.

Beim Installieren eine Batch-Datei ausführen

Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet die Datei **NcpInstall.bat**, wird diese vom Installer am Ende der Installation ausgeführt. Der

Rückgabewert wird nicht berücksichtigt. Tritt bei der Ausführung der Batch-Datei ein Fehler auf, so bricht die Installation nicht ab. Die Ausführungen sind dem Installer nicht bekannt und er kann diese auch nicht verwalten.

Testversion sofort starten

In manchen Projekten besteht der Wunsch, dass beim ersten Start des Monitors die Testversion ohne Abfrage „Testversion jetzt starten?" sofort gestartet wird. Dies wird jetzt über den Kommandozeilenparameter „STARTTESTVERSION=1" ermöglicht:
msiexec /i myproduct.msi STARTTESTVERSION=1

Silent Installation und Deinstallation

Die frühere Silent Installation wird durch eine neue Form ersetzt, wobei der Windows Installer eingesetzt wird. Er unterstützt eine eigene Silent Installation, welche über die Anzeigeoptionen angeben werden kann. Z.B.: msiexec /i myproduct.msi /qn myproduct.exe /v"/qn"

Die frühere Form der Silent Deinstallation wird abgelöst über eine, welche über die Anzeigeoptionen durchgeführt wird. Z.B.: msiexec /x myproduct.msi /qn

Protokollierung

Früher konnte über die NCP-spezifische SetupExt.ini ein Teil des Setups protokolliert werden. Jetzt gestattet der Windows Installer eine eigene sehr umfangreiche Protokollierung. Über die Protokollierungsoptionen kann diese konfiguriert werden.
Z.B.: msiexec /i myproduct.msi /log "c:\temp\myinstall.log"
myproduct.exe /v"/log "c:\temp\myinstall.log""

MSI-Datei extrahieren

Die MSI-Datei ist in der bereitgestellten EXE-Datei enthalten. Sie kann durch folgende Eingabe aus der EXE-Datei extrahiert werden:
setup.exe /b"C:\FolderInWhichMSIWillBeExtracted"

Das gestartete Installations-Setup kann nun abgebrochen werden und die MSI-Datei aus dem angegebenen Verzeichnis verwendet werden. Für die Softwareverteilung darf die MSI-Datei nicht umbenannt werden, da es im Update-Fall hier zu Fehlersituationen kommen kann. Aus diesem Grund stellt NCP ausschließlich die ausführbare EXE-Datei zur Verfügung, die im Dateinamen auch die aktuelle Version enthält. Die aktuelle Version ist im Namen der MSI-Datei nicht enthalten.

Bei Deinstallation alle Dateien löschen

Früher wurde bei der Deinstallation über die GUI im letzten Dialog abgefragt, ob die persönlichen Daten gelöscht werden sollen, bevor sie entfernt wurden. Bei der Silent-Deinstallation konnte das Attribut -delall angegeben werden.

Dies ändert sich jetzt mit der Art der Deinstallation. Wird der Client mit dem Assistenten deinstalliert, erfolgt die Abfrage, ob alle Dateien entfernt werden sollen, bevor dies erfolgt. Wird er direkt deinstalliert (kleiner Dialog), erfolgt keine Abfrage und die persönlichen Daten bleiben erhalten. In diesem Fall kann über die Kommandozeile die Eigenschaft DELETEALL=1 gesetzt werden, damit alle Dateien entfernt werden. Z.B.: msiexec /x myproduct.msi DELETEALL=1

2. Verbesserungen / Fehlerbehebungen

OpenSSL Version 1.0.1j

In der Client Software wird OpenSSL 1.0.1j eingesetzt. Sicherheitsdefizite in Verbindung mit früheren Versionen der OpenSSL Libraries sind damit behoben.

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/download-software/versionsinformationen.html

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

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Beachten Sie dazu die „Voraussetzungen" auf Seite 1.

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 einschl. Mobility and Multihoming Protocol (MOBIKE)
  - 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 (and associated Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) – (Benutzername und Passwort für Client-Authentisierung 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 die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP)
- 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-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; 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 für asymmetrischen Schlüsselaustausch und PFS.
- Diffie Hellman Gruppen 19 - 21, 25 - 26 mit Algorithmus elliptischer Kurven.

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
- Option: ausgehenden Verkehr mit Reject quittieren

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 NCP Server-Komponenten (Secure Enterprise VPN Server);
  - zur Datenübertragung innerhalb des VPN-Tunnels wird IPv4 genutzt

Verbindungs-Medien

- LAN
- WLAN
- GPRS / 3G (UMTS, HSDPA), GSM (einschl. HSCSD)
- xDSL (PPPoE)
- 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
- WLAN Roaming (handover)
- Modi des Verbindunsaufbaus
  - 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, GPRS/UMTS, xDSL, 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

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 v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (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),

Zusätzliche Extended Key Usages:

- id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17)
- 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

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.

Client Monitor

Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch, Spanisch)
  - Monitor & Setup: en, de, fr, es
  - Online Hilfe und Lizenz en, de, es
- 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 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
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)

Hinweise

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

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