Collax iOS-VPN Howto

Inhalt

Status: Final Version: 7.0 Datum: 05.12.2016

Vorbereitungen

Allgemeines

Die Dokumentation beschreibt die Konfiguration einer VPN-Verbindung zwischen einem Collax Server und einem iOS Client mittels L2TP/Ipsec. Folgende Beispielkonfiguration ist gegeben:

- Collax Security Gateway
  FQDN: csg.collax.com
- Localnet: 172.16.17.0/24
- Client: iPhone iOS 10

Einstellungen

DHCP Server aktivieren

Der DHCP-Server wird nur benötigt, wenn sich mehrere Clients gleichzeitig einwählen sollen.

Soll sich nur ein Client einwählen, können Sie diesen Schritt überspringen.

Aktiveren Sie zuerst den DHCP-Server unter “Einstellungen → Netzwerk → DHCP → Allgemein”.

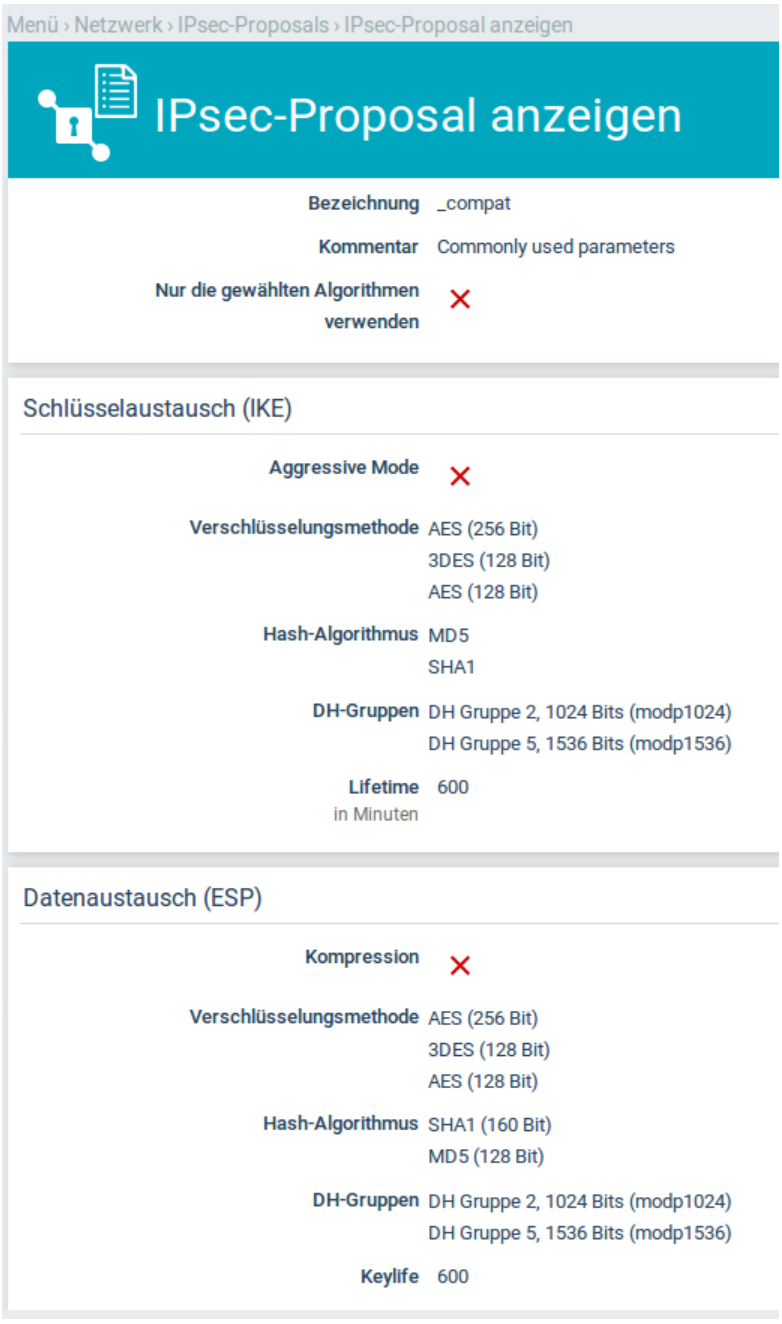
IPSec-Proposal anlegen

Bei IPSec-Proposals handelt es sich um Verschlüsselungsmethoden und Hash-Algorithmen für die verschiedenen Stufen von VPN-Verbindungen.

Für eine Verbindung zum iOS verwenden Sie das Proposal **_compat** oder ein gleiches Proposal, das die Einstellungen und Algorithmen wie im Screenshot enthält.

Wir verwenden ein Proposal mit dem Namen “iPhone” das die Einstellungen wie im folgenden Screenshot hat.

Ein neues Proposal können erstellen Sie ggf. Unter *Netzwerk → Links → IPSec-Proposals*



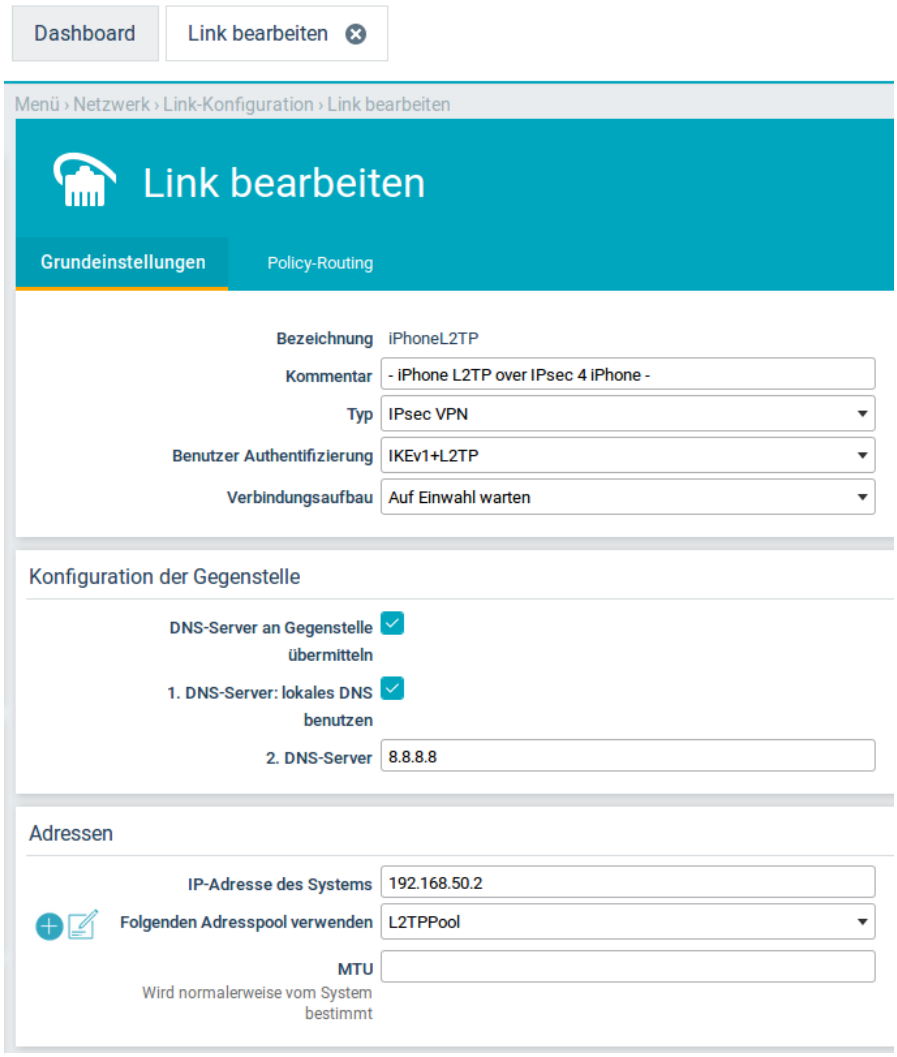
Unter “Einstellungen → Netzwerk → Links → Allgemein“ wählen wir es in der Liste als „Standard-Proposal“ aus.

Konfiguration des Collax Security Gateways

L2TP Link definieren

- Legen Sie unter “Netzwerk → Links” einen Link vom Typ “IPsec VPN” an.
- Setzen Sie folgende Parameter
  - “Benutzerauthentifizierung” = “IKEv1+L2TP”
  - ”Verbindungsaufbau” = “Auf Einwahl warten”

- Die eigene IP-Adresse des Systems muss aus demselben IP Adressbereich sein wie das oben angelegte Netz.
- “Folgenden Adresspool verwenden”. Falls noch kein Adresspool vorhanden ist, klicken Sie auf das (+)Zeichen



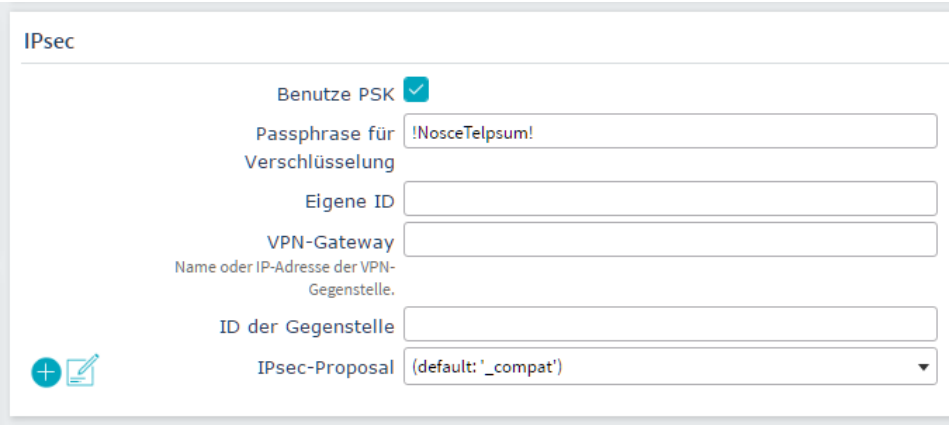
DHCP-Adress-Pool einrichten

- Fügen Sie einen Pool hinzu, und setzen Sie diese Parameter
  - Bezeichnung
  - Typ = VPN (L2TP/PPTP)
  - Netzwerk und entsprechende IP-Adressen an, die der Gegenstelle zugewiesen werden sollen.

- Ist noch kein passendes Netzwerk vorhanden, fügen Sie eines über den (+)-Zeichen hinzu

Netzwerk anlegen

Dieses dient der Zuweisung von IP Adressen bei Einwahl der Clients. Es darf daher vom Server nicht lokal geroutet werden.



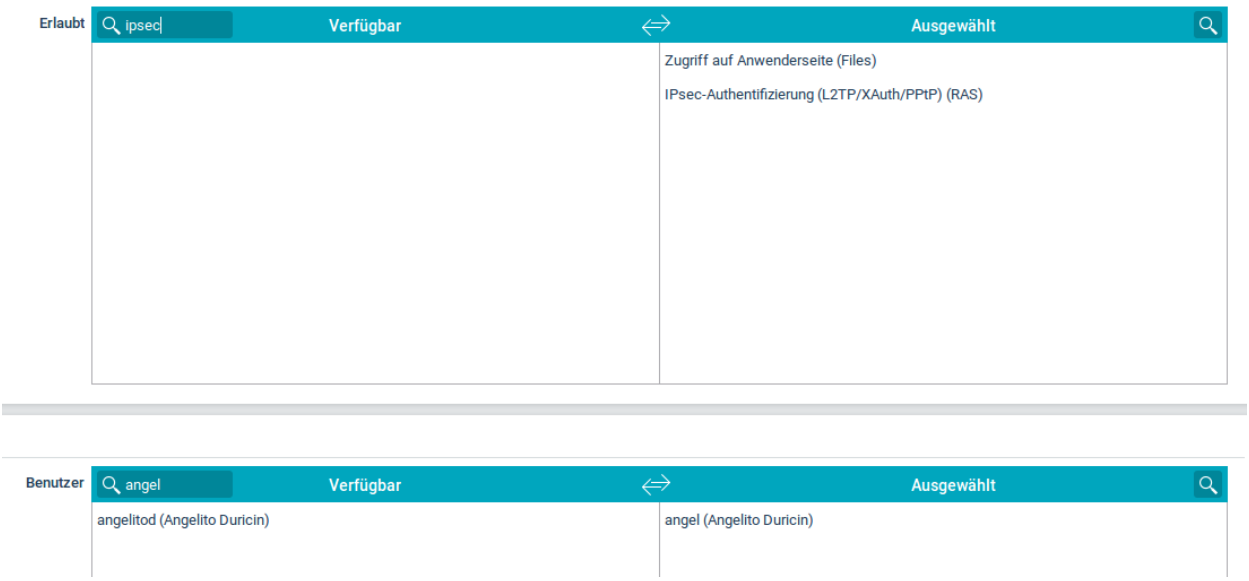
- Aktivieren Sie “Benutze PSK” und bauen Sie zunächst die Verbindung mit einem Pre-Shared Key (PSK) auf.
- Geben Sie bei “Passphrase für die Verschlüsselung” den Pre-Shared Key ein.

Berechtigung einer Benutzergruppe geben

Nun sollen Benutzer noch Berechtigungen erhalten. Fügen Sie unter "Einstellungen -> Benutzungsrichtlinien -> Richtlinien -> Gruppen" eine Gruppe hinzu oder bearbeiten Sie entsprechend eine bestehende Gruppe.

Diese Gruppe braucht die Berechtigung „IPSec-Authentifizierung (L2TP/XAuth)“. Diese Berechtigung zählt zur Kategorie RAS.

Die Benutzer, die Sie dieser Gruppe hinzufügen, können sich nach Beendigung der Konfiguration auf dem CSG einwählen.



Firewall-Zugriff konfigurieren:

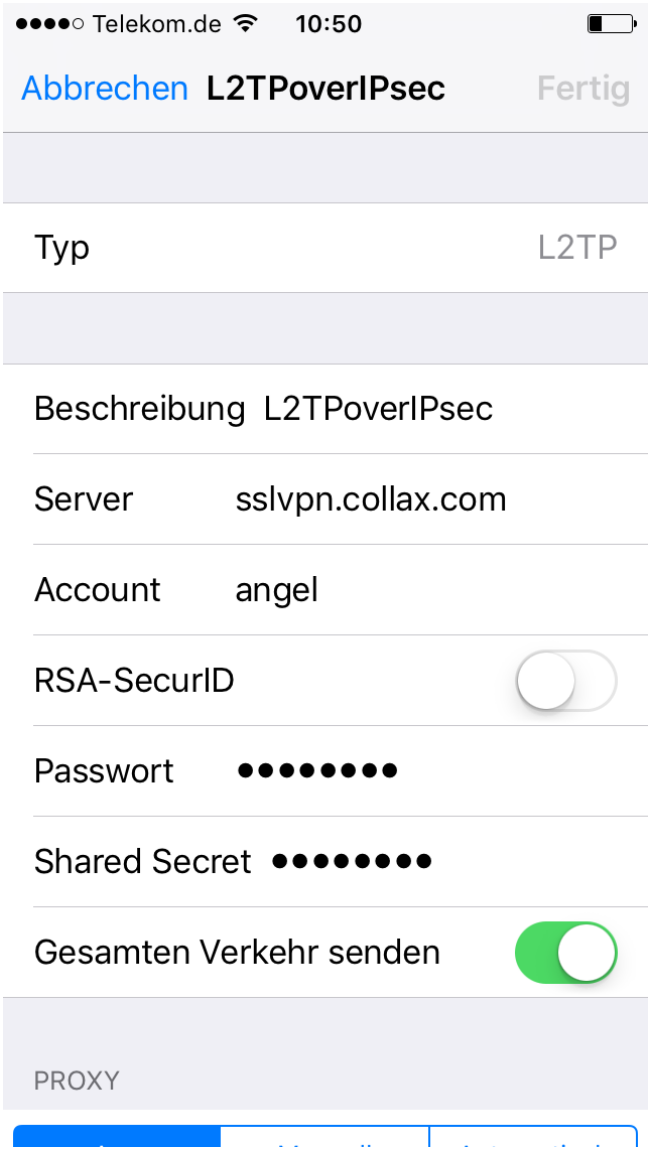
Damit ein Zugriff ins Lokale Netz erfolgen kann, konfigurieren sie die Firewall entsprechend unter “Einstellungen → Netzwerk → Firewall → Matrix”. Für den ersten Test ist es ratsam allen Verkehr zuzulassen, also von Netzwerk “L2TP-Netz” nach “Localnet” -> Dienst “any”, Regel “erlauben”.

Konfiguration von iOS:

Version iOS 10

- Fügen Sie eine neue VPN-Verbindung hinzu.
- Verbindungsart (Typ) = L2TP (mit PSK)

- Geben Sie als Server den Namen oder die statische IP-Adresse des Collax Servers an
- Account = Login-Name eines Benutzers aus der Gruppe, mit den L2TP-Berechtigungen angegeben
- RSA-SecurID = aus
- Passwort = Passwort des Benutzers mit L2TP-Berechtigung
- SharedSecret = PSK des L2TP-Links



Verbindungsaufbau

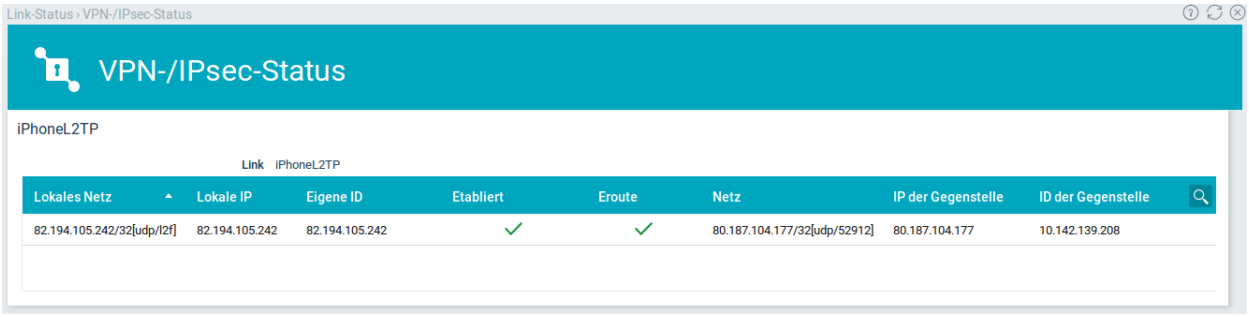
Aufbau auf dem iPhone

Statusinformation auf Collax

Wenn die L2TP-Verbindung in Ordnung ist, wird der Status der Verbindung im Dialog *Link-Status* mit **Up** gekennzeichnet.

Um den genauen Status der VPN-Verbindung zu sehen, klicken Sie auf den Typ **vpn**

Die Spalte “Etabliert” kennzeichnet, dass der VPN-Link aufgebaut wurde, “Eroute” kennzeichnet, dass der Link auf geroutet wird.



Troubleshooting

iOS neu starten

Wenn Sie sichergestellt haben, dass alle Werte korrekt sind und dennoch keine VPN-Verbindung aufgebaut werden kann, starten Sie das iOS-System neu.