Release Notes

NCP Secure Enterprise Linux Client

Service Release: **3.23 Build 038**
Date: **Februar 2012**

1. Neue Leistungsmerkmale und Erweiterungen

Im folgenden die wichtigsten Leistungsmerkmale, die gegenüber den Versionen des Secure Enterprise Client Linux 2.10 Build 028 und Secure GovNet Client Linux 2.31 Build 013 hinzugekommen sind:

Unterstützung von Linux Betriebssystemen 32 Bit und 64 Bit

Der Enterprise Client unterstützt die folgenden Betriebssysteme in 32- und 64-Bit-Versionen: Ubuntu Desktop 10.04.3 LTS, open SUSE 11.3, 11.4, 12.1, Fedora 16, Debian 5.0.8.

Oberfläche des Monitors

Die Oberfläche des Enterprise Client-Monitors ist durchgehend plattformübergreifend gestaltet, sodass lokal für den Benutzer wie auch am Secure Enterprise Management (SEM) für den Administrator die Konfiguration ohne relevante Systemunterschiede vorgenommen werden kann. Dies gilt für die unterstützten Betriebssysteme Linux, Mac OS X und Windows (siehe Leistungsumfang).

Multi-Zertifikatsunterstützung und Konfiguration

In der Konfiguration des Clients kann eine Vielzahl individueller Zertifikatseinstellungen als Multi-Zertifikatskonfiguration hinterlegt werden. Aus den verschiedenen Zertifikatskonfigurationen kann pro Profil jeweils eine selektiert werden. Dadurch besteht die Möglichkeit der Authentisierung mit unterschiedlichen Zertifikaten gegen verschiedene VPN-Gegenstellen, z. B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Smartcard gespeicherten Zertifikat.

Im Konfigurationsfeld "Security" kann das Zertifikat dieser Zertifikatskonfiguration für die Verschlüsselung und Authentisierung im Security-Modus L2Sec oder für die erweiterte Authentisierung (Extended Authentication) im Security-Modus IPSec selektiert werden.

Die Zertifikatskonfiguration des Clients ist vorkonfigurierbar über:

- Management Server: Version 2.05
- Management Console: Version 2.05
- Client Plug-in: Version 9.30 Build 48

VPN Path Finder mit Proxy-Unterstützung

Der VPN Path Finder schaltet automatisch auf das alternative Verbindungsprotokoll TCP Encapsulation mit SSL Header (Port 443) um, sobald Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist.

Dies ist dann von Bedeutung, wenn für den Client nur der HTTPS Port 443 zur Verfügung steht und eine reine IPsec-Verbindung nicht möglich ist, wie dies z. B. in Hotels oder an Hotspots der Fall sein kann.

Die Konfiguration erfolgt in den Profil-Einstellungen unter "Erweiterte IPsec-Einstellungen" und im Konfigurations-Menü des Monitors.

Der VPN Path Finder setzt als Gegenstelle ein NCP Gateway (>= V. 8) voraus. Dort muss in den VPN / IPsec-Einstellungen des lokalen Systems ein "alternativer" Port konfiguriert sein.

Wird der VPN Path Finder verwendet und muss der Internet-Verbindung ein Proxy Server vorgeschaltet sein, so kann im Konfigurations-Menü des Monitors unter "Proxy für VPN Pathfinder" der Proxy Server des Browser selektiert werden oder ein firmeneigener Proxy Server angegeben werden.

Wurde die Verbindung mit der VPN Path Finder Technology über den Port 443 aufgebaut, wird dies über ein Icon in der Statusanzeige des Monitors (rechts unter dem HQ/Gateway) angezeigt. Das Icon erscheint in der Monitor-Oberfläche bei der VPN-Einwahl.

Hotspot-Anmeldung via Browser

Beim ersten Öffnen der Konfigurationseinstellungen ist die Verwendung des Standard-Browsers für die Hotspot-Anmeldung aktiviert (sofern vom Administrator nichts anderes vordefiniert wurde).

Die Hotspot-Automatik der Personal Firewall des Clients sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN auf den eigenen Rechner werden unterbunden. Die Firewall gibt dynamisch die Ports für http (80) bzw. https (443) für Anmeldung und Abmeldung am Hotspot frei, sobald der Menüpunkt „Hotspot-Anmeldung" angeklickt wird, und verhindert, dass sich der Benutzer frei im Internet bewegen kann.

Friendly Net Detection

Mittels der Friendly Net Detection können unterschiedliche Firewall-Regeln für bekannte und unbekannte Netzwerke definiert werden. So lassen sich beispielsweise in einem bekannten Firmennetz gezielte Freigaben auf den Anwenderrechner zu Administrationszwecken definieren. Dagegen ist der Rechner im unbekannten Netzwerk komplett abgeschottet.

Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Dies kann erfolgen durch eine manuelle Konfiguration oder mittels des Automatismus über Friendly Net Detection, welche die Installation eines Friendly Net Detection Servers im Firmennetz voraussetzt.

Die manuelle Definition eines bekannten Netzes durch den Administrator und die automatische Erkennung eines bekannten Netzes mittels Friendly Net Detection schließen sich nicht aus, sondern können gleichzeitig eingesetzt und über die Registerkarten "Manuell" und "Automatisch" konfiguriert werden.

Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, das sich grün färbt, sobald sich der Client mit einem Friendly Net verbunden hat.

Der FND Server kann auch über DHCP zugewiesen werden. Über eine DHCP-Option (159) am DHCP Server kann die Zieladresse des FND-Servers an den Enterprise Client übermittelt werden, sodass sich der Client im LAN sogleich in seinem ihm zugewiesenen Friendly Net befindet. (Adressen von FND Servern in der Firewall-Konfiguration des Clients werden solange außer Kraft gesetzt, wie der Client eine FND-Adresse über DHCP zugewiesen bekommt.) Der entsprechende Parameter befindet sich im Konfigurationsmenü unter Firewall / Bekannte Netze / Automatisch.

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 die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- 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 oder 256 Bit oder Triple DES

Erweiterte 3G / UMTS-Konfiguration

In den Profil-Einstellungen wurde für das Verbindungsmedium "GPRS / UMTS" (GPRS / 3G auf Englisch) ein eigenes Parameterfeld angelegt.

Darin werden drei Varianten der UMTS-Konfiguration angeboten:

Providerliste (Standardeinstellung): Hier wird durch die Auswahl des Providers der APN und die Einwahlnummer vorgeschlagen;

APN von SIM Karte: Hier wird der APN aus der SIM-Karte gelesen. (Dies funktioniert nur wenn ein APN in der SIM-Karte konfiguriert ist);

Benutzerdefiniert: Hier kann der Anwender sämtliche Einwahlparameter manuell konfigurieren.

Die Providerliste kann über die Datei APN.ini (im Installationsverzeichnis) beliebig erweitert werden.

2. Fehlerbehebungen

Keine

3. Bekannte Einschränkungen

Verwendung von Sonderzeichen und Umlauten

Die Verwendung von Sonderzeichen und Umlauten innerhalb der Konfiguration oder dem VPN-Verbindungsaufbau wird nicht empfohlen, da diese Zeichen u.U. nicht korrekt interpretiert werden, sodass sich Authentisierungsfehler ereignen können.

4. Hinweise zum NCP Secure Enterprise Linux Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/vpn-client.html

Weitere Unterstützung bei Fragen zum , 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 Enterprise Client - Helpdesk message

5. Leistungsmerkmale

Zentrale Verwaltung

Das NCP Secure Enterprise Management (SEM) bietet als ***Single Point of Administration*** alle Funktionalitäten und Automatismen für Rollout, Inbetriebnahme und den wirtschaftlichen Einsatz eines Secure Enterprise Clients.
Das Secure Enterprise Management (SEM) versorgt den Enterprise Client über die VPN-Verbindung oder LAN (im Firmennetz) automatisch mit

- Konfigurations-Updates
- Zertifikats-Updates
- Aktualisierungen des Update Clients

Network Access Control / Endpoint Security

Die Richtlinien für eine Endpoint Security (Endpoint Policy Enforcement) werden am Secure Enterprise Management (SEM) zentral erstellt. Entsprechend der erstellten Regeln erhält der Enterprise Client Zugang zum Firmennetz.

High Availability Services

Der NCP Secure Enterprise Client unterstützt die NCP HA Services, die nach dem Client Server-Prinzip arbeiten und in unterschiedlichen Betriebsmodi (Load Balancing- und Failsafe-Modus) eingesetzt werden können. Die VPN-Verbindung wird für den Anwender des Enterprise Clients im Hintergrund auch bei hohem Lastaufkommen oder einem Serverausfall ohne zeitliche Verzögerung sicher ins Firmennetz aufgebaut.

Betriebssysteme

Linux 32 & 64 Bits
Distributions: Ubuntu Desktop: 10.04.3 LTS; openSUSE: 11.3, 11.4, 12.1; Fedora 16; Debian 5.0.8

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)
  - Kommunication 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 und Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP)
  - Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure

- Benutzer-Authentisierung:
  - XAUTH für erweiterte Benutzer-Authentisierung
  - One-Time-Passwörter und Challenge Response Systeme
  - Zugangsdaten aus Zertifikate (PKI)
- Unterstützung von Zertifikaten in einer PKI:
- Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless Rekeying
- PAP, CHAP
- HTTP Authentisierung vor VPN
- Hotspot Anmeldung mit HTTP
- 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 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
  - Soft-Zertifikate
  - PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- PIN Richtlinien: Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- 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, mit DHCP-Servers oder eines NCP FND-Servers
- Sichere Hotspot Anmeldung
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports, Applikationen und Adressen
  - Schutz des LAN adapter
- Zentrale Administration [ii]
- IPv4 Fähigkeit

Endpoint Security

- Endpoint Policy Enforcement [ii]

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
- GPRS / 3G (UMTS, HSDPA), GSM (einschl. HSCSD)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)

Dialers

- NCP Secure Dialer

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

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 bis HTTPS (port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist [iii]

Datenkompression

- IPsec Compression: lzs, deflate

Link Firewall

- Stateful Packet Inspection

Weitere Features

- VoIP Prioritization

- UDP Encapsulation
- IPsec Roaming [iii]

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)

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)
- Monitor & Setup: en, de
- Online Hilfe und Lizenz en, de
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – overview of :
  - 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
- Unterstutzung von Mobile Connect Cards (PCMCIA, embedded) integriert
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool fur Fehlerdiagnose

Hinweis

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 Management

iii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später

Weitere Informationen zum NCP Secure Enterprise Linux Client finden Sie hier:
http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung.html