NCP Secure Client – Juniper Edition

Release: **9.32 Build 218**
Datum: **März 2014**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 8.1, 32/64 Bit
- Windows 8, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit
- Windows XP, 32/64 Bit

1. Neue Leistungsmerkmale und Erweiterungen

Logbuch-Anzeige von VPN Tunnel-Verbindungen und Datenvolumen

Zusätzlich zu den bisherigen Anzeigen werden Informationen zu erfolgreichem Auf- und Abbau von VPN Tunnel-Verbindungen so wie den darüber übertragenen Datenvolumen im Logbuch mit blauer Schrift angezeigt.

Weitere Informationen werden insbesondere zu den Medientypen UMTS und WLAN ebenfals in blauer Schrift ausgegeben.

Im Logbuch erscheinen entsprechend folgende Meldungen:

Nach erfolgtem Verbindungsaufbau:

03.02.2014 15:59:35 INFO - MONITOR: Connected -> Test Connection IPsec Native

03.02.2014 15:59:35 INFO - MONITOR: Media=GPRS / UMTS, Tx=1176 Byte, Rx=0 Byte

nur bei MediaType 3G zusätzlich:

03.02.2014 15:59:35 INFO - MONITOR: Provider=T-Mobile D, Media=UMTS

nur bei Mediatype WLAN zusätzlich:

03.02.2014 15:59:35 INFO - MONITOR: SSID=MyHomeWlan

Nach erfolgtem Verbindungsabbau:

03.02.2014 16:00:10 INFO - MONITOR: Disconnected

03.02.2014 16:00:10 INFO - MONITOR: Media=GPRS / UMTS, Tx=15509 Byte, Rx=0 Byte

Bei gescheitertem Verbindungsaufbau werden weiterhin die Errorcodes in roter Schrift angezeigt. (Siehe ErrorCodes_(en/de).txt im lokalen Installationsverzeichnis).

2. Verbesserungen / Fehlerbehebungen

Windows 8 oder Windows 8.1 und UMTS Handling

Fehler behoben

PathFinder

Fehler behoben

Forcing NAT-T in IKEv2

Fehler behoben

3. Bekannte Einschränkungen

Keine

Release: **9.32 Build 160**
Datum: **November 2013**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.32 Build 160

Windows 8.1-Anspassung

Der Secure Entry Client unterstützt das Windows Betriebssystem 8.1.

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 „Profile / Verbindungssteuerung" mit „Aktiviere Tunnel Traffic Monitoring" ein automatischer Ping auf eine beliebige Zieladresse im Remote-Netzwerk konfigurieren. Wird der Ping nicht beantwortet, so wird der VPN-Tunnelstatus entsprechend gesetzt.

IPv6-Unterstützung

Der Secure Entry Client unterstützt sowohl IPv4- als auch IPv6-Adress-Formate. D.h. als Tunnel-Endpunkte des VPN Gateways können nicht nur IPv4- sondern gegebenenfalls auch IPv6-Adressen angegeben werden.

Unabhängig von der Art der Adressierung des Tunnel-Endpunkts wird innerhalb des VPN-Tunnels immer das IPv4-Protokoll eingesetzt.

Eine IPv6-Adressierung setzt am VPN Gateway folgende Versionen voraus:

NCP Secure Enterprise VPN Server (WIN): Version 8.11 Build 180
NCP Secure Enterprise VPN Server (Linux): Version 8.11 ab Rev. 5620
(Das IPv6-Format kann auch zur Adressierung von VPN Gateways fremder Hersteller eingesetzt werden, sofern diese IPv6 unterstützen.)

Zusätzliche Informationen im System Tray

Wird der Client extern über RWSCMD oder API gesteuert, werden System Tray Balloon Tips angezeigt. Diese „Sprechblasen" informieren über den erfolgreichen Verbindungsaufbau bzw. über Konfigurationsfehler wenn die Verbindung nicht zustande kommt.

System Tray Balloon Tips informieren auch über die Nutzung von SmartCards in Verbindung mit dem Entry Client.

Verbergen des NCP-Adapters im System

Ab dem Betriebssystem Windows 7 wird der Netzwerkadapter des NCP Secure Entry Clients sichtbar installiert, um die Kompatibilität zu Fremdapplikationen zu verbessern. Ist dies nicht gewünscht, und der Adapter soll wie bei vorhergehenden Versionen unsichtbar im System sein, so ist vor der Installation der Parameter NoHideAdapter in der setupext.ini auf 0 zu setzen.

Bei einem bereits installierten Client kann der Adapter auch nachträglich von sichtbar auf unsichtbar umgeschaltet werden. Hierzu ist folgender Eintrag in der Windows-Registry zu ändern:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ncprwsnt
NoHideAdapter (DWORD): 0

2. Verbesserungen / Fehlerbehebungen

USB SmartCard Fehlerbehebungen

Ziehen und Stecken eines USB-SmartCard-Lesers unter dem Windows 8-Betriebssystem wird vom Client korrekt erkannt.

Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Beachten Sie bei einem Windows Update auf 8.1

Nach einem Windows 8.1 Update ist der NCP Secure Entry Client nicht mehr funktionsfähig. Deinstallieren Sie vor dem Update auf Windows 8.1 den Client unter Beibehaltung der Einstellungen. Anschließend installieren Sie den aktuellen Juniper Client 9.32 160.

Release: 9.31 Build 104
Datum: Januar 2013

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.31 Build 104

Unterstützung von Windows 8

Mit diesem Release der NCP Secure Client Software wird Microsoft Windows 8 unterstützt, sowohl in der Professional- als auch in der Enterprise-Version. Bei der Installation dieser Version des NCP Secure Clients auf einem neu installierten System mit Windows 8 gibt es keinerlei Einschränkungen.

Beim Upgrade eines Systems mit MS Windows 7 und NCP Secure Client Software auf MS Windows 8

Bei einem Upgrade eines Windows 7-Systems mit installiertem NCP Secure Client auf Windows 8 können unter bestimmten Umständen Fehler in der Registry auftreten, die den NCP Secure Client betreffen. Für diesen Fall empfehlen wir folgende Vorgehensweise für die jeweiligen Komponenten einzuhalten:

- Profil-Einstellungen: Erstellen Sie für die Profil-Einstellungen des Secure Clients eine Profil-Sicherung über das Konfigurationsmenü des Monitors ("Konfiguration / Profil-Sicherung / Erstellen"). Als "NCPPHONE.SAV" werden die Profil-Einstellungen im Installationsverzeichnis gesichert.
- Zertifikate: Vergewissern Sie sich, dass Kopien der Soft-Zertifikate (PKCS#12-Dateien) vorliegen. Sofern Zertifikate im Microsoft CSP User Certificate Store hinterlegt sind, folgen Sie den Anweisungen von Microsoft für ein Backup des CSP Stores oder Sie stellen sicher, dass die Original-Zertifikate verfügbar sind, die für den CSP Store verwendet wurden.
- Sichern Sie alle Backup-Dateien auf einem externen Datenträger.
- Führen Sie nun das Upgrade auf Windows 8 durch.
- Führen Sie anschließend mit der aktuellsten Client-Version eine Installation über den bereits bestehenden Client durch. Das Setup-Programm erkennt automatisch, dass bereits eine Version installiert ist, aktualisiert die entsprechenden Programmdateien und sichert die bestehenden Konfigurations-Einstellungen.

Die gesicherten Backup-Dateien werden nur für den Fall benötigt, dass Einstellungen oder Zertifikate beschädigt wurden.

Änderung im Monitor-Hauptmenü

Das Log-Buch-Untermenü wurde in das Hilfe-Menü verschoben.

Monitor für Anzeigemodus "Hoher Kontrast" kompatibel

Optimierung des NCP Secure Clients bezüglich einer barrierefreien Benutzung.

Die Microsoft Betriebssystemoption „Hoher Kontrast" (Tastenkombination UMSCHALTTASTE + ALT (links) + DRUCK) wird ab sofort unterstützt.

Profilgruppen innerhalb Kontextmenü und Profilauswahl im Tray-Icon

Das aktuelle Verbindungs-Profil kann über drei Wege gewechselt werden: über das Konfigurations-Menü des Monitors unter „Profile", über das Kontext-Menü oberhalb der Weltkarte des Client-Monitors oder im Menü des Tray-Icons. Konnten bei Verwendung von Profil-Gruppen in den beiden letzten Fällen bislang nur die Profile der vorselektierten Gruppen ausgewählt werden, so lassen sich nun auch die Profil-Gruppen und deren einzelne Profile auswählen.

Client deaktivieren

Um eine lizenzierte Client Software bei einem Rechnerwechsel ohne Einschränkungen weiterhin benutzen zu können, müssen die Lizenzdaten (Seriennummer und Lizenzschlüssel), die an Hardware

und Betriebssystem gebunden sind, vorher vom NCP Aktivierungs-Server für eine erneute Lizenzierung freigegeben werden.

Der Anwender gibt dem Aktivierungs-Server bekannt, dass er vorübergehend seine Lizenz nicht einsetzt, indem er im Hilfe-Menü des Monitors den Menüpunkt „Client deaktivieren" selektiert. In einer Eingabemaske gibt der Anwender daraufhin seinen Namen, optional auch den seiner Firma, sowie eine gültige E-Mail-Adresse an. Klickt der Benutzer auf „abschicken", werden diese Daten plus Seriennummer, Lizenzschlüssel und die Sprach-ID an den Aktivierungsserver geschickt.

Der Client deaktiviert sich daraufhin, erkennbar am Text „Software nicht aktiviert", der in einem Banner der Client-Oberfläche dargestellt wird.

Der Anwender erhält an die angegebene E-Mail-Adresse eine Nachricht mit einem Link. Erst nachdem der Link angeklickt wurde, wird die Lizenz am Aktivierungs-Server zurückgesetzt, d.h. die Lizenzdaten können für eine Aktivierung der Client Software an einem anderen Rechner erneut eingegeben werden.

Import von Profil-Dateien ANSI- und im UTF8-Format

INI-Dateien, welche Client-Profile auch mit Umlauten oder Sonderzeichen enthalten, werden sowohl im ANSI- als auch im UTF8-Format von der Client-Software korrekt verarbeitet.

2. Verbesserungen/Fehlerbehebungen in Release 9.31 Build 104

Keine

3. Bekannte Einschränkungen in Release 9.31 Build 104

Keine

Release: **9.30 Build 186**
Datum: **Juli 2012**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.30 Build 186

Beim Start des Monitors können die Wartezeiten für die Dienste konfigurierte werden

In seltenen Fällen kann es vorkommen, dass die voreingestellten Zeiten nach dem Start des Monitors nicht ausreichen um die NCP-Dienste zu starten und es kommt zu einer Fehlermeldung. Die Ursache für die Startverzögerung liegt in den Systemeinstellungen des Rechners. Ab sofort kann die Wartezeit wahlweise konfiguriert werden.

Beschreibung: Wird der Monitor gestartet, wartet dieser zunächst maximal 60 Sekunden bis der NCPCLCFG-Dienst gestartet und anschließend noch einmal maximal 120 Sekunden bis der NCPRWSNT-Dienst gestartet ist. Reichen diese Zeiten nicht aus, kann die Wartezeit in der NCPMON.INI durch Änderungen im Abschnitt „General" bedarfsgerecht konfiguriert werden:

[GENERAL]

WaitForConfigService = 60 (NcpClCfg-Dienst, Standard 60 Sekunden)

WaitForDriverService = 120 (NcpRwsnt-Dienst, Standard 120 Sekunden)

Die Ursachen der Verzögerung sind von der Konfiguration des Betriebs-Systems abhängig. Folgende Fehlermeldungen werden gezeigt:

- *Service "NCPCLCFG" ist nicht gestartet*
  In diesem Fall erhöhen Sie den Wert für den Parameter WaitForConfigService.
- *Die Client Software hat ein Problem mit der Treiber-Schnittstelle festgestellt (Mif32Init). Bitte starten Sie das System neu. Sollte das Problem weiter bestehen kontaktieren Sie den Support.*
  In diesem Fall erhöhen Sie den Wert für den Parameter WaitForDriverService.

Die ursächlichen Systemeinstellungen des Rechners können ggf. mit Hilfe des Supports korrigiert werden. Die Verlängerung der Wartezeiten sollte allerdings nur eine Interimslösung sein.

Support Assistent und erweiterte Log-Einstellungen

Zwei neue Hilfe-Menüpunkte erhöhen die Benutzerfreundlichkeit:

- „Support-Assistent": Assistent mit Auswahlliste welche Informationen via E-Mail an den Herstellersupport mitgeteilt werden.
- „Erweiterte Log-Einstellungen": Aktivieren erweiterter Logs und Trace-Funktionalität für den Supportfall.

Wichtiger Hinweis: Achtung beim Update von Windows 7 auf Windows 8

Beim Update des Betriebssystems Windows 7 auf Windows 8 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. Ist das Update auf Windows 8 abgeschlossen, sollte die neueste Version der NCP Secure Clients von der NCP-Website heruntergeladen und installiert werden. Erfolgt das Windows-Update ohne vorherige Deinstallation des NCP Secure Clients kann eine Neuinstallation von Windows 8 notwendig werden.

2. Verbesserungen/Fehlerbehebungen in Release 9.30 Build 186

Kompatibilitätsprobleme mit dem Symantec Security Center

Probleme beseitigt.

Änderungen der Proposals für Pre-shared key/XAUTH

Folgende Proposals wurden beim aggressive Mode in Verbindung mit Pre-shared key/XAUTH entfernt:
{ AES_CBC , HASH_SHA , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_MD5 , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_SHA , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 },
{ AES_CBC , HASH_MD5 , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192 }

3. Bekannte Einschränkungen in Release 9.30 Build 186

Keine

Release: **9.30 Build 146**
Datum: **April 2012**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.30 Build 146

Neue Option: Anti-replay Protection

Zeitversetzt eintreffende IP-Pakete könnten korrupt sein. Mit dieser Funktion (nach RFC 2064) werden diese Pakete verworfen.

(Profil Einstellungen / Erweiterte IPsec-Optionen / Anti-replay Protection)

Folgende Meldung zeigt das Erkennen und Verwerfen der Pakete an:
"Esp: Warning - AntiReplay error on sequence number=xxxx"

2. Verbesserungen / Fehlerbehebungen in Release 9.30 Build 146

Symantec Network Threat Protection

Es wurde ein Kompatibilitätsproblem in Verbindung mit einer Symantec Network Threat Protection behoben.

3. Bekannte Einschränkungen in Release 9.30 Build 146

Keine

Release: **9.30 Build 133**
Datum: **März 2012**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.30 Build 133

Erweiterung der Zertifikats-Konfiguration

Wird ein Hardware-Zertifikat im lokalen Computer-Zertifikatsspeicher (CSP) von Windows abgelegt, d. h. unter Windows in diesen Zertifikatsspeicher importiert, so kann dieses Zertifikat vom Client zur Authentisierung genutzt werden. Wurden mehrere Zertifikate in den Computer-Zertifikatsspeicher importiert, so kann in der Konfigurationsoberfläche das gewünschte Zertifikat durch Eingabe von Common Name des Antragstellers und Ausstellers (Subject CN und Issuer CN) selektiert werden.

Künftige Unterstützung der Plattform Windows 8

Der NCP Secure Client kann auf Windows 8 Beta-Versionen installiert werden. Das zugrunde liegende Betriebssystem wird zur Zeit nur experimentell unterstützt. NCP kann daher keine Gewähr für die korrekte Funktion des NCP Secure Clients unter dem aktuell vorliegenden Windows 8 geben. Bei Installation des Clients wird darauf hingewiesen, dass es zu Fehlfunktionen kommen kann.

Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen

In der Standardeinstellung des Clients bleibt der VPN-Tunnel weiterhin bestehen, nachdem die Verbindung über das jeweilige Verbindungsmedium eines VPN-Profils unterbrochen wurde. D. h. der VPN-Tunnel wird über einen beliebig langen Zeitraum bis zum Wiederaufbau der physikalischen Verbindung über das jeweilige Medium logisch gehalten.

Während der Haltedauer der logischen Verbindung wird der grüne Balken der VPN-Verbindung im Client-Monitor in gestrichelter Form dargestellt. Während dieser Zeitspanne leuchtet das Ampellicht im Systemtray gleichzeitig grün und gelb bis die physikalische Verbindung wieder hergestellt ist (grünes Licht).

Dieses Verhalten des Monitors geht verloren, wenn das voreingestellte Standardverhalten umgeschaltet wird (Profil Einstellungen / Verbindungssteuerung).

2. Verbesserungen / Fehlerbehebungen in Release 9.30 Build 133

Keine

3. Bekannte Einschränkungen in Release 9.30 Build 133

Keine

Release: **9.30 Build 102**
Datum: **Februar 2012**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.30 Build 102

Optische Rückmeldung beim logischen Halten des Tunnels

Wenn die Verbindung über das jeweilige Verbindungsmedium eines VPN-Profils unterbrochen wird, bleibt der VPN-Tunnel weiterhin bestehen. D. h. der VPN-Tunnel wird über einen beliebig langen Zeitraum bis zum Wiederaufbau der physikalischen Verbindung über das jeweilige Medium logisch gehalten.

Während der Haltedauer der logischen Verbindung wird der grüne Balken der VPN-Verbindung im Client-Monitor in gestrichelter Form dargestellt. Während dieser Zeitspanne leuchtet das Ampellicht im System-tray gleichzeitig grün und gelb bis die physikalische Verbindung wieder hergestellt ist (grünes Licht).

Verliert der Client die Internet-Verbindung und der Tunnel wird logisch gehalten, wird dieser Status mit einem Ballon über dem Tray-Icon angezeigt. Somit wird der Benutzer auch darüber informiert, wenn der Monitor minimiert ist.

Erweiterungen von Online-Hilfe und Tipps

Die Hilfetexte wurden der aktuellsten Version des Clients angepasst. Der Dialog für die Profil-Gruppen wurde um einen Hilfe-Button erweitert. Alle Hilfetexte können wie üblich über einen Hilfe-Button oder kontextsensitiv mit der F1-Taste aufgerufen werden.

2. Verbesserungen / Fehlerbehebungen in Release 9.30 Build 102

Blockierter Monitor

Wurde eine PKI-Fehlermeldung über die Callback-Funktion angezeigt, bevor der Monitor aufgebaut war und der Monitor minimierte sich beim Start, konnte die Fehlermeldung nicht angezeigt werden und der Monitor war blockiert.

Fehler beim Aufbau der Routing-Tabelle

Der Client überwacht DHCP Requests an alle Netzwerk-Adapter, um IP-Informationen über jeden Adapter zu erhalten. In bestimmten Situationen ist es erforderlich, dass der Client einen DHCP-Austausch mit einem RENEW-Kommando anstößt. Wird dieses RENEW-Kommando für einen Adapter ohne IP-Adresse oder ohne Verbindungsstatus ausgeführt, so konnte die Routing-Tabelle für einige Minuten nicht aufgebaut werden.

Fehler beim Setzen der Routen im Split-Tunneling

In bestimmten Fällen wurden die Routen bei Verwendung von Split-Tunneling nicht korrekt gesetzt.

Fehlerhafte Export-Datei auf Netzlaufwerk

Bisher konnten die Profil-Einstellungen eines Clients nicht direkt in eine Datei auf einem Netzlaufwerk exportiert werden.

3. Bekannte Einschränkungen in Release 9.30 Build 102

Keine

Release: **9.30 Build 75**
Datum: **November 2011**

1. Neue Leistungsmerkmale und Erweiterungen in Release 9.30 Build 75

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.

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".

Kommandozeilen-Tool "NcpClientCmd"

Alternatives Kommandozeilenprogramm zu rwscmd welches über keinerlei graphische Ausgabe verfügt.

2. Verbesserungen / Fehlerbehebungen in Release 9.30 Build 75

Keine

3. Bekannte Einschränkungen in Release 9.30 Build 75

Keine

4. Hinweise zum NCP Secure Client – Juniper Edition

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

E-Mail: juniperhelpdesk@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Microsoft Windows (32 und 64 Bit): Windows 8, Windows 7, Windows Vista, Windows XP

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

Der NCP Secure Client – Juniper Edition unterstützt alle IPsec-Standards der Internet Society's Security Architecture für das Internet-Protokoll (IPsec) sowie alle zugehörigen RFCs.

Virtual Private Networking

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

Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode und Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für die dynamische Zuteilung einer privaten Adresse aus einem Adress-Pool
  - 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
- Unterstützung von Zertifikaten in einer PKI:
  - Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless rekeying (PFS)
- 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-256, SHA-384, SHA-512, MD5
- Diffie Hellman-Gruppen 1, 2, 5 und 14 für asymmetrischen Schlüsselaustausch und PFS

Public Key Infrastructure (PKI) – Starke Authentisierung

- X.509 v.3 Standard
- 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
- PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- Certificate Status Protocol (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- 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

LAN Emulation

- Virtueller 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

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Serve

Line Management

- Dead Peer Detection mit konfigurierbarem Zeitintervall

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 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 und Deutsch)
- 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)
- Trace Tool zur Fehlerdiagnose
- Tests zur Internet-Verfügbarkeit
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)