

Konfigurieren eines VPN-Clients für Telearbeiter auf dem Router der Serie RV34x

Ziel

Die Telearbeiter-VPN-Client-Funktion minimiert die Konfigurationsanforderungen an entfernten Standorten, da das Gerät als Cisco VPN-Hardware-Client fungieren kann. Wenn der Telearbeiter-VPN-Client die VPN-Verbindung startet, überträgt der IPSec-VPN-Server die IPSec-Richtlinien an den Telearbeiter-VPN-Client und erstellt den entsprechenden Tunnel.

In diesem Artikel wird erläutert, wie Sie den Telearbeiter-VPN-Client auf dem Router der Serie RV34x konfigurieren.

Unterstützte Geräte

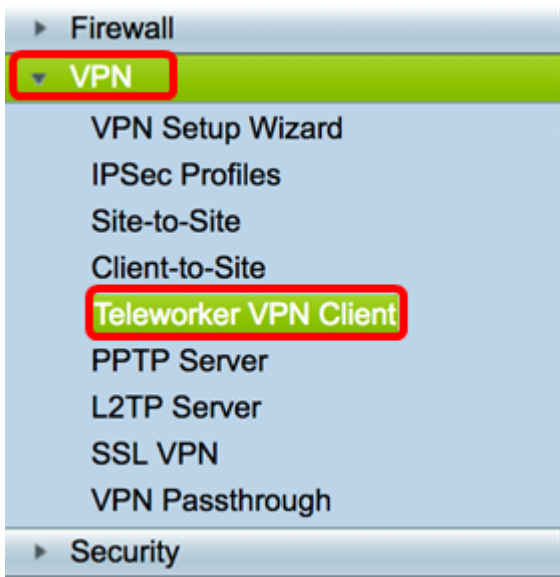
- Router der Serie RV34x

Software-Version

- 1.0.01.17

Konfigurieren des Telearbeiter-VPN-Clients

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie VPN > Telearbeiter-VPN-Client.



Schritt 2: Klicken Sie im Bereich Telearbeiter-VPN-Client auf das Optionsfeld Ein, um den Telearbeit-VPN-Client zu aktivieren.

Anmerkung: Nur ein einzelner Telearbeiter-VPN-Client kann beim Start eine aktive Verbindung aufweisen.

Teleworker VPN Client

Teleworker VPN Client: ☒ On ☐ Off

Auto Initiation Retry: ☐ On ☒ Off

Retry Interval: seconds (Range: 120-1800)

Retry Limit: times (Range: 0-16)

Schritt 3: (Optional) Klicken Sie im Bereich "Auto Initiation Retry" (Automatisch initiieren, Wiederholen) auf ein Optionsfeld On (Ein) oder Off (Aus), um einen automatischen Initiierungsversuch nach einem Fehler zu aktivieren oder zu deaktivieren. Klicken Sie auf Ein, um den Router nach einem Fehler zu initiieren.

Anmerkung: In diesem Beispiel wird On ausgewählt.

Teleworker VPN Client

Teleworker VPN Client: ☒ On ☐ Off

Auto Initiation Retry: ☒ On ☐ Off

Retry Interval: seconds (Range: 120-1800)

Retry Limit: times (Range: 0-16)

Schritt 4: Geben Sie im Feld Retry Interval (Wiederholungsintervall) einen Wert in Sekunden ein, mit dem der Router versucht, eine Verbindung herzustellen. Der Standardwert ist 120 Sekunden.

Anmerkung: In diesem Beispiel wird der Standardwert verwendet.

Teleworker VPN Client

Teleworker VPN Client: ☒ On ☐ Off

Auto Initiation Retry: ☒ On ☐ Off

Retry Interval: seconds (Range: 120-1800)

Retry Limit: times (Range: 0-16)

Schritt 5: Geben Sie im Feld Retry Limit (Wiederholungslimit) an, wie oft der Router nach einem Fehler automatisch versucht, eine Initiierung durchzuführen.

Anmerkung: In diesem Beispiel ist die eingegebene Zahl 2.

Teleworker VPN Client

Teleworker VPN Client: ☒ On ☐ Off

Auto Initiation Retry: ☒ On ☐ Off

Retry Interval: seconds (Range: 120-1800)

Retry Limit: times (Range: 0-16)

Konfigurieren der Grundeinstellungen

Schritt 6: Klicken Sie in der Tabelle Telearbeiter-VPN-Clients auf Hinzufügen, um einen Telearbeiter-VPN-Client zu erstellen und zu konfigurieren.

Teleworker VPN Clients

☐	Name	Host (Remote ...	Activat
--------------------------	------	------------------	---------

Schritt 7: Geben Sie im Bereich "Basic Settings" (Grundeinstellungen) einen Namen für den VPN-

Tunnel in das Feld "Name" ein.

Anmerkung: In diesem Beispiel wird Dracarys verwendet.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Schritt. 8. Geben Sie im Feld Server (Remote-Adresse) die IP-Adresse des Remote-Servers ein.

Anmerkung: In diesem Beispiel wird 128.13.22.12 verwendet.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Schritt 9: Um eine Verbindung beim Start zu initiieren, klicken Sie im Bereich "Active Connection on Startup" (Aktive Verbindung beim Start) auf On. Um eine Verbindung manuell zu starten, klicken Sie auf Aus.

Anmerkung: In diesem Beispiel wird On ausgewählt.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:	Dracarys
Server (Remote Address):	128.12.22.12
Active Connection on Startup:	☒ On ☐ Off
IKE Authentication Method:	☒ Pre-shared Key
Group Name:	
Password	
☐ Certificate	Default ▾
Mode:	☒ Client ☐ NEM
VLAN:	1
User Name	
User Password	
Confirm User Password	

Schritt 10: Wählen Sie im Bereich "IKE Authentication Method" eine Authentifizierungsmethode aus, die in IKE-Verhandlungen im IKE-basierten Tunnel verwendet werden soll. Folgende Optionen sind verfügbar:

- Pre-Shared Key - IKE-Peers authentifizieren sich gegenseitig, indem sie einen verschlüsselten Hash von Daten berechnen und senden, der den Pre-Shared Key enthält. Wenn der empfangende Peer in der Lage ist, den gleichen Hash unabhängig unter Verwendung des vorinstallierten Schlüssels zu erstellen, weiß er, dass beide Peers denselben geheimen Schlüssel gemeinsam nutzen müssen, um den anderen Peer zu authentifizieren. Pre-Shared Keys lassen sich nicht gut skalieren, da jeder IPSec-Peer mit dem Pre-Shared Key jedes anderen Peers konfiguriert werden muss, mit dem er eine Sitzung herstellt. Wenn Sie diese Option auswählen, fahren Sie mit dem nächsten Schritt fort.
- Zertifikat - Das digitale Zertifikat ist ein Paket, das Informationen wie die Zertifikatsidentität des Trägers enthält: Name oder IP-Adresse, das Ablaufdatum der Seriennummer des Zertifikats und eine Kopie des öffentlichen Schlüssels des Zertifikatsinhabers. Das Standard-Format für digitale Zertifikate ist in der X.509-Spezifikation definiert. X.509 Version 3 definiert die Datenstruktur für Zertifikate. Fahren Sie bei Auswahl dieser Option mit [Schritt 13 fort](#).

Anmerkung: In diesem Beispiel wird Pre-shared Key (Vorinstallierter Schlüssel) ausgewählt.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☒ On ☐ Off

IKE Authentication Method: ☒ Pre-shared Key

Group Name:

Password

☐ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name

User Password

Confirm User Password

Schritt 11: Wenn Sie in Schritt 10 den vorinstallierten Schlüssel ausgewählt haben, geben Sie im Feld Gruppenname einen Gruppennamen ein.

Anmerkung: In diesem Beispiel wird FreeFolk als Gruppenname verwendet.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☒ On ☐ Off

IKE Authentication Method: ☒ Pre-shared Key

Group Name:

Password:

☐ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Schritt 12: Geben Sie im Feld Kennwort ein Kennwort ein, das der Gruppe zugeordnet werden soll.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:	Dracarys
Server (Remote Address):	128.12.22.12
Active Connection on Startup:	☒ On ☐ Off
IKE Authentication Method:	☒ Pre-shared Key
	Group Name: FreeFolk
	Password: *****
	☐ Certificate Default
Mode:	☒ Client ☐ NEM
VLAN:	1
User Name	
User Password	
Confirm User Password	

Schritt 13. Wenn Sie in Schritt 10 "Zertifikat" ausgewählt haben, wählen Sie das entsprechende Zertifikat für Ihren Router aus.

Anmerkung: In diesem Beispiel wird "Default" (Standard) ausgewählt.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate ☒ Client ☐ NEM

Mode: ☒ Certificate ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Options:

- ☒ Default
- ☐ FindIT

Schritt 14: Klicken Sie auf ein Optionsfeld, um einen Modus auszuwählen. Folgende Optionen sind verfügbar:

- Client - Diese Option ermöglicht dem Client, eine IP-Adresse anzufordern, und der Server stellt die IP-Adressen aus dem konfigurierten Adressbereich bereit. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 16 fort](#).
- Network Extension Mode (NEM) - Mit dieser Option können Clients ihr Subnetz vorschlagen, für das VPN-Services auf Datenverkehr zwischen LAN hinter dem Server und dem vom Client vorgeschlagenen Subnetz angewendet werden müssen. Sie werden außerdem aufgefordert, ein VLAN auszuwählen. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 15 fort](#).

Anmerkung: In diesem Beispiel wird Client ausgewählt.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Schritt 15: Wenn in Schritt 14 NEM ausgewählt wurde, wählen Sie ein VLAN aus der Dropdown-Liste aus. Die Optionen können je nach den vorkonfigurierten VLAN-Einstellungen variieren.

Anmerkung: In diesem Beispiel wird 25 ausgewählt.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate

Mode: ☐ Client ☒ NEM

VLAN:

1

✓ 25

30

User Name:

User Password:

Confirm User Password:

Schritt 16: Geben Sie im Feld User Name (Benutzername) einen Benutzernamen ein, der dem Telework VPN Client zugeordnet werden soll.

Anmerkung: In diesem Beispiel wird Tormound verwendet.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:	Dracarys
Server (Remote Address):	128.12.22.12
Active Connection on Startup:	☐ On ☒ Off
IKE Authentication Method:	☐ Pre-shared Key
Group Name:	FreeFolk
Password	
	☒ Certificate Default ▾
Mode:	☒ Client ☐ NEM
VLAN:	1
User Name	Tormound
User Password	
Confirm User Password	

Schritt 17: Geben Sie im Feld Benutzerkennwort ein Kennwort für den Benutzernamen ein.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:	Dracarys
Server (Remote Address):	128.12.22.12
Active Connection on Startup:	☐ On ☒ Off
IKE Authentication Method:	☐ Pre-shared Key
Group Name:	FreeFolk
Password	
	☒ Certificate Default ▾
Mode:	☒ Client ☐ NEM
VLAN:	1
User Name	Tormound
User Password	
Confirm User Password	

Schritt 18: Geben Sie im Feld Benutzerkennwort bestätigen das Kennwort erneut ein, um es zu bestätigen. Wenn Sie ein falsches Kennwort eingeben, wird das Feld rot.

Teleworker VPN Client - Add/Edit

Basic Settings

Name:

Server (Remote Address):

Active Connection on Startup: ☐ On ☒ Off

IKE Authentication Method: ☐ Pre-shared Key

Group Name:

Password:

☒ Certificate

Mode: ☒ Client ☐ NEM

VLAN:

User Name:

User Password:

Confirm User Password:

Schritt 19: Klicken Sie auf Apply, um die Einstellungen zu speichern.

Teleworker VPN Client - Add/Edit

Basic Settings
Name:
Server (Remote Address):
Active Connection on Startup: ☐ On ☒ Off
IKE Authentication Method: ☐ Pre-shared Key
Group Name:
Password:
☒ Certificate
Mode: ☐ Client ☒ NEM
VLAN:
User Name:
User Password:
Confirm User Password:

Advanced Settings
Backup Server 1: (IP Address or Domain Name)
Backup Server 2: (IP Address or Domain Name)
Backup Server 3: (IP Address or Domain Name)
Peer Timeout: seconds (30-480)

Schritt 20. Ein Popup-Fenster wird angezeigt, in dem Sie aufgefordert werden, die Verbindung zu aktivieren, während die Einstellungen gespeichert werden. Klicken Sie auf die Schaltfläche Verbindung aktivieren, um die Aktivierung zu bestätigen, und auf die Schaltfläche Nicht aktivieren, um die Verbindung zu einem späteren Zeitpunkt zu aktivieren.

Anmerkung: In diesem Beispiel wird Verbindung aktivieren ausgewählt.

 Do you want to make this connection active when the settings are saved?
(Only one connection can be active at a time.)

Sie gelangen zurück zur Hauptseite des Telearbeiter-VPN-Clients.

Teleworker VPN Client

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

Teleworker VPN Client: ☒ On ☐ Off

Auto Initiation Retry: ☒ On ☐ Off

Retry Interval: seconds (Range: 120-1800)

Retry Limit: times (Range: 0-16)

Teleworker VPN Clients									
☐	Name	Host (Re...	Activate Connection on Startup	Authenica...	Group Na...	User Name	Backup Se...	Peer Timeout	Mode
☐	Dracarys	128.12.22...	☒	Certificate		Tormound		120	Client

Sie sollten nun die Grundeinstellungen für den Telearbeiter-VPN-Client auf dem Router der Serie RV34x erfolgreich konfiguriert haben.

Konfigurieren der erweiterten Einstellungen

Schritt 1: (Optional) Geben Sie im Feld Backup Server 1 die IP-Adresse oder den Domännennamen des Backup-Servers ein. Hier kann das Gerät die VPN-Verbindung starten, falls der primäre IPSec-VPN-Server ausfällt. Sie können bis zu drei Backup-Server in die dafür vorgesehenen Felder eingeben. Der Sicherungsserver 1 hat die höchste Priorität unter den drei Servern, der Sicherungsserver 3 die niedrigste.

Anmerkung: In diesem Beispiel wird „brienneofarth.com“ verwendet.

Advanced Settings

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Peer Timeout: seconds (30-480)

Schritt 2: Geben Sie im Feld Peer-Timeout die Zeit in Sekunden ein, die ein Peer inaktiv bleiben kann, bevor die Verbindung getrennt wird. Der Bereich liegt zwischen 30 und 480 Sekunden. Der Standardwert ist 120.

Advanced Settings

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Peer Timeout: seconds (30-480)

Schritt 3: Klicken Sie auf Anwenden.

Advanced Settings

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Peer Timeout: seconds (30-480)

Sie sollten jetzt die erweiterten Einstellungen des Telearbeiter-VPN auf dem Router der Serie RV34x erfolgreich konfiguriert haben.

Klicken Sie auf die folgenden Links für Artikel zu folgenden Themen:

- [Konfigurieren der VPN-Verbindung \(Virtual Private Network\) zwischen Clients auf dem Router der Serie RV34x](#)
- [Produktseite: Links zu allen Artikeln auf Routern der RV34x-Serie](#)

Video zu diesem Artikel anzeigen ...

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.