Collax L2TP-, IKEv2 IPsec VPN Howto

Inhalt

Status: Final Version: 7.0 Datum: 26.7.2018

Vorbereitungen

Allgemeines

Die Dokumentation beschreibt die Konfiguration einer VPN-Verbindung zwischen einem Collax Server und einem Client mittels L2TP- und IKEv2-IPsec. Folgende Beispielkonfiguration ist gegeben:

- Collax Security Gateway
  FQDN: csg.collax.com
- Localnet: 172.16.17.0/24
- Client: Windows 8.1 (L2TP)

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.

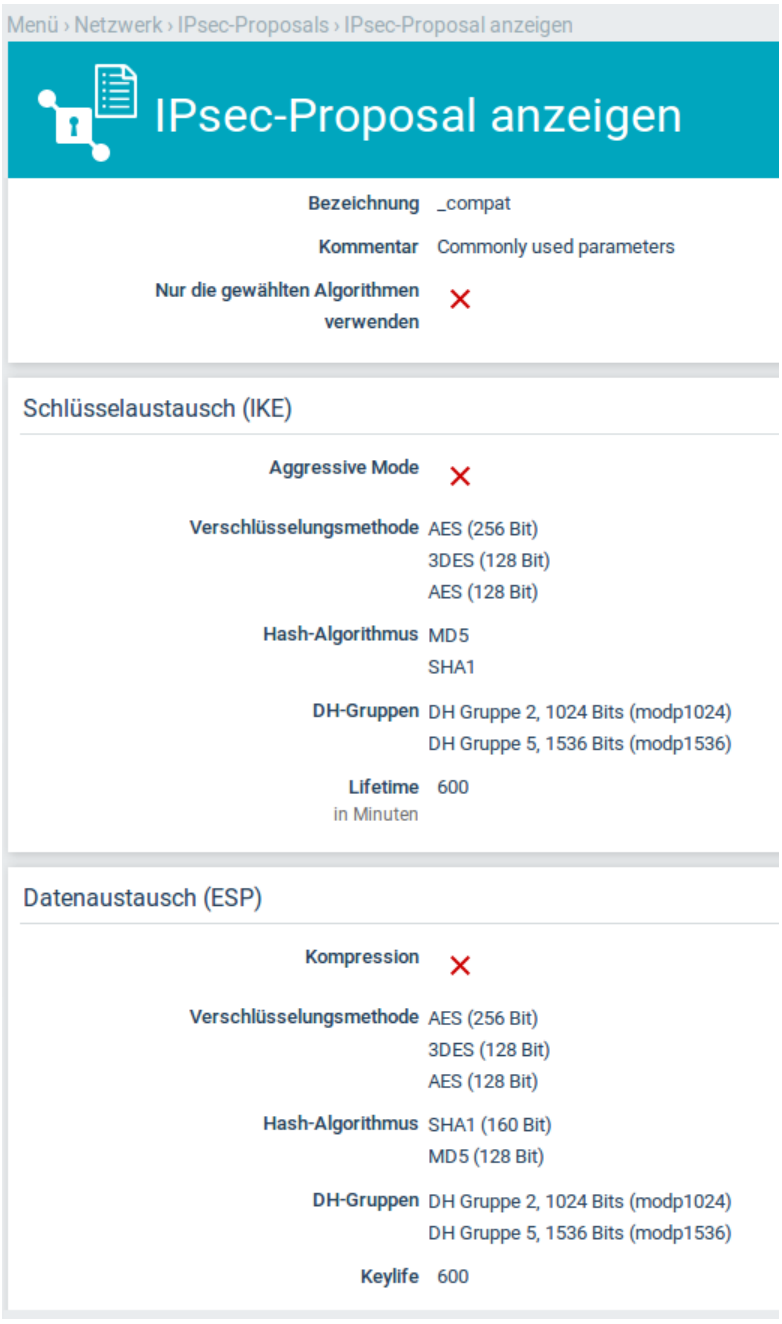
Aktiveren Sie zuerst den DHCP-Server unter "Einstellungen → Netzwerk → DHCP → Allgemein".

IPSec-Proposal anlegen

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

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

Ein neues Proposal können Sie ggf. unter „Netzwerk → Links → IPSec-Proposals" erstellen.

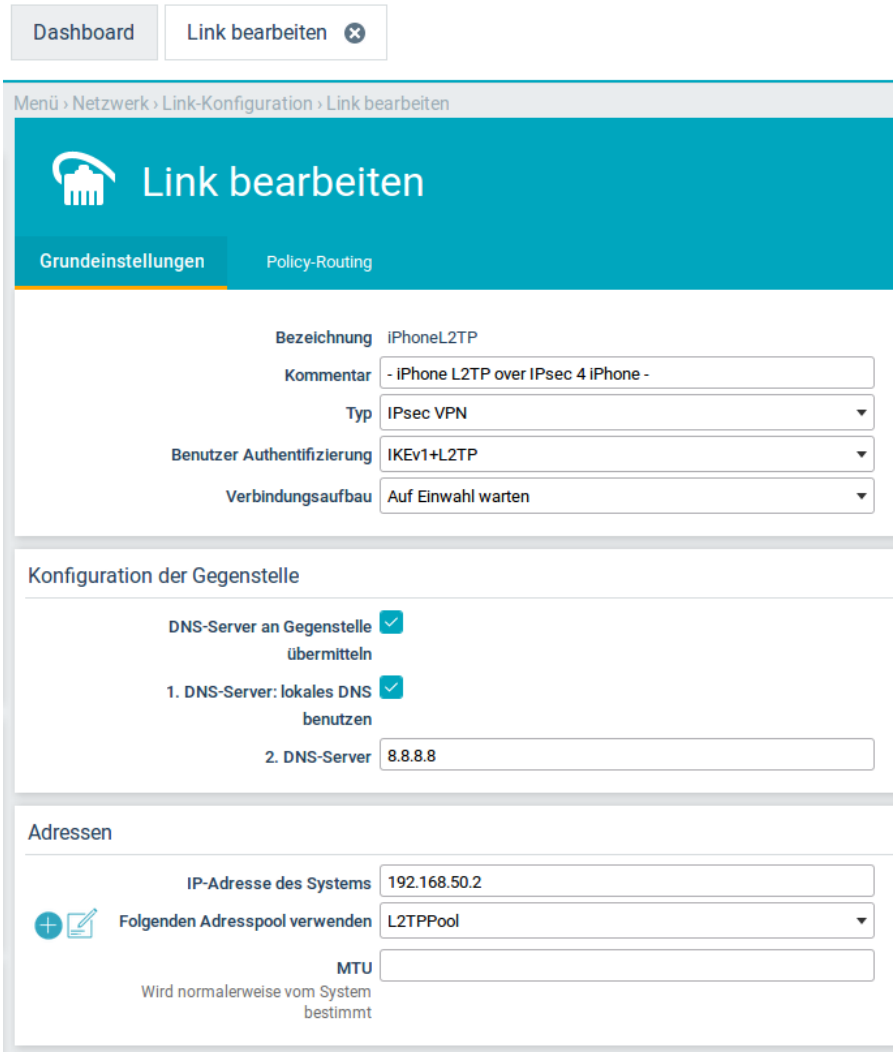


Unter “Einstellungen → Netzwerk → Links → Allgemein“ wählen wir es in der Liste als „Standard-Proposal“ aus.

Konfiguration des Collax Servers

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



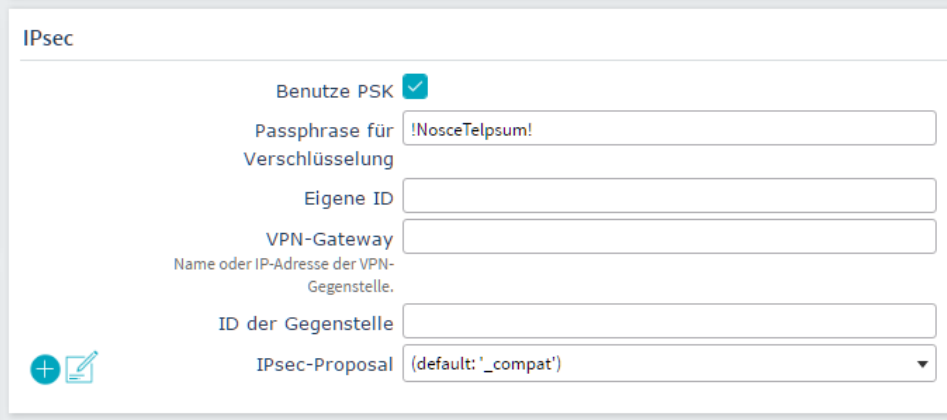
DHCP-Adress-Pool einrichten

- 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.

IKEv2 Link definieren

- Legen Sie unter “Netzwerk → Links” einen Link vom Typ “IPsec VPN” an.
- Setzen Sie folgende Parameter
  - “Benutzerauthentifizierung” = “IKEv2+RSA+EAP”
  - ”Verbindungsaufbau” = “Auf Einwahl warten”
  - Geben Sein einen DHCP-Adresspool an: “Folgenden Adresspool verwenden”.
  - Geben Sie ein Zertifikat an. Wenn das Zertifikat von einer offiziellen CA abgeleitet wurden, muss für den Client nichts weiter getan werden. Ansonsten exportieren Sie den Public-Anteil der entsprechenden CA.

    Hinweis: Wenn die Clients mit dem CA-Zertifikat des Server-Zertifikats konfiguriert werden sollen, muss das Server-Zertifikat die ID des Server enthalten. Das ist üblicherweise der FQDN.

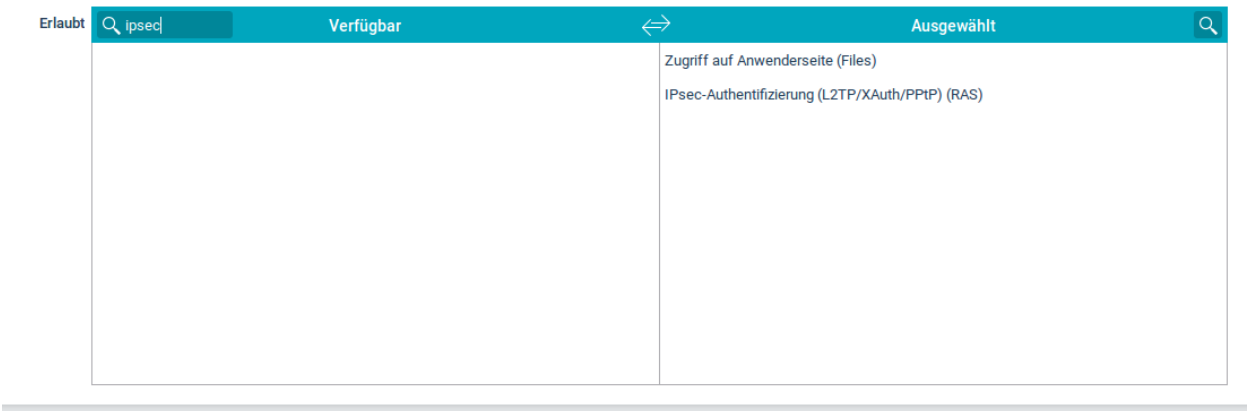
  - Bei Routing geben sie das Netzwerk an, in das geroutet werden soll.
    Hinweis: Maskieren Sie das VPN Netzwerk auf dem entsprechenden Link ins lokale Netzwerk

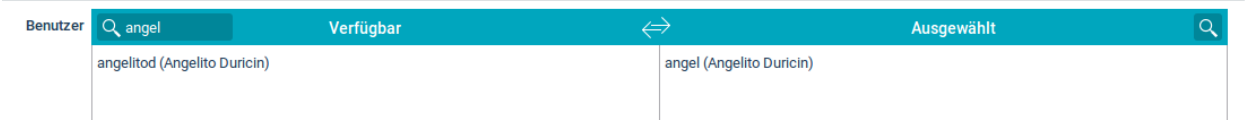
Berechtigung einer Benutzergruppe geben

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.





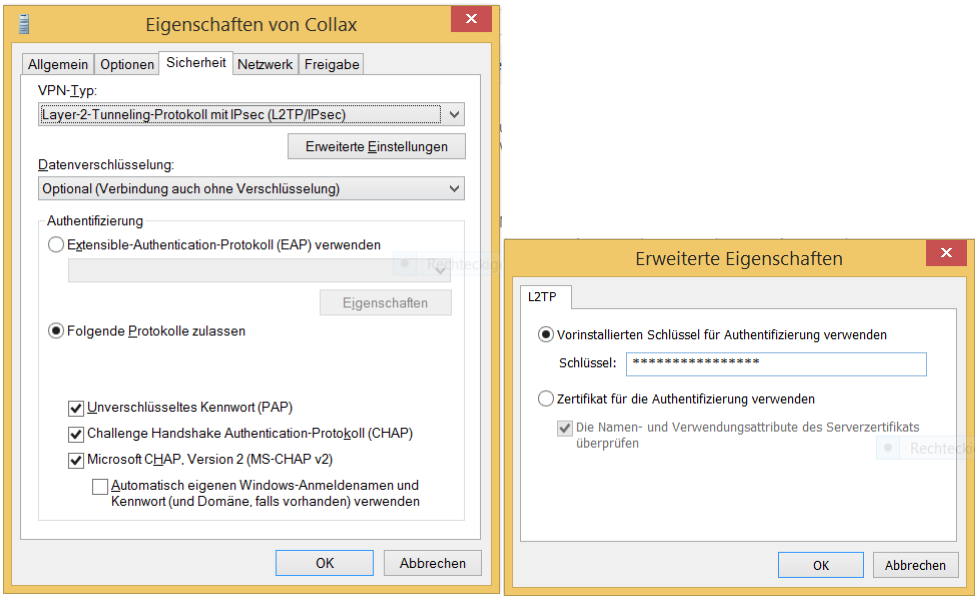
Firewall-Zugriff konfigurieren

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”.

L2TP-Konfiguration von Windows

Windows 8.1

- Fügen Sie eine neue VPN-Verbindung hinzu
- Geben Sie als Internetadresse den Namen oder die statische IP-Adresse des Collax Servers an
- Öffnen Sie die Adaptereinstellungen der neuen Netzwerkverbindung
- Ändern Sie im Reiter „Sicherheit“ den VPN-Typ auf „Layer-2-Tunneling-Protokoll mit IPsec (L2TP/IPsec)“
- Unter „Folgende Protokolle zulassen“ muss CHAP angehakt sein
- In den „Erweiterten Einstellungen“ tragen Sie den PSK-Schlüssel ein



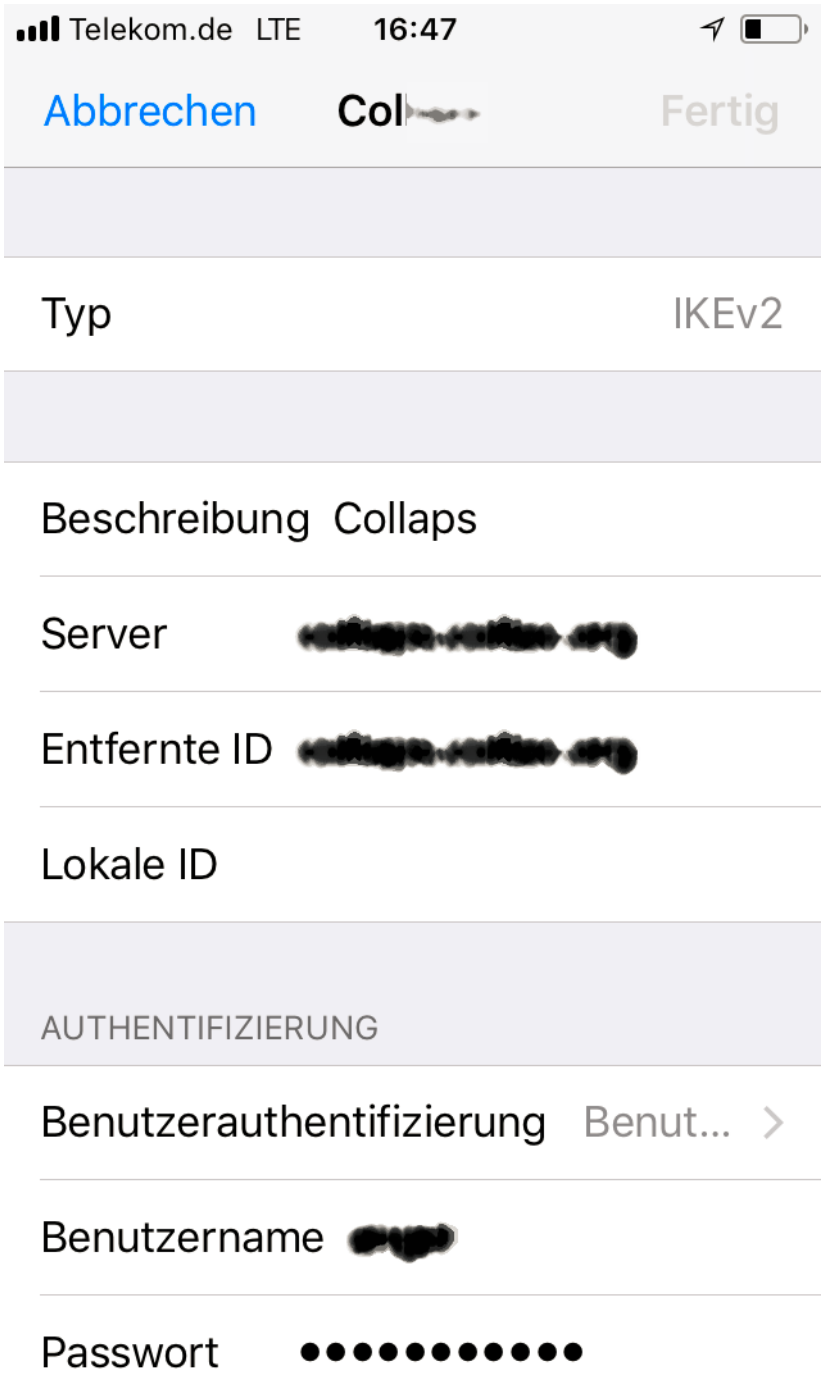
Aufbau der Verbindung in Windows

- Benutzername = Login-Name eines Benutzers aus der Gruppe, mit den L2TP-Berechtigungen angegeben
- Kennwort = Passwort des Benutzers mit L2TP-Berechtigung

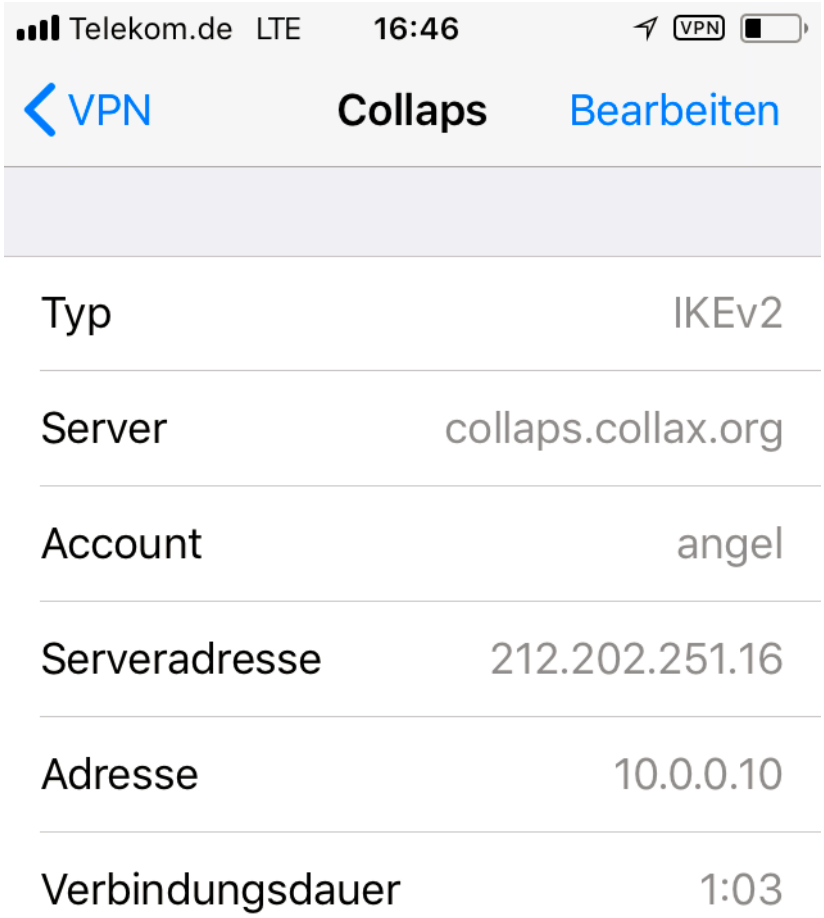
IKEv2-Konfiguration von iOS

- Wenn das Zertifikat des Servers nicht von einer CA stammt, dann importieren Sie den Public-Anteil des Zertifikats des Collax Servers auf dem iOS unter Profile. (Bspw. ein Let's Encrypt Zertifikat)

- Legen Sie eine VPN-Verbindung an:
  - Typ „IKEv2" und geben sie den entsprechenden Benutzernamen-Login eines Benutzers aus der Gruppe, mit den IPsec-Berechtigungen an.



- Starten Sie die Verbindung



Statusinformation auf Collax

Wenn die VPN-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.