Konfigurieren einer Site-to-Site Virtual Private Network (VPN)-Verbindung auf einem RV340- oder RV345-Router

Ziel

Ein Virtual Private Network (VPN) ist die Verbindung zwischen dem lokalen Netzwerk und einem Remote-Host über das Internet. Beim lokalen und dem Remote-Host kann es sich um einen Computer oder ein anderes Netzwerk handeln, dessen Einstellungen synchronisiert wurden, um ihnen die Kommunikation zu ermöglichen. Dies gilt für alle VPN-Typen. In der Regel haben beide Netzwerke Zugriff auf die Ressourcen auf beiden Seiten der Verbindung. Eine VPN-Verbindung wird in der Regel für die Verbindung einer zweiten Niederlassung mit der Hauptniederlassung oder für die Verbindung eines entfernten Mitarbeiters mit dem Computernetzwerk des Büros verwendet, selbst wenn dieser nicht physisch mit der Netzwerkinfrastruktur verbunden ist. Remote-Mitarbeiter stellen in der Regel eine Verbindung über einen VPN-Software-Client wie AnyConnect, Shrew Soft, GreenBow und viele andere her.

In diesem Artikel erfahren Sie, wie Sie eine Site-to-Site-VPN-Verbindung zwischen einem RV340 und einem RV345-Router konfigurieren. Dabei wird der primäre Router als lokaler Router und der sekundäre Router als Remote-Router bezeichnet. Stellen Sie sicher, dass Sie Remote- oder physischen Zugriff auf den sekundären Router haben.

LAN-Netzwerke müssen sich in verschiedenen Subnetzen befinden (z. B. 192.168.1.x und 192.168.2.x) oder in völlig unterschiedlichen Netzwerken (z. B. 192.168.1.x und 10.10.1.x). Wenn sich beide Netzwerke im selben Subnetz befanden, würden die Router niemals versuchen, Pakete über das VPN zu senden.

Unterstützte Geräte

- RV340
- RV340 W
- RV345
- RV345P

Software-Version

- 1.0.03.15

Besonderer Hinweis: Lizenzierungsstruktur - Firmware-Versionen 1.0.3.15 und höher. AnyConnect wird *nur* für Client-Lizenzen in Rechnung gestellt.

Sie müssen Kundenlizenzen von einem Partner wie CDW oder über die Beschaffung von Geräten Ihres Unternehmens erwerben. Es gibt Optionen für 1 Benutzer (L-AC-PLS-3Y-S5) oder Pakete mit Lizenzen, einschließlich eines Jahres für 25 Benutzer (AC-PLS-P-25-S). Weitere Lizenzoptionen sind ebenfalls verfügbar, einschließlich unbefristete Lizenzen. Weitere Einzelheiten zur Lizenzierung finden Sie unter den Links im Abschnitt *Lizenzinformationen* unten.

Weitere Informationen zur AnyConnect-Lizenzierung für Router der Serie RV340 finden Sie im

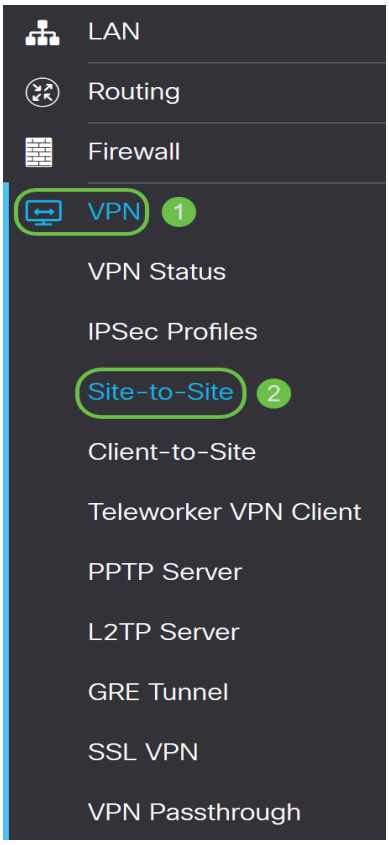
Artikel AnyConnect Licensing for the RV340 Series Routers.

Konfigurieren einer VPN-Verbindung

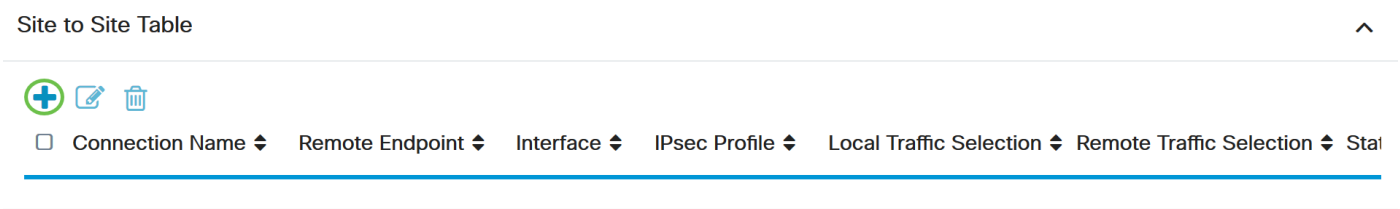
Lokaler Router

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

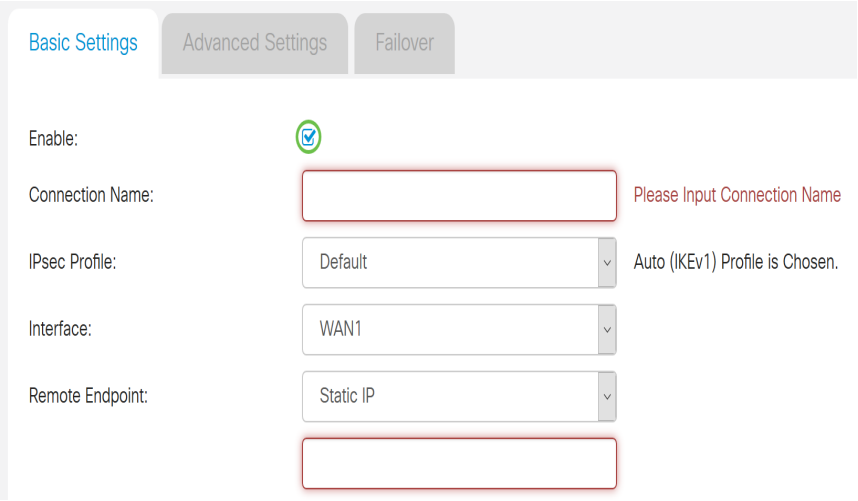
Hinweis: In diesem Beispiel wird ein RV340 verwendet.



Schritt 2: Klicken Sie auf das **Pluszeichen**.

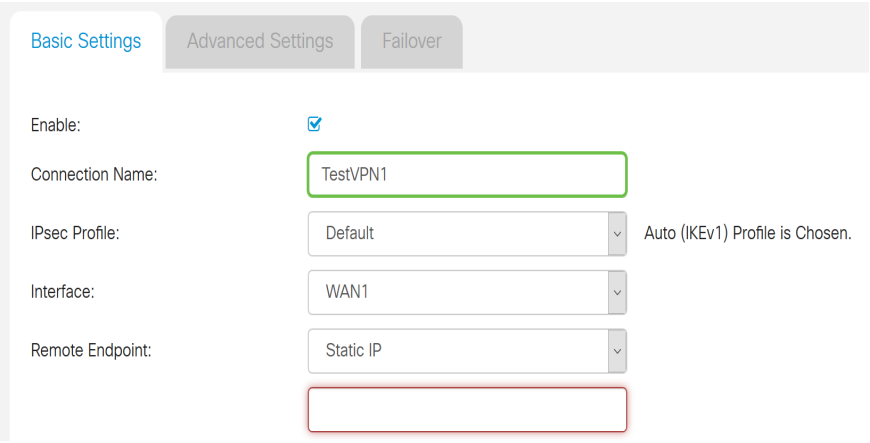


Schritt 3: Stellen Sie sicher, dass das Kontrollkästchen **Aktivieren** aktiviert ist. Es ist standardmäßig aktiviert.



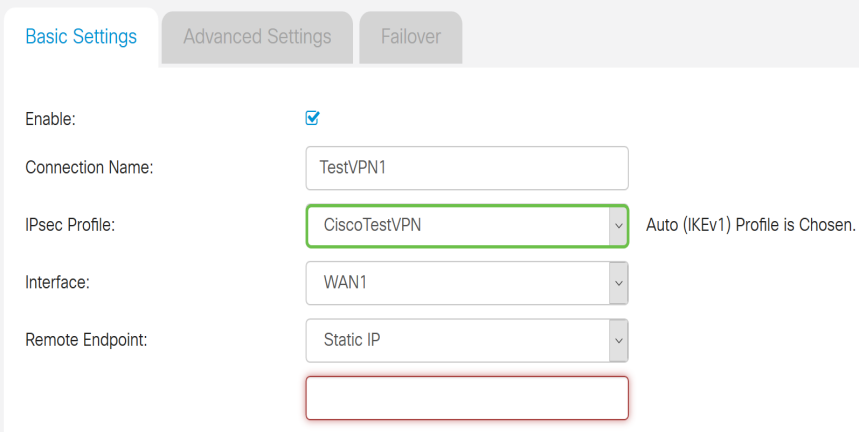
Schritt 4: Geben Sie den Namen der Verbindung in das Feld *Verbindungsname ein*.

Hinweis: In diesem Beispiel lautet der Name TestVPN1.



Schritt 5: Wählen Sie die Sicherheitseinstellungen der Verbindung aus der Dropdown-Liste IPSec Profile (IPSec-Profil) aus. Die Optionen hängen von den erstellten IPSec-Profilen ab. Anweisungen zum Erstellen eines IPSec-Profils erhalten Sie hier.

Hinweis: In diesem Beispiel wird CiscoTestVPN ausgewählt.

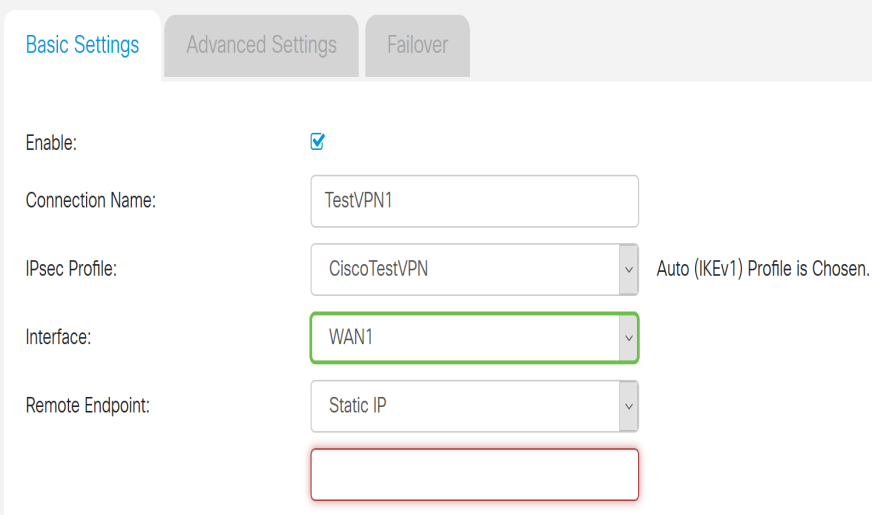


Schritt 6: Wählen Sie die Schnittstelle aus, die vom lokalen Router verwendet werden soll. Folgende Optionen sind verfügbar:

- WAN1: Bei dieser Option wird die IP-Adresse der Wide Area Network 1 (WAN1)-Schnittstelle des lokalen Routers für die VPN-Verbindung verwendet.
- WAN2: Bei dieser Option wird die IP-Adresse der WAN2-Schnittstelle des lokalen Routers für die VPN-Verbindung verwendet. WAN2 ist bei Single-WAN-Routern nicht verfügbar.
- USB1: Diese Option verwendet die IP-Adresse der USB 1-Schnittstelle (Universal Serial Bus

1) des lokalen Routers für die VPN-Verbindung.
- USB2: Diese Option verwendet die IP-Adresse der USB2-Schnittstelle des lokalen Routers für die VPN-Verbindung. USB2 ist für Single-USB-Router nicht verfügbar.

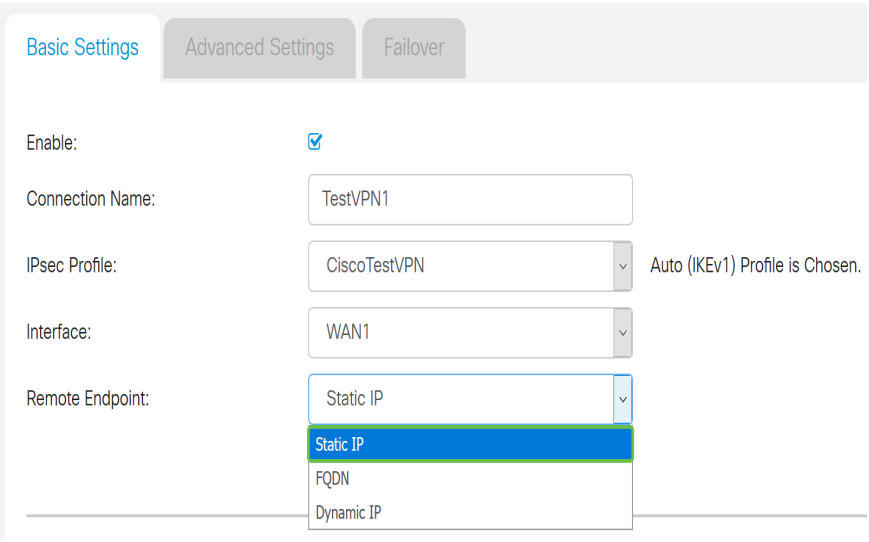
Hinweis: In diesem Beispiel wird WAN1 ausgewählt.



Schritt 7: Wählen Sie die Kennung der WAN-Schnittstelle des Remote-Routers aus. Folgende Optionen sind verfügbar:

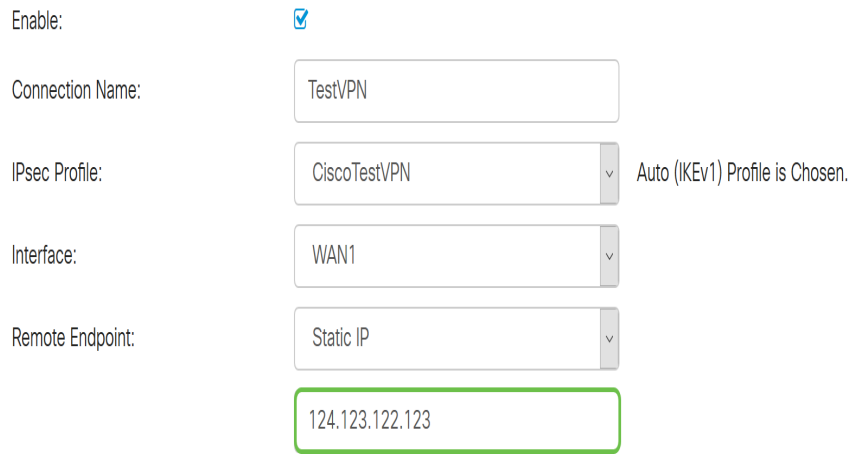
- Static IP (Statische IP): Mit dieser Option kann der lokale Router beim Herstellen einer VPN-Verbindung die statische IP-Adresse des Remote-Routers verwenden. Wenn diese Option auf dem lokalen Router gewählt wird, sollte der Remote-Router ebenfalls mit derselben Option konfiguriert werden.
- FQDN: Bei dieser Option wird beim Herstellen der VPN-Verbindung der Fully Qualified Domain Name (FQDN) des Remote-Routers verwendet.
- Dynamic IP (Dynamische IP): Diese Option verwendet die dynamische IP-Adresse des Remote-Routers, wenn eine VPN-Verbindung hergestellt wird.

Hinweis: Die Schnittstellenkennung auf dem Remote-Router muss mit der Schnittstellenkennung des lokalen Routers übereinstimmen. In diesem Beispiel wird die statische IP ausgewählt.



Schritt 8: Geben Sie die IP-Adresse der WAN-Schnittstelle des Remote-Routers ein.

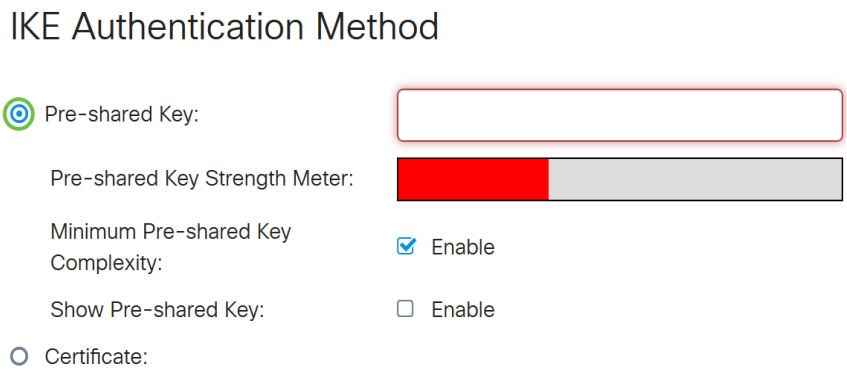
Hinweis: In diesem Beispiel wird 124.123.122.123 verwendet.



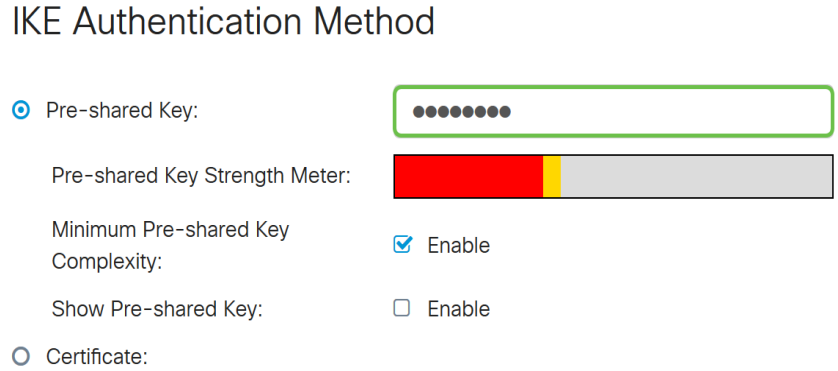
Schritt 9: Klicken Sie auf das Optionsfeld für die gewünschte Internet Key Exchange (IKE)-Authentifizierungsmethode. Folgende Optionen sind verfügbar:

- Preshared Key (Vorinstallierter Schlüssel): Diese Option bedeutet, dass für die Verbindung ein Kennwort erforderlich ist, um die Verbindung herzustellen. Der vorinstallierte Schlüssel muss an beiden Enden der VPN-Verbindung identisch sein.
- Certificate (Zertifikat): Diese Option bedeutet, dass die Authentifizierungsmethode bei der Verbindung ein vom Router generiertes Zertifikat anstelle eines Kennworts verwendet.

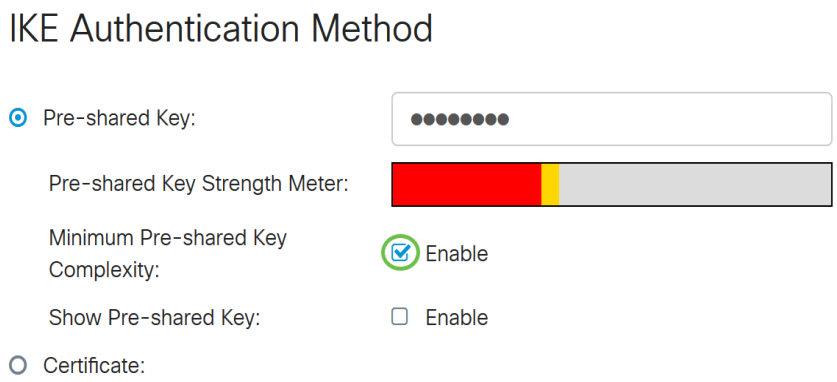
Hinweis: In diesem Beispiel wird der vorinstallierte Schlüssel ausgewählt.



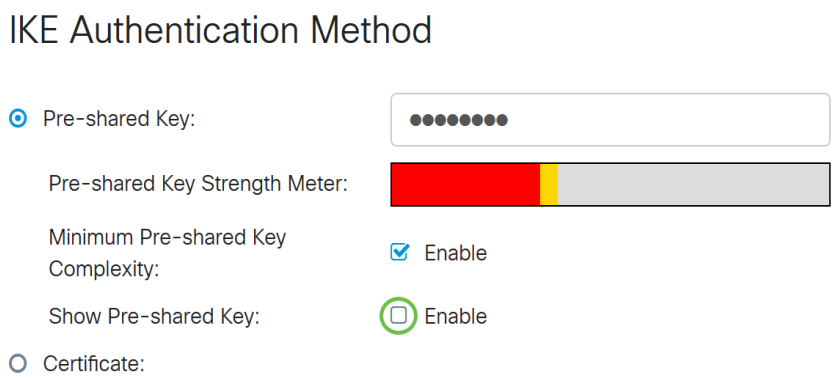
Schritt 10: Geben Sie den vorinstallierten Schlüssel für die VPN-Verbindung in das Feld *Vorinstallierter Schlüssel ein*.



Schritt 11: (Optional) Deaktivieren Sie das Kontrollkästchen **Enable** (Minimale **Komplexität für** gemeinsam genutzten Schlüssel aktivieren), wenn Sie ein einfaches Kennwort für die VPN-Verbindung verwenden möchten. Dies ist standardmäßig aktiviert.



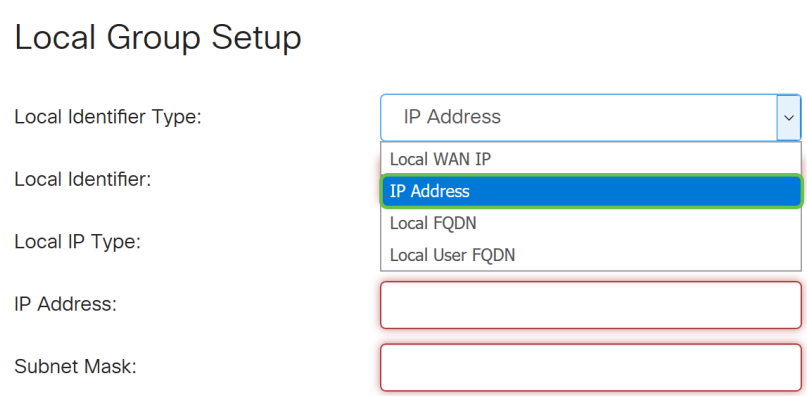
Schritt 12: (Optional) Aktivieren Sie das Kontrollkästchen Nur Text anzeigen, wenn **Aktivieren** bearbeitet wird, um den vorinstallierten Schlüssel im Klartext anzuzeigen. Standardmäßig ist diese Option deaktiviert.



Schritt 13: Wählen Sie den Identifizierungstyp des lokalen Netzwerks aus der Dropdown-Liste Local Identifier Type (Lokaler Identifizierungstyp) aus. Folgende Optionen sind verfügbar:

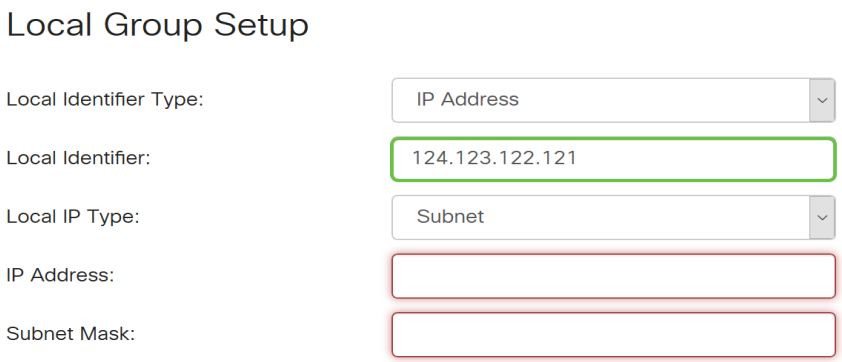
- Local WAN IP (Lokale WAN-IP): Diese Option identifiziert das lokale Netzwerk über die WAN-IP-Adresse der Schnittstelle.
- IP Address (IP-Adresse): Diese Option identifiziert das lokale Netzwerk über die lokale IP-Adresse.
- Lokaler FQDN - Diese Option identifiziert das lokale Netzwerk über den FQDN, falls vorhanden.
- Local User FQDN (Lokaler Benutzer-FQDN): Diese Option identifiziert das lokale Netzwerk über den FQDN des Benutzers, wobei es sich um seine E-Mail-Adresse handeln kann.

Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt.



Schritt 14: Geben Sie die Kennung des lokalen Netzwerks im Feld *Lokale Kennung ein*.

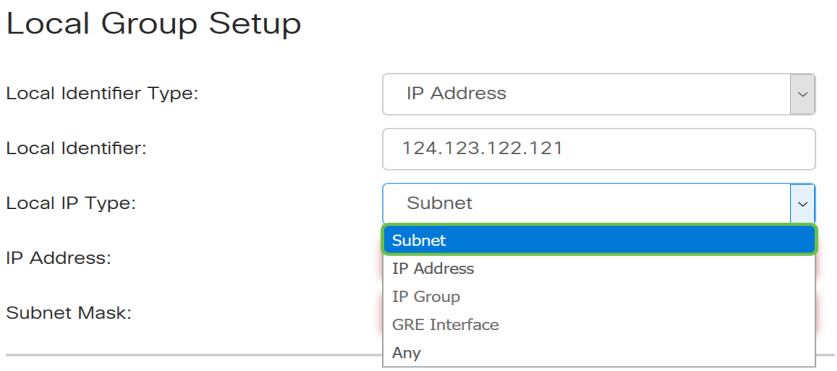
Hinweis: In diesem Beispiel wird 124.123.122.121 eingegeben.



Schritt 15: Wählen Sie aus der Dropdown-Liste Lokaler IP-Typ den IP-Adresstyp aus, auf den der VPN-Client zugreifen kann. Folgende Optionen sind verfügbar:

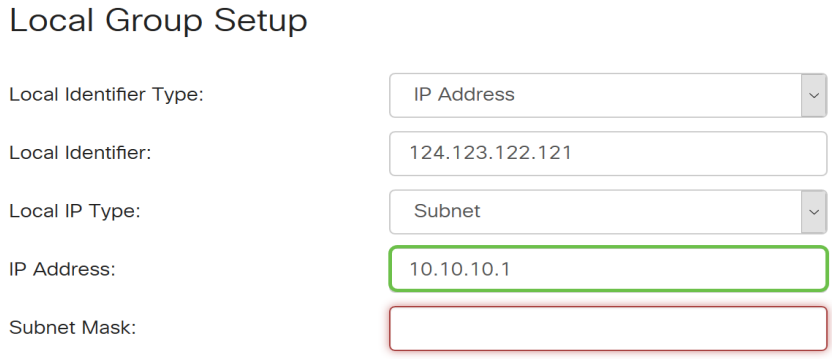
- Subnetz - Diese Option ermöglicht der Außenseite des VPN den Zugriff auf die lokalen Hosts im angegebenen Subnetz.
- IP Address (IP-Adresse): Mit dieser Option kann die Remote-Seite des VPN auf den lokalen Host mit der angegebenen IP-Adresse zugreifen.
- Any (Beliebig): Mit dieser Option kann die Remote-Seite des VPN auf einen der lokalen Hosts zugreifen.

Hinweis: In diesem Beispiel wird Subnet ausgewählt.



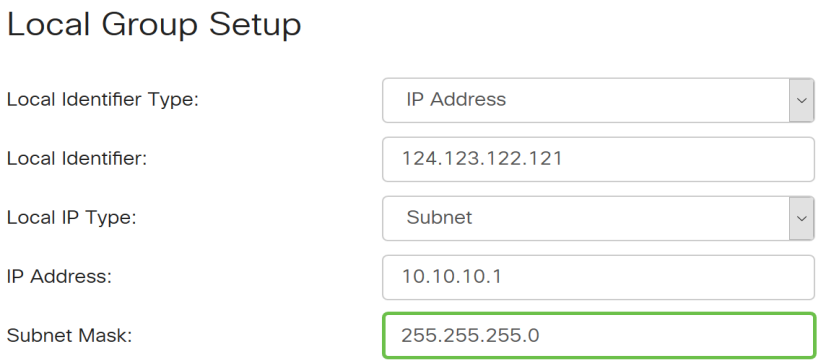
Schritt 16: Geben Sie im Feld *IP-Adresse* die IP-Adresse des Netzwerks oder Hosts ein, auf den der VPN-Client zugreifen soll.

Hinweis: In diesem Beispiel lautet die IP-Adresse 10.10.10.1.



Schritt 17: Geben Sie die Subnetzmaske der IP-Adresse im Feld *Subnetzmaske ein*.

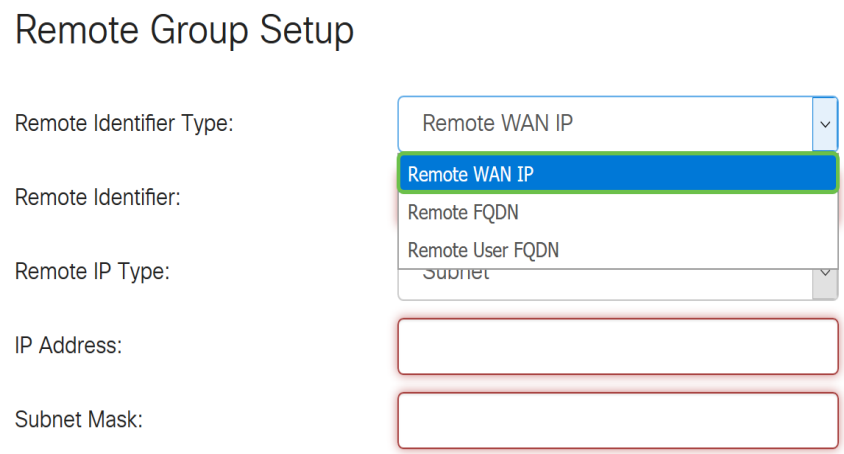
Hinweis: In diesem Beispiel ist die Subnetzmaske 255.255.255.0.



Schritt 18: Wählen Sie den Typ der Remote-Kennung aus der Dropdown-Liste aus. Folgende Optionen sind verfügbar:

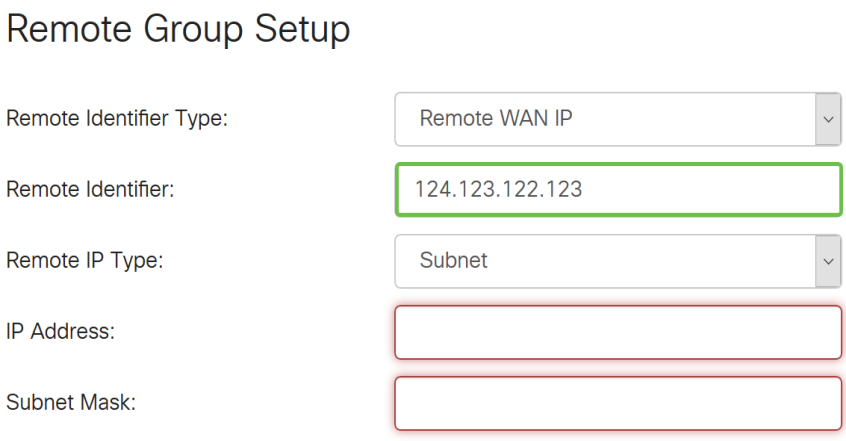
- Remote-WAN-IP: Diese Option identifiziert das Remote-Netzwerk über die WAN-IP-Adresse der Schnittstelle.
- Remote FQDN - Diese Option identifiziert das Remote-Netzwerk über den FQDN, falls vorhanden.
- Remote User FQDN (FQDN für Remote-Benutzer): Mit dieser Option wird das Remote-Netzwerk über den FQDN des Benutzers identifiziert, wobei es sich um seine E-Mail-Adresse handeln kann.

Hinweis: In diesem Beispiel wird Remote-WAN-IP ausgewählt.



Schritt 19: Geben Sie die WAN-IP-Adresse des Remote-Routers in das Feld *Remote Identifier (Remote-Identifizierung)* ein.

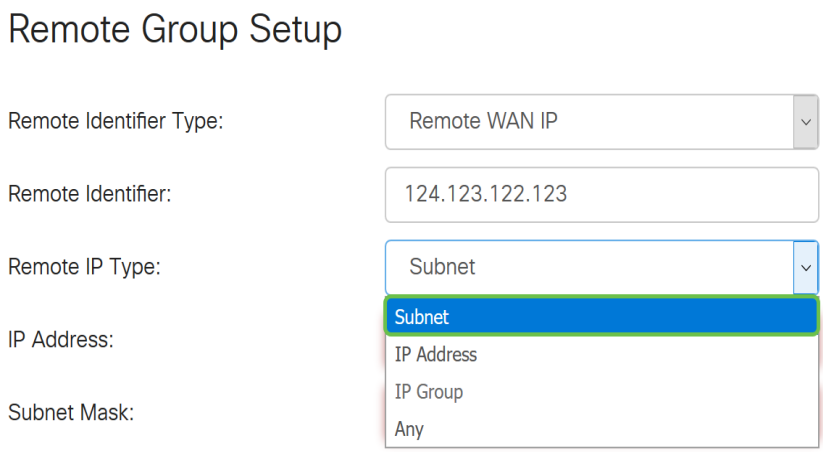
Hinweis: In diesem Beispiel lautet die Remote-ID 124.123.122.123.



Schritt 20: Wählen Sie in der Dropdown-Liste Remote IP Type (Remote-IP-Typ) den Netzwerktyp

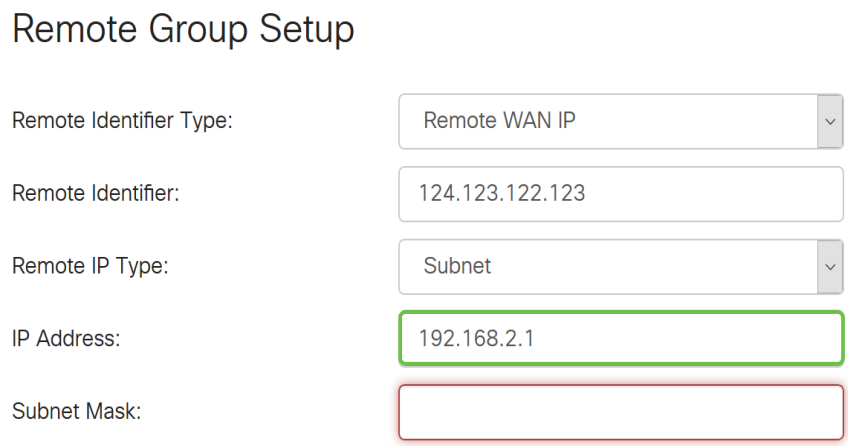
aus, auf den das lokale Netzwerk zugreifen muss. Folgende Optionen sind verfügbar:

- IP Address (IP-Adresse): Mit dieser Option können die lokalen Hosts mit der angegebenen IP-Adresse auf den Remote-Host zugreifen.
- Subnetz - Mit dieser Option können die lokalen Hosts mit dem angegebenen Subnetz auf die Ressourcen auf dem Remotehost zugreifen.
- Any (Beliebig): Mit dieser Option können die lokalen Hosts mit einer beliebigen IP-Adresse auf die Ressourcen auf dem Remote-Host zugreifen.



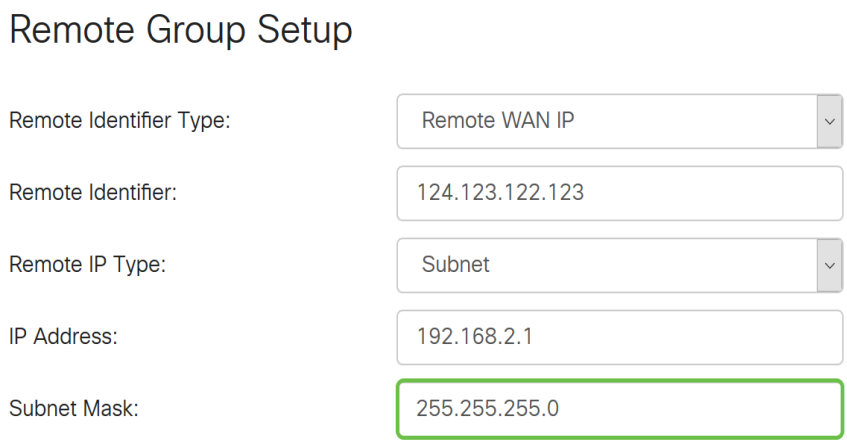
Schritt 21: Geben Sie die LAN-IP-Adresse des Remote-Netzwerks in das Feld *IP-Adresse ein*.

Hinweis: In diesem Beispiel lautet die IP-Adresse 192.168.2.1.

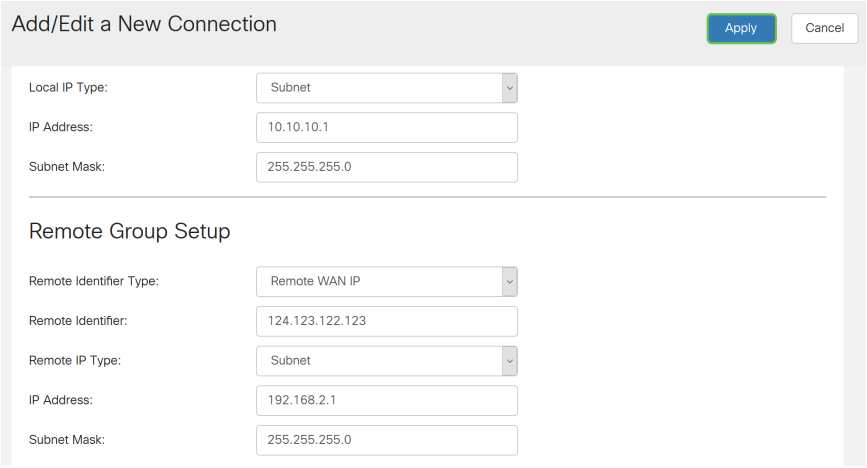


Schritt 22: Geben Sie die Subnetzmaske des Remote-Netzwerks in das Feld *Subnetzmaske ein*.

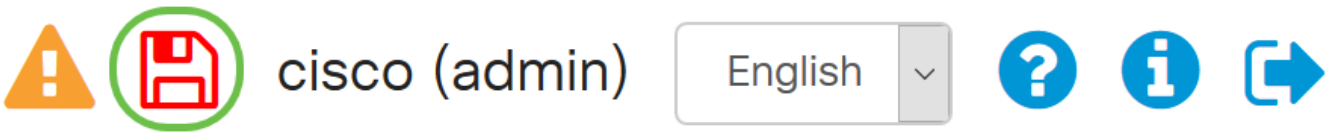
Hinweis: In diesem Beispiel ist die Subnetzmaske 255.255.255.0.



Schritt 23: Klicken Sie auf **Apply** (Anwenden).



Schritt 24: Klicken Sie auf **Speichern**.



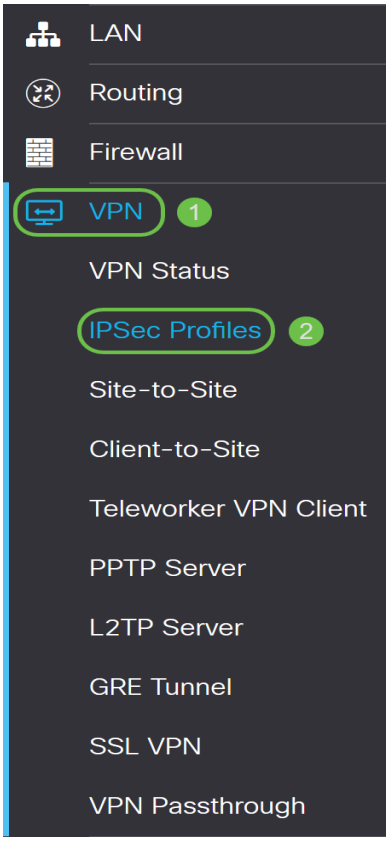
Sie sollten jetzt die VPN-Einstellungen auf dem lokalen Router konfiguriert haben.

Remote-Router

Schritt 1: Bestimmen Sie die VPN-Einstellungen des lokalen Routers, z. B.:

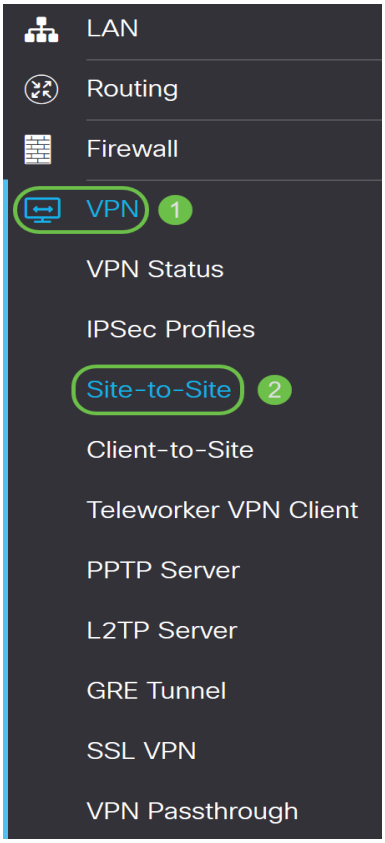
- Schnittstelle des für die VPN-Verbindung zu verwendenden lokalen und Remote-Routers.
- Wide Area Network (WAN) Internet Protocol (IP)-Adresse des lokalen und Remote-Routers.
- Local Area Network (LAN)-Adresse und Subnetzmaske des lokalen und des Remote-Netzwerks
- Vorinstallierter Schlüssel, Kennwort oder Zertifikat für die VPN-Verbindung.
- Sicherheitseinstellungen des lokalen Routers.
- Firewall-Freistellung für die VPN-Verbindung.

Schritt 2: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **VPN > IPSec-Profile aus**.

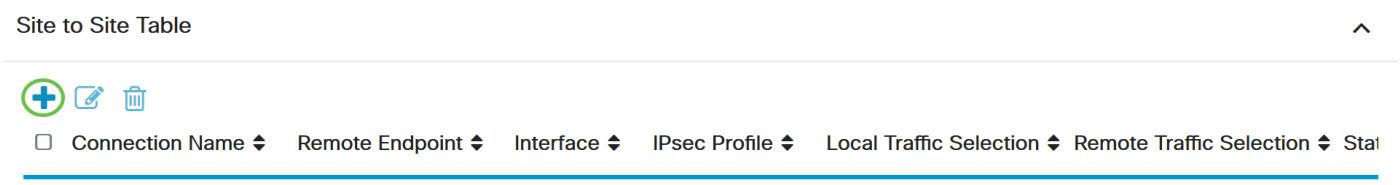


Schritt 3: Konfigurieren Sie die VPN-Sicherheitseinstellungen des Remote-Routers entsprechend den VPN-Sicherheitseinstellungen des lokalen Routers. Anweisungen hierzu erhalten Sie hier.

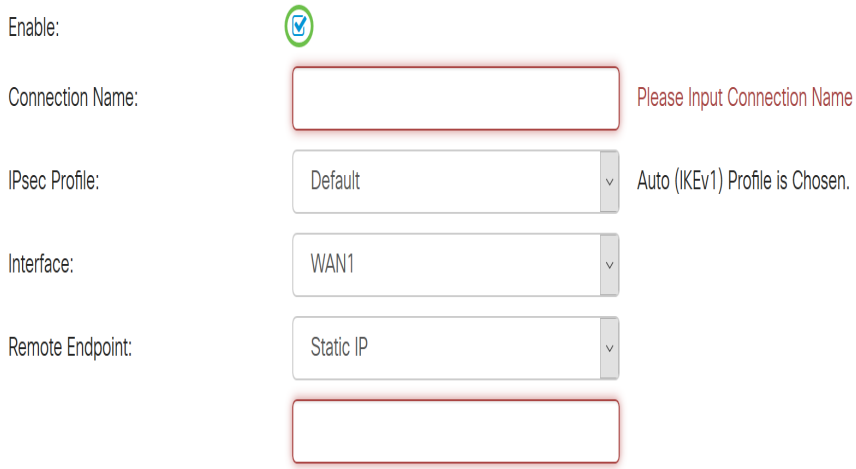
Schritt 4: Wählen Sie im webbasierten Dienstprogramm des lokalen Routers **VPN > Site-to-Site aus**.



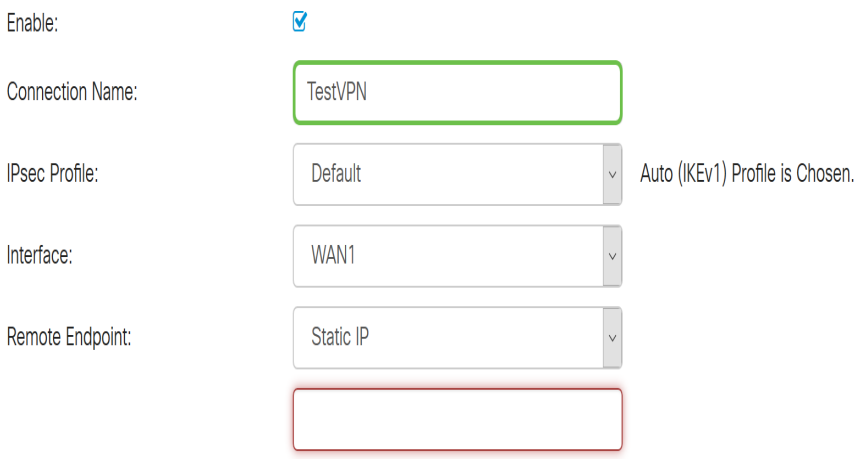
Schritt 5: Klicken Sie auf das **Pluszeichen**.



Schritt 6: Stellen Sie sicher, dass das Kontrollkästchen **Aktivieren** aktiviert ist. Es ist standardmäßig aktiviert.



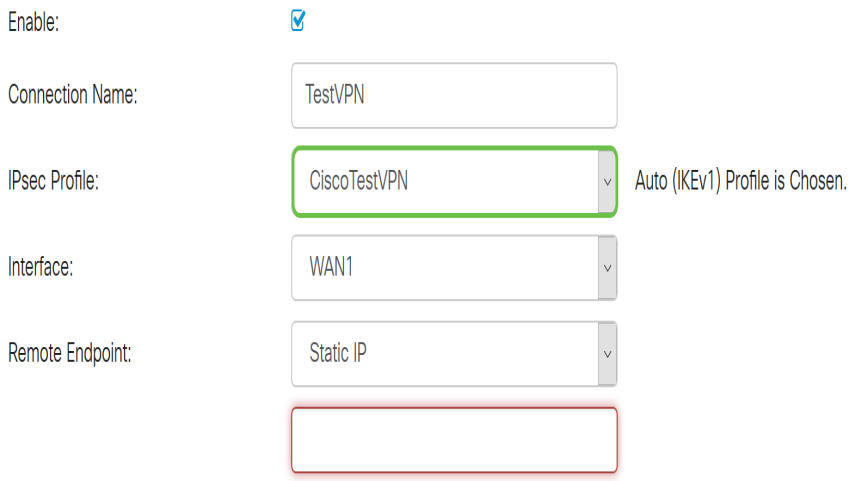
Schritt 7: Geben Sie den Namen der VPN-Verbindung im Feld *Verbindungsname ein*. Der Verbindungsname des Remote-Routers kann sich von dem im lokalen Router angegebenen Verbindungsnamen unterscheiden.



Hinweis: In diesem Beispiel ist der Verbindungsname TestVPN.

Schritt 8: Wählen Sie aus der Dropdown-Liste das IPSec-Profil aus. Die Optionen hängen von den erstellten IPSec-Profilen ab. Anweisungen zum Erstellen eines IPSec-Profils erhalten Sie hier.

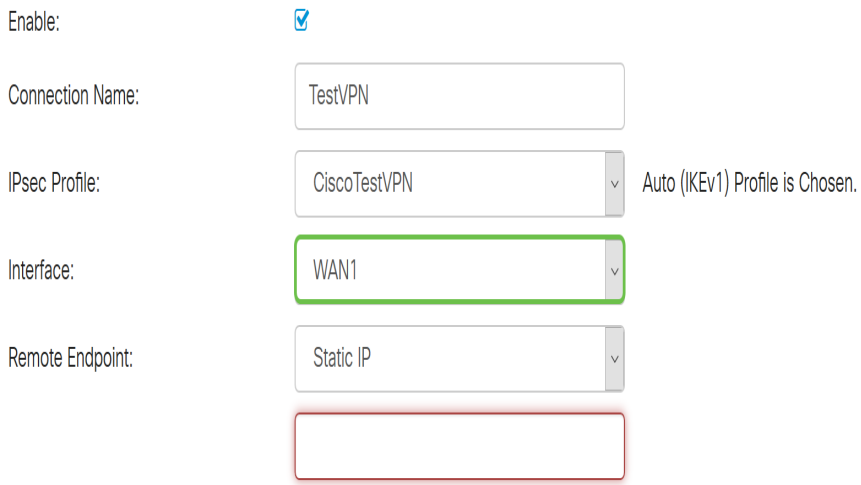
Hinweis: In diesem Beispiel wird CiscoTestVPN ausgewählt.



Schritt 9: Wählen Sie aus der Dropdown-Liste die Schnittstelle aus, die der Remote-Router für die VPN-Verbindung verwenden soll. Folgende Optionen sind verfügbar:

- WAN1: Diese Option verwendet die IP-Adresse der Wide Area Network 1 (WAN1)-Schnittstelle des Remote-Routers für die VPN-Verbindung.
- WAN2: Diese Option verwendet die IP-Adresse der WAN2-Schnittstelle des Remote-Routers für die VPN-Verbindung. WAN2 ist bei Single-WAN-Routern nicht verfügbar.
- USB1: Diese Option verwendet die IP-Adresse der USB1-Schnittstelle (Universal Serial Bus 1) des Remote-Routers für die VPN-Verbindung.
- USB2: Diese Option verwendet die IP-Adresse der USB2-Schnittstelle des Remote-Routers für die VPN-Verbindung. USB2 ist für Single-USB-Router nicht verfügbar.

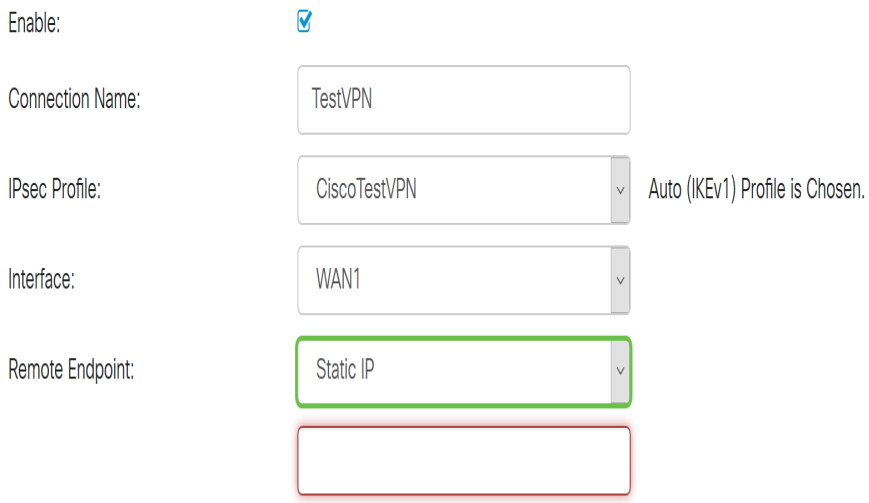
Hinweis: In diesem Beispiel wird WAN1 ausgewählt.



Schritt 10: Wählen Sie die Kennung der WAN-Schnittstelle des lokalen Routers aus der Dropdown-Liste Remote Endpoint (Remote-Endpunkt) aus. Folgende Optionen sind verfügbar:

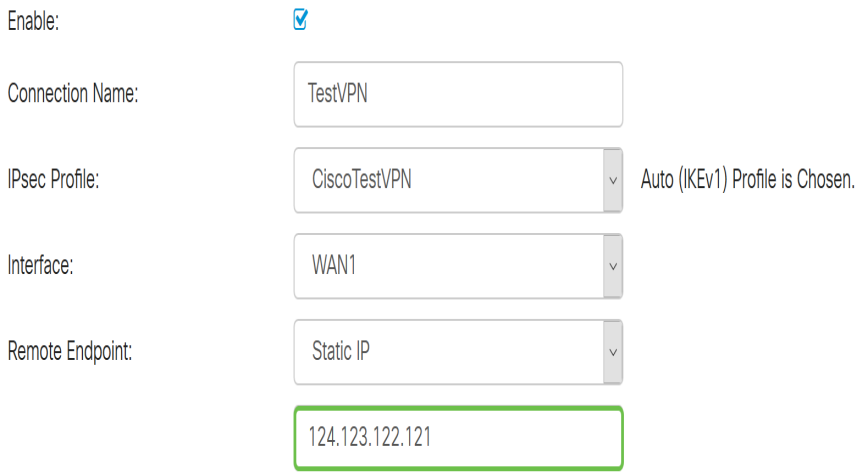
- Static IP (Statische IP): Mit dieser Option kann der Remote-Router beim Herstellen einer VPN-Verbindung die statische IP-Adresse des lokalen Routers verwenden. Wenn diese Option auf dem lokalen Router gewählt wird, sollte der Remote-Router ebenfalls mit derselben Option konfiguriert werden.
- FQDN: Bei dieser Option wird beim Herstellen der VPN-Verbindung der Fully Qualified Domain Name (FQDN) der lokalen Route verwendet.
- Dynamic IP (Dynamische IP): Diese Option verwendet die dynamische IP-Adresse des lokalen Routers, wenn eine VPN-Verbindung hergestellt wird.

Hinweis: Die Schnittstellenkennung auf dem Remote-Router muss mit der Schnittstellenkennung des lokalen Routers übereinstimmen. In diesem Beispiel wird die statische IP ausgewählt.



Schritt 11: Geben Sie die WAN-IP-Adresse des lokalen Routers ein.

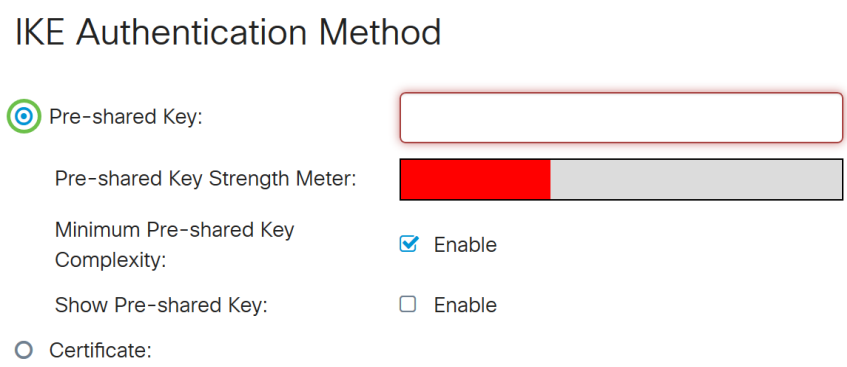
Hinweis: In diesem Beispiel lautet die IP-Adresse 124.123.122.121.



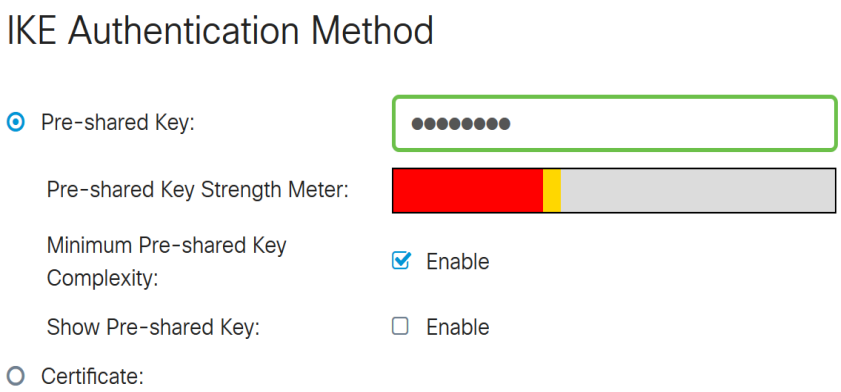
Schritt 12: Klicken Sie auf das Optionsfeld für die gewünschte Internet Key Exchange (IKE)-Authentifizierungsmethode. Folgende Optionen sind verfügbar:

- Preshared Key (Vorinstallierter Schlüssel): Diese Option bedeutet, dass für die Verbindung ein Kennwort erforderlich ist, um die Verbindung herzustellen. Der vorinstallierte Schlüssel muss an beiden Enden der VPN-Verbindung identisch sein.
- Certificate (Zertifikat): Diese Option bedeutet, dass die Authentifizierungsmethode bei der Verbindung ein vom Router generiertes Zertifikat anstelle eines Kennworts verwendet.

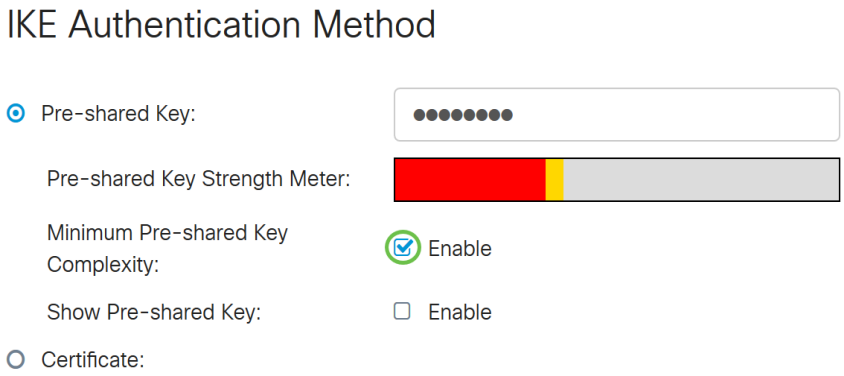
Hinweis: In diesem Beispiel wird der vorinstallierte Schlüssel ausgewählt.



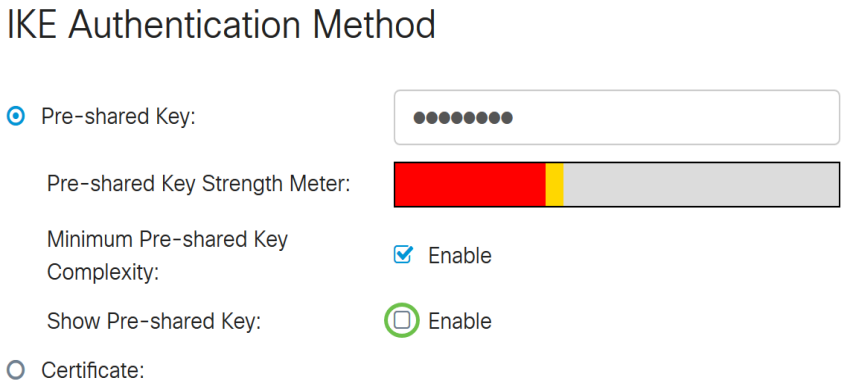
Schritt 13: Geben Sie den vorinstallierten Schlüssel für die VPN-Verbindung in das Feld *Vorinstallierter Schlüssel ein*.



Schritt 14: (Optional) Deaktivieren Sie das Kontrollkästchen Minimale Komplexität des vorinstallierten Schlüssels **aktivieren**, wenn Sie ein einfaches Kennwort für die VPN-Verbindung verwenden möchten. Dies ist standardmäßig aktiviert.



Schritt 15: (Optional) Aktivieren Sie das Kontrollkästchen Nur Text anzeigen, wenn **Aktivieren** bearbeitet wird, um den vorinstallierten Schlüssel im Klartext anzuzeigen. Standardmäßig ist diese Option deaktiviert.

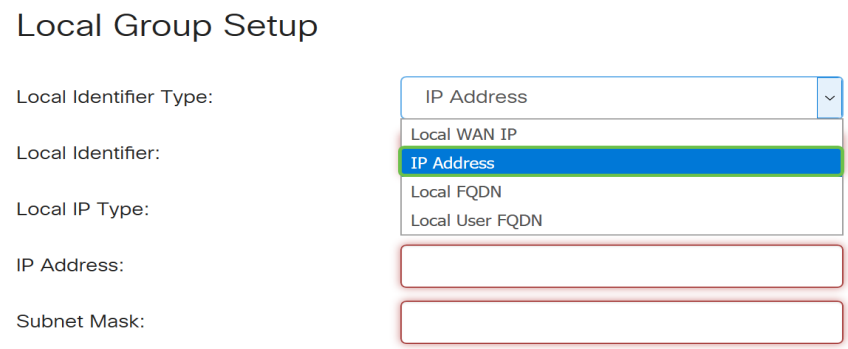


Schritt 16: Wählen Sie in der Dropdown-Liste Local Identifier Type (Typ der lokalen Identifizierung) des Remote-Routers den Identifizierungstyp des Remote-Netzwerks aus. Folgende Optionen sind

verfügbar:

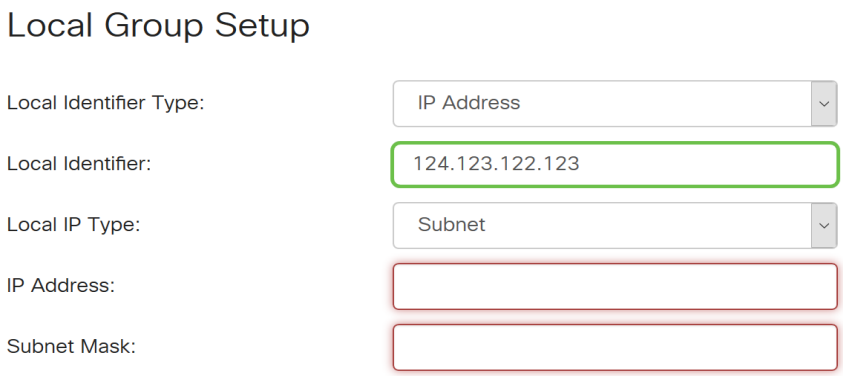
- Local WAN IP (Lokale WAN-IP): Diese Option identifiziert das Remote-Netzwerk über die WAN-IP-Adresse der Schnittstelle.
- IP Address (IP-Adresse): Diese Option identifiziert das Remote-Netzwerk über die lokale IP-Adresse.
- Local FQDN (Lokaler FQDN): Diese Option identifiziert das Remote-Netzwerk über den FQDN, falls vorhanden.
- Local User FQDN (Lokaler Benutzer-FQDN): Diese Option identifiziert das Remote-Netzwerk über den FQDN des Benutzers, wobei es sich um seine E-Mail-Adresse handeln kann.

Hinweis: In diesem Beispiel wird die IP-Adresse ausgewählt.



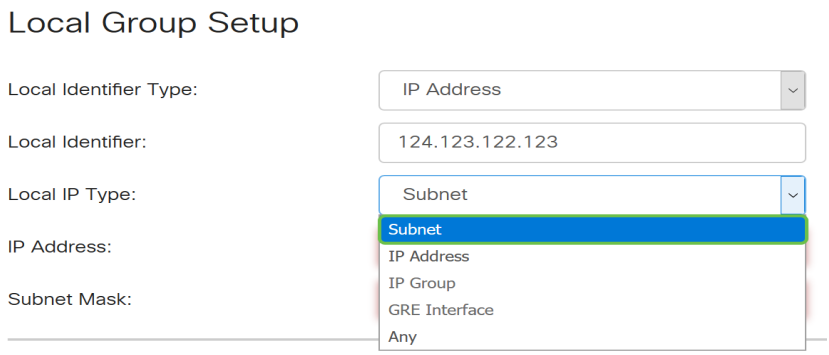
Schritt 17: Geben Sie die Kennung des Remote-Netzwerks im Feld *Local Identifier (Lokale Kennung*) des Remote-Routers ein.

Hinweis: In diesem Beispiel wird 124.123.122.123 eingegeben.



Schritt 18: Wählen Sie aus der Dropdown-Liste Lokaler IP-Typ den IP-Adresstyp aus, auf den der VPN-Client zugreifen kann. Folgende Optionen sind verfügbar:

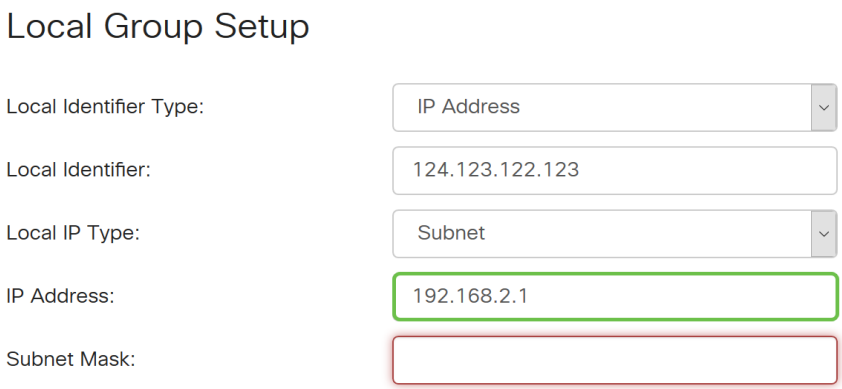
- Subnetz - Diese Option ermöglicht der lokalen Seite des VPN den Zugriff auf die Remote-Hosts im angegebenen Subnetz.
- IP Address (IP-Adresse): Mit dieser Option kann die lokale Seite des VPN auf den Remote-Host mit der angegebenen IP-Adresse zugreifen.
- Any (Beliebig): Mit dieser Option kann die lokale Seite des VPN auf einen der Remote-Hosts zugreifen.



Hinweis: In diesem Beispiel wird Subnet ausgewählt.

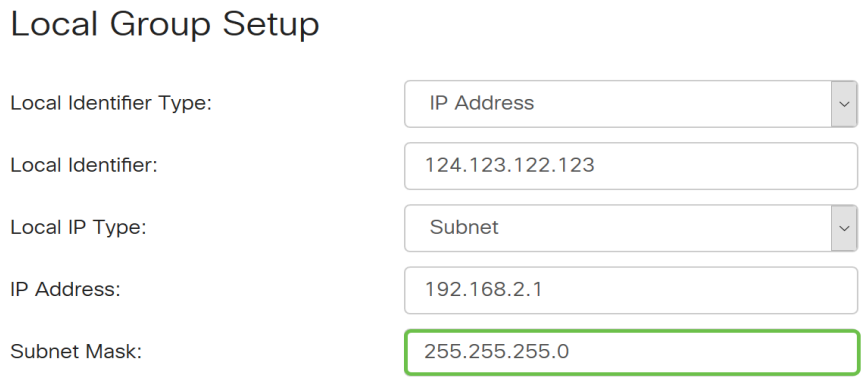
Schritt 19: Geben Sie im Feld *IP-Adresse* die IP-Adresse des Netzwerks oder Hosts ein, auf den der VPN-Client zugreifen soll.

Hinweis: In diesem Beispiel lautet die IP-Adresse 192.168.2.1.



Schritt 20: Geben Sie die Subnetzmaske der IP-Adresse im Feld *Subnetzmaske ein*.

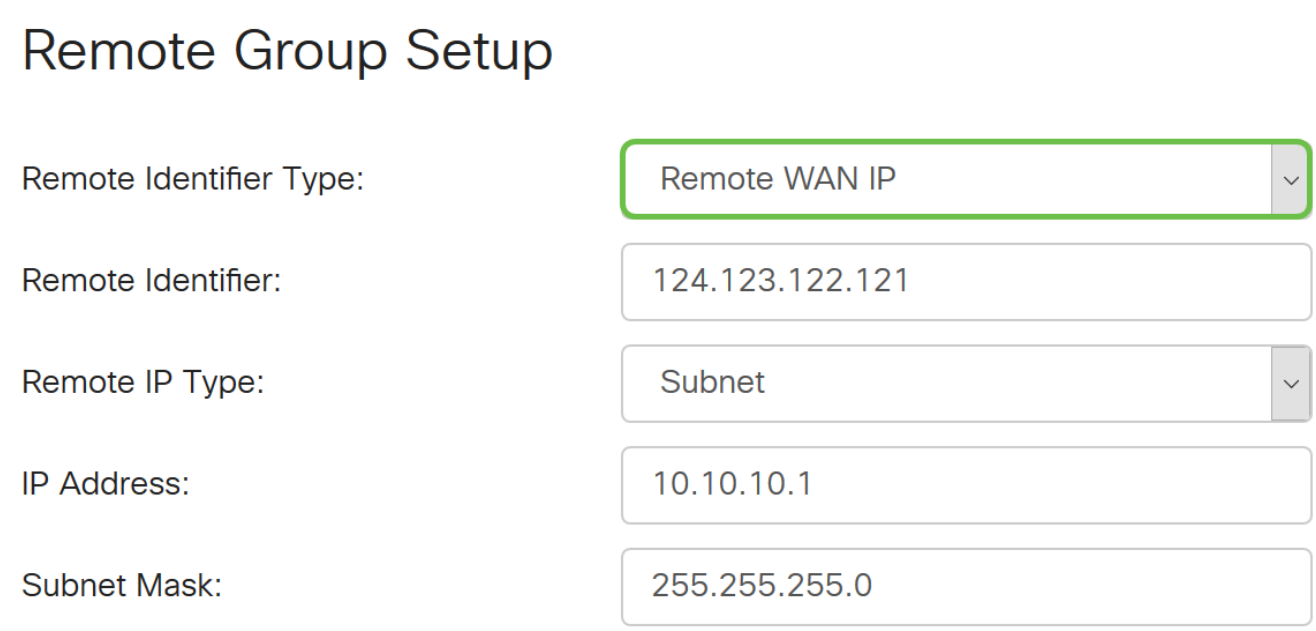
Hinweis: In diesem Beispiel ist die Subnetzmaske 255.255.255.0.



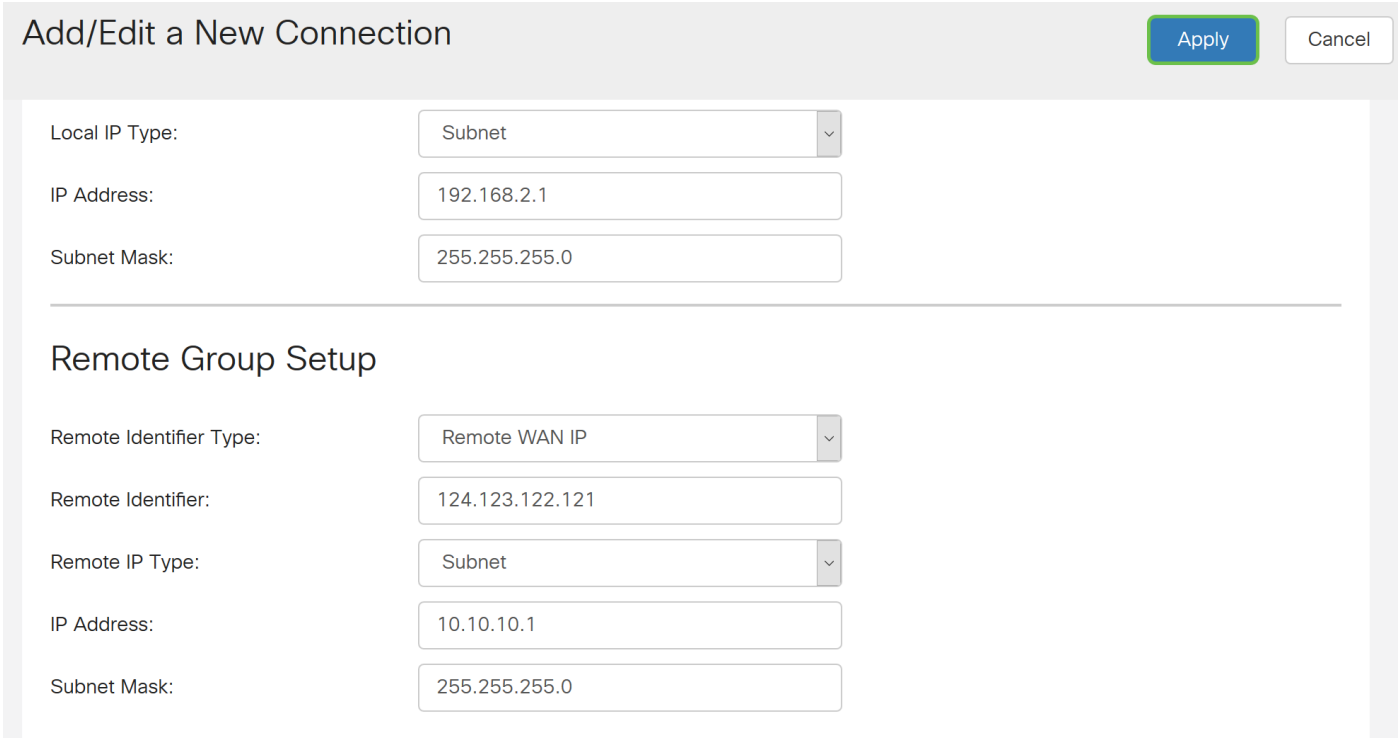
Schritt 21: Wählen Sie in der Dropdown-Liste den lokalen Identifizierungstyp aus. Folgende Optionen sind verfügbar:

- Remote-WAN-IP: Diese Option identifiziert das lokale Netzwerk über die WAN-IP-Adresse der Schnittstelle.
- Remote FQDN - Diese Option identifiziert das lokale Netzwerk über den FQDN, falls vorhanden.
- Remote User FQDN (FQDN für Remote-Benutzer): Mit dieser Option wird das lokale Netzwerk über den FQDN des Benutzers identifiziert, wobei es sich um seine E-Mail-Adresse handeln kann.

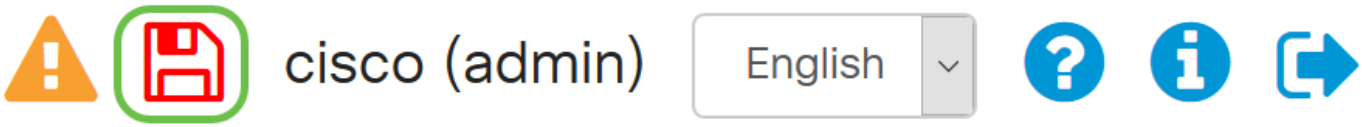
Hinweis: In diesem Beispiel wird Remote-WAN-IP ausgewählt.



Schritt 22: Klicken Sie auf **Apply** (Anwenden).



Schritt 23: Klicken Sie auf **Speichern**.



Sie sollten jetzt die VPN-Einstellungen auf dem Remote-Router konfiguriert haben.

Sehen Sie sich ein Video zu diesem Artikel an..

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