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).

Vorraussetzungen

- 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.

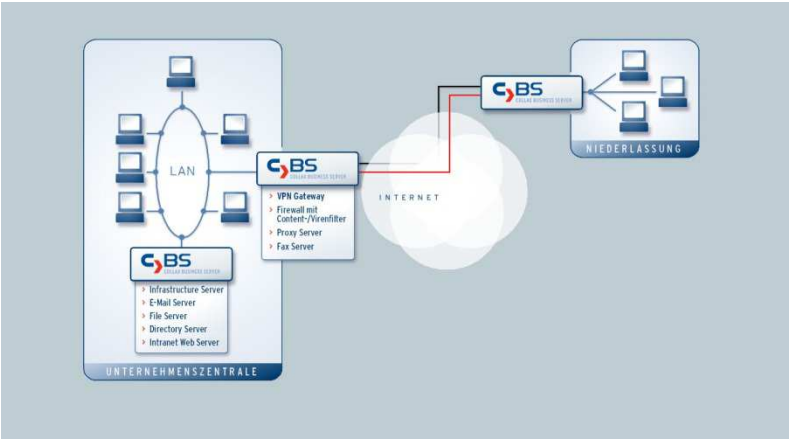
Grundsätzliches

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

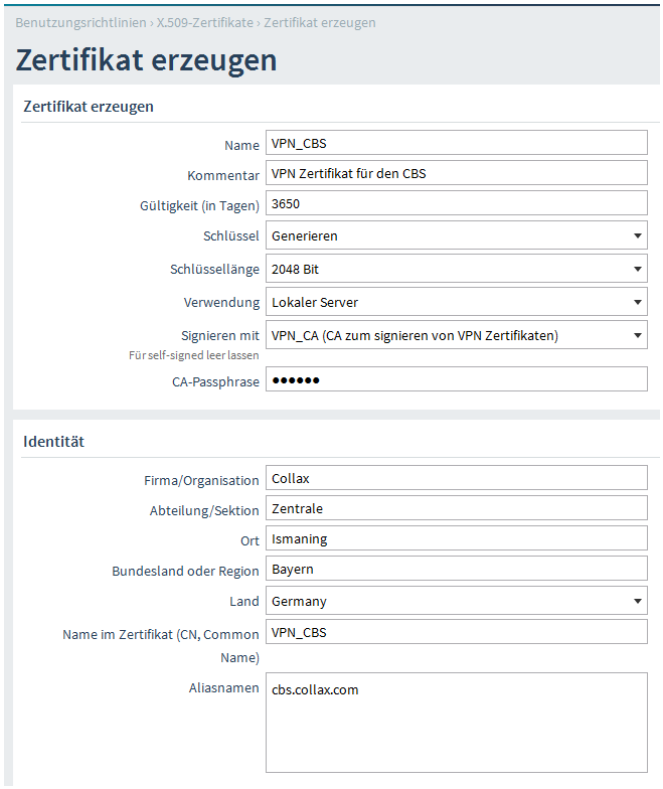
Zuallererst erstellen wir auf dem CBS eine CA. Die CA generieren Sie im Menü *„System → Benutzungsrichtlinien → Zertifikate → X.509-Zertifikate“*. Mithilfe der CA werden im weiteren Verlauf der Zertifikatserstellung für den CBS ein Lokales- und für das CSG ein Nicht Lokales Serverzertifikat erstellt.

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.

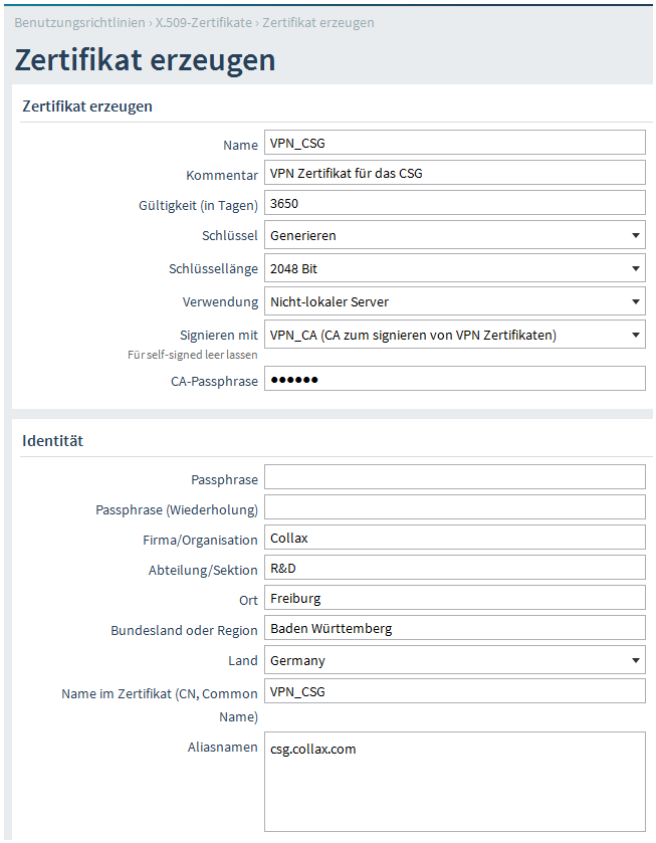
Lokales Serverzertifikat erstellen

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



Nicht Lokales Serverzertifikat erstellen

Mit dem Nicht Lokalen Serverzertifikat verfahren wir identisch. Beachten Sie, diesmal als *Verwendung „Nicht lokaler Server“* zu wählen.



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).

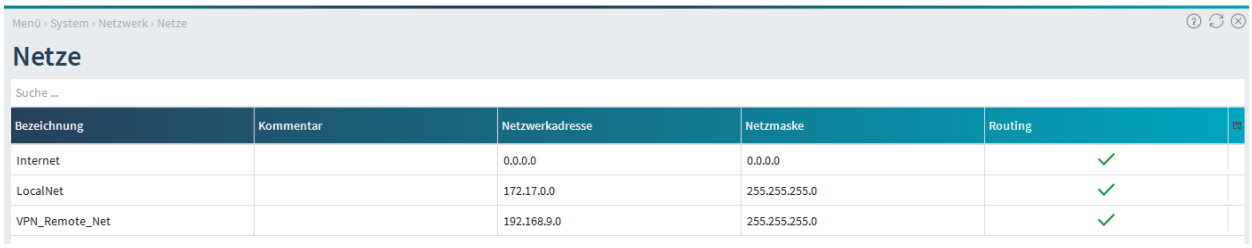
Durch Rechtklick auf die Zertifikate in der Übersicht können diese exportiert werden. Achten Sie darauf, dass das nicht lokale Zertifikat (VPN_CSG) mit privatem Schlüssel exportiert werden muss.

Nach erfolgtem Export und Speichern der Dateien tragen diese die Namen „VPN_CBS.crt“ und „VPN_CSG.crt“.

VPN Netzwerk definieren

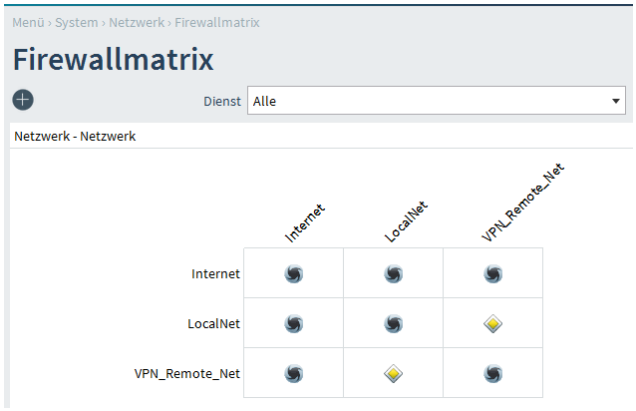
Bevor Sie einen VPN Link erzeugen, muss das LAN der Gegenstelle definiert werden. Diesen Schritt führen Sie unter *„System →Netzwerk →Links →Netze“* durch.

Auf dem CBS wird dazu das VPN_Remote_Netz 192.168.9.0/24 angelegt.



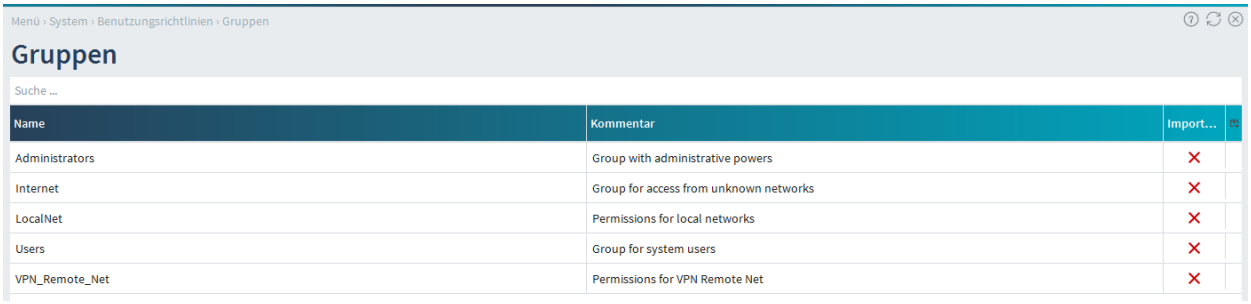
Routing

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.



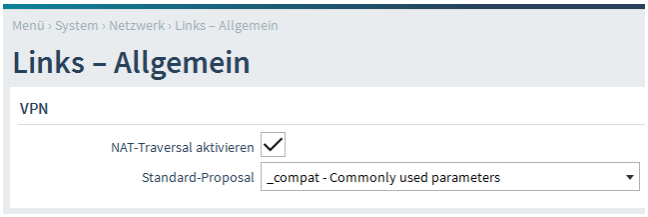
Firewall

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.



NAT-Traversal

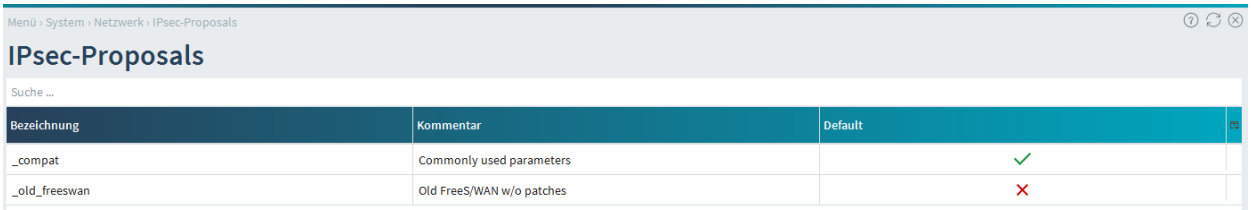
Befinden sich einer oder beide Server hinter einem Router, muss auf den Collax Servern NAT-Traversal aktiviert sein. Dieser Dialog befindet sich unter *„System → Netzwerk → Links → Allgemein“*.



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

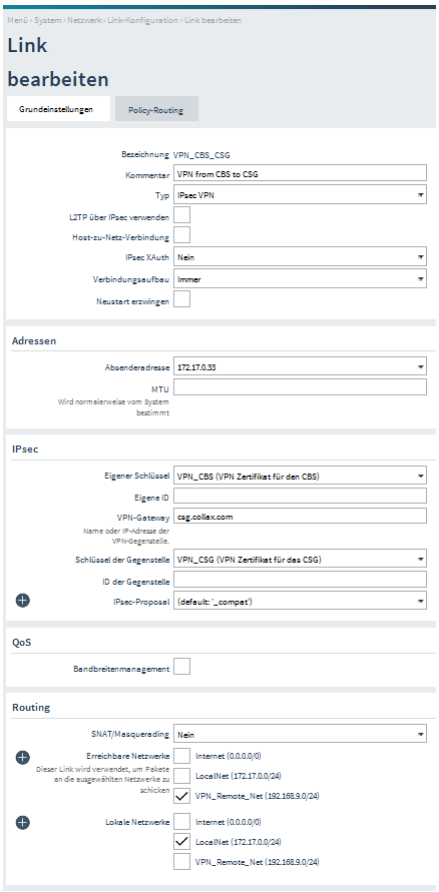
IPSec-Proposals

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.



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“*.



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

Konfiguration CSG

Zertifikate importieren

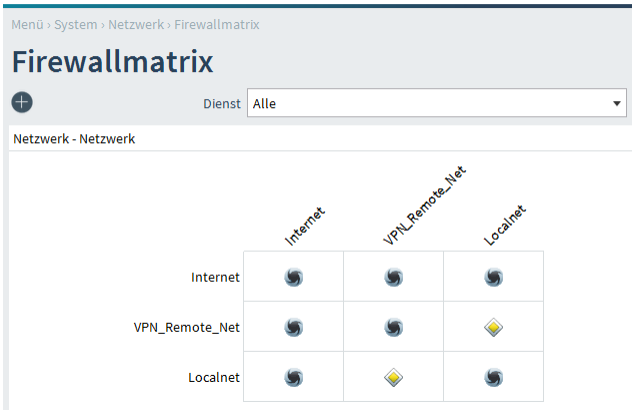
Importieren Sie die zuvor exportierten Zertifikate über den Menüpunkt *„System → Benutzungsrichtlinien → Zertifikate → X.509-Zertifikate“*.

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.

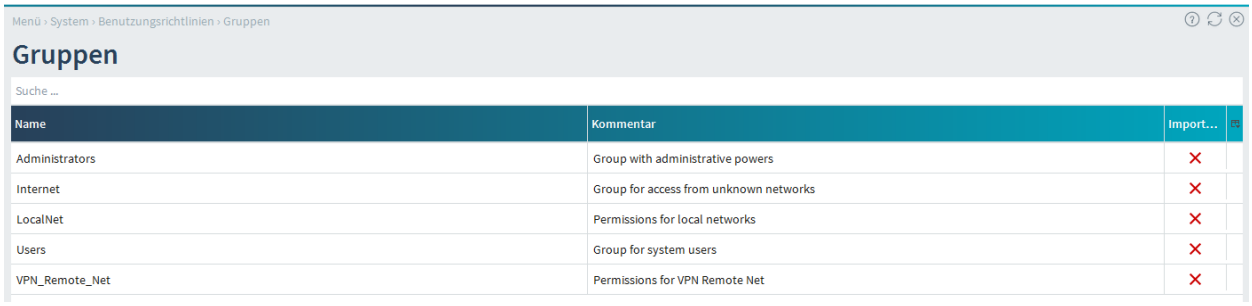
Routing

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.



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.

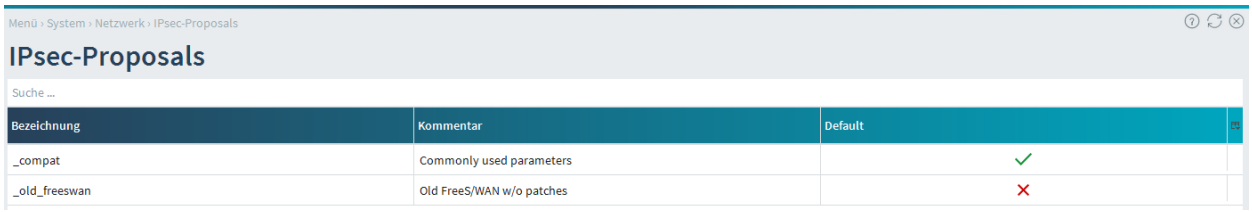


NAT-Traversal

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.

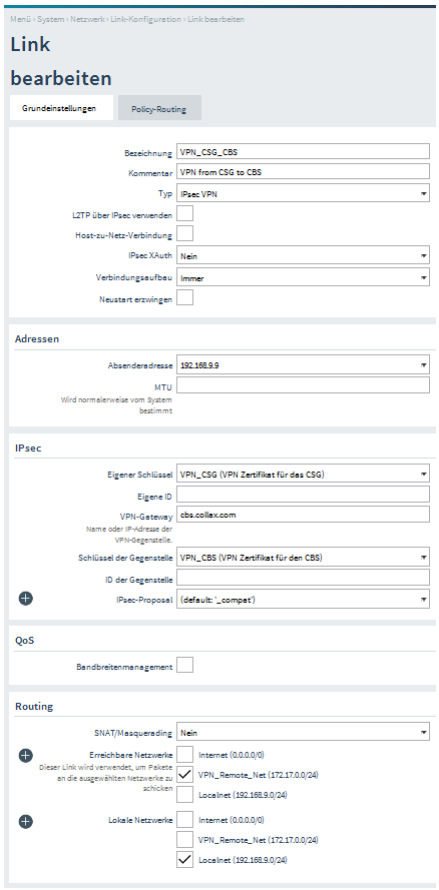
IPSec-Proposals

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.



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“*.



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