Collax NCP-VPN

Howto

Dieses Howto beschreibt wie eine VPN-Verbindung zwischen einem Collax Server und dem NCP Secure Entry Client (NCP) eingerichtet werden kann. Der NCP ist ein sehr einfach zu bedienender VPN-Client, basierend auf modernster IPSec Technologie. Umgangssprachlich spricht man dabei auch von einer *Road Warrior* Verbindung.

Voraussetzungen

- Collax Security Gateway
- Collax Business Server
- Collax Platform Server inkl. Collax Modul Gatekeeper
- Windows mit installiertem NCP Secure Entry Client (Version 9.30)

Die Einwahl des Road Warriors erfolgt dabei auf dem Collax Server, um Zugriff auf das lokale Netzwerk (LAN) zu erlangen. Für die Verschlüsselung der VPN-Verbindung werden Zertifikate nach dem gängigen X.509 Standard eingesetzt.

Grundsätzliches

Sowohl Server als auch Client müssen mit dem Internet verbunden sein. Der Collax Server, auf dem die Einwahl erfolgt, muß entweder per statischer IP-Adresse oder per Hostname/DynDNS-Adresse erreichbar sein. Für die IP-Adresszuweisung an den Client muß zudem ein Netzwerk angelegt werden. Verwenden Sie dabei unbedingt eine ungenutzte Netzwerkadresse, damit keine Adresskonflikte entstehen.

Beispielkonfiguration

Collax Business Server (CBS)

Hostname: vpn.collax.com

Localnet: 172.17.0.0/24

Zertifikat: VPN_CBS

NCP Client

Virtuelles Netz: 192.168.9.0/24

Virtuelle IP Adresse: 192.168.9.10

Zertifikat: VPN_NCP

NAT-Traversal

Befinden sich Server und/oder Client hinter einem Router, muss auf dem Collax Server NAT-Traversal aktiviert sein. Dieser Dialog befindet sich unter *„System → Netzwerk → Links → Allgemein“*.

Auf den Routern zwischen den IPSec Endpunkten müssen die UDP-Ports 500 und 4500 freigeschaltet sein. Die Option nennt sich oftmals VPN-Passthrough.

Zertifikate

Für die Verschlüsselung der Verbindung wird ein Schlüsselpaar Lokale- und Nicht-lokale Serverzertifikate verwendet. Falls sich mehrere Clients über einen Link einwählen sollen, verwendet man eine Certificate Authority (CA), um damit das Schlüsselpaar zu signieren. Als Schlüssel der Gegenstelle wird dabei im VPN-Einwahllink die CA angeben.

In unserem Beispiel erstellen wir eine CA, um damit anschließend ein Lokales- und ein Nicht-lokales Serverzertifikat signieren zu können.

Konfiguration CBS

Certificate Authority erstellen

Wir erstellen zuerst eine CA. Mithilfe der CA werden im weiteren Verlauf der Zertifikatserstellung ein Lokales- und ein Nicht-lokales Serverzertifikat signiert.

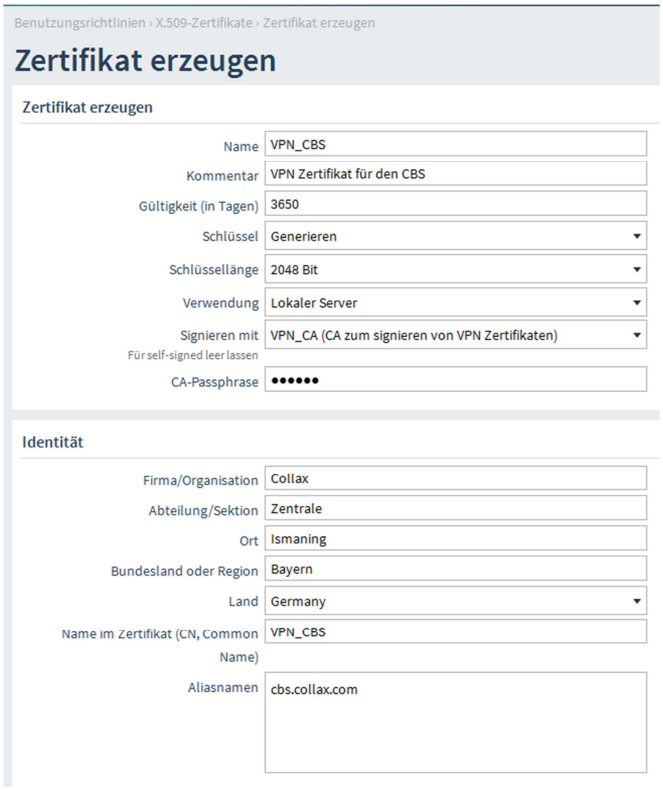
Dieser Dialog befindet sich unter *„System → Benutzungsrichtlinien → Zertifikate → X.509-Zertifikate“*

Achten Sie bitte darauf, für den Common Name (CN) immer einen eindeutigen Namen zu wählen.

Die Gültigkeit des CA Zertifikates sollte zudem ausreichend lange gewählt werden, da die CA sowie alle damit signierten Zertifikate nach Ablauf unbrauchbar sind. Die Gültigkeit kann auch nachträglich nicht verlängert werden, womit man neue Zertifikate erstellen müsste.

Lokales Serverzertifikat erstellen

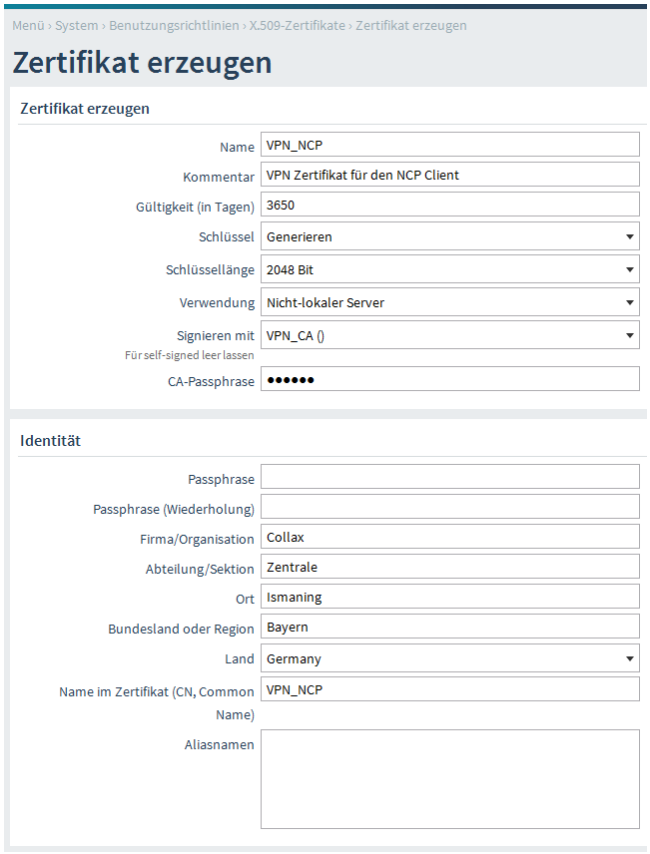
Als nächstes erzeugen wir ein *Lokales Serverzertifikat* und signieren es mit der zuvor erstellten CA.



Nicht-lokales Serverzertifikat erstellen

Mit dem Nicht-lokalen Serverzertifikat verfahren wir identisch. Beachten Sie, diesmal als Verwendung *Nicht-lokaler Server* zu wählen.

Wichtig: Bei der Identität darf **keine Paßphrase** vergeben werden.



Zertifikat exportieren

Das Nicht-lokale Serverzertifikat wird exportiert. Es dient dem anschließenden Import auf Seiten des NCP. Das Exportpasswort dient der Sicherheit und wird beim Import im NCP als PIN abgefragt.

VPN Netzwerk definieren

Bevor ein VPN-Link angelegt werden kann, definieren wir ein neues Netzwerk für die IP-Adresszuweisung an die Clients. Dieser Dialog befindet sich unter *„System → Netzwerk → Links → Netze“*

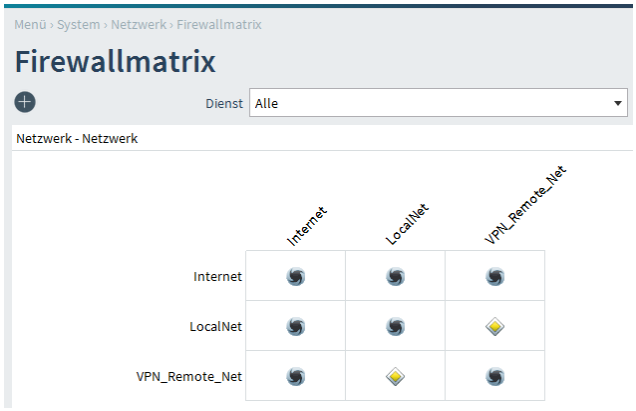
Auf dem Collax Server wird dazu das VPN_Remote_Net 192.168.9.0/24 angelegt.

Routing

Um das lokale Netzwerk erreichen zu können, muss das Routing über die Firewallmatrix konfiguriert werden.

Dieser Dialog befindet sich unter *„System → Netzwerk → Firewall → Matrix“*

Die Firewallmatrix ist eine visuelle Darstellung der integrierten Firewall. Hier wird festgelegt, welche Netzwerkverbindungen erlaubt bzw. geblockt sind. Es empfiehlt sich, den Verbindungsaufbau in beide Richtungen zu erlauben.



Firewall

Um den Zugriff der Clients aus dem VPN_Remote_Netz auf Dienste des CBS zu ermöglichen, erstellen wir eine neue Gruppe.

Dieser Dialog befindet sich unter *„System → Benutzungsrichtlinien → Richtlinien → Gruppen“*.

Als Mitglieder-Netz der Gruppe wählen wir das VPN_Remote_Netz, da die Anfragen der Clients aus diesem Netzwerk erfolgen. Durch setzen der entsprechenden Gruppenberechtigungen kann somit der Zugriff auf beliebige Dienste erlaubt werden.

IPSec-Proposals

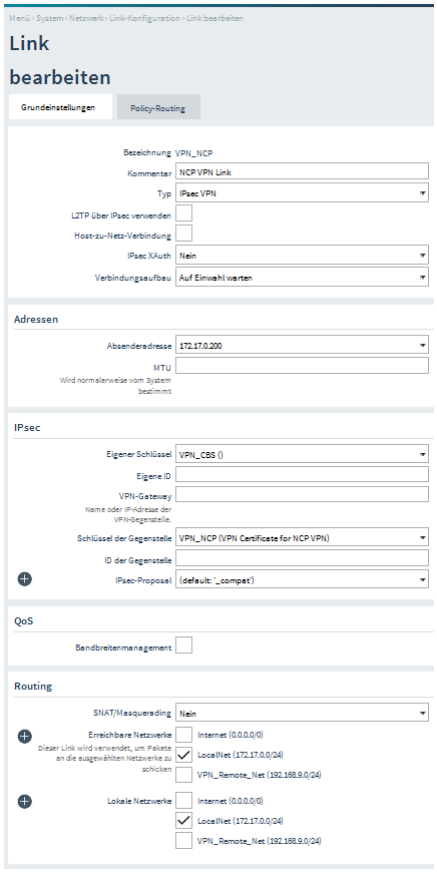
Um VPN/IPSec-Verbindungen aufbauen zu können, müssen verschiedene Parameter für den Schlüssel- und Datenaustausch definiert werden. Diese Parameter werden zur vereinfachten Handhabung und für zusätzliche Stabilität von VPN-Verbindungen in einem Extradialog erstellt.

Dieser Dialog befindet sich unter *„System → Netzwerk → Links → IPSec-Proposals“* und kann in den VPN-Links aus einer Auswahl-Box gewählt werden. Zusätzlich kann unter *„System → Netzwerk → Links → Allgemein“* ein vordefiniertes IPSec-Proposal als Standard (default) angegeben werden.

VPN Einwahllink konfigurieren

Dieser Dialog befindet sich unter *„System → Netzwerk → Links → Links“*

Als Typ wählen wir *„IPSec VPN“*



Konfiguration NCP Client

Auf den folgenden Seiten finden Sie eine bebilderte Schritt-für-Schritt Anleitung zur Einrichtung eines Profils für Ihren NCP Client.

Verbindungsassistenten starten

Durch den Assistenten wurden die wichtigsten Einstellungen vorgenommen und Sie können das Profil „Fertigstellen“.

Profil anpassen (VPN IP Netz)

Begeben Sie sich nun in die Profileinstellungen und wählen das zuvor angelegte Profil aus.

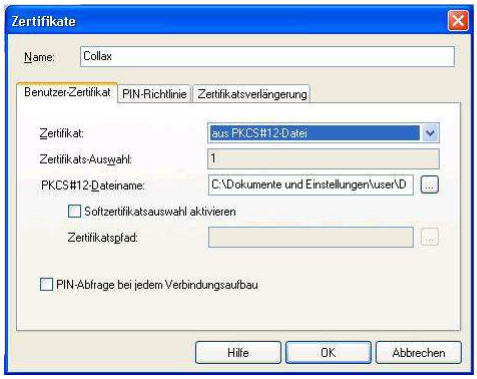
Passen Sie noch das VPN IP-Netz an. Es handelt sich dabei um das Lokale Netzwerk Ihres Collax Servers.

Zertifikat importieren

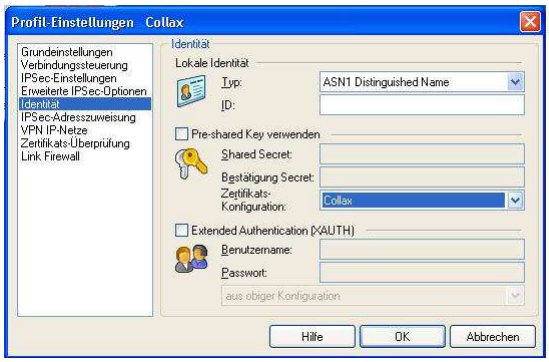
Importieren Sie nun das vom Collax Server exportierte Nicht-lokale Serverzertifikat.

Dieser Dialog befindet sich unter *"Konfiguration → Zertifikate"*.

Vergeben Sie einen Namen für diese Vorlage. Hier kann auch angegeben werden, ob die PIN (Export-Passwort des Zertifikats) bei jedem Verbindungsaufbau eingegeben werden soll.



Jetzt muss noch einmal das Profil aufgerufen werden und das Formular „Identität“ bearbeitet werden. Wählen Sie unter *„Zertifikatskonfiguration“* die zuvor angelegte Vorlage aus.



Verbindung herstellen

Nach Import des Zertifikates können Sie die Verbindung herstellen. Sie werden zuvor noch nach der Passphraße des Zertifikates gefragt.

Die Konfiguration ist abgeschlossen und die Einwahl in das Firmennetz erfolgt nach Eingabe der PIN.

Die Verbindung wurde erfolgreich hergestellt.