

# Konfigurieren der L2TP-Servereinstellungen (Layer 2 Transport Protocol) auf einem Router der Serie RV34x

## Ziel

Layer 2 Tunneling Protocol (L2TP) stellt ein Virtual Private Network (VPN) her, über das Remote-Hosts über einen sicheren Tunnel miteinander verbunden werden können. Sie stellt keine Verschlüsselung oder Vertraulichkeit allein bereit, sondern stützt sich auf ein Verschlüsselungsprotokoll, das im Tunnel weitergeleitet wird, um Datenschutz zu gewährleisten.

Einer der größten Vorteile von L2TP besteht darin, dass es den Authentifizierungsprozess verschlüsselt, wodurch es für jemanden erschwert wird, auf Ihre Übertragung "zuhören", um die Daten abzufangen und zu knacken. L2TP bietet nicht nur Vertraulichkeit, sondern auch Datenintegrität. Datenintegrität ist ein Schutz gegen die Änderung des Datums zwischen dem Verlassen des Absenders und dem Erreichen des Empfängers.

In diesem Dokument wird erläutert, wie Sie die L2TP-Servereinstellungen auf dem Router der Serie RV34x konfigurieren.

## Anwendbare Geräte

- Serie RV34x

## Softwareversion

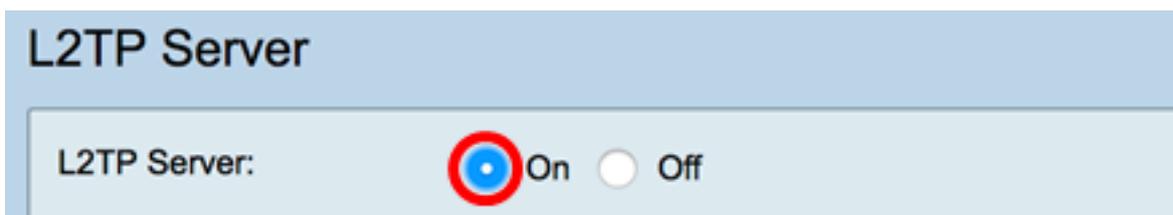
- 1,0/01,16

## Konfigurieren von L2TP

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **VPN > L2TP Server** aus.



Schritt 2: Klicken Sie auf das Optionsfeld **On** L2TP Server, um den L2TP-Server zu aktivieren.



Schritt 3: Geben Sie im *MTU*-Feld eine Zahl zwischen 128 und 1400 ein. Die Maximum Transmission Unit (MTU) definiert die größte Paketgröße, die eine Schnittstelle ohne Fragmentierung übertragen kann. Der Standardwert ist 1400.

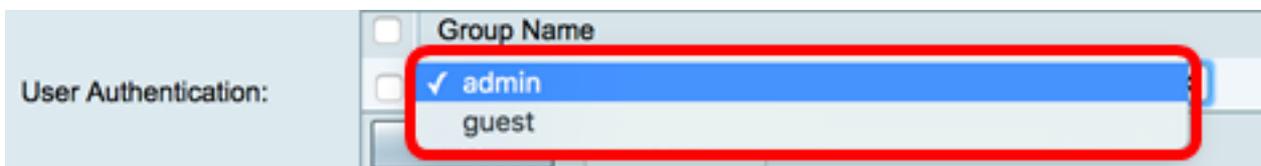
**Hinweis:** In diesem Beispiel wird 1399 verwendet.



Schritt 4: Klicken Sie im Bereich User Authentication (Benutzerauthentifizierung) auf Add (Hinzufügen), um einen zusätzlichen Satz auszuwählen, in dem ein Gruppenprofil ausgewählt wird, in dem die Benutzer authentifiziert werden sollen. Die Optionen hängen davon ab, ob zuvor ein Gruppenprofil konfiguriert wurde. Die Standardoptionen sind:

- admin - Spezielle Privilegien für Lese-/Schreibvorgänge über Einstellungen
- guest — schreibgeschützte Berechtigungen

**Hinweis:** In diesem Beispiel wird admin ausgewählt.



Schritt 5: Geben Sie im Feld *Start IP Address* (IP-Startadresse) die Start-IP-Adresse des IP-Adressbereichs ein, der den Benutzern zugewiesen werden soll. Hierbei handelt es sich um reservierte IP-Adressen für L2TP-Benutzer. Es werden maximal 25 Sitzungen unterstützt.

**Hinweis:** In diesem Beispiel wird 10.0.1.224 verwendet.

Address Pool:

Start IP Address:

Schritt 6: Geben Sie im Feld *End IP Address* (EndIP-Adresse) die End-IP-Adresse des IP-Adressbereichs ein.

**Hinweis:** In diesem Beispiel wird 10.0.1.254 verwendet.

End IP Address:

Schritt 7: Geben Sie im Feld *DNS1 IP Address* (DNS1-IP-Adresse) die IP-Adresse des DNS-Servers ein.

**Hinweis:** In diesem Beispiel wird 192.168.1.1 verwendet.

DNS1 IP Address:

Schritt 8: (Optional) Geben Sie im Feld *DNS2 IP Address* (DNS-IP-Adresse) die IP-Adresse des zweiten DNS-Servers ein. Der Standardwert ist leer.

DNS2 IP Address:

Schritt 9: (Optional) Klicken Sie auf das Optionsfeld **On** IPsec, um die IPsec-Funktion für L2TP zu aktivieren. Internet Protocol Security (IPsec) bietet Sicherheit für die Übertragung vertraulicher Informationen über ungeschützte Netzwerke.

**Hinweis:** Wenn Sie "Aus" gewählt haben, fahren Sie mit [Schritt 13 fort](#).

IPsec:  On  Off

Schritt 10: Wählen Sie im Dropdown-Menü "IPsec Profile" ein Profil aus. Folgende Optionen stehen zur Verfügung:

- Amazon\_Web\_Services - Ein Cloud-Service von Amazon, bereitgestellt von Amazon.
- Standard - Standardprofil
- Microsoft\_Azure - Ein Cloud-Service von Microsoft.

**Hinweis:** In diesem Beispiel wird Microsoft\_Azure ausgewählt.



IPSec: Amazon\_Web\_Services  
Default  
IPSec Profile: ✓ Microsoft\_Azure

Schritt 11: Geben Sie im Feld *Pre-Shared Key* (Vorinstallierter Schlüssel) einen Schlüssel für die Authentifizierung an einem Remote-Internet Key Exchange (IKE)-Peer ein. Sie können bis zu 30 Hexadezimalzeichen eingeben.

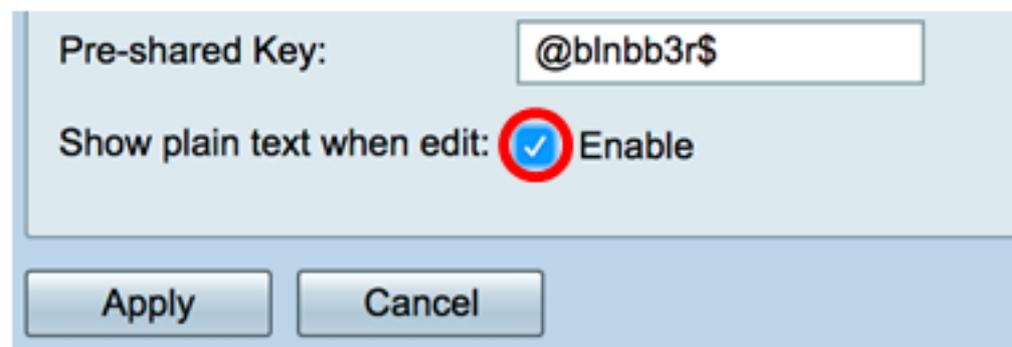
**Hinweis:** An beiden Enden des VPN-Tunnels muss derselbe vorinstallierte Schlüssel verwendet werden. Es wird empfohlen, den Schlüssel regelmäßig zu aktualisieren, um die VPN-Sicherheit zu maximieren.



Pre-shared Key: .....

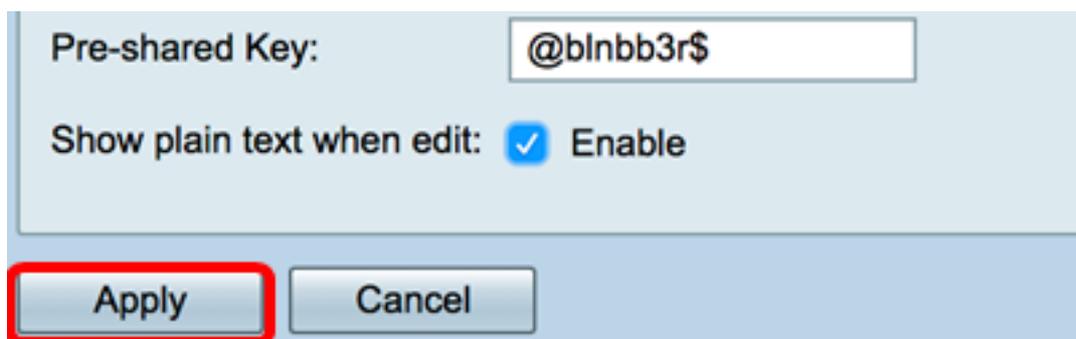
Schritt 12: (Optional) Aktivieren Sie das Kontrollkästchen *Nur bei der Bearbeitung anzeigen*, um den Pre-Shared Key im Klartext anzuzeigen.

**Hinweis:** In diesem Beispiel wird bei aktivierter Option *Nur Text anzeigen* angezeigt.



Pre-shared Key: @blnbb3r\$  
Show plain text when edit:  Enable  
Apply Cancel

[Schritt 13:](#) Klicken Sie auf **Apply**, um die Einstellungen zu speichern.



Pre-shared Key: @blnbb3r\$  
Show plain text when edit:  Enable  
Apply Cancel

Schritt 14: (Optional) Um die Konfiguration in der Startkonfigurationsdatei zu speichern, gehen Sie zur Seite **Copy/Save** Configuration (Konfiguration **kopieren/speichern**), oder klicken Sie auf das  **Save** Symbol oben auf der Seite.

## L2TP Server



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

L2TP Server:	<input checked="" type="radio"/> On <input type="radio"/> Off						
MTU:	<input type="text" value="1399"/> bytes (Range: 128-1400, Default: 1400)						
User Authentication:	<table border="1"><tr><td><input type="checkbox"/></td><td>Group Name</td></tr><tr><td><input type="checkbox"/></td><td>admin</td></tr><tr><td><input type="button" value="Add"/></td><td><input type="button" value="Delete"/></td></tr></table>	<input type="checkbox"/>	Group Name	<input type="checkbox"/>	admin	<input type="button" value="Add"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	Group Name						
<input type="checkbox"/>	admin						
<input type="button" value="Add"/>	<input type="button" value="Delete"/>						
Address Pool:							
Start IP Address:	<input type="text" value="10.0.1.224"/>						
End IP Address:	<input type="text" value="10.0.1.254"/>						
DNS1 IP Address:	<input type="text" value="192.168.1.1"/>						
DNS2 IP Address:	<input type="text"/>						
IPSec:	<input checked="" type="radio"/> On <input type="radio"/> Off						
IPSec Profile:	<input type="text" value="Default"/>						
Pre-shared Key:	<input type="text" value="*****"/>						
Show plain text when edit:	<input type="checkbox"/> Enable						

Sie sollten jetzt die L2TP-Servereinstellungen auf dem Router der Serie RV34x erfolgreich konfiguriert haben.