NCP Secure Client – Juniper Edition
Release Notes

Service Release: **10.11 r32792**
Datum: **November 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden 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.

1. Neue Leistungsmerkmale und Erweiterungen

VPN-Bypass

Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Diese Funktion kann unter anderem dazu genutzt werden, um regelmäßig notwendige, nicht sicherheitsrelevante Datenübertragung von der zentralen Infrastruktur fernzuhalten, um deren Performance nicht zu beeinträchtigen. Zum Beispiel könnten Updates des Betriebssystems oder des Virenscanners (mit bekannter Domäne) ohne Umweg über die VPN-Verbindung zugelassen werden, oder bei bestimmten Cloud-Services der direkte Zugriff einer Anwendungen über das Internet ermöglicht werden.
Die Konfiguration erfolgt über den Client-Monitor über „Konfiguration / VPN-Bypass“ und in den Profileinstellungen unter „Split Tunneling / VPN-Bypassliste“.

Auswahl eines Benutzer- oder Computer-Zertifikats im Windows-CSP

Im Konfigurationsmenü des Clients unter „Zertifikate“ kann anhand der Erweiterten Schlüsselverwendung (Extended Key Usage) die Auswahl eines bestimmten Benutzer- oder Computer-Zertifikats voreingestellt werden.

Ausgabe des MediaType mit dem Tool ncpclientcmd.exe

Das Kommandozeilen-Tool „ncpclientcmd.exe“ zeigt bei Eingabe des Kommandos „NcpClientCmd /getConnecionMedium“ das Verbindungsmedium bzw. den MediaType an.

Neues Produkt- und Status-Icon

Mit dieser Version wurden die Icons modernisiert.

Die Farben des Status-Icons wechseln beim Verbindungsaufbau von rot nach grün.

Projekt-Icon	*Status-Icons*			
	ohne VPN-Tunnel	| Tunnel-aufbau	| logischen Tunnel halten	| Tunnel aufgebaut

IKEv2 Signature Authentication nach RFC 7427

Die Client Software unterstützt für den IKEv2 die zertifikatsbasierte Authentisierung nach RFC 7427, womit auch modernes Padding-Verfahren (RSASSA-PSS) möglich ist.

2. Verbesserungen / Fehlerbehebungen

Keine

3. Bekannte Einschränkungen

Keine

Service Release: **10.10.03 r30578**
Datum: **Juni 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden 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.

4. Neue Leistungsmerkmale und Erweiterungen

Keine

5. Verbesserungen / Fehlerbehebungen

Fehlerhafte Lizenzdatei

In manchen Fällen konnte die Lizenzdatei *ncp.de* beschädigt oder gelöscht werden. Das Handling der Lizenzdatei des Clients wurde optimiert, so dass dieser Fehler nicht mehr auftritt.

Aktualisierung Installationsdateisignatur

Die Signatur der Installationsdatei wird während der Installation online vom Internet Explorer geprüft. Diese Prüfung fiel negativ aus, da das Zertifikat mittlerweile abgelaufen ist. Das Zertifikat sowie die Signatur wurden aktualisiert.

Korrektur bei manuellem Trennen und Verbinden des VPN-Tunnels

Wurde der Verbinden/Trennen-Button schnell hintereinander gedrückt, so konnte der Client in einen Zustand fallen, der keinen Verbindungsaufbau mehr zuließ. Dieser Zustand konnte nur durch einen Profilwechsel behoben werden.

Korrektur des Update-Verhaltens bei lokalem Update

6. Bekannte Einschränkungen

Keine

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

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.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Client – Juniper Edition (Win32/64)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/service/download-vpn-client/versionsinformationen.html

Weitere Unterstützung bei Fragen zum Enterprise, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://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.

Unterstützung von Juniper Gateways mit Junos- und ScreenOS-Betriebssystemen

Voraussetzung

Juniper IPsec Gateway (support for ScreenOS)

Lizenzierung

Der NCP Secure Client – Juniper Edition unterstützt wahlweise drei Arten der Lizenzierung:

Offline

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden.

Online

In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

Lizenzierung über Initialisierungs-Datei

Der Client authentisiert sich am Lizenzserver im Firmennetz mit einer durch den Administrator verteilten Initialisierungsdatei. Der Client erhält daraufhin seine eigentliche Lizenz und ist freigeschaltet. (Voraussetzung: NCP Volume License Server - vorherigen Namen NCP Local License Server)

Security Features

Unterstützung aller IPsec-Standards nach RFC

Virtual Private Networking

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

Authentisierung

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - 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 (und entsprechende 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 dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
- Benutzer-Authentisierung:
  - XAUTH (IKEv1) 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
- RSA SecurID Ready

Verschlüsselung (Encryption)

Symmetrisch: AES-GCM 128, 256 bits (nur IKEv2 & IPsec); AES-CTR 128, 256 bits (nur IKEv2 und IPsec); AES (CBC) 128, 256 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, 18, 19 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 Service Provider (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL vormals CRL)
  - Certification Authority Revocation List, (CARL vormals ARL)
  - Online Certificate Status Protocol (OCSP)

Networking Features

Sichere Netzwerk Schnittstelle

- LAN Emulation
  - Ethernet-Adapter mit NDIS-Schnittstelle

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-Medium

- LAN

Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- Modi des Verbindungsaufbaus
  - 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)

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

Datenkompression

- IPsec Kompression

Weitere Leistungsmerkmale

- Import der Dateiformate:*.ini und *.spd

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)
- UDP encapsulation of IPsec Packets (RFC 3948),

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 wird:

- 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, 256 Bit oder Triple DES

Secure 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 – 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)
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool für Fehlerdiagnose
- Tests zur Internet-Verfügbarkeit
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com