

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 angegeben.

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“

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat erzeugen

Zertifikat erzeugen

Zertifikat erzeugen

Name	VPN_CA
Kommentar	CA zum signieren von VPN Zertifikaten
Gültigkeit (in Tagen)	3650
Schlüssel	Generieren
Schlüssellänge	2048 Bit
Verwendung	CA
Signieren mit	
<small>Fürself-signed leer lassen</small>	

Identität

Passphrase	••••••
Passphrase (Wiederholung)	••••••
Firma/Organisation	Collax
Abteilung/Sektion	Zentrale
Ort	Ismaning
Bundesland oder Region	Bayern
Land	Germany
Name im Zertifikat (CN, Common Name)	VPN_CA
E-Mail-Adresse	admin@collax.com

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.

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat erzeugen

Zertifikat erzeugen

Zertifikat erzeugen

Name	VPN_CBS
Kommentar	VPN Zertifikat für den CBS
Gültigkeit (in Tagen)	3650
Schlüssel	Generieren
Schlüssellänge	2048 Bit
Verwendung	Lokaler Server
Signieren mit	VPN_CA (CA zum signieren von VPN Zertifikaten)
Für self-signed leer lassen	
CA-Passphrase	•••••

Identität

Firma/Organisation	Collax
Abteilung/Sektion	Zentrale
Ort	Ismaning
Bundesland oder Region	Bayern
Land	Germany
Name im Zertifikat (CN, Common Name)	VPN_CBS
Aliasnamen	cbs.collax.com

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.

Menü > System > Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat erzeugen

Zertifikat erzeugen

Zertifikat erzeugen

Name	VPN_NCP
Kommentar	VPN Zertifikat für den NCP Client
Gültigkeit (in Tagen)	3650
Schlüssel	Generieren
Schlüssellänge	2048 Bit
Verwendung	Nicht-lokaler Server
Signieren mit	VPN_CA ()
Für self-signed leer lassen	<input type="checkbox"/>
CA-Passphrase	•••••

Identität

Passphrase	<input type="password"/>
Passphrase (Wiederholung)	<input type="password"/>
Firma/Organisation	Collax
Abteilung/Sektion	Zentrale
Ort	Ismaning
Bundesland oder Region	Bayern
Land	Germany
Name im Zertifikat (CN, Common Name)	VPN_NCP
Aliasnamen	<input type="text"/>

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.

Menü > System > Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat exportieren

Zertifikat exportieren

Zertifikat	VPN_NCP
Format	PEM
Mit privatem Schlüssel	<input type="checkbox"/>
CA-Zertifikat	<input type="checkbox"/>

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.

Menü > System > Netzwerk > Netze > Netzwerk bearbeiten

Netzwerk bearbeiten

Grundeinstellungen Gruppenzugehörigkeit Optionen

Grundeinstellungen

Bezeichnung des Netzwerks: VPN_Remote_Net

Kommentar:

Netzwerkadresse: 192.168.9.0

Netzmaske: 255.255.255.000 (24 bit)

Netz verwenden für: Routing (Links), Berechtigungen und Firewall-Matrix

Link:

Auf diesen Link werden Pakete für dieses Netzwerk geroutet.

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.

Menü > System > Netzwerk > Firewallmatrix > Regel bearbeiten

Regel bearbeiten

Dienst: any

Von Netzwerk: LocalNet (172.17.0.0/24)

Nach Netzwerk: VPN_Remote_Net (192.168.9.0/24)

Protokollieren:

Regel: Erlauben

Traffic-Policy:

Menü > System > Netzwerk > Firewallmatrix

Firewallmatrix

Dienst: Alle

Netzwerk - Netzwerk

	Internet	LocalNet	VPN_Remote_Net
Internet			
LocalNet			
VPN_Remote_Net			

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.

Menü > System > Netzwerk > IPSec-Proposals > IPSec-Proposal anzeigen

IPsec-Proposal anzeigen

Bezeichnung _compat
Kommentar Commonly used parameters

Schlüsselaustausch (IKE)

Aggressive Mode

Verschlüsselungsmethode 3DES (128 bit)
AES (256 bit)
AES (128 bit)

Hash-Algorithmus SHA1
MD5

DH-Gruppen dh gruppe 5, 1536 bit (modp1536)
dh gruppe 2, 1024 bit (modp1024)

Lifetime 600
in Minuten

Perfect Forwarding Secrecy

Datenaustausch (ESP)

Kompression

Verschlüsselungsmethode 3DES (128 bit)
AES (256 bit)
AES (128 bit)

Hash-Algorithmus SHA1 (160 bit)
MD5 (128 bit)

Keylife 600

VPN Einwahllink konfigurieren

Dieser Dialog befindet sich unter „System → Netzwerk → Links → Links“
Als Typ wählen wir „IPSec VPN“

Menü > System > Netzwerk > Link-Konfiguration > Link bearbeiten

Link bearbeiten

Grundeinstellungen Policy-Routing

Bezeichnung: VPN_NCP
 Kommentar: NCP VPN Link
 Typ: IPsec VPN
 L2TP über IPsec verwenden:
 Host-zu-Netz-Verbindung:
 IPsec XAuth: Nein
 Verbindungsaufbau: Auf Einwahl warten

Adressen
 Absenderadresse: 172.17.0.200
 MTU:
Wird normalerweise vom System bestimmt

IPsec
 Eigener Schlüssel: VPN_CBS ()
 Eigene ID:
 VPN-Gateway/
Name oder IP-Adresse der VPN-Gegenstelle.
 Schlüssel der Gegenstelle: VPN_NCP (VPN Certificate for NCP VPN)
 ID der Gegenstelle:
 IPsec-Proposal: (default: _compat)

QoS
 Bandbreitenmanagement:

Routing
 SNAT/Masquerading: Nein
 Erreichbare Netzwerke: Internet (0.0.0.0)
 LocalNet (172.17.0.0/24)
Dieser Link wird verwendet, um Pakete an die ausgewählten Netzwerke zu schicken
 VPN_Remote_Net (192.168.9.0/24)
 Lokale Netzwerke: Internet (0.0.0.0)
 LocalNet (172.17.0.0/24)
 VPN_Remote_Net (192.168.9.0/24)

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

Assistent für neues Profil

Verbindungstyp
 Wie soll die Verbindung zur Gegenstelle hergestellt werden?

NCP

Verbindung zum Firmennetz über IPsec
 Erstellt eine Verbindung zum Firmennetz über ein virtuelles privates Netzwerk (VPN), abgesichert über IPsec.

Verbindung mit dem Internet herstellen
 Erstellt eine Verbindung zum Internet ohne weitere Parameter für ein virtuelles privates Netzwerk (VPN).

< Zurück Weiter > Abbrechen

Assistent für neues Profil

Name des Profils
 Geben Sie hier einen unverwechselbaren Namen für das Profil ein.

NCP

Der Name des Profils darf jedes alphanumerische und numerische Zeichen beinhalten und Leerzeichen eingerechnet, bis zu 39 Zeichen lang sein.

★ Profil-Name:
 Collax

< Zurück Weiter > Abbrechen

Assistent für neues Profil

Verbindungsmedium
Auswahl des Mediums, über das die Verbindung hergestellt werden soll.

Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Das Verbindungsmedium wird für jedes Profil eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert. Soll z. B. das Internet über Modem genutzt werden, stellen Sie unter Verbindungsmedium "Modem" ein und wählen anschließend das gewünschte Modem aus.

Verbindungsmedium: LAN (over IP)

< Zurück Weiter > Abbrechen

Assistent für neues Profil

VPN Gateway-Parameter
Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?

Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist. Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt.

Gateway (Tunnel-Endpunkt): vpn.collax.com

Erweiterte Authentisierung (XAUTH)

Benutzername: _____

Passwort: _____ Passwort (Wiederholung): _____

< Zurück Weiter > Abbrechen

Assistent für neues Profil

IPSec-Konfiguration
Konfiguration der grundlegenden Parameter für IPSec.

Hier können sie grundlegende Parameter für IPSec angeben. Für die Richtlinien der IPSec-Verhandlung wird die Einstellung "Automatischer Modus" verwendet. Sollen bestimmte IKE / IPSec-Richtlinien verwendet werden, müssen diese anschließend in den Profil-Einstellungen definiert und zugewiesen werden.

Austausch-Modus: Main Mode

IPSec-Gruppe: DH-Gruppe 5 (1536 Bit)

Benutze IP-Kompression

< Zurück Weiter > Abbrechen

Assistent für neues Profil

IPSec-Konfiguration - IP-Adressen
Welche IP-Adressen sollen verwendet werden?

Geben Sie hier die IP-Adresse an, welche dem Client zugewiesen werden soll. Soll die IP-Adresse dynamisch durch die Gegenstelle zugewiesen werden, muss die Option "IKE Config Mode verwenden" gewählt werden. Desweiteren kann eine IP-Adresse für den DNS- bzw. WINS-Server angegeben werden.

IP-Adressen-Zuweisung: IP-Adresse manuell vergeben

IP-Adresse: 192.168.9.10

DNS / WINS Server

DNS Server: 0.0.0.0 WINS Server: 0.0.0.0

< Zurück Weiter > Abbrechen

Assistent für neues Profil

IPSec-Konfiguration - Pre-shared Key
Gemeinsamer Schlüssel für die IPSec

Werden für die Authentisierung keine Zertifikate verwendet, wird für die Datenverschlüsselung ein gemeinsamer Schlüssel benötigt, der auf beiden Seiten (VPN Client und VPN Gateway) hinterlegt sein muss. Für die IKE ID muss je nach ausgewähltem IKE ID-Typ der zugehörige String eingetragen werden.

Pre-shared Key _____

Shared Secret: _____ Shared Secret (Wiederholung): _____

Lokale Identität

Type: ASN1 Distinguished Name

ID: _____

< Zurück Weiter > Abbrechen

Assistent für neues Profil

Firewall-Einstellungen
Welche Einstellungen sollen für die Firewall verwendet werden?

Aktivieren Sie hier die gewünschte Firewall-Option. Ist Stateful Inspection aktiviert, werden keine Pakete von anderen Hosts akzeptiert. Zusätzlich kann NetBIOS über IP deaktiviert werden.

Firewall _____

Stateful Inspection: auf

Ausschließlich Kommunikation im Tunnel

NetBIOS über IP

< Zurück Fertigstellen Abbrechen

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.

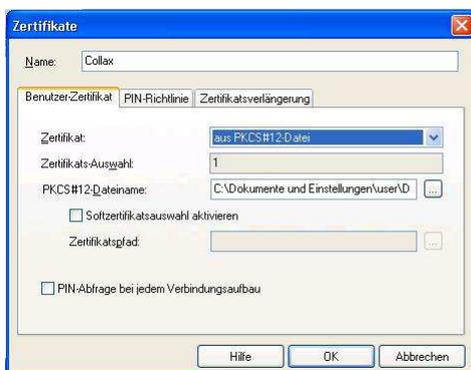


Zertifikat importieren

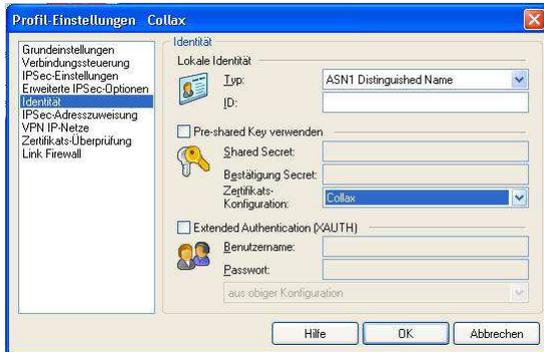
Importieren Sie nun das vom Collax Server exportierte Nicht-lokale Serverzertifikat.

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 Passphrase des Zertifikates gefragt.



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



Die Verbindung wurde erfolgreich hergestellt.