

Collax iOS-VPN Howto

Inhalt

Vorbereitungen	2
Allgemeines	2
Einstellungen	2
DHCP Server aktivieren	2
IPSec-Proposal anlegen	2
Konfiguration des Collax Security Gateways	3
L2TP Link definieren	3
DHCP-Adress-Pool einrichten	4
Netzwerk anlegen	4
Berechtigung einer Benutzergruppe geben	6
Firewall-Zugriff konfigurieren:	6
Konfiguration von iOS:	7
Verbindungsaufbau	8
Aufbau auf dem iPhone	8
Statusinformation auf Collax	9
Troubleshooting	9
iOS neu starten	9

Vorbereitungen

Allgemeines

Die Dokumentation beschreibt die Konfiguration einer VPN-Verbindung zwischen einem Collax Server und einem iOS Client mittels L2TP/Ipssec. 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.

Aktivieren 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*

Menü > Netzwerk > IPsec-Proposals > IPsec-Proposal anzeigen



IPsec-Proposal anzeigen

Bezeichnung _compat

Kommentar Commonly used parameters

Nur die gewählten Algorithmen verwenden ✘

Schlüsselaustausch (IKE)

Aggressive Mode ✘

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

Hash-Algorithmus MD5
SHA1

DH-Gruppen DH Gruppe 2, 1024 Bits (modp1024)
DH Gruppe 5, 1536 Bits (modp1536)

Lifetime 600
in Minuten

Datenaustausch (ESP)

Kompression ✘

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

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

DH-Gruppen DH Gruppe 2, 1024 Bits (modp1024)
DH Gruppe 5, 1536 Bits (modp1536)

Keylife 600

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

Dashboard
Link bearbeiten ✕

Menü > Netzwerk > Link-Konfiguration > Link bearbeiten

Link bearbeiten

Grundeinstellungen

Policy-Routing

Bezeichnung iPhoneL2TP

Kommentar - iPhone L2TP over IPsec 4 iPhone -

Typ IPsec VPN

Benutzer Authentifizierung IKEv1+L2TP

Verbindungsaufbau Auf Einwahl warten

Konfiguration der Gegenstelle

DNS-Server an Gegenstelle übermitteln

1. DNS-Server: lokales DNS benutzen

2. DNS-Server 8.8.8.8

Adressen

IP-Adresse des Systems 192.168.50.2

Folgenden Adresspool verwenden L2TPPool

MTU

Wird normalerweise vom System bestimmt

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.

IPsec

Benutze PSK


Passphrase für Verschlüsselung

Eigene ID

VPN-Gateway
Name oder IP-Adresse der VPN-Gegenstelle.

ID der Gegenstelle

IPsec-Proposal



- 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.

The screenshot shows two panels from the COLLAX management interface. The top panel is titled 'Erlaubt' (Allowed) and shows a search for 'ipsec'. The 'Verfügbar' (Available) list is empty, and the 'Ausgewählt' (Selected) list contains two items: 'Zugriff auf Anwenderseite (Files)' and 'IPsec-Authentifizierung (L2TP/XAuth/PPiP) (RAS)'. The bottom panel is titled 'Benutzer' (Users) and shows a search for 'angel'. The 'Verfügbar' list contains 'angelitod (Angelito Duricin)', and the 'Ausgewählt' list contains 'angel (Angelito Duricin)'.

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

The screenshot shows the configuration screen for a new L2TP over IPsec VPN connection on an iPhone. At the top, the status bar shows 'Telekom.de', signal strength, Wi-Fi, time '10:50', and battery level. The title bar contains 'Abbrechen' (cancel), 'L2TP over IPsec', and 'Fertig' (done). The configuration fields are as follows:

Typ	L2TP
Beschreibung	L2TP over IPsec
Server	sslvpn.collax.com
Account	angel
RSA-SecurID	<input type="checkbox"/>
Passwort	●●●●●●●●
Shared Secret	●●●●●●●●
Gesamten Verkehr senden	<input checked="" type="checkbox"/>
PROXY	

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, "Eroutet" kennzeichnet, dass der Link auf geroutet wird.

The screenshot shows the 'VPN-/IPsec-Status' dialog for 'iPhoneL2TP'. It contains a table with the following data:

Lokales Netz	Lokale IP	Eigene ID	Etabliert	Eroutet	Netz	IP der Gegenstelle	ID der Gegenstelle
82.194.105.242/32[udp/12f]	82.194.105.242	82.194.105.242	✓	✓	80.187.104.177/32[udp/52912]	80.187.104.177	10.142.139.208

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.