

# Collax PPTP-VPN

## Howto

Dieses Howto beschreibt wie ein Collax Server innerhalb weniger Schritte als PPTP-VPN Server eingerichtet werden kann, um Clients Zugriff ins Unternehmensnetzwerk von außen zu ermöglichen. Für die Nutzung stehen PPTP-Clients für Windows, Mac OS X, Linux und BSD zur Verfügung. Zudem kann für Android und iOS Smartphones ebenfalls leicht ein VPN eingerichtet werden.

Zielsetzung ist der Aufbau eines PPTP-VPN zwischen dem Collax Server und einem Windows Client. PPTP wird von Windows nativ unterstützt und ist Bestandteil des Betriebssystems.

### Voraussetzungen

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

### PPTP über eine Firewall

Befindet sich der Collax Server hinter einer Firewall, muss diese den für die Kommunikation verwendeten Server-Port 1723 (TCP) sowie das Protokoll 47 (GRE) weiterleiten.

Befindet sich der Client hinter einer Firewall müssen die Dienste von innen geöffnet sein.

### PPTP Netzwerk

Bevor ein PPTP-Einwahl-Link angelegt werden kann, definieren wir ein neues Netzwerk für die IP-Adresszuweisung an die Clients.

Dieser Dialog befindet sich unter „System → Benutzungsrichtlinien → Richtlinien → Netze“

Menü > System > Benutzungsrichtlinien > Netze > Netzwerk bearbeiten

## Netzwerk bearbeiten

Grundeinstellungen Gruppenzugehörigkeit Optionen

**Grundeinstellungen**

Bezeichnung des Netzwerks: PPTP-Netz

Kommentar:

Netzwerkadresse: 192.168.100.0

Netzmaske: 255.255.255.000 (24 bit) ▼

Netz verwenden für: Routing (Links), Berechtigungen und Firewall-Matrix ▼

Link:  ▼

Auf diesen Link werden Pakete für dieses Netzwerk geroutet.

Verwenden Sie dazu unbedingt eine ungenutzte Netzwerkadresse, damit keine Adresskonflikte auftreten.

## IP-Adresspool

Der DHCP-Dienst vergibt IP-Adressen aus festgelegten Bereichen, den sogenannten „IP-Adresspools“. Hier kann ein neuer Pool für die IP-Adressvergabe an die PPTP Clients angelegt werden.

Dieser Dialog befindet sich unter „Dienste → Infrastruktur → DHCP → IP-Adresspools“

Menü > Dienste > Infrastruktur > IP-Adresspools > Adresspool bearbeiten

### Adresspool bearbeiten

Grundeinstellungen

Grundeinstellungen

Bezeichnung	PPTP_Pool
Kommentar	PPTP Adresspool
Typ	VPN (L2TP/PPTP) ▼
Netzwerk	PPTP-Netz (192.168.100.0/24) ▼
Erste IP-Adresse	192.168.100.100
Letzte IP-Adresse	192.168.100.110

**Typ** Hier wird festgelegt, welcher Dienst den Pool nutzen darf.

**Netzwerk** Hier muß das Netzwerk angelegt werden.

**Erste IP-Adresse** Hier wird die erste IP-Adresse für diesen Adresspool angegeben. Wird hier keine Adresse angegeben, wird die kleinste mögliche Adresse verwendet.

**Letzte IP-Adresse** Hier wird die letzte IP-Adresse für diesen Adresspool angegeben. Wird hier keine Adresse angegeben, wird die größte mögliche Adresse verwendet.

## PPTP-Link

Um den Clients die PPTP-Verbindung zu ermöglichen, legen wir einen PPTP-Link an.

Dieser Dialog befindet sich unter „System → Netzwerk → Links → Links“

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

## Link bearbeiten

Grundeinstellungen Policy-Routing

Bezeichnung   
 Kommentar   
 Typ

**Konfiguration der Gegenstelle**

DNS-Server an Gegenstelle   
 übermitteln  
 1. DNS-Server: lokales DNS   
 benutzen  
 2. DNS-Server

**Adressen**

IP-Adresse des Systems   
 Folgenden Adresspool   
 verwenden  
 MTU   
Wird normalerweise vom System bestimmt

**PPTP**

Verschlüsselungsalgorithmus  40 Bit  
 56 Bit  
 128 Bit  
 Auf Verschlüsselung bestehen

**Typ** Hier wird als Linktyp „PPTP VPN“ angegeben.

**DNS-Server an Gegenstelle übermitteln** Mit dem Aktivieren dieser Option wird der Gegenstelle beim Verbindungsaufbau ein DNS-Server zugewiesen.

**1. DNS-Server: lokales DNS benutzen** Durch das Aktivieren dieser Option wird der Collax Server der Gegenstelle als erster DNS-Server zugewiesen. Wenn diese Option deaktiviert ist, kann alternativ die IP-Adresse eines anderen Nameservers angegeben werden, der als erster DNS-Server zugewiesen wird.

**IP-Adresse des Systems** Hier wird die lokale IP-Adresse für den Link angegeben.

**Folgenden Adresspool verwenden** Hier kann der Adresspool für die IP-Adressenverteilung gewählt werden.

**Verschlüsselungsalgorithmus** Hier werden die unterstützten Schlüssellängen für den Algorithmus der PPTP-Verbindung ausgewählt. Zur Auswahl stehen 40, 56 und 128 Bit. Grundsätzlich bietet eine größere Schlüssellänge eine höhere Sicherheit.

**Auf Verschlüsselung bestehen** Das Aktivieren dieser Option verhindert unverschlüsselte Verbindungen.

## Benutzer und Gruppen

Für den Zugriff auf die PPTP-Verbindung legen wir uns eine separate Berechtigungsgruppe und einen Benutzer an.

Dieser Dialog befindet sich unter „System → Benutzungsrichtlinien → Richtlinien → Gruppen“ bzw. „System → Benutzungsrichtlinien → Richtlinien → Benutzer“

Der Gruppe vergeben wir die Berechtigung für den „PPTP-Zugang(RAS)“

Als Mitglieder-Netz der Gruppe geben wir das „Internet“ an, um den Zugriff von Clients aus dem Internet zu ermöglichen.

Die Benutzer, die wir der Gruppe hinzufügen, werden für die Authentifizierung am PPTP-Server verwendet.

Menü > System > Benutzungsrichtlinien > Gruppen > Gruppe bearbeiten

### Gruppe bearbeiten

**Berechtigungen**

Erlaubt	Verfügbar	Ausgewählt
<input type="checkbox"/>	Rekursive DNS-Anfragen (Firewall)	<input checked="" type="checkbox"/> PPTP-Zugang (RAS)
<input type="checkbox"/>	Fax-Administrator (Fax)	
<input type="checkbox"/>	Lesen von Backup (Files)	
<input type="checkbox"/>	Lesen von BackupTarget_Default_local_target (Files)	
<input type="checkbox"/>	Lesen von IsoArchive (Files)	
<input type="checkbox"/>	Lesen von TestSYNC (Files)	
<input type="checkbox"/>	Lesen von VirusInfectedFiles (Files)	
<input type="checkbox"/>	Lesen von freigabe (Files)	
<input type="checkbox"/>	Lesen von joomla (Files)	
<input type="checkbox"/>	Lesen von ntopng (Files)	

**Zugehörigkeit**

**Benutzer**

- collax ()
- Ivan (Johan Kutepov)
- kayse (Stefan Kaysersberg)
- ssluser ()

**Netwerke**

- Internet (0.0.0.0/0)
- LocalNet (172.17.0.0/24)
- PPTP-Netz (192.168.100.0/24)
- WANNetz (192.168.200.0/24)

## Routing

Um das lokale Netzwerk erreichen zu können, muss das Routing über die Firewallmatrix konfiguriert werden.

Dieser Dialog befindet sich unter „System → Netzwerk → Firewall → Matrix“

Die Firewallmatrix ist eine visuelle Darstellung der integrierten Firewall. Hier wird festgelegt, welche Netzwerkverbindungen erlaubt bzw. geblockt sind. Es empfiehlt sich, den Verbindungsaufbau in beide Richtungen zu erlauben.

Menü > System > Netzwerk > Firewallmatrix > Regel bearbeiten

### Regel bearbeiten

Dienst any

Von Netzwerk PPTP-Netz (192.168.100.0/24)

Nach Netzwerk LocalNet (172.17.0.0/24)

Protokollieren

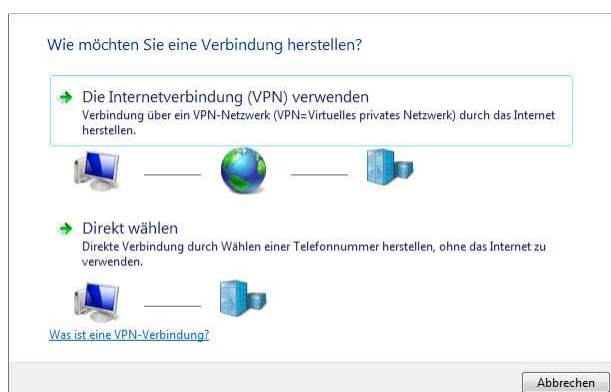
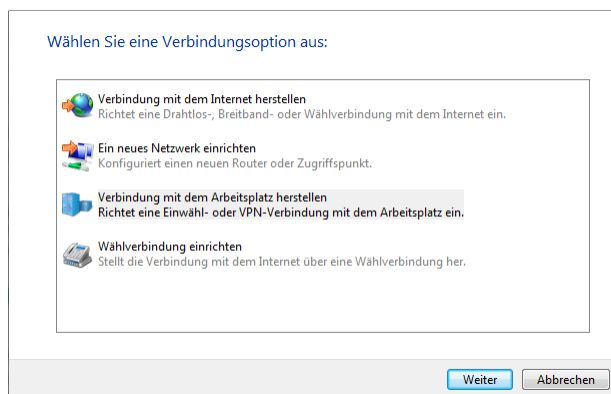
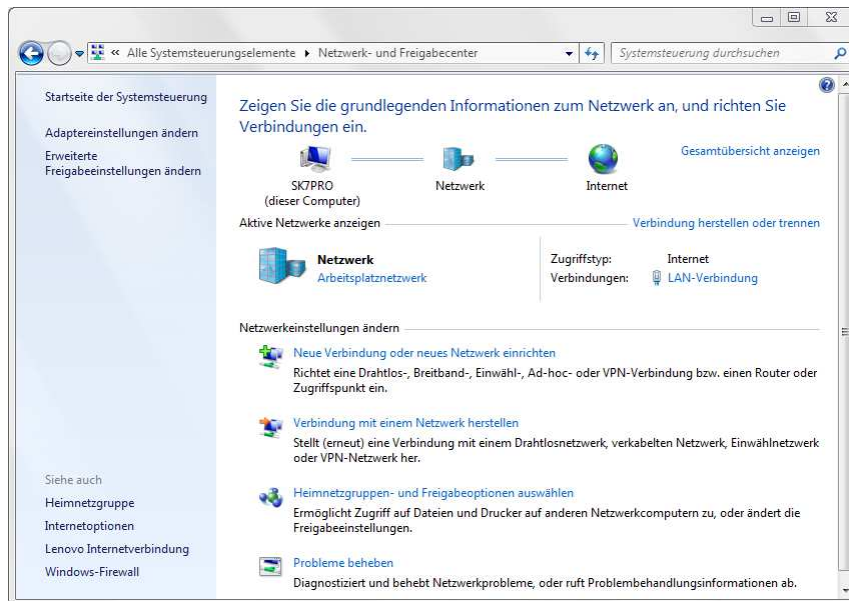
Regel Erlauben

Traffic-Policy

## Konfiguration Windows Client

### Verbindung anlegen

Unter Windows steht Ihnen ein Assistent zur Konfiguration der PPTP-Verbindung zur Verfügung. Sie finden den Assistenten in der Systemsteuerung im Netzwerk- und Freigabecenter. Wählen Sie hier den Punkt "Neue Verbindung einrichten" aus und stellen Sie darüber eine VPN-Verbindung her.



Hier geben wir die IP Adresse oder den Hostnamen ein, über den der Collax Server im Internet erreichbar ist.

Geben Sie die Internetadresse zum Herstellen einer Verbindung ein.

Diese Adresse können Sie vom Netzwerkadministrator erhalten.

Internetadresse:

Zielname:

Eine Smartcard verwenden

Anderen Benutzern erlauben, diese Verbindung zu verwenden  
Erlaubt jedem, der Zugang zu diesem Computer hat, diese Verbindung zu verwenden.

Jetzt nicht verbinden, nur für spätere Verwendung einrichten

Geben Sie hier „Benutzername“ und „Kennwort“ des Benutzers ein, der auf dem Collax Server Mitglied der PPTP Berechtigungsgruppe ist.

Geben Sie den Benutzernamen und das Kennwort ein.

Benutzername:

Kennwort:

Zeichen anzeigen

Dieses Kennwort speichern

Domäne (optional):

Bestätigen Sie den Punkt *“Verbinden”* um die Verbindung zum Collax Server aufzubauen.

### Hinweis

Sobald die Verbindung aufgebaut wurde, ist keine Verbindung mehr ins Internet möglich, da die Daten über die PPTP-Verbindung geschickt werden. Dieses Verhalten ist Standard. Um weiterhin Zugriff auf das Internet zu erhalten, entfernen Sie das Häkchen bei *„Standardgateway für das Remotenetzwerk verwenden“*. Sie finden die Einstellung unter den Eigenschaften der PPTP-Verbindung im Bereich *„Netzwerk → Internetprotokoll Version 4 (TCP/IPv4) → Erweitert → IP-Einstellungen“*

IP-Einstellungen DNS WINS

Dieses Kontrollkästchen trifft nur zu, wenn Sie gleichzeitig mit einem lokalen und einem Einwahlnetzwerk verbunden sind. Wenn das Kästchen aktiviert ist, werden Daten, die nicht an das lokale Netzwerk gesendet werden können, an das Einwahlnetzwerk weitergeleitet.

Standardgateway für das Remotenetzwerk verwenden

Klassenbasiertes Hinzufügen der Route deaktivieren

Automatische Metrik

Schrittstellermetrik:

Sie können alternativ auch über den Collax Server ins Internet gelangen. Konfigurieren Sie dazu das Routing vom PPTP-Netz ins Internet entsprechend über die Firewallmatrix oder verwenden Sie den Proxy Dienst.