NCP Exclusive Remote Access Management

für Windows

Release Notes

Service Release: **5.30 r46836**
Datum: **Februar 2020**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2019 Version
- Windows Server 2016 64 Bit
- Windows Server 2012 R2 64 Bit

Das NCP Exclusive Remote Access Management ist nur in der 64 Bit Variante verfügbar.

Datenbank:

Folgende x64 Datenbanken mit zugehörigem Treiber wurden getestet und freigegeben:

Datenbank	Treiber
MariaDB 10.2.10 (x64)	MariaDB Connector/C 3.0.2 (x64) oder neuer
MS SQL Server 2016	MS SQL Server 10.00.14393.00
MS SQL Server 2019	MS SQL Server 10.00.17763.01
Oracle 12c Release 2 (12.2.0.1) Enterprise x64	ODBC InstantClient 12.2.0.1.0

Im Allgemeinen wird der Einsatz eines Connector/C-Treibers statt eines ODBC-Treibers empfohlen.

Voraussetzung für den Betrieb des NCP Exclusive Remote Access Managements

Um diese Management Version nutzen zu können bedarf es der folgenden Komponenten:

- NCP Management Console: Version 5.30
- Client Configuration Plug-in: Version 12.01 oder neuer (bei Bedarf)
- License Plug-in: Version 12.01 oder neuer (bei Bedarf)
- Radius-Plug-in: Version 5.30 oder neuer

1. Neue Leistungsmerkmale und Erweiterungen

Neue 2-Faktor-Authentisierung gemäß Time-based One-time Password Verfahren

Integration der Time-based One-time Password Authentisierung für eine 2-Faktor-Authentisierung des VPN Clients. Zur Erzeugung des Einmalpasswortes nach dem TOTP-Verfahren ist ein Software-Token wie beispielsweise der NCP Authenticator notwendig.

Voraussetzung: Client Configuration Plug-in 11.21 oder neuer

Über ein vom NCP Exclusive Remote Access Management zur Verfügung gestelltes Web-Interface ist es Anwendern möglich, in ihrer Smartphone App ein VPN-Konto für die 2-Faktor Authentisierung beim VPN-Tunnelaufbau anzulegen. Der Import der dazu notwendigen Information kann über einen QR-Code oder durch das Klicken auf einen Link im Webbrowser des Smartphones erfolgen (letzteres sofern das Web-Interface direkt über das Smartphone aufgerufen wird).
NCP empfiehlt als Smartphone App den NCP Authenticator, verfügbar im Apple App Store sowie in Google Play Store:

Erhältlich im App Store

JETZT BEI Google play

Nach dem erfolgreichen Import des QR-Codes und damit dem Anlegen eines Kontos im NCP Authenticator, werden von diesem Passcodes gemäß RFC 6238 generiert. Als Besonderheit des NCP Authenticators, verglichen mit anderen Authenticator Apps, ist hervorzuheben, dass durch das NCP Management eine Benutzerauthentisierung am Smartphone mittels Fingerabdruck- oder Gesichtserkennung zwingend vorgegeben werden kann.
Im Rahmen der Benutzerkonfiguration im NCP Management könnte beispielsweise der Zugriff auf das Web-Interface durch den Endanwender mittels Eingabe des Benutzernamens und Domänenpasswortes vergeben werden. Der Zugriff via VPN-Client dagegen durch Eingabe des Passcodes und ggf. Überprüfung des Maschinenzertifikates.

Konfiguration der Passwortkomplexität bei Anmeldung am Exclusive Remote Access Management

Im Exclusive Remote Access Management ist es jetzt möglich die Passwortkomplexität für die Anmeldung über die NCP Management Console festzulegen.

2. Verbesserungen / Fehlerbehebungen

Erweiterung der Suche in der Management Konsole

In der Suche der Management-Konsole kann nun nach Lizenzseriennummern in Abhängigkeit von deren Status (freie/reservierte/benutzte Seriennummer) gesucht werden. Ebenso wurde ein Fehler bei der Lizenz-Detailansicht behoben sofern mehr als 1000 Lizenzen ausgegeben wurden.

Intern verwendete IP-Ports können nicht mehr in der Konsole verändert werden

Ab der Version 5.30 können intern verwendete Ports nicht mehr innerhalb der Management Konsole verändert, sondern nur noch ausgelesen werden. Eine Portänderung bedingt zudem den Neustart des dafür zuständigen Management-Dienstes.
Ist eine Portänderung notwendig, so ist dies in der Datei `ncprsu.conf` im Abschnitt `[General]` umzusetzen.

Fehlerbehebung im NCP-Scripting

Mit dem Aufruf der NCP-Script Funktion `UpdateDest` wurde ein bereits vergebenes OTP-Secret gelöscht. Dieser Fehler wurde behoben.

Fehlerbehebung im Bereich OTP

Es wurde ein Fehler behoben bei dem ein Benutzer trotz überschreiten der maximal zulässigen Anmeldeversuche nicht deaktiviert/gesperrt wurde. Ebenso wurde ein Fehler im Bereich der 2-Faktor-Authentisierung mit SMS behoben. Hier meldete der RADIUS-Server kein Reject wenn die SMS nicht versendet werden konnte.

Fehlerbehebung beim periodischen Ausführen von NCP-Scripten

Es wurde ein Fehler in der ausführbaren Datei `ncpscriptexe.exe` behoben, der dazu führte, dass die periodische Ausführung eines NCP-Scriptes nach einer gewissen Zeit stoppte.

Fehlerbehebung bei externer Authentisierung mit Kerberos

Es wurde ein Fehler behoben sofern externe Authentisierung mit Kerberos und UPN-Suffixen verwendet wurde.

Fehler beim Upload von Upload-Paketen mit Unterverzeichnissen

Enthält ein Upload-Paket welches auf das Exclusive Remote Access Management hochgeladen werden soll Unterverzeichnisse, so bricht der Upload des Pakets mit einer Fehlermeldung ab. Dieses Problem wurde behoben.

Maximale Laufzeit von Scripten

Die maximale Laufzeit eines Scriptes hängt von der Länge des Aufruf-Intervalls ab. Für eine Wiederholung des Scriptes bis zu einer Stunde Aufruf-Intervall beträgt die maximale Laufzeit des Scriptes eine Stunde. Bei längeren Aufruf-Intervallen darf ein Script maximal 23 Stunden und 59 Minuten Laufzeit haben.

Maximale Anzahl fehlerhafter RADIUS-Anmeldungen

Der Eintrag der maximal fehlerhaften RADIUS Anmeldungen innerhalb der RADIUS Gruppen-Einstellungen war nicht wirksam. Ein Benutzer wurde immer nach fünf falschen Eingaben gesperrt. Dieses Problem wurde behoben.

Replikationsdienst muss nach Änderungen in der Backup-Server-Konfiguration neu gestartet werden

Bei Anlage oder Änderungen der Backup-Server-Konfiguration musste der Replikationsdienst neu gestartet werden. Dieses Problem wurde behoben. Die Konfigurationsänderungen werden sofort übernommen.

Anzeigefehler beim Ablaufdatum des CA-Zertifikats

Die Warnmeldung zum Ablauf eines CA-Zertifikates zeigte ein falsches Datum an. Dieser Fehler wurde behoben.

„Invalid incoming Attribute“-Fehler bei RADIUS-Anmeldung

Wurde mit einem Script eine RADIUS Gruppen Konfiguration geändert, so konnte dies einen „Invalid incoming Attribute“-Fehler bei RADIUS-Anmeldung hervorrufen. Dieses Problem wurde behoben.

Fehler bei externer RADIUS-Authentisierung

Bei der Authentisierung über einen externen RADIUS-Server wurde aufgrund vom Benutzer unterschiedlich eingegebener Groß-/Kleinschreibung beim Suffix des Benutzernamens, der Suffix nicht immer korrekt entfernt. Dieses Problem wurde behoben.

Fehlerbehebung innerhalb Administrator Anmeldung

Sofern ein neuer Management-Administrator innerhalb des Active Directory in einer OU mit Umlauten angelegt wurde, konnte sich dieser Administrator nicht korrekt am Exclusive Remote Access Management anmelden. Dieses Problem wurde behoben.

In Dialogen der Management-Einstellungen lassen sich nun die Parameter nach den Namen der Spalten sortieren.

Änderung des Standart-Ports in der NCP Management Script-IDE auf 12504

Viele Log-Meldungen nach fehlerhafter RADIUS-Anmeldung

Erfolgte die Anmeldung am RADIUS-Server des Backup-Managements mit einem falschen Passwort, so wurde eine große Anzahl an Log-Meldungen erzeugt. Dieser Fehler wurde behoben.

Absturz des RADIUS-Dienstes

Unter bestimmten Umständen konnte der RADIUS-Dienst abstürzen. Dieser Fehler wurde behoben.

Falsche Darstellung von Umlauten nach Update des Management Servers

Bei der Verwendung des Connector/C wurden in der Management Konsole Umlaute falsch dargestellt. Dieses Problem wurde durch die Konfiguration der Codepage in der Datei *ncprsu.conf* innerhalb der Gruppe „DB“ oder „DB-MgmBackup“ mit „CharSet=…“ behoben.

SQL-Fehler beim Betrieb mit einer Oracle Datenbank

Wurde der Backup Management Server mit einer Oracle-Datenbank betrieben, so kam es beim Start des Backup Management Servers zu einem SQL-Fehler. Dieser Fehler wurde behoben.

Absturz des Client Session Dienstes

Bei der Verlängerung bzw. dem Versenden einen erneuerten Hardware-Zertifikates an den Client stürzte der Client Session Dienst ab. Dieser Fehler wurde behoben.

Administrator-Passwort zurücksetzen

Der Aufruf `ncprsud -clearadminpw` zum Zurücksetzen des Administrator-Passwortes zeigte keine Wirkung, wenn gleichzeitig der Management Server gestartet war. Dieser Fehler wurde behoben.

Absturz der Management Konsole

War eine große Anzahl von Benutzer mit RADIUS-Authentisierung via VPN verbunden, so stürzte die Management Konsole beim Aufruf der zugehörigen Link Profile in Statistik ab. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine.

Servicerelease: **5.01 r40724**
Datum: **August 2018**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2016 64 Bit
- Windows Server 2012 R2 64 Bit

Das NCP Exclusive Remote Access Management (kurz: Management) ist nur in der 64 Bit Variante verfügbar.

Datenbank:
Folgende x64 Datenbanken mit zugehörigem Treiber wurden getestet und freigegeben:

Datenbank	Treiber
MySQL Server 5.x	MariaDB ODBC 3.0.3 oder neuer [1]
MariaDB 10.2.10	MariaDB ODBC 3.0.3 oder neuer
MS SQL Server 2016	MS SQL Server 10.00.14393.00
Oracle 11g Express	ODBC InstantClient 12.01.00.02
Oracle 12c Enterprise	ODBC InstantClient 12.01.00.02

[1] Der MariaDB ODBC Treiber kann nicht via Socket mit der MySQL Datenbank kommunizieren.

NCP Management Console 5.0 zur Konfiguration.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Problembehebung beim Erstellen eines Backup-Management

Wurden am primären Management Plug-ins gelöscht, z.B. nach dem Einspielen einer aktuelleren Version des Plug-ins, so konnte ein Backup-Management nicht fehlerfrei in Betrieb genommen werden. Dieser Fehler wurde behoben.

Problembehebung bei Lizenzeingabe und Verwendung eines Backup-Management Servers

Im Falle eines heruntergefahrenen Backup-Management Servers konnte das Einspielen neuer Lizenzen am primärem Management Server, den Backup Server in einen nicht funktionsfähigen Zustand versetzen. Dieser Fehler wurde behoben.

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Fehlerhafte Konsolenanmeldung

Bei der Verwendung der nativen Datenbankanbindung (C-Connector) von MySQL/MariaDB konnte es bei der Konsolenanmeldung zu dem Fehler *„Fehlerhafte Anmeldung“* kommen. Die darauffolgende Anmeldung verlief korrekt. Dieser Fehler wurde behoben.

Fehler bei der Erstellung von Vorlagen mit dem Verbindungsmedium ISDN

Die Erzeugung eines Vorlagenprofils mit dem Verbindungsmedium ISDN erzeugt eine Fehlermeldung. Dieser Fehler wurde behoben.

Unerwartetes Beenden des RADIUS-Dienstes

Ist der externe Authentisierungsserver (MS Active Directory) während der Anmeldephase eines Benutzers nicht erreichbar (z.B. via MC CHAPv2), so führte dies zum Beenden des RADIUS-Dienstes. Dieser Fehler wurde behoben.

Löschen von statischen Routen funktioniert nicht

Bei der Verwendung von MariaDB mit dem MariaDB C-Connector 3.0.5 konnten statische Routen im SES nicht gelöscht werden. Dieser Fehler wurde behoben.

Keine Fehlermeldung, wenn DB nicht verbunden ist

Ist beim Start des Managements die Datenbank nicht erreichbar, so wurde der Verbindungsversuch der Konsole abgelehnt aber die entsprechende Fehlermeldung nicht angezeigt. Dieser Fehler ist behoben

RADIUS MSCHAPv2: Die Fehlermeldung "Password expired" wurde nicht weitergeleitet

Gibt der externe Authentisierungsserver (MS Active Directory) während der Anmeldephase eines Benutzers die Fehlermeldung *„Password expired“* aus, so wurde diese Meldung nicht an den Client weitergeleitet. Dieser Fehler wurde behoben.

Falsche Management Benachrichtigung "Zertifikat abgelaufen"

Die Management Benachrichtigung "Zertifikat abgelaufen" wurde weiterhin angezeigt, obwohl das abgelaufene Zertifikat bereits gelöscht wurde

3. Bekannte Einschränkungen

Keine.

4. Hinweise zum NCP Exclusive Remote Access Management

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/service/
Weitere Unterstützung bei Fragen zum NCP Exclusive Remote Access Management, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://www.ncp-e.com/en/support/

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Zentrale Verwaltung

Das NCP Exclusive Remote Access Management (Management) ist der zentrale Bestandteil der NCP Next Generation Network Access Technology. Als **Single Point of Administration** schafft es die erforderliche Transparenz für Netzwerkadministratoren, um mobile und stationäre Telearbeitsplätze sowie remote VPN-Gateways in Filialnetzen zentral zu verwalten. Das NCP Software-Tool bietet alle Funktionalitäten und Automatismen, die für die Inbetriebnahme und den Betrieb eines Remote Access-Projektes erforderlich sind.
Mit dem Exclusive Remote Access Management werden Konfigurationen, Zertifikate und Software Updates zentral erzeugt und gespeichert bzw. verteilt und aktualisiert oder ausgerollt.

Komponenten des Secure Enterprise Managements

Das NCP Exclusive Remote Access Management besteht aus dem Management Server und der Management Console. Das Datenbank-System ist nicht im Lieferumfang enthalten.

Voraussetzungen für die Server-Komponente

64-Bit Betriebssysteme
Windows Server 2016
Windows Server 2012 R2
Rechner
CPU mind. Pentium III-800 MHz (abhängig von der Anzahl der Managed Units)
Mit RADIUS Plug-in: Pentium IV-1,5 GHz
Festplatte: min. 50 MB freier Speicher zzgl. Speicherplatz für Log-Dateien und ca. 20 MB pro Software-Paket

Unterstützte Datenbanken

Der Management Server ist ein datenbankbasiertes System und korrespondiert mit nahezu jeder Datenbank über ODBC:

- MySQL Server 5.x
- MariaDB 10.2.10
- MS SQL Server 2016
- Oracle 11g Express
- Oracle 12c Enterprise

Alle systemrelevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess eingebunden. Dazu gehören unter anderem: Benutzer-Profile (Konfigurationen der Managed Units), Lizenzkeys und Authentisierungsdaten, Zertifikate, Providerkennungen etc. Unter Windows xxxx 64bit-Systemen gibt es zwei ODBC Data Sources. NCP empfiehlt, die Datenbank-Verbindung direkt über die NCP Secure Management Server - Konfiguration Utility (Start / NCP Management Server / Konfiguration) anzulegen.

Backup-System

Optional steht ein Backup-System mit integriertem Replikationsdienst für den Management Server zur Verfügung.

Unterstützte Certification Authorities

Microsoft Certificate Services als integrierte und stand alone CA.

Voraussetzungen für die Console

Über die Management Console werden die VPN-Benutzerdaten zentral verwaltet.

Betriebssysteme

Windows Desktop Betriebssysteme 32-Bit und 64-Bit

Management Server-Module

Die Management Server-Module werden als Plug-ins von jedem Rechner im lokalen Netzwerk unter Angabe der IP-Adresse des Management Servers auf diesem installiert. Dies gilt auch für die Management Console, die ebenfalls als Plug-in installiert werden kann. (Das Datenbank-System ist nicht im Produktumfang enthalten.)

Verfügbare Plug-ins

- Client Configuration Plug-in
- Firewall Plug-in
- License Management Plug-in
- PKI Management Plug-in
- Script Plug-in
- RADIUS Plug-in
- System Monitor Plug-in (experimental)

Unterstützte RFCs und Drafts

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2433 Microsoft CHAP
- RFC 2759 Microsoft CHAP V2
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol
- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2716 Certificate Management Protocol
- RFC 2511 Certificate Request Message Format
- Draft-ietf-pkix-cmp-transport-protocols-04.txt, Transport Protocols for CMP
- Draft-ietf-pkix-rfc2511bis-05.txt, Certificate Request Message Format (CRMF)

Zentrale Funktionalitäten

Administratoren-Management und Mandantenfähigkeit (Multi-Company Support)
Die Mandantenfähigkeit prädestiniert das Exclusive Remote Access Management für den Einsatz bei Managed Security Service Providern (MSSP) in sog. „Managed VPNs“ oder Remote Access-Strukturen, in denen mehrere Firmen gemeinsam eine VPN-Plattform nutzen (VPN Sharing).
Über die zentrale Administratoren-Verwaltung werden die Zugriffsrechte für die jeweiligen Administratoren auf die jeweiligen selbständigen Firmen mit angeschlossenen VPN-Benutzern definiert. Durch Gruppenzuordnung werden die Rechte der Administratoren so angelegt, dass jeder ausschließlich Zugriff auf seinen zu verwaltenden Mandantenkreis (Organisationsgruppe) hat. Ein Übergriff auf Daten anderer Mandanten ist ausgeschlossen.

Lizenz-Management (License Management Plug-in)
Mit der Lizenzierung steht die Gesamtzahl der Managed Units für den Management Server zur freien Verfügung. Die Managed Units können entweder als Benutzer- oder Remote Server-Lizenzen eingesetzt werden. Alle Lizenzen werden in einen Pool übernommen und nach festgelegten Richtlinien automatisiert verwaltet:

- Lizenzübernahme kann automatisiert erfolgen oder manuell vorgenommen werden
- Lizenz wird nach Ausscheiden eines Mitarbeiters in den Pool zurück gestellt
- Meldung wird ausgegeben wenn keine Lizenz mehr verfügbar ist

Erzeugung der Konfigurationen für die Managed Units

Mit der Management Console werden User-Daten abgerufen oder Konfigurationen und Zertifikate gespeichert. Alle relevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess des VPN-Betreibers eingebunden.
Die Eingabe aller relevanten Daten kann an der Management Console interaktiv durch den Administrator vorgenommen oder skriptgesteuert über das Script Plug-in erfolgen.

Automatic Update (über LAN und VPN)
Der Update Service des Exclusive Remote Access Managements gestattet alle für das Remote Access-Umfeld relevanten Software-Komponenten zentral verfügbar zu halten. Sobald eine Verbindung zwischen Client und Corporate Network besteht, werden diese Komponenten automatisch auf der Client-Seite eingespielt. Sollte es während der Übertragung zu Störungen kommen, bleiben der bereits vorhandene Softwarestand sowie die Konfiguration unberührt. Erst nach einem kompletten, fehlerfreien Transfer aller vordefinierten Daten findet das Update statt.

- Steuerung der Update-Pakete
  Mittels Update-Liste, die der Administrator nach den jeweiligen Erfordernissen zusammenstellt, erfolgt die Verteilung der Software-Komponenten. Dabei kann pro Komponente nach Verbindungsmedium, Häufigkeit der Ablehnungen eines Updates und Art des Updates differenziert werden.
- Update-Komponenten
  Folgende Software-Komponenten können für das automatische Update bereitgestellt werden:
  - Konfigurationen (Profile und Monitor-Einstellungen des Exclusive Remote Access Clients)
  - Benutzer-Zertifikate (Soft-Zertifikate, p12-Format)
  - Aussteller-Zertifikate (Soft-Zertifikate, cer- und pem-Formate)
  - Update Client
  - Software-Versionen (Software Updates / Upgrades sind für Clients nur unter Windows Desktop-Betriebssystemen möglich)

- Verbindungsmedium
  Alle Verbindungsmedien, die die Remote-Seite unterstützt, können einer der Update-Komponenten zugeordnet werden. So lässt sich zum Beispiel steuern, dass für große Datenmengen schnelle Verbindungsmedien genutzt werden.
- Update-Verfahren
  Alternativ zu einem Update über VPN, kann die Option des LAN Updates genutzt werden. Bei einem Update über VPN werden alle Daten durch den Tunnel verschlüsselt übertragen. Bei einem LAN Update, wenn sich der Client PC im heimischen Firmennetz befindet, wird die SSL-Verschlüsselung eingesetzt.

Beschreibung der Plug-ins

System Monitor Plug-in (experimental)
Dieses Plug-in dient der schnellen Information über alle wichtigen Ereignisse innerhalb einer VPN-Installation als Balken- oder Linien-Diagramme. Der Administrator kann über den System Monitor je nach Bedarf aktuelle Status-Informationen in Echtzeit abrufen bzw. auf bereits gespeicherte Datenbestände der Remote Access-Umgebung zugreifen. Im jeweiligen Diagramm kann im Zeitraum beliebig zurück bzw. vorwärts geblättert werden. Die grafische Darstellung der Diagramme ist frei wählbar.

Client Configuration Plug-in
Hiermit werden die Profile der Secure Enterprise Clients erstellt, konfiguriert und verwaltet. Folgende Einstellungen sind damit möglich:

- alle gruppenspezifischen und verbindungstechnischen Parameter können mithilfe von Vorlagen (Templates) automatisiert generiert werden
- nur personenbezogene Daten werden manuell eingegeben (Authentisierungsdaten für Erstverbindung bei Rollout)
- Parametersperren, die der entfernte Benutzer nicht verändern kann, können definiert werden
- automatische Konfiguration der Benutzer-Profile für Zentralkomponenten (RADIUS, LDAP, SNMP)
- umfassendes Logging (Versionsstände, Zeitstempel für Konfigurationsänderungen, automatischer Upload von Client-Logdateien)
- Erzeugung eines generalisierten Init-Benutzers für Rollout
- automatisierte Erzeugung und Bereitstellung von Konfigurations-Updates

Firewall Plug-in
Zur Konfiguration der Personal Firewall in den Secure Enterprise Clients und der Dynamic Personal Firewall der Client Suite. Folgende Einstellungen können vorgenommen werden:

- applikations- und verbindungsabhängige Filterregeln
- protokoll-, port- und adressbezogene Filterregeln
- Vorgaben für die Erkennung von „friendly networks“ (IP-Adresse Netzwerk, Netzwerkmaske, IP-Adresse des DHCP-Server, MAC-Adresse)
- Logging-Einstellungen
- FND-Serverkonfiguration (Friendly Net Detection)
- Firewall-Einstellungen, die der entfernte Benutzer nicht verändern kann, können definiert werden

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

PKI Enrollment Plug-in

Das Plug-in fungiert als Registration Authority (RA). Im Zusammenwirken mit unterschiedlichen Certification Authorities (CA) werden elektronische Zertifikate (X.509 v3) erstellt und verwaltet. Eine erzeugtes Zertifikat kann wahlweise zur Verwendung als Soft-Zertifikat (PKCS#12) oder für den Einsatz auf Smart Card oder USB-Token (PKCS#11) abgelegt werden. Die im Lieferumfang enthaltene NCP Demo-CA kann während der Testphase für die Abbildung einer PKI genutzt werden, ist jedoch nicht für den produktiven Einsatz vorgesehen. Die Umstellung auf eine externe CA ist problemlos möglich. Die wichtigsten Funktionalitäten des PKI Plug-ins sind:

- Erstellen von Benutzer- und Hardware-Zertifikaten (auch Bulk Mode)
- Verlängern der Zertifikatsgültigkeit (PKCS#7)
- Sperren von Zertifikaten
- Verteilung der Zertifikate (auch Multi-Client-Zertifikate)
- Anlegen der Benutzerkonfiguration über LDAP im Verzeichnisdienst
- Erstellen eines PAC-Briefes (Personal Authentication Code) für Erstverbindung und Lizenzierung
- Generieren und Verteilen von Server-Zertifikaten

RADIUS Plug-in

Für die Konfiguration der Managed Units (Benutzern) in den zentralen VPN-Gateways steht optional die RADIUS-Schnittstelle zur Verfügung. Das RADIUS Plug-in dient der Verwaltung des integrierten RADIUS Servers und deckt folgende Funktionen ab:

- Automatische Anlage von RADIUS-Accounts über die Client- und Remote Server Configuration Plug-ins
- Unterstützung von PAP/CHAP-Requests
- Erfassung von Accounting-Daten
- Sperren von Benutzern bei wiederholten fehlerhaften Anmeldungen
- Verwaltung von mehreren RADIUS-Konfigurationen unterschiedlicher Gateways
- RSA Authentication Manager Proxy-Funktionalität

Optional steht ein Backup RADIUS-Server zur Verfügung. Dies gestattet vorhandene RADIUS Server durch den integrierten RADIUS Server des Management-Systems zu ersetzen.