

# Konfiguration des Easy Client to Gateway Virtual Private Network (VPN) auf den VPN-Routern der Serien RV320 und RV325

## Ziel

Ein Virtual Private Network (VPN) bietet Sicherheit für Remote-Benutzer, die über ein öffentliches oder nicht vertrauenswürdiges Netzwerk eine Verbindung zum Internet herstellen. Eine der Arten von VPNs ist ein Client-to-Gateway-VPN. Mit dem Client-to-Gateway können Sie verschiedene Zweigstellen Ihres Unternehmens in verschiedenen geografischen Regionen per Fernzugriff verbinden, um die Daten sicherer zwischen den Gebieten zu übertragen und zu empfangen. Easy VPN ermöglicht die schnelle Einrichtung und Konfiguration von VPNs über das Cisco VPN Client-Dienstprogramm.

In diesem Dokument wird erläutert, wie Sie ein Easy Client-to-Gateway-VPN auf der RV32x VPN-Router-Serie konfigurieren.

## Anwendbare Geräte | Firmware-Version

- RV320 Dual-WAN VPN-Router | 1.1.0.09 ([aktueller Download](#))
- RV325 Dual-WAN-VPN-Router mit Gigabit | 1.1.0.09 ([aktueller Download](#))

## Konfigurieren des Easy Client-to-Gateway-VPN

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > Client to Gateway aus**. Die Seite *Client to Gateway* wird geöffnet:

## Client to Gateway

### Add a New Tunnel

Tunnel     Group VPN     Easy VPN

Tunnel No. 1  
Tunnel Name:   
Interface: WAN1   
Keying Mode: IKE with Preshared key   
Enable:

### Local Group Setup

Local Security Gateway Type: IP Only   
IP Address: 0.0.0.0  
Local Security Group Type: Subnet   
IP Address: 192.168.1.0  
Subnet Mask: 255.255.255.0

### Remote Client Setup

Remote Security Gateway Type: IP Only   
IP Address :

Schritt 2: Klicken Sie auf das Optionsfeld **Easy VPN**.

### Client to Gateway

**Add a New Easy VPN**


Tunnel     Group VPN     Easy VPN

Group No.    1

Name:   

Minimum Password Complexity:  Enable

Password:   

Password Strength Meter:    

Interface:   

Enable:   

Tunnel Mode:   

IP Address:   

Subnet Mask:   

Extended Authentication:   


**Hinweis:** Die *Gruppennummer* stellt die Nummer der Gruppe dar. Es ist ein automatisch generiertes Feld.

Schritt 3: Geben Sie im Feld *Name* den Namen des Tunnels ein.

**Client to Gateway**

**Add a New Easy VPN**

Tunnel
  Group VPN
  Easy VPN

Group No. 1  
 Name: group\_1  
 Minimum Password Complexity:  Enable  
 Password: password\_1  
 Password Strength Meter: 

Interface: WAN1  
 Enable:   
 Tunnel Mode: Full Tunnel  
 IP Address: 192.168.1.0  
 Subnet Mask: 255.255.255.0  
 Extended Authentication: Default - Local Database

Schritt 4: (Optional) Wenn Sie die Kraftanzeige für den vorinstallierten Schlüssel aktivieren möchten, aktivieren Sie das Kontrollkästchen **Minimale Kennwortkomplexität**.

Schritt 5: Geben Sie im Feld *Kennwort* ein Kennwort ein.

- Kennwort Strength Meter - Zeigt die Stärke des Kennworts durch farbige Balken an. Rot bedeutet schwache Stärke, Gelb bedeutet akzeptable Stärke und Grün bedeutet starke Stärke. Wenn Sie das Kontrollkästchen **Minimale Kennwortkomplexität** in Schritt 4 nicht aktiviert haben, wird die Kennwortstärkeregelung nicht angezeigt.

Schritt 6: Wählen Sie aus der Dropdown-Liste "*Schnittstelle*" die entsprechende Schnittstelle aus, über die der Client Easy VPN zum Gateway herstellt.

### Client to Gateway

**Add a New Easy VPN**


Tunnel     Group VPN     Easy VPN

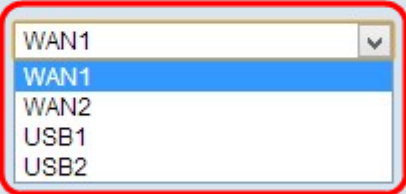
Group No.    1

Name:   

Minimum Password Complexity:  Enable

Password:   

Password Strength Meter:    

Interface:     

Enable:   

Tunnel Mode:

IP Address:   

Subnet Mask:   

Extended Authentication:   

Schritt 7: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um das VPN zwischen Client und Gateway zu aktivieren. Standardmäßig ist sie aktiviert.

### Client to Gateway

**Add a New Easy VPN**


Tunnel     Group VPN     Easy VPN

Group No.    1

Name:   

Minimum Password Complexity:  Enable

Password:   

Password Strength Meter:    

Interface:   

**Enable:**   

Tunnel Mode:   

IP Address:   

Subnet Mask:   

Extended Authentication:   

Schritt 8: Wählen Sie in der Dropdown-Liste *Tunnelmodus* den entsprechenden Tunneling-Modus aus.

### Client to Gateway

**Add a New Easy VPN**


Tunnel     Group VPN     Easy VPN

Group No.    1

Name:   

Minimum Password Complexity:  Enable

Password:   

Password Strength Meter:    

Interface:   

Enable:   

Tunnel Mode:   

IP Address:   

Subnet Mask:   

Extended Authentication:

Die verfügbaren Optionen sind wie folgt definiert:

- Full Tunnel - Sendet den gesamten Datenverkehr über den VPN-Tunnel, wodurch mehr Sicherheit für den Datenverkehr gewährleistet wird. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 11 fort](#).
- Split Tunnel (Tunnel teilen): Ermöglicht dem VPN-Client, gleichzeitig auf das öffentliche Internet und die VPN-Ressourcen zuzugreifen, wodurch Bandbreite eingespart wird.

Schritt 9: Geben Sie im Feld *IP-Adresse* die IP-Adresse ein, die Sie der Schnittstelle des Easy VPN zuweisen möchten.

The screenshot shows the 'Client to Gateway' configuration window. The title is 'Client to Gateway'. Below the title is a section 'Add a New Easy VPN'. There are three radio buttons: 'Tunnel', 'Group VPN', and 'Easy VPN'. The 'Easy VPN' radio button is selected. Below the radio buttons are several fields: 'Group No.' with the value '1', 'Name' with the value 'group\_1', 'Minimum Password Complexity' with a checked checkbox and the label 'Enable', 'Password' with the value 'password\_1', 'Password Strength Meter' with a progress bar showing 2 yellow bars and 4 red bars, 'Interface' with a dropdown menu showing 'WAN2', 'Enable' with a checked checkbox, 'Tunnel Mode' with a dropdown menu showing 'Split Tunnel', 'IP Address' with the value '192.168.2.0', 'Subnet Mask' with the value '255.255.255.0', and 'Extended Authentication' with a dropdown menu showing 'Default - Local Database'. There is an 'Add/Edit' button next to the 'Extended Authentication' dropdown. At the bottom of the window are 'Save' and 'Cancel' buttons.

Schritt 10: Geben Sie im Feld *Subnetzmaske* die Subnetzmaske der zugewiesenen IP-Adresse der Easy VPN-Schnittstelle ein.

Schritt 11: Wählen Sie aus der Dropdown-Liste *Extended Authentication (Erweiterte Authentifizierung)* die entsprechende Authentifizierung für den VPN-Client aus, um einen IPSec-Hostbenutzernamen und ein Kennwort für die Authentifizierung von VPN-Clients zu verwenden oder die in User Management (Benutzerverwaltung) gefundene Datenbank zu verwenden. Diese Funktion muss auf beiden Geräten aktiviert sein, damit sie funktioniert.

### Client to Gateway

**Add a New Easy VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No.

Name:

Minimum Password Complexity:  Enable

Password:

Password Strength Meter:

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Die verfügbaren Optionen sind wie folgt definiert:

- 1 - Active Directory - Die Authentifizierung wird durch Active Directory erweitert. Active Directory ist ein Dienst, der die Netzwerksicherheit in einem Windows-Domänennetzwerk bereitstellt. Klicken Sie auf **Hinzufügen/Bearbeiten**, wenn Sie ein neues Verzeichnis hinzufügen oder das vorhandene Verzeichnis bearbeiten möchten.
- Standard - Lokale Datenbank - Die Authentifizierung wird vom Router durchgeführt. Klicken Sie auf **Hinzufügen/Bearbeiten**, wenn Sie die Datenbank hinzufügen oder bearbeiten möchten.

**Hinweis:** Weitere Informationen zum Hinzufügen oder Bearbeiten des aktiven Verzeichnisses oder der lokalen Datenbank finden Sie im Dokument mit dem Titel [User and Domain Management Configuration on RV320 and RV325 VPN Router Series](#).

Schritt 12: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.