Konfigurieren von Site-to-Site-VPN auf dem RV160 und RV260

Ziel

Ziel dieses Dokuments ist die Erstellung eines Site-to-Site-VPN für die Router der Serien RV160 und RV260.

Einführung

Ein virtuelles privates Netzwerk (VPN) ist eine hervorragende Möglichkeit, externe Mitarbeiter mit einem sicheren Netzwerk zu verbinden. Mit einem VPN kann ein Remote-Host so agieren, als ob er mit dem gesicherten Netzwerk vor Ort verbunden wäre. In einem Site-to-Site-VPN stellt der lokale Router an einem Standort über einen VPN-Tunnel eine Verbindung zu einem Remote-Router her. Dieser Tunnel kapselt Daten sicher mithilfe von branchenüblichen Verschlüsselungs- und Authentifizierungsverfahren, um die gesendeten Daten zu schützen.

Beachten Sie, dass bei der Konfiguration eines Site-to-Site-VPN die Subnetze des Local Area Network (LAN) auf beiden Seiten des Tunnels nicht im gleichen Netzwerk angeordnet sein können. Wenn beispielsweise das LAN von Standort A das Subnetz 192.168.***1***.x/24 verwendet, kann Standort B nicht dasselbe Subnetz verwenden. Standort B muss ein anderes Subnetz verwenden, z. B. 192.168.***2***.x/24.

Um einen Tunnel richtig zu konfigurieren, geben Sie bei der Konfiguration der beiden Router die entsprechenden Einstellungen ein (lokale und Remote-Umkehr). Angenommen, dieser Router ist als Router A gekennzeichnet. Geben Sie die entsprechenden Einstellungen im Abschnitt "Local Group Setup" (Einrichtung der lokalen Gruppe) ein, während Sie die Einstellungen für den anderen Router (Router B) im Abschnitt "Remote Group Setup" (Einrichtung der Remote-Gruppe) eingeben. Wenn Sie den anderen Router (Router B) konfigurieren, geben Sie seine Einstellungen im Abschnitt für die Einrichtung der lokalen Gruppe ein, und geben Sie die Einstellungen für Router A im Remote Group Setup ein.

Nachfolgend finden Sie eine Tabelle der Konfiguration für Router A und Router B. Die fettgedruckten Parameter sind die im Umkehrschluss des anderen Routers dargestellten Parameter. Alle anderen Parameter bleiben unverändert. In diesem Dokument wird der lokale Router mithilfe von Router A konfiguriert.

Felder	Router A (lokal) WAN-IP-Adresse: 140.x.x.x Lokale IP-Adresse: 192.168.2.0/24	Router B (Remote) WAN-IP-Adresse: 145.x.x.x Lokale IP-Adresse: 10.1.1.0/24
Verbindungsname	**VPNTest**	**VPNTestB**
IPSec-Profil	**HomeOffice (hat die gleiche Konfiguration wie RemoteOffice)**	**RemoteOffice (hat die gleiche Konfiguration wie HomeOffice)**
Schnittstelle	WAN	WAN
Remote-Endgeräte	**Statische IP:**	**Statische IP: 140.x.x.x**

	145.x.x.x	
IKE-Authentifizierungsmethode	Vorinstallierter Schlüssel Vorinstallierter Schlüssel: CiscoTest123!	Vorinstallierter Schlüssel Vorinstallierter Schlüssel: CiscoTest123!
Lokaler Identifizierungstyp	Lokale WAN-IP	Lokale WAN-IP
Lokale Kennung	**140.x.x.x**	**145.x.x.x**
Lokaler IP-Typ	Subnetz	Subnetz
Lokale IP-Adresse	**192.168.2.0**	**10.1.1.0**
Lokale Subnetzmaske	255.255.255,0	255.255.255,0
Typ der Remote-Kennung	Remote-WAN-IP	Remote-WAN-IP
Remote-Kennung	**145.x.x.x**	**140.x.x.x**
Remote-IP-Typ	Subnetz	Subnetz
Remote-IP-Adresse	**10.1.1.0**	**192.168.2.0**
Remote-Subnetzmaske	255.255.255,0	255.255.255,0
Aggressive Mode	Deaktiviert	Deaktiviert

Weitere Informationen zum Konfigurieren des IPsec-Profils finden Sie im Artikel unter: Konfigurieren von IPSec-Profilen (Auto Keying Mode) auf dem RV160 und dem RV260.

Informationen zum Konfigurieren von Site-to-Site-VPN mithilfe des Setup-Assistenten finden Sie in folgendem Artikel: Konfigurieren des VPN-Setup-Assistenten auf dem RV160 und dem RV260.

Anwendbare Geräte

- RV160
- RV260

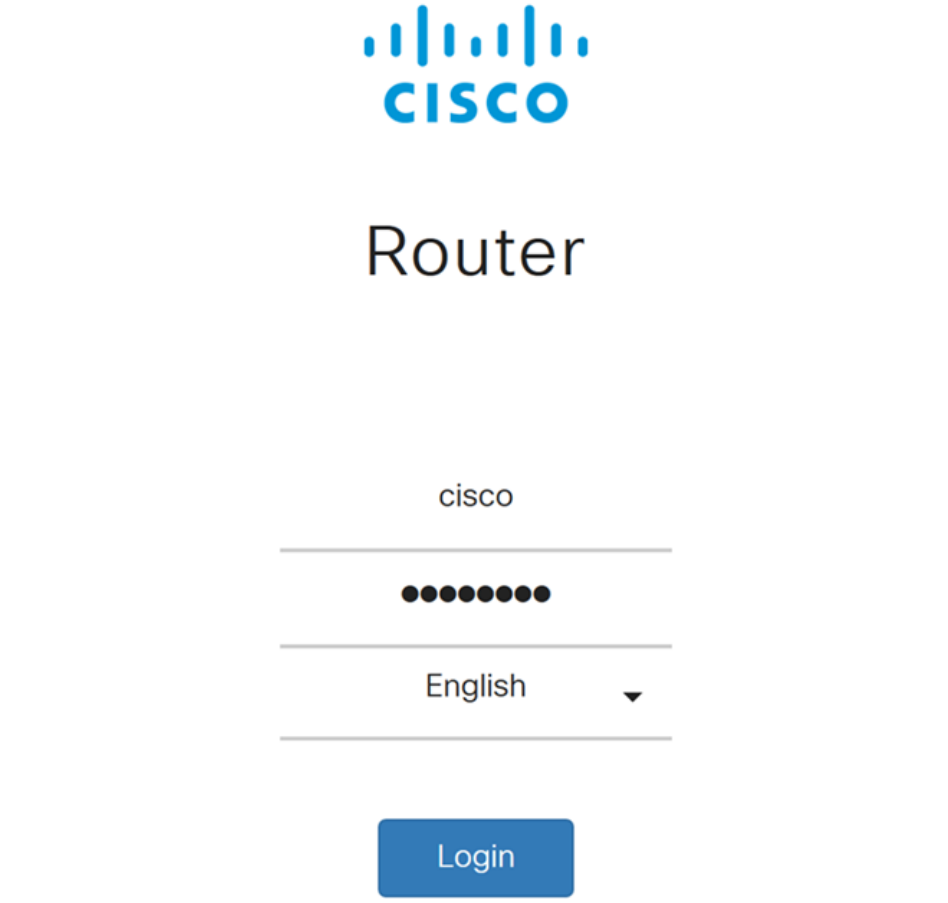
Softwareversion

- 1.0.00.13

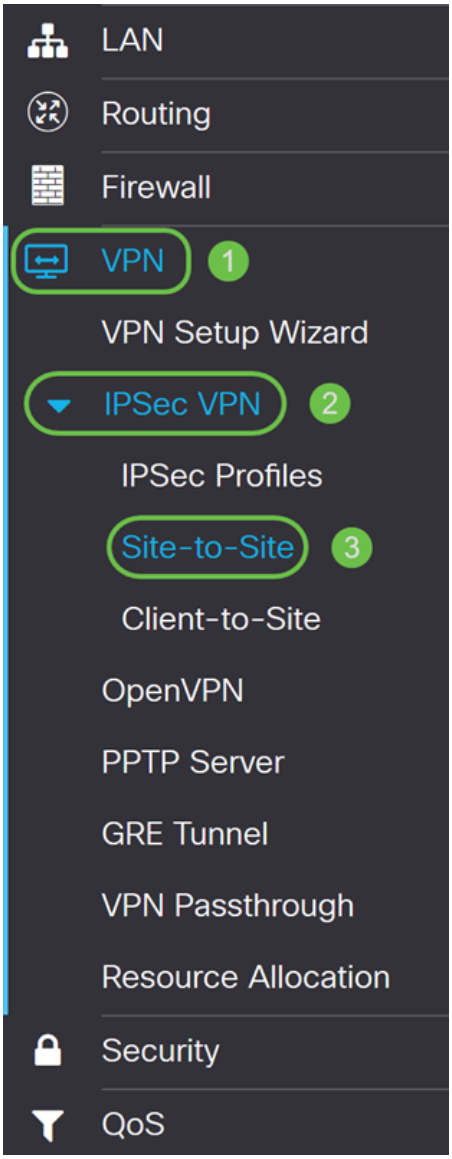
Konfigurieren der Site-to-Site-VPN-Verbindung - Router A

Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers A an.

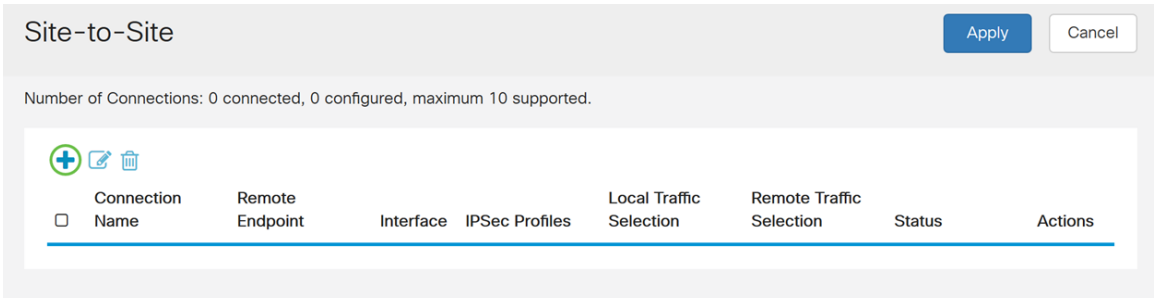
Hinweis: Für beide Router wird RV160 verwendet.



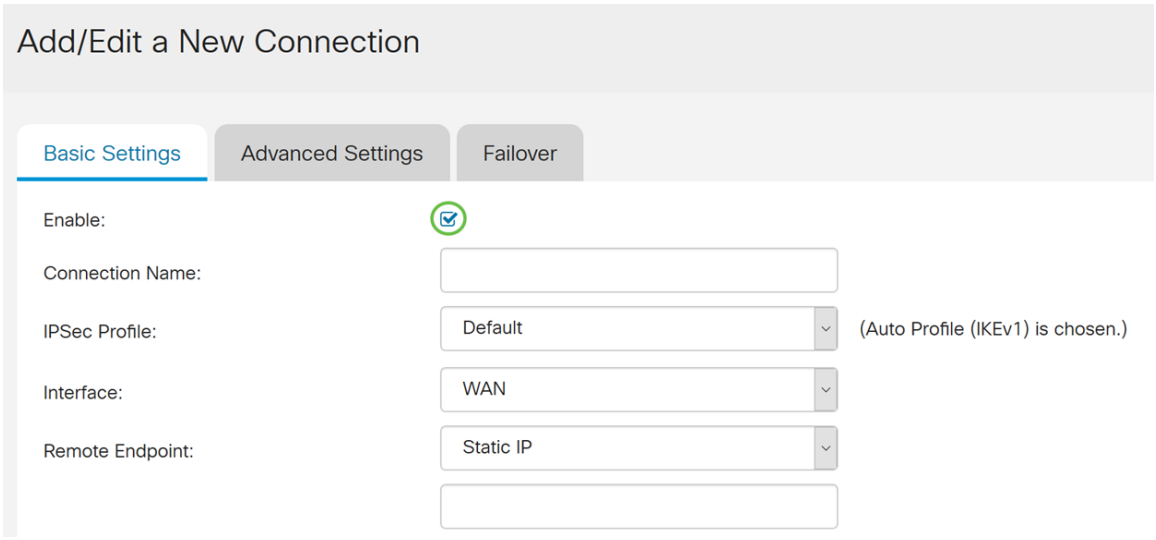
Schritt 2: Navigieren Sie zu **VPN > IPSec VPN > Site-to-Site**.



Schritt 3: Klicken Sie auf die **Add**-Schaltfläche, um eine neue Site-to-Site-VPN-Verbindung hinzuzufügen.

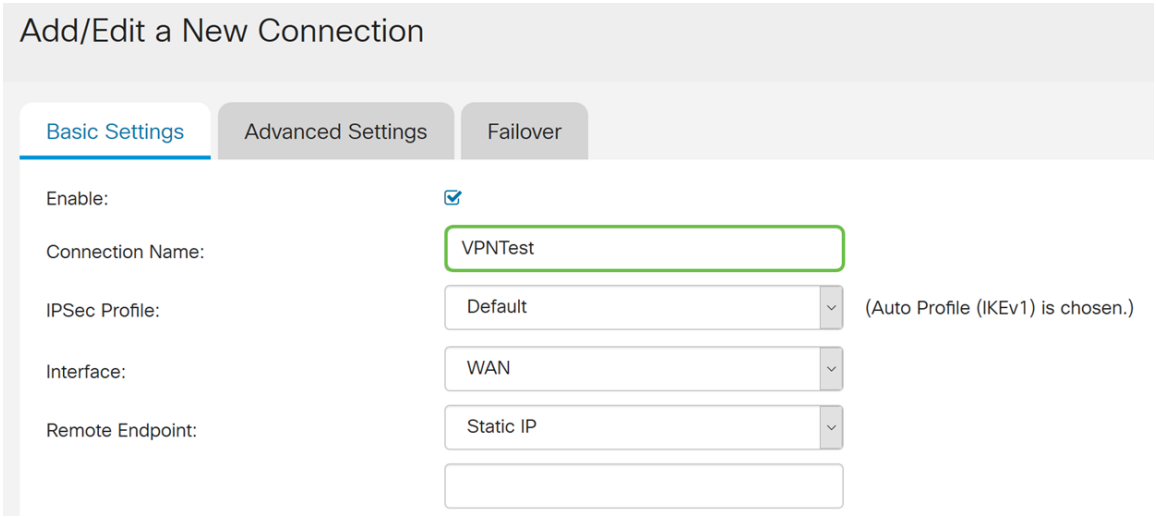


Schritt 4: Aktivieren Sie **Aktivieren**, um die Konfiguration zu aktivieren. Dies ist standardmäßig aktiviert.



Schritt 5: Geben Sie einen Verbindungsnamen für den VPN-Tunnel ein. Diese Beschreibung dient als Referenz und muss nicht mit dem am anderen Ende des Tunnels verwendeten Namen übereinstimmen.

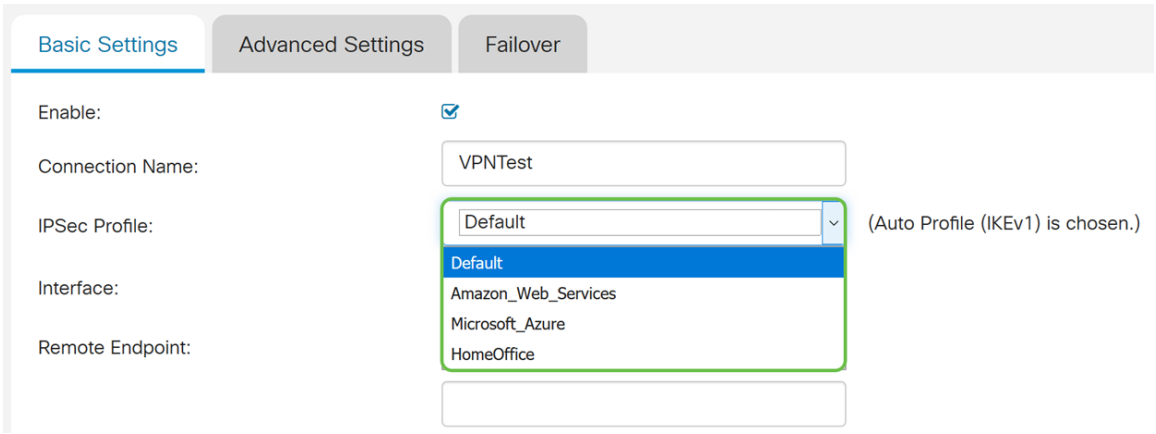
In diesem Beispiel geben wir **VPNTest** als unseren Verbindungsnamen ein.



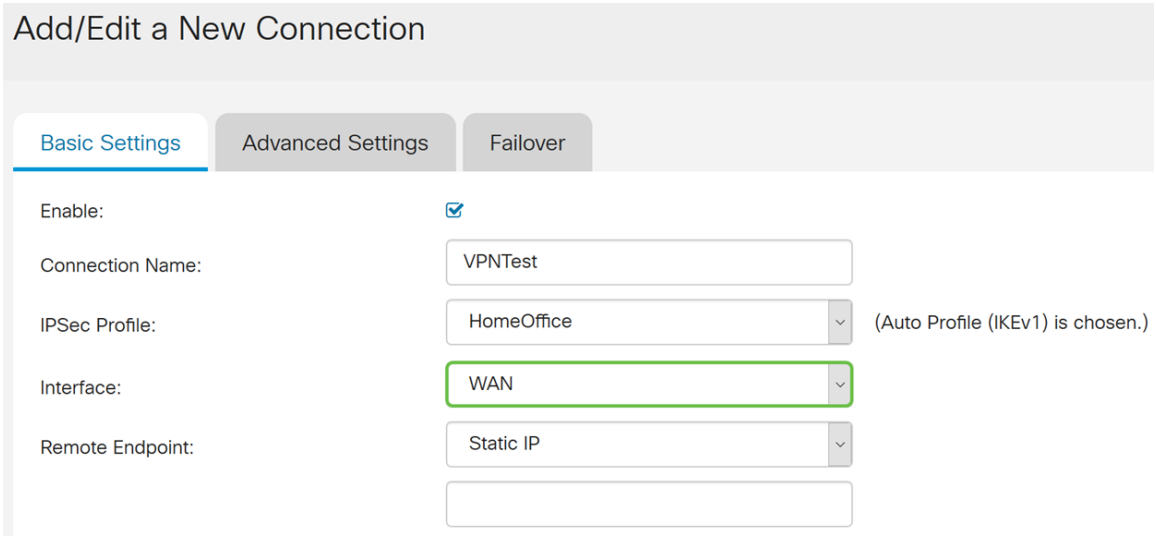
Schritt 6: Wenn Sie ein neues IPsec-Profil erstellt haben oder ein vorgefertigtes Profil verwenden möchten (Amazon_Web_Services, Microsoft_Azure), wählen Sie das IPsec-Profil aus, das Sie für das VPN verwenden möchten. Standardmäßig wird das Auto Profile ausgewählt. IPsec-Profil ist die zentrale Konfiguration in IPsec, die Algorithmen wie Verschlüsselung, Authentifizierung und DH-Gruppe (Diffie-Hellman) für Phase I- und Phase II-Aushandlung definiert.

In diesem Beispiel wählen wir **HomeOffice** als unser IPsec-Profil aus.

Hinweis: Weitere Informationen zum Erstellen eines IPsec-Profils finden Sie in folgendem Artikel: Konfigurieren von IPSec-Profilen (Auto Keying Mode) auf dem RV160 und dem RV260.

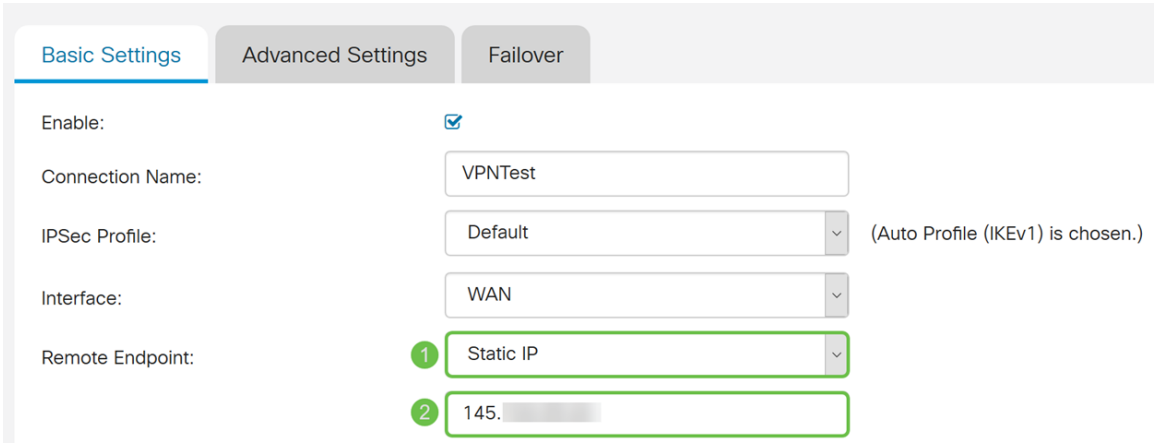


Schritt 7: Wählen Sie im Feld *Schnittstelle* die Schnittstelle aus, die für den Tunnel verwendet wird. In diesem Beispiel wird **WAN** als Schnittstelle verwendet.



Schritt 8: Wählen Sie entweder **Static IP**, **Fully Qualified Domain Name (FQDN)** oder **Dynamic IP** für den *Remote-Endpunkt aus*. Geben Sie die IP-Adresse oder den FQDN des Remote-Endpunkts entsprechend Ihrer Auswahl ein.

Wir haben die **statische IP** ausgewählt und die IP-Adresse unseres Remote-Endgeräts eingegeben.



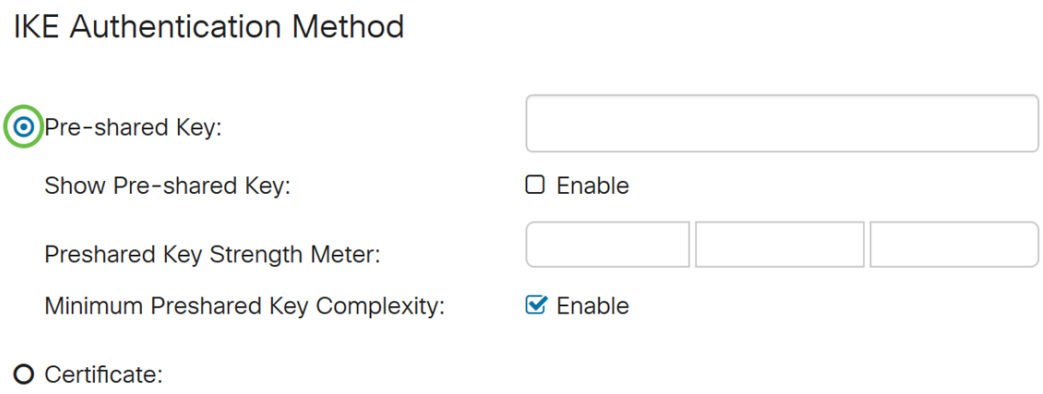
Konfigurieren der IKE-Authentifizierungsmethode

Schritt 1: Wählen Sie entweder **Pre-shared Key** oder **Certificate aus**. Für diese Demonstration wählen wir **Pre-shared Key** als IKE-Authentifizierungsmethode aus.

IKE-Peers authentifizieren sich gegenseitig durch Computing und Senden eines verschlüsselten Hashs von Daten, der den vorinstallierten Schlüssel enthält. Wenn der

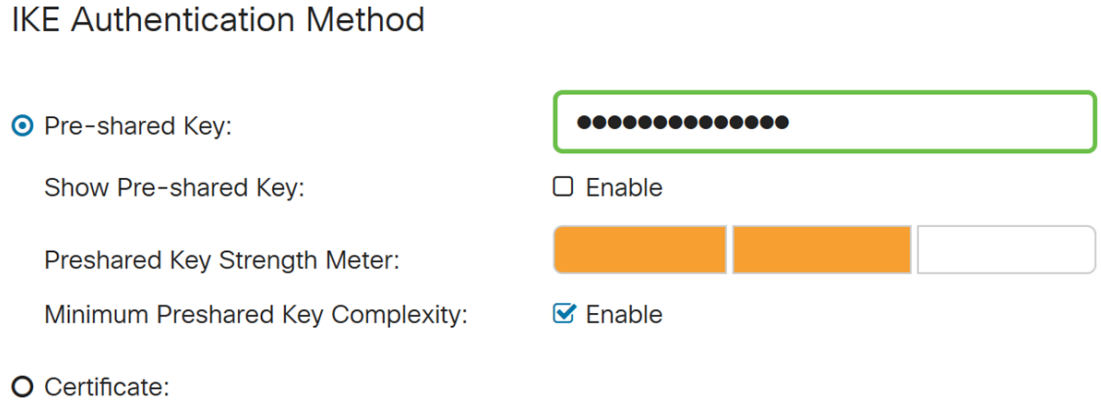
empfangende Peer in der Lage ist, den gleichen Hash unabhängig mithilfe seines vorinstallierten Schlüssels zu erstellen, weiß er, dass beide Peers denselben geheimen Schlüssel teilen und so den anderen Peer authentifizieren müssen. Vorinstallierte Schlüssel lassen sich nicht gut skalieren, da jeder IPsec-Peer mit dem vorinstallierten Schlüssel jedes anderen Peers konfiguriert werden muss, mit dem er eine Sitzung aufbaut.

Das digitale Zertifikat ist ein Paket, das Informationen wie die Identifizierung eines Zertifikatsinhabers enthält: Name oder IP-Adresse, die Seriennummer des Zertifikats, das Ablaufdatum 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. Wenn Sie **Zertifikat** ausgewählt haben, stellen Sie sicher, dass das signierte Zertifikat unter **Administration > Certificate** importiert wird. Wählen Sie das Zertifikat aus der Dropdown-Liste für lokal und remote aus.

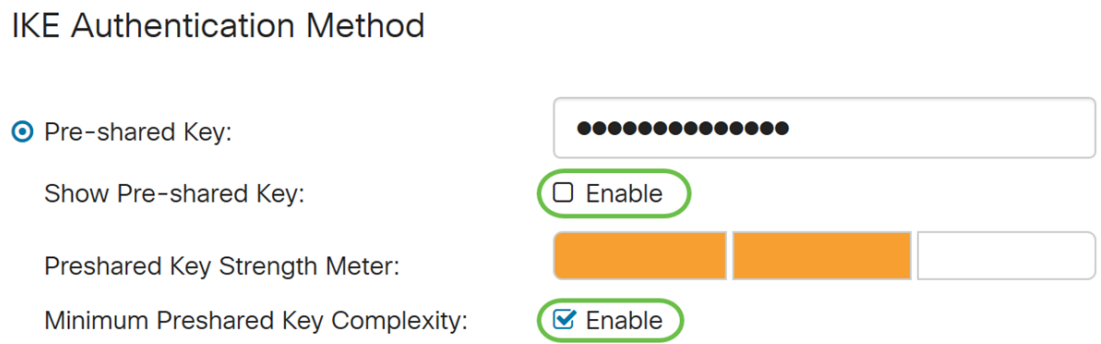


Schritt 2: Geben Sie im Feld *Vorinstallierter Schlüssel* einen vorinstallierten Schlüssel ein.

Hinweis: Stellen Sie sicher, dass der Remote-Router den gleichen vorinstallierten Schlüssel verwendet.

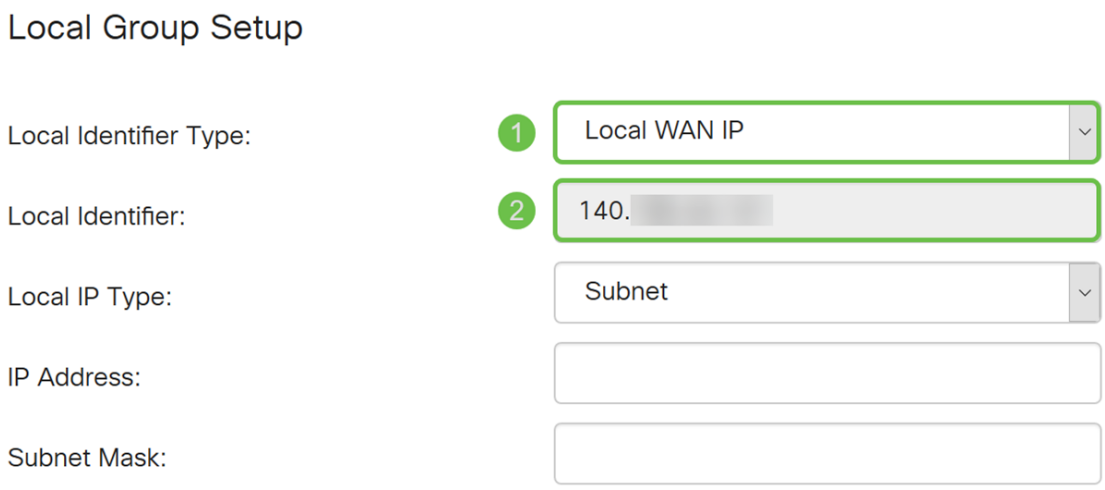


Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren**, wenn der vorinstallierte Schlüssel angezeigt werden soll. Das *Preshared Key Strength Meter* zeigt die Stärke des vorinstallierten Schlüssels durch farbige Balken an. Aktivieren Sie **Aktivieren**, um die minimale Komplexität des vorinstallierten Schlüssels zu aktivieren. Fahren Sie anschließend mit dem Abschnitt *für die Einrichtung der lokalen Gruppe fort*.



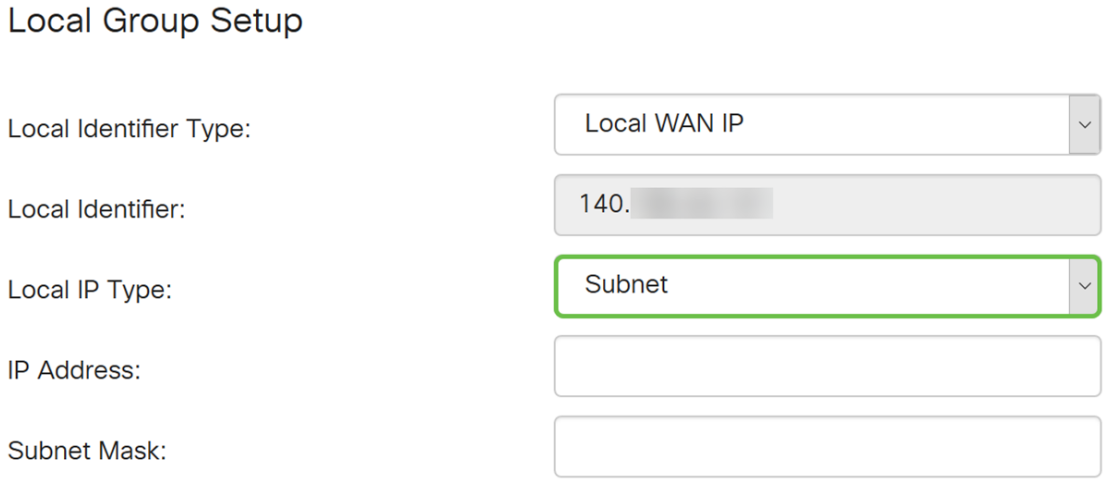
Für die lokale Gruppeneinrichtung

Schritt 1: Wählen Sie **Local WAN IP**, **IP Address**, **Local FQDN** oder **Local User FQDN** aus der Dropdown-Liste aus. Geben Sie den Identifikationsnamen oder die IP-Adresse basierend auf Ihrer Auswahl ein. Wenn Sie **Local WAN IP** ausgewählt haben, sollte die WAN-IP-Adresse Ihres Routers automatisch eingegeben werden.



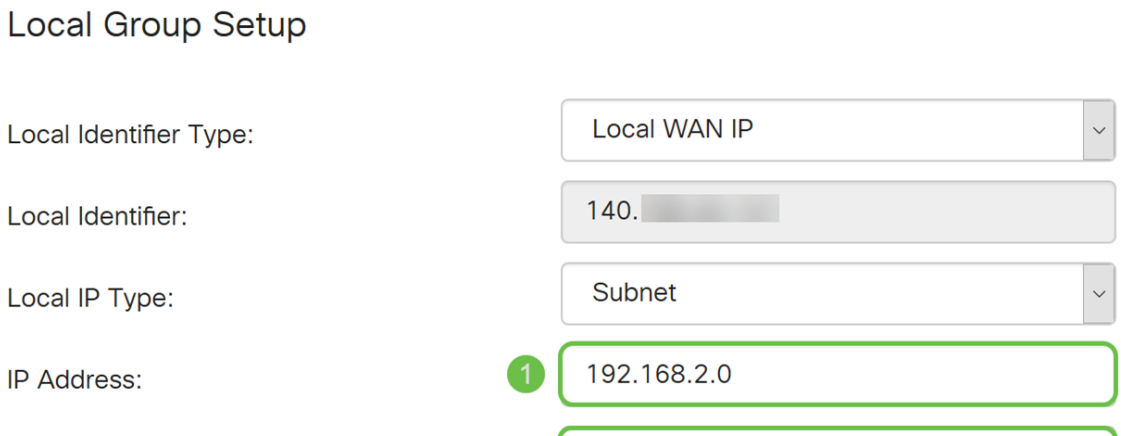
Schritt 2: Wählen Sie für den *lokalen IP-Typ* **Subnetz**, **Single**, **Any**, **IP Group oder GRE Interface aus der Dropdown-Liste aus.**

In diesem Beispiel wurde **Subnetz** ausgewählt.



Schritt 3: Geben Sie die IP-Adresse des Geräts ein, das diesen Tunnel verwenden kann. Geben Sie dann die Subnetzmaske ein.

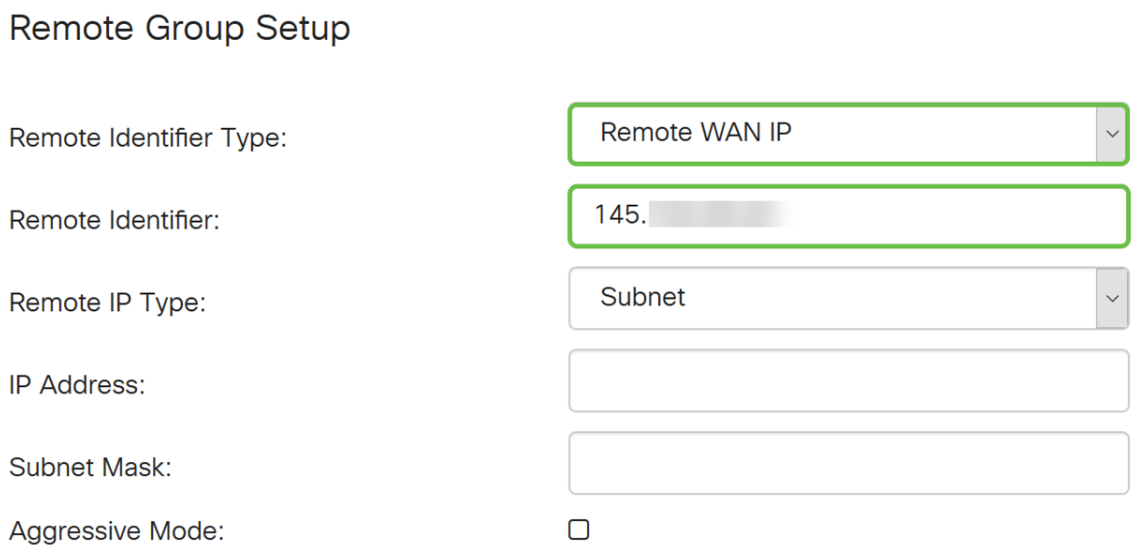
Für diese Demonstration geben Sie **192.168.2.0** als lokale IP-Adresse und **255.255.255.0** für die Subnetzmaske ein.



Remote-Gruppeneinrichtung

Schritt 1: Wählen Sie **Remote WAN IP**, **Remote FQDN** oder **Remote User FQDN** aus der Dropdown-Liste aus. Geben Sie den Identifikationsnamen oder die IP-Adresse basierend auf Ihrer Auswahl ein.

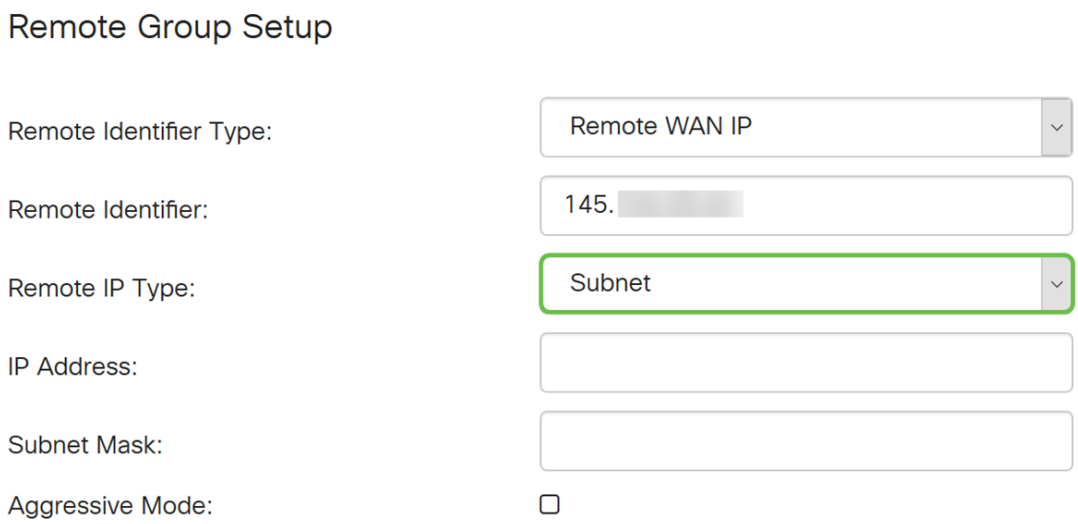
Wir haben **Remote WAN IP** als *Remote Identifier Type* ausgewählt und in die IP-Adresse des Remote-Routers eingegeben.



Schritt 2: Wählen Sie **Subnet**, **Single**, **Any**, **IP Group** aus der *Dropdown-Liste Remote-IP-Typ aus.*

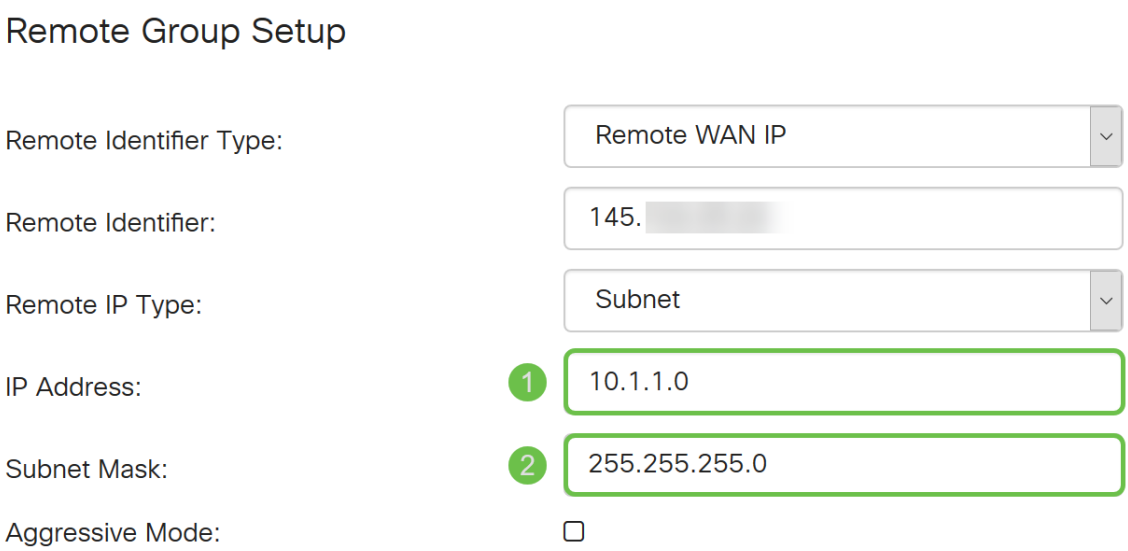
In diesem Beispiel wählen wir **Subnet** aus.

Hinweis: Wenn Sie IP Group (IP-Gruppe) als Remote-IP-Typ ausgewählt haben, wird ein Popup-Fenster zum Erstellen einer neuen IP-Gruppe angezeigt.



Schritt 3: Geben Sie die lokale Remote-IP-Adresse und die Subnetzmaske des Geräts ein, das diesen Tunnel verwenden kann.

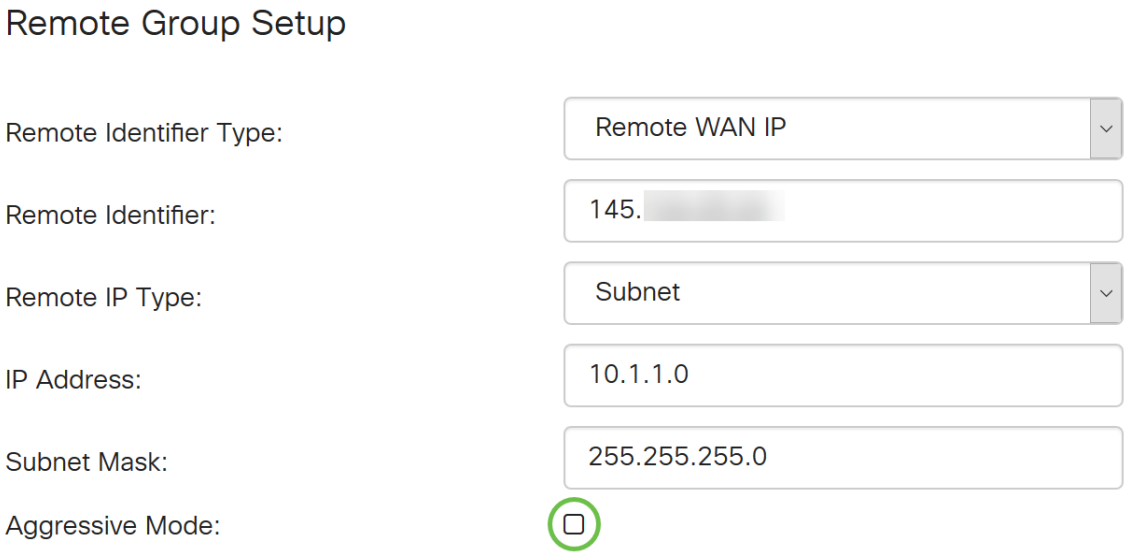
Wir haben **10.1.1.0** für die lokale Remote-IP-Adresse eingegeben, die diesen Tunnel und die Subnetzmaske **255.255.0** verwenden kann.



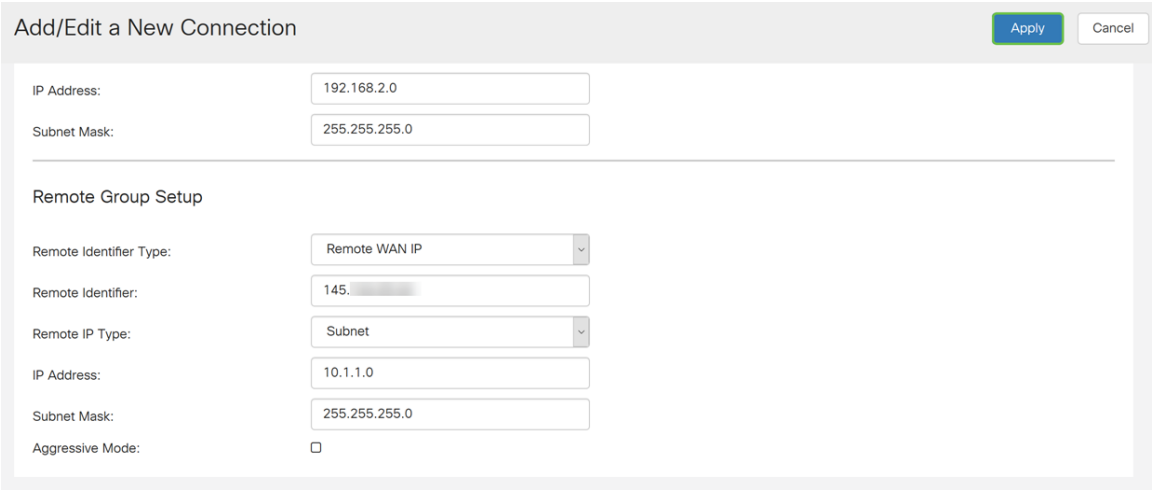
Schritt 4: Aktivieren Sie das Kontrollkästchen, um den aggressiven Modus zu aktivieren. Der aggressive Modus ist der Fall, wenn die Aushandlung für IKE SA in drei Pakete komprimiert wird, wobei alle SA-erforderlichen Daten vom Initiator übergeben werden müssen. Die Verhandlung ist schneller, aber sie haben eine Verwundbarkeit des Austauschs von Identitäten im Klartext.

In diesem Beispiel lassen wir es ungeprüft.

Hinweis: Weitere Informationen zum Hauptmodus und aggressiven Modus finden Sie unter: [Hauptmodus vs. aggressiver Modus]



Schritt 5: Klicken Sie auf **Apply**, um eine neue Site-to-Site-VPN-Verbindung zu erstellen.

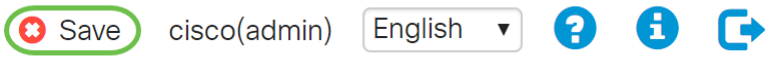


Schlussfolgerung

Sie sollten jetzt erfolgreich eine neue Site-to-Site-VPN-Verbindung für Ihren lokalen Router hinzugefügt haben. Sie müssen den Remote-Router (Router B) mithilfe der Rückinformationen konfigurieren.

Alle Konfigurationen, die der Router derzeit verwendet, befinden sich in der Running Configuration-Datei, die flüchtig ist, da sie zwischen Neustarts nicht beibehalten wird.

Schritt 1: Klicken Sie oben auf der Seite auf die Schaltfläche **Speichern**, um zur *Konfigurationsverwaltung* zu navigieren, um die aktuelle Konfiguration in der Startkonfiguration zu speichern. Dadurch wird die Konfiguration zwischen Neustarts beibehalten.



Schritt 2: Vergewissern Sie sich im *Konfigurationsmanagement*, dass die *Quelle* die **Konfiguration ausführt** und das *Ziel* die **Startkonfiguration** *ist*. Drücken Sie anschließend **Apply**, um die aktuelle Konfiguration in der Startkonfiguration zu speichern. Alle Konfigurationen, die der Router derzeit verwendet, befinden sich in der Running Configuration-Datei, die flüchtig ist und zwischen Neustarts nicht beibehalten wird. Beim Kopieren der Running Configuration-Datei in die Startkonfigurationsdatei wird die gesamte Konfiguration zwischen Neustarts beibehalten.