Konfigurieren der VPN-Verbindung (Client-to-Site Virtual Private Network) auf dem Router der Serie RV34x

Ziel

In einer VPN-Verbindung (Client-to-Site Virtual Private Network) können sich Clients aus dem Internet mit dem Server verbinden, um auf das Unternehmensnetzwerk oder auf das LAN hinter dem Server zuzugreifen, ohne die Sicherheit des Netzwerks und seiner Ressourcen zu beeinträchtigen. Diese Funktion ist sehr nützlich, da sie einen neuen VPN-Tunnel erstellt, über den Telearbeiter und Geschäftsreisende mithilfe einer VPN-Client-Software auf Ihr Netzwerk zugreifen können, ohne den Datenschutz und die Sicherheit zu beeinträchtigen.

In diesem Dokument wird erläutert, wie Sie eine Client-to-Site-VPN-Verbindung auf dem Router der Serie RV34x konfigurieren.

Anwendbare Geräte

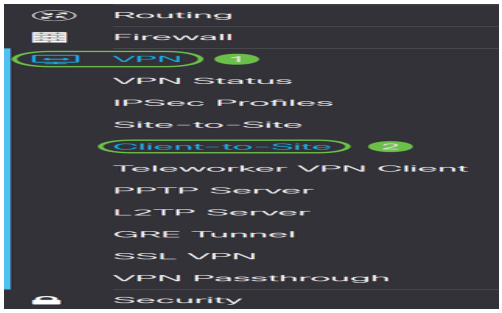
- Serie RV34x

Softwareversion

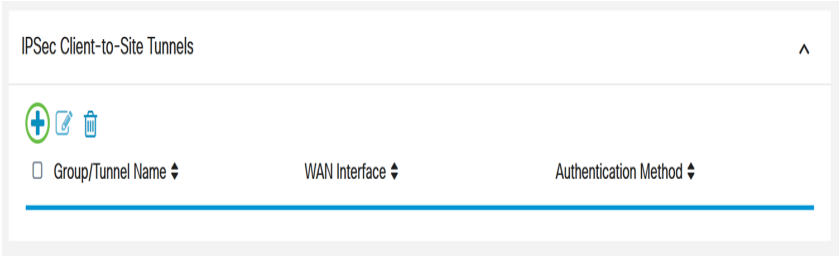
- 1,0/01,16

Konfigurieren von Client-to-Site-VPN

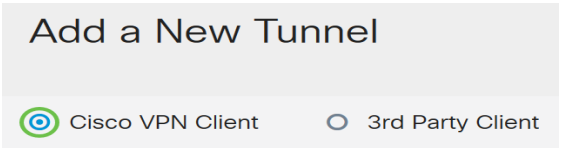
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **VPN > Client-to-Site aus**.



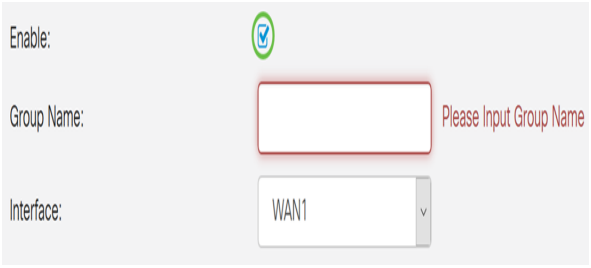
Schritt 2: Klicken Sie im Abschnitt "IPSec-Client-to-Site-Tunnel" auf die **Schaltfläche Hinzufügen**.



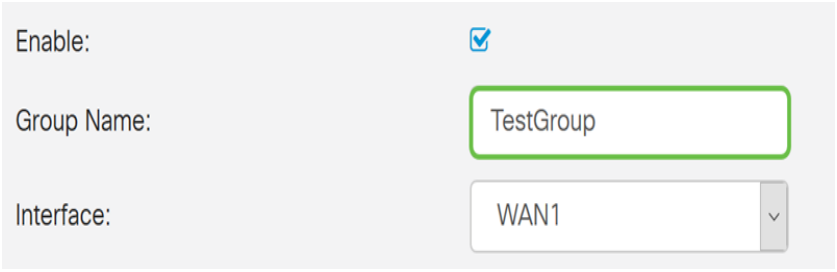
Schritt 3: Klicken Sie im Bereich *Neuen Tunnel hinzufügen* auf das Optionsfeld **Cisco VPN Client**.



Schritt 4: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Konfiguration zu aktivieren.



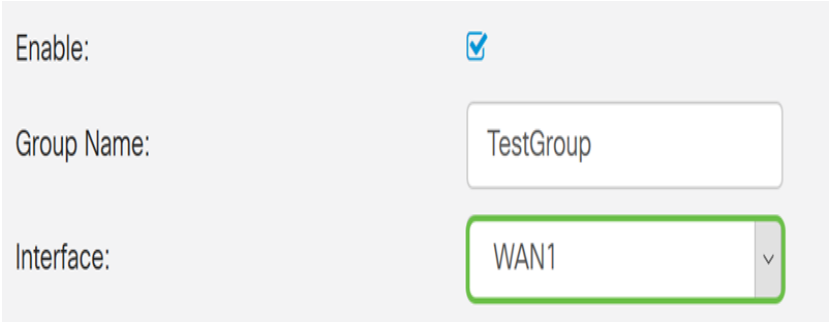
Schritt 5: Geben Sie im angezeigten Feld einen Gruppennamen ein. Dies dient als Kennung für alle Mitglieder dieser Gruppe während der Internet Key Exchange (IKE)-Verhandlungen.



Hinweis: Geben Sie Zeichen zwischen A bis Z oder 0 bis 9 ein. Leerzeichen und Sonderzeichen sind für den Gruppennamen nicht zulässig. In diesem Beispiel wird TestGroup verwendet.

Schritt 6: Klicken Sie auf die Dropdown-Liste, um die Schnittstelle auszuwählen. Folgende Optionen stehen zur Verfügung:

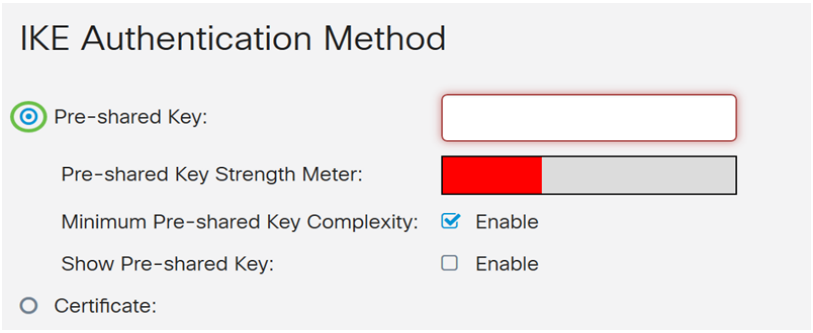
- WAN1
- WAN2
- USB1
- USB2



Hinweis: In diesem Beispiel wird WAN1 ausgewählt. Dies ist die Standardeinstellung.

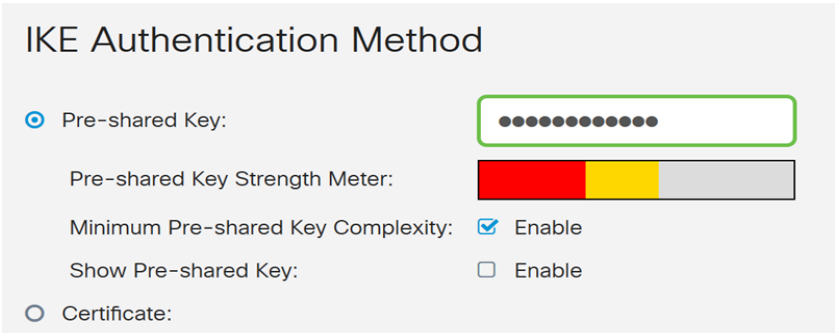
Schritt 7: Wählen Sie im Bereich IKE Authentication Method (IKE-Authentifizierungsmethode) eine Authentifizierungsmethode für IKE-Verhandlungen im IKE-basierten Tunnel aus. Folgende Optionen stehen zur Verfügung:

- Pre-shared Key - IKE-Peers authentifizieren sich gegenseitig durch Computing und Senden eines verschlüsselten Hashs von Daten, der den Pre-shared Key enthält. Wenn der empfangende Peer in der Lage ist, den gleichen Hash mit seinem Pre-shared Key unabhängig zu erstellen, weiß er, dass beide Peers denselben geheimen Schlüssel teilen und so den anderen Peer authentifizieren müssen. Vorinstallierte Schlüssel 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 aufbaut.
- Zertifikat - Das digitale Zertifikat ist ein Paket, das Informationen wie eine Zertifikatsidentität des Inhabers enthält: Name oder IP-Adresse, das Ablaufdatum der Seriennummer des Zertifikats und eine Kopie des öffentlichen Schlüssels des Zertifikatsinhabers. Das standardmäßige digitale Zertifikatsformat ist in der X.509-Spezifikation definiert. Die X.509-Version 3 definiert die Datenstruktur für Zertifikate.



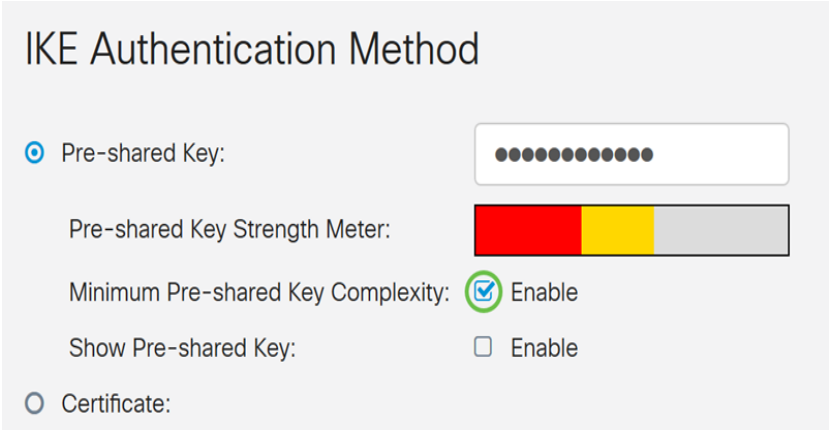
Hinweis: In diesem Beispiel wird der Pre-shared Key ausgewählt. Dies ist die Standardeinstellung.

Schritt 8: Geben Sie in das Feld einen vorinstallierten Schlüssel ein. Dies ist der Authentifizierungsschlüssel für Ihre Gruppe von IKE-Peers.

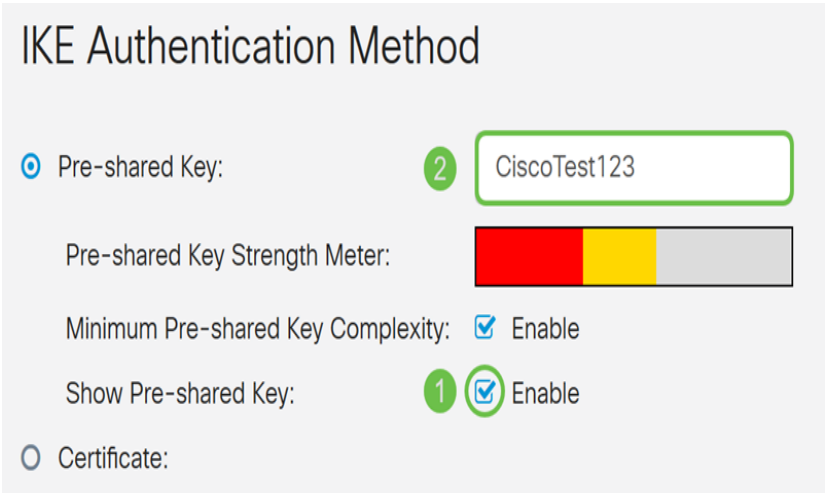


Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Mindestkomplexität des vorinstallierten Schlüssels anzuzeigen und die Stärke Ihres Schlüssels zu bestimmen. Die Stärke Ihres Schlüssels wird wie folgt definiert:

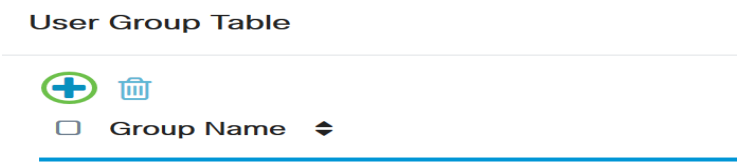
- Rot - Das Kennwort ist schwach.
- Orange - Das Passwort ist ziemlich stark.
- Grün - Das Kennwort ist stark.



Hinweis: Sie können das Kontrollkästchen **Aktivieren** im Feld *Vorinstallierten Schlüssel anzeigen* aktivieren, um Ihr Kennwort im Klartext zu überprüfen.

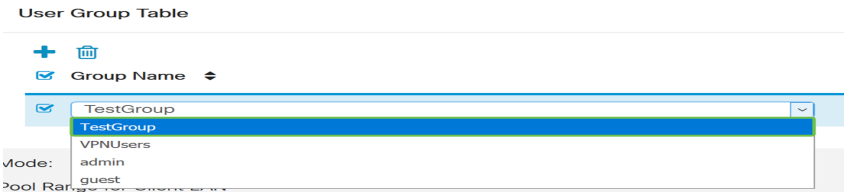


Schritt 10: (Optional) Klicken Sie in der Tabelle "Benutzergruppe" auf das **Pluszeichen**, um eine Gruppe hinzuzufügen.



Schritt 11: (Optional) Wählen Sie aus der Dropdown-Liste aus, ob die Benutzergruppe für Administratoren oder Gäste bestimmt ist. Wenn Sie Ihre eigene Benutzergruppe mit Benutzerkonten erstellt haben, können Sie diese auswählen. In diesem Beispiel wählen Sie TestGroup.

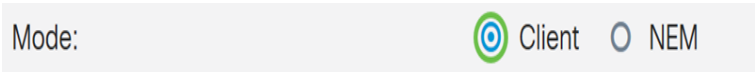
Hinweis: TestGroup ist eine Benutzergruppe, die wir unter **Systemkonfiguration > Benutzergruppen** erstellt haben.



Hinweis: In diesem Beispiel wird TestGroup ausgewählt. Sie können auch das Kontrollkästchen neben der Benutzergruppe aktivieren und dann auf die Schaltfläche **Löschen** klicken, wenn Sie eine Benutzergruppe löschen möchten.

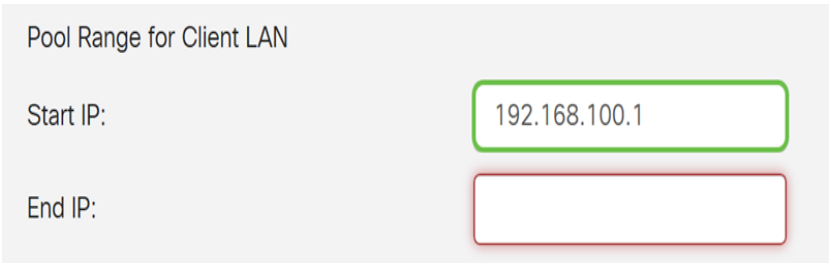
Schritt 12: Klicken Sie auf ein Optionsfeld, um einen Modus auszuwählen. Folgende Optionen stehen zur Verfügung:

- Client: Mit dieser Option kann der Client eine IP-Adresse anfordern, und der Server stellt die IP-Adressen aus dem konfigurierten Adressbereich bereit.
- Network Extension Mode (NEM) (Netzwerkerweiterungsmodus) - Mit dieser Option können Kunden ihr Subnetz vorschlagen, für das VPN-Services auf den vom Client vorgeschlagenen Datenverkehr zwischen LAN hinter dem Server und dem Subnetz angewendet werden müssen.



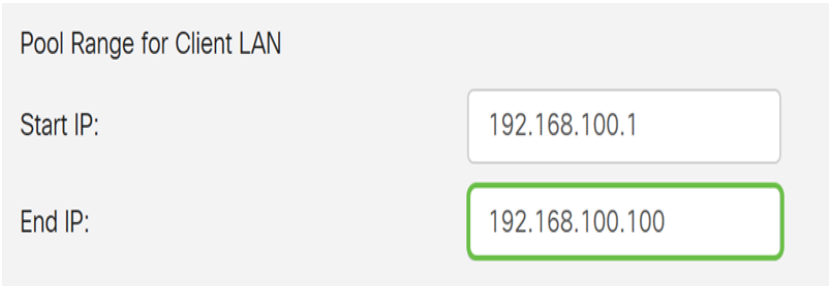
Hinweis: In diesem Beispiel wird Client ausgewählt.

Schritt 13: Geben Sie die Start-IP-Adresse in das Feld *Start-IP ein*. Dies ist die erste IP-Adresse im Pool, die einem Client zugewiesen werden kann.



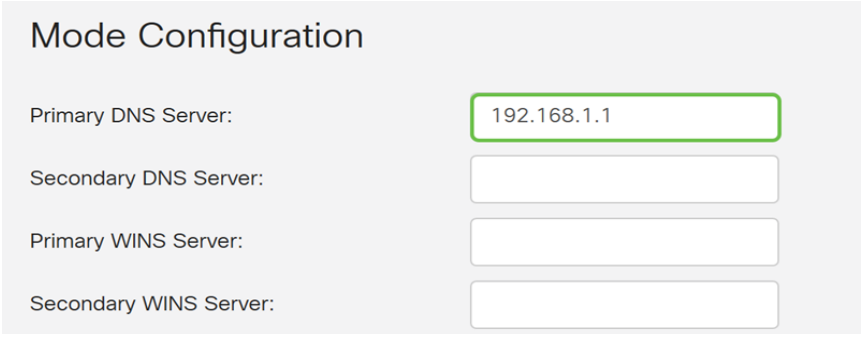
Hinweis: In diesem Beispiel wird 192.168.100.1 verwendet.

Schritt 14: Geben Sie die End-IP-Adresse in das Feld *End IP (IP-Ende*) ein. Dies ist die letzte IP-Adresse im Pool, die einem Client zugewiesen werden kann.



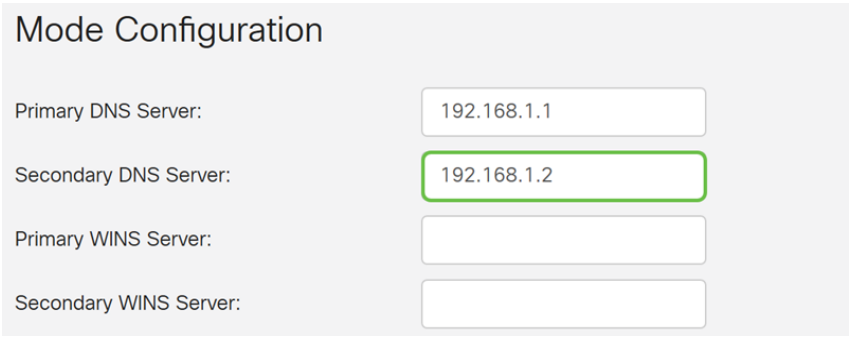
Hinweis: In diesem Beispiel wird 192.168.100.100 verwendet.

Schritt 15: (Optional) Geben Sie im Bereich "*Mode Configuration*" (*Moduskonfiguration*) die IP-Adresse des primären DNS-Servers in das angegebene Feld ein.



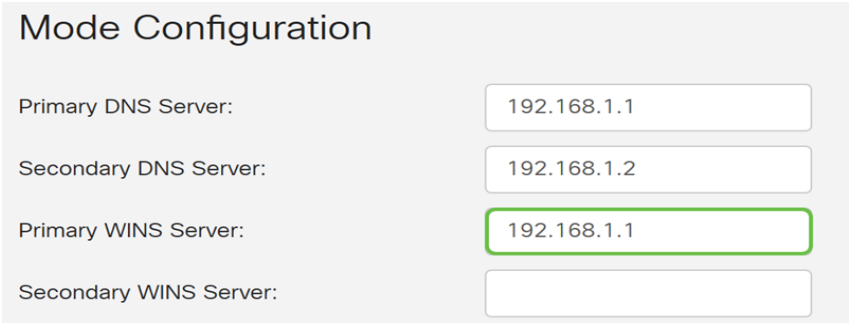
Hinweis: In diesem Beispiel wird 192.168.1.1 verwendet.

Schritt 16: (Optional) Geben Sie die IP-Adresse des sekundären DNS-Servers in das angegebene Feld ein.



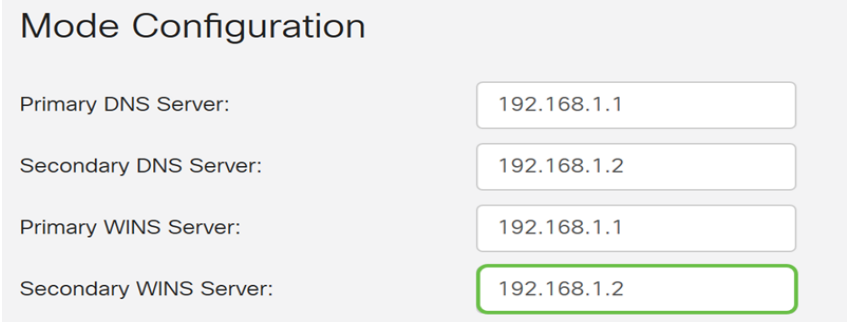
Hinweis: In diesem Beispiel wird 192.168.1.2 verwendet.

Schritt 17: (Optional) Geben Sie die IP-Adresse des primären WINS-Servers in das angegebene Feld ein.



Hinweis: In diesem Beispiel wird 192.168.1.1 verwendet.

Schritt 18: (Optional) Geben Sie die IP-Adresse des sekundären WINS-Servers in das angegebene Feld ein.



Hinweis: In diesem Beispiel wird 192.168.1.2 verwendet.

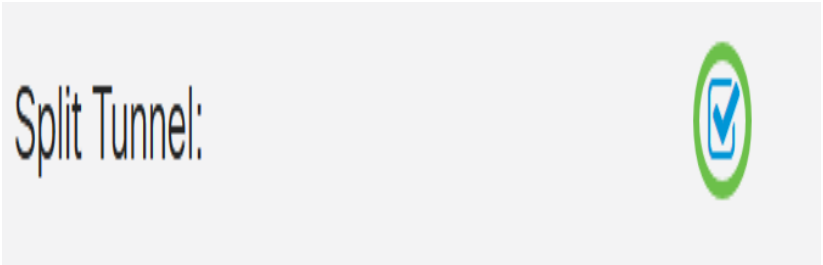
Schritt 19: (Optional) Geben Sie die Standarddomäne für das Remote-Netzwerk in das angegebene Feld ein.

Hinweis: In diesem Beispiel wird sample.com verwendet.

Schritt 20: (Optional) Geben Sie im Feld *Backup Server 1* die IP-Adresse oder den Domänennamen des Backup-Servers ein. Hier kann das Gerät die VPN-Verbindung starten, falls der primäre IPSec VPN-Server ausfällt. Sie können in die dafür vorgesehenen Felder bis zu drei Backup-Server eingeben. Der Backup-Server 1 hat die höchste Priorität unter den drei Servern und der Backup-Server 3 die niedrigste.

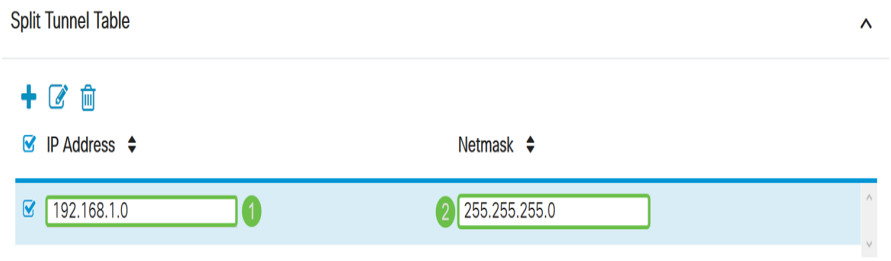
Hinweis: In diesem Beispiel wird Example.com für Backup Server 1 verwendet.

Schritt 21: (Optional) Aktivieren Sie das Kontrollkästchen **Split Tunnel** (Tunnel teilen), um Split Tunnel zu aktivieren. Split Tunneling ermöglicht den gleichzeitigen Zugriff auf die Ressourcen eines privaten Netzwerks und des Internets.



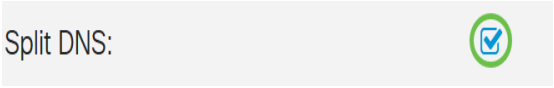
Schritt 22: (Optional) Klicken Sie unter der *Split Tunnel Table* auf das **Plus**-Symbol, um eine IP-Adresse für Split Tunnel hinzuzufügen.

Schritt 23: (Optional) Geben Sie die IP-Adresse und die Netzmaske des Split-Tunnels in die dafür vorgesehenen Felder ein.

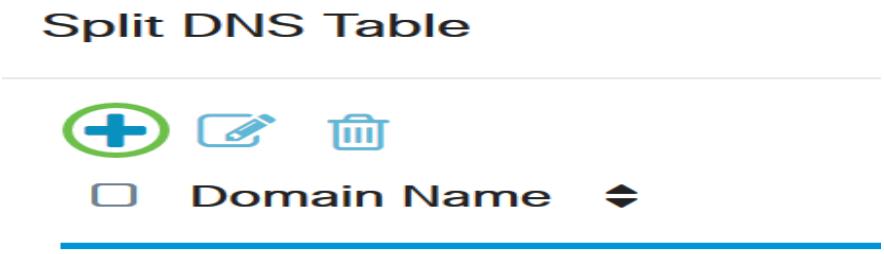


Hinweis: In diesem Beispiel werden 192.168.1.0 und 255.255.255.0 verwendet. Sie können das Kontrollkästchen auch aktivieren und auf die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen** klicken, um einen Split-Tunnel hinzuzufügen, zu bearbeiten oder zu löschen.

Schritt 24: (Optional) Aktivieren Sie das Kontrollkästchen **Split DNS (DNS aufteilen)**, um Split DNS zu aktivieren. Mit Split DNS können Sie separate DNS-Server für interne und externe Netzwerke erstellen, um die Sicherheit und den Schutz der Netzwerkressourcen zu gewährleisten.



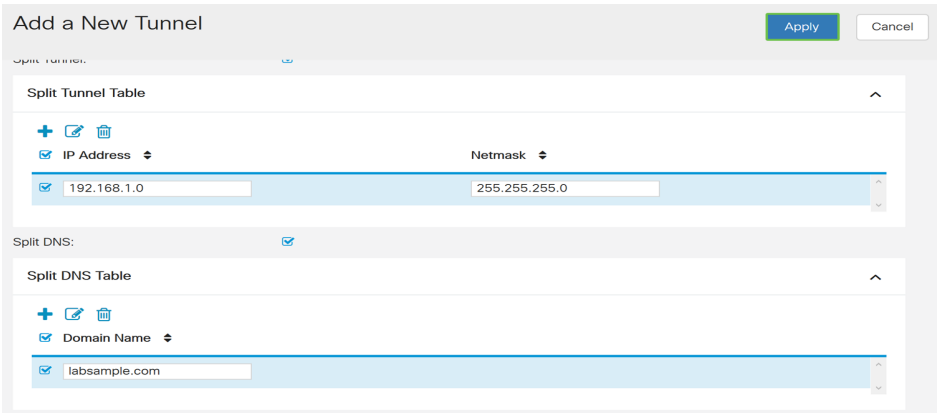
Schritt 25: (Optional) Klicken Sie auf das **Pluszeichen** unter der *Split DNS Table*, um einen Domänennamen für Split DNS hinzuzufügen.



Schritt 26: (Optional) Geben Sie den Domänennamen des geteilten DNS in das angegebene Feld ein.

Hinweis: In diesem Beispiel wird labsample.com verwendet. Sie können das Kontrollkästchen auch aktivieren und auf die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen** klicken, um einen geteilten DNS hinzuzufügen, zu bearbeiten oder zu löschen.

Schritt 27: Klicken Sie auf **Übernehmen**.



Schlussfolgerung

Auf dem Router der Serie RV34x sollte jetzt die Verbindung zwischen Client und Standort erfolgreich konfiguriert sein.

Klicken Sie auf die folgenden Artikel, um mehr über die folgenden Themen zu erfahren:

- Konfigurieren eines Telearbeiter-VPN-Clients auf dem Router der Serie RV34x
- Verwenden des GreenBow VPN-Clients für die Verbindung mit dem Router der Serie RV34x
- Erstellen eines Benutzerkontos für das VPN-Client-Setup auf dem RV34x-Router
- Erstellen einer Benutzergruppe für das VPN-Setup auf dem RV34x-Router

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.