

# Collax VPN

## Howto

Dieses Howto beschreibt exemplarisch die Einrichtung einer VPN Verbindung zwischen zwei Standorten anhand eines Collax Business Servers (CBS) und eines Collax Security Gateways (CSG).

### Voraussetzungen

- Collax Security Gateway
- Collax Business Server
- Collax Platform Server inkl. Collax Modul Gatekeeper

Es sollen jeweils die lokalen Netze (LAN) der beiden Standorte miteinander verbunden werden. Für die Verschlüsselung der VPN Verbindung werden Zertifikate nach dem gängigen X.509 Standard eingesetzt.

### Fremde Gegenstellen

Auch nicht Collax Produkte können eine VPN Verbindung mit einem Collax Server aufbauen. Hierzu müssen die Einstellungen der beiden Server ähnlich der Beispielkonfiguration aufeinander abgestimmt werden. Das Fremd-Produkt muss sich lediglich an den IPSec Standard halten, damit die Verbindung aufgebaut werden kann.

### Grundsätzliches

Um zwei Collax Server via VPN miteinander zu verbinden, muss sich das jeweilige LAN von dem der Gegenstelle unterscheiden. Zwei LAN´s mit identischem IP Adressraum lassen sich nur umständlich durch spezielle Tricks miteinander verbinden.

Stellen Sie sicher, dass beide Collax Server im Internet entweder per statischer IP-Adresse oder per Hostname / DynDNS-Adresse erreichbar sind.

### Beispielkonfiguration

Folgende Beispielkonfiguration ist gegeben:

#### Collax Business Server (CBS):

Hostname: cbs.collax.com

Localnet: 172.17.0.0/24

Zertifikat: VPN\_CBS

Standort: Ismaning

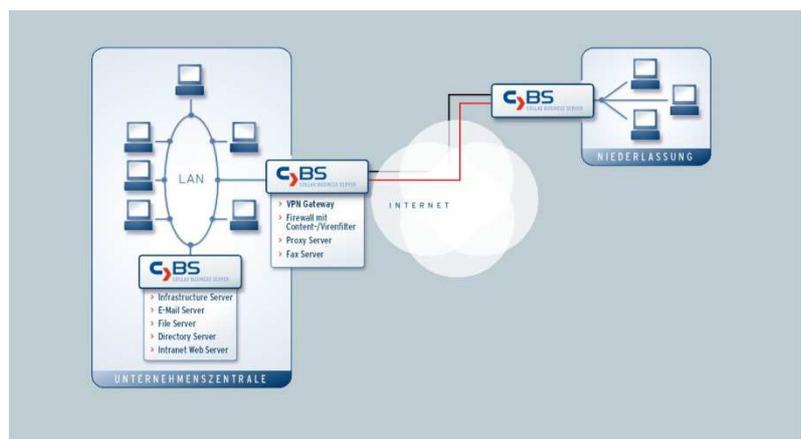
#### Collax Security Gateway (CSG):

Hostname: csg.collax.com

Localnet: 192.168.9.0/24

Zertifikat: VPN\_CSG

Standort: Freiburg



## Zertifikate

Für eine Verbindung zwischen zwei Collax Servern ist es ausreichend, wenn auf beiden Systemen ein Lokales Serverzertifikat erstellt wird. Falls Sie mehrere VPN Verbindungen anlegen möchten, kann es auch sinnvoll sein, auf einem System eine Certificate Authority (CA) anzulegen und anschließend ein Lokales und ein Nicht Lokales Serverzertifikat damit zu signieren. Wir gehen daher auf das zweite Beispiel ein und erstellen von der CA signierte Zertifikate.

## Konfiguration CBS

### CA erstellen

Zuallererst erstellen wir auf dem CBS eine CA. Die CA generieren Sie im Menü „System → Benutzungsrichtlinien → Zertifikate → X.509-Zertifikate“. Mithilfe der CA werden im weiteren Verlauf der Zertifikaterstellung für den CBS ein Lokales und für das CSG ein Nicht Lokales Serverzertifikat erstellt.

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	

Für self-signed leer lassen

---

### 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 darauf, für den „Common Name (CN)“ **immer** einen einmaligen Namen zu wählen. Das Anlegen eines weiteren Zertifikats mit dem identischen CN ist nicht erlaubt.

Die „Gültigkeit“ des CA Zertifikates sollte zudem ausreichend lange gewählt werden, da die CA sowie alle damit signierten Zertifikate nach Ablauf ungültig werden. Die Gültigkeit kann auch nachträglich nicht verlängert werden, weshalb Sie neue Zertifikate erstellen müssten.

### Lokales Serverzertifikat erstellen

Als nächstes erzeugen wir als eigenes Zertifikat ein „*Lokales Server Zertifikat*“ und signieren es mit der CA.

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat erzeugen

## Zertifikat erzeugen

**Zertifikat erzeugen**

Name	<input type="text" value="VPN_CBS"/>
Kommentar	<input type="text" value="VPN Zertifikat für den CBS"/>
Gültigkeit (in Tagen)	<input type="text" value="3650"/>
Schlüssel	<input type="text" value="Generieren"/>
Schlüssellänge	<input type="text" value="2048 Bit"/>
Verwendung	<input type="text" value="Lokaler Server"/>
Signieren mit	<input type="text" value="VPN_CA (CA zum signieren von VPN Zertifikaten)"/>
Für self-signed leer lassen	<input type="checkbox"/>
CA-Passphrase	<input type="text" value="•••••"/>

---

**Identität**

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

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat erzeugen

## Zertifikat erzeugen

Zertifikat erzeugen

Name	VPN_CSG
Kommentar	VPN Zertifikat für das CSG
Gültigkeit (in Tagen)	3650
Schlüssel	Generieren
Schlüssellänge	2048 Bit
Verwendung	Nicht-lokaler Server
Signieren mit	VPN_CA (CA zum signieren von VPN Zertifikaten)
Für self-signed leer lassen	
CA-Passphrase	•••••

---

Identität

Passphrase	
Passphrase (Wiederholung)	
Firma/Organisation	Collax
Abteilung/Sektion	R&D
Ort	Freiburg
Bundesland oder Region	Baden Württemberg
Land	Germany
Name im Zertifikat (CN, Common Name)	VPN_CSG
Aliasnamen	csg.collax.com

Achten Sie bitte darauf, keine „Passphrase“ zu vergeben.

### Zertifikate exportieren

Exportieren Sie die beiden Zertifikate. Sie dienen dem anschließenden Import auf Seiten der Gegenstelle (CSG).

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat exportieren

## Zertifikat exportieren

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

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat exportieren

## Zertifikat exportieren

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

Durch Rechtsklick auf die Zertifikate in der Übersicht können diese exportiert werden. Achten Sie darauf, dass das nicht lokale Zertifikat (VPN\_CSG) mit privatem Schlüssel exportiert werden muss.

Nach erfolgreichem Export und Speichern der Dateien tragen diese die Namen „VPN\_CBS.crt“ und „VPN\_CSG.crt“.

### VPN Netzwerk definieren

Bevor Sie einen VPN Link erzeugen, muss das LAN der Gegenstelle definiert werden. Diesen Schritt führen Sie unter „System → Netzwerk → Links → Netze“ durch.

Auf dem CBS wird dazu das VPN\_Remote\_Netz 192.168.9.0/24 angelegt.

Menü > System > Netzwerk > Netze

### Netze

Suche ...

Bezeichnung	Kommentar	Netzwerkadresse	Netzmaske	Routing
Internet		0.0.0.0	0.0.0.0	✓
LocalNet		172.17.0.0	255.255.255.0	✓
VPN_Remote_Net		192.168.9.0	255.255.255.0	✓

### Routing

Um das gegenüberliegende Netz erreichen zu können, muss das Routing über die Firewallmatrix konfiguriert werden. Sie finden die Einstellungen im Menü „System → Netzwerk → Firewall → Matrix“. Für den ersten Testlauf sollten Sie die Verbindung in beide Richtungen komplett freigeben.

Menü > System > Netzwerk > Firewallmatrix > Regel bearbeiten

### Regel bearbeiten

Dienst any

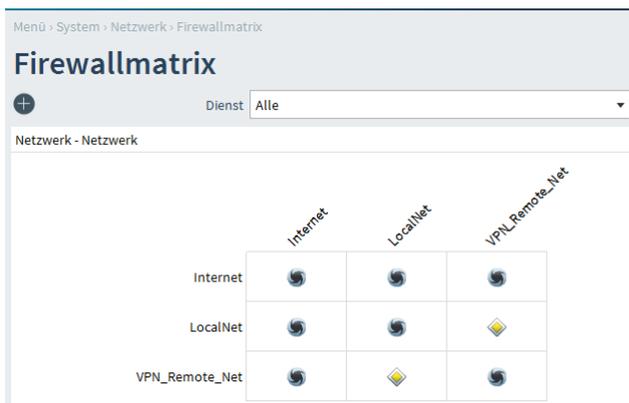
Von Netzwerk LocalNet (172.17.0.0/24)

Nach Netzwerk VPN\_Remote\_Net (192.168.9.0/24)

Protokollieren

Regel Erlauben

Traffic-Policy



### Firewall

Um den Zugriff der Clients aus dem VPN\_Remote\_Netz auf Dienste des CBS zu ermöglichen, erzeugen Sie über das Menü „System → Benutzungsrichtlinien → Richtlinien → Gruppen“ eine neue Gruppe. Als „Netz“ der Gruppe wählen Sie das „VPN\_Remote\_Netz“, da die Anfragen der Clients aus diesem Netz erfolgen. Durch setzen der entsprechenden Gruppenberechtigungen kann somit der Zugriff auf beliebige Dienste erlaubt werden.

Menü > System > Benutzungsrichtlinien > Gruppen

### Gruppen

Suche ...

Name	Kommentar	Import...
Administrators	Group with administrative powers	✗
Internet	Group for access from unknown networks	✗
LocalNet	Permissions for local networks	✗
Users	Group for system users	✗
VPN_Remote_Net	Permissions for VPN Remote Net	✗

### NAT-Traversal

Befinden sich einer oder beide Server hinter einem Router, muss auf den Collax Servern NAT-Traversal aktiviert sein. Dieser Dialog befindet sich unter „System → Netzwerk → Links → Allgemein“.

Menü > System > Netzwerk > Links – Allgemein

### Links – Allgemein

VPN

NAT-Traversal aktivieren

Standard-Proposal

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

### IPSec-Proposals

Um VPN/IPSec-Verbindungen aufbauen zu können, müssen verschiedene Parameter zu Schlüssel- und Datenaustausch definiert werden. Zur vereinfachten Handhabung und für zusätzliche Stabilität von VPN-Verbindungen werden diese Parameter in dem Formular „System → Netzwerk → Links → IPSec-Proposals“ zusammengefasst und können dann 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. Bei Links mit dem Typ „Auf Einwahl warten“ kann nur das Standard-Proposal ausgewählt werden.

Menü > System > Netzwerk > IPSec-Proposals

### IPSec-Proposals

Suche ...

Bezeichnung	Kommentar	Default
_compat	Commonly used parameters	✓
_old_freeswan	Old FreeS/WAN w/o patches	✗

## VPN Link konfigurieren

Auf dem CBS definieren Sie über den Menüpunkt „System → Netzwerk → Links → Links“ einen VPN Link. Den Wert des Feldes „Initiieren“ setzen Sie dabei auf „Immer“.

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

### Link bearbeiten

Grundeinstellungen Policy-Routing

Bezeichnung VPN\_CBS\_CSG  
 Kommentar VPN from CBS to CSG  
 Typ IPsec VPN  
 L2TP über IPsec verwenden   
 Host-zu-Netz-Verbindung   
 IPsec XAuth Nein  
 Verbindungsaufbau Immer  
 Neustart erzwingen

Adressen  
 Absenderadresse 172.17.0.33  
 MTU  
Wird normalerweise vom System bestimmt

IPsec  
 Eigener Schlüssel VPN\_CBS (VPN Zertifikat für den CBS)  
 Eigene ID  
 VPN-Gateway csg.collax.com  
Name oder IP-Adresse der IPsec-Gegenstelle  
 Schlüssel der Gegenstelle VPN\_CSG (VPN Zertifikat für das CSG)  
 ID der Gegenstelle  
 IPsec-Proposal (default: „compat“)

QoS  
 Bandbreitenmanagement

Routing  
 SNAT/Masquerading Nein  
 Erreichbare Netzwerke  
Dieser Link wird verwendet, um Pakete an die ausgewählten Netzwerke zu schicken  
 Internet (0.0.0.0/0)  
 LocalNet (172.17.0.0/24)  
 VPN\_Remote\_Net (192.168.9.0/24)  
 Lokale Netzwerke  
 Internet (0.0.0.0/0)  
 LocalNet (172.17.0.0/24)  
 VPN\_Remote\_Net (192.168.9.0/24)

Nachdem Sie die Konfiguration des CBS abgeschlossen haben, wechseln Sie auf das CSG.

## Konfiguration CSG

### Zertifikate importieren

Importieren Sie die zuvor exportierten Zertifikate über den Menüpunkt „System → Benutzungsrichtlinien → Zertifikate → X.509-Zertifikate“.

Benutzungsrichtlinien > X.509-Zertifikate > Zertifikat importieren

### Zertifikat importieren

Name für das Zertifikat VPN\_CBS  
 Passwort  
 Zertifikat Browse VPN\_CBS.crt  
 Privater Schlüssel Browse  
 CA-Zertifikat Browse

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

## Zertifikat importieren

Name für das Zertifikat

Passwort

Zertifikat  VPN\_CSG.crt

Privater Schlüssel

CA-Zertifikat

### VPN Netzwerk definieren

Anschließend muss das LAN der Gegenstelle definiert werden. Diesen Schritt führen Sie unter „System → Netzwerk → Links → Netze“ durch. Auf dem CSG wird dazu das VPN\_Remote\_Netz 172.17.0.0/24 angelegt.

Menü > System > Netzwerk > Netze

## Netze

Suche ...

Bezeichnung	Netz verwenden für	Netzwerkadresse	Netzmaske	Routing	ES
Internet		0.0.0.0	0.0.0.0	✓	
VPN_Remote_Net		172.17.0.0	255.255.255.0	✓	
Localnet		192.168.9.0	255.255.255.0	✓	

### Routing

Um das gegenüberliegende Netz erreichen zu können, muss das Routing über die Firewallmatrix konfiguriert werden. Sie finden die Einstellungen im Menü „System → Netzwerk → Firewall → Matrix“. Für den ersten Testlauf sollten Sie die Verbindung in beide Richtungen komplett freigeben.

Menü > System > Netzwerk > Firewallmatrix > Regel bearbeiten

## Regel bearbeiten

Dienst any

Von Netzwerk VPN\_Remote\_Net (172.17.0.0/24)

Nach Netzwerk Localnet (192.168.9.0/24)

Protokollieren

Regel Erlauben

Traffic-Policy

Menü > System > Netzwerk > Firewallmatrix

## Firewallmatrix

Dienst Alle

Netzwerk - Netzwerk

	Internet	VPN_Remote_Net	Localnet
Internet			
VPN_Remote_Net			
Localnet			

## Firewall

Um den Zugriff der Clients aus dem VPN\_Remote\_Netz auf Dienste des CSG zu ermöglichen, erzeugen Sie über das Menü „System → Benutzungsrichtlinien → Richtlinien → Gruppen“ eine neue Gruppe. Als „Netz“ der Gruppe wählen Sie das „VPN\_Remote\_Netz“, da die Anfragen der Clients aus diesem Netz erfolgen. Durch setzen der entsprechenden Gruppenberechtigungen kann somit der Zugriff auf beliebige Dienste erlaubt werden.

Menü > System > Benutzungsrichtlinien > Gruppen

### Gruppen

Suche ...

Name	Kommentar	Import...	
Administrators	Group with administrative powers	✗	
Internet	Group for access from unknown networks	✗	
LocalNet	Permissions for local networks	✗	
Users	Group for system users	✗	
VPN_Remote_Net	Permissions for VPN Remote Net	✗	

## NAT-Traversal

Befindet sich einer der Collax Server hinter einem weiteren Router, muss auf beiden Collax Servern NAT-Traversal aktiviert sein. Sie finden diese Einstellung im Menü „System → Netzwerk → Links → Allgemein“. Der vor dem Collax Server befindliche Router muss die UDP-Ports 500 und 4500 durchlassen. Bei den meisten Routern wird dies über die Option „VPN-Passthrough“ erreicht.

## IPsec-Proposals

Um VPN/IPsec-Verbindungen aufbauen zu können, müssen verschiedene Parameter zu Schlüssel- und Datenaustausch definiert werden. Zur vereinfachten Handhabung und für zusätzliche Stabilität von VPN-Verbindungen werden diese Parameter in dem Formular „System → Netzwerk → Links → IPsec-Proposals“ zusammengefasst und können dann 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. Bei Links mit dem Typ „Auf Einwahl warten“ kann nur das Standard-Proposal ausgewählt werden.

Menü > System > Netzwerk > IPsec-Proposals

### IPsec-Proposals

Suche ...

Bezeichnung	Kommentar	Default	
_compat	Commonly used parameters	✓	
_old_freeswan	Old FreeS/WAN w/o patches	✗	

## VPN Link konfigurieren

Auf dem CSG definieren Sie über den Menüpunkt „Einstellungen → Netzwerk → Links → Konfiguration“ einen VPN Link. Den Wert des Feldes „Initiieren“ setzen Sie dabei auf „Immer“.

Menü » System » Netzwerk » Link-Konfiguration » Link bearbeiten

### Link bearbeiten

Grundeinstellungen Policy-Routing

Bezeichnung: VPN\_CSG\_CBS  
 Kommentar: VPN from CSG to CBS  
 Typ: IPsec VPN  
 LTP über IPsec verwenden  
 Host-zu-Netz-Verbindung  
 IPsec XAuth: Nein  
 Verbindungsaufbau: Immer  
 Neustart erzwingen

Adressen  
 Absenderadresse: 192.168.9.9  
 MTU:  
Wird normalerweise vom System bestimmt

IPsec  
 Eigener Schlüssel: VPN\_CSG (VPN Zertifikat für das CSG)  
 Eigene ID:  
 VPN-Gateway: cbs.collax.com  
Name oder IP-Adresse der VPN-Gegenstelle  
 Schlüssel der Gegenstelle: VPN\_CBS (VPN Zertifikat für den CBS)  
 ID der Gegenstelle:  
 IPsec-Proposal: (default: '\_compat')

QoS  
 Bandbreitenmanagement

Routing  
 SNAT/Masquerading: Nein  
 Erreichbare Netzwerke  
Dieser Link wird verwendet, um Pakete an die ausgewählten Netzwerke zu schicken  
 Internet (0.0.0.0/0)  
 VPN\_Remote\_Net (172.17.0.0/24)  
 LocalNet (192.168.9.0/24)  
 Lokale Netzwerke  
 Internet (0.0.0.0/0)  
 VPN\_Remote\_Net (172.17.0.0/24)  
 LocalNet (192.168.9.0/24)

Die Konfiguration ist abgeschlossen und die VPN Verbindung sollte nach Aktivierung der beiden Konfigurationen automatisch starten.