Site-to-site VPN configureren op de RV160 en RV260

Doel

Het doel van dit document is om een site-to-site VPN te maken op de RV160- en RV260-Series routers.

Inleiding

Een Virtual Private Network (VPN) is een goede manier om externe medewerkers aan te sluiten op een beveiligd netwerk. Een VPN kan een externe host inschakelen om op te treden alsof ze was verbonden met het beveiligde onsite netwerk. In een site-to-site VPN sluit de lokale router op één locatie zich aan op een externe router door een VPN-tunnel. Deze tunnel kapselt gegevens veilig in door middel van industriestandaard encryptie- en authenticatietechnieken om verzonden gegevens te beveiligen.

Merk op dat wanneer u site-to-site VPN configureren het LAN-subnetwerk (Local Area Network) aan weerszijden van de tunnel niet op hetzelfde netwerk kunt zijn. Bijvoorbeeld, als het LAN van de Site A LAN 192.168.***1***.x/24 Subnet gebruikt, kan Site B niet het zelfde net gebruiken. Site B moet een andere vorm gebruiken zoals 192.168.***2***.x/24.

Om een tunnel goed te configureren voert u corresponderende instellingen in (lokale en afstandsbediening) bij het configureren van de twee routers. Stel dat deze router als router A. wordt geïdentificeerd Voer de instellingen ervan in de sectie Setup Local Group in terwijl u de instellingen voor de andere router (router B) in het gedeelte Remote Group Setup invoert. Wanneer u de andere router (router B) vormt, voer dan de instellingen in de sectie Local Group Setup in en voer de instellingen Router A in de instelling Remote Group in.

Hieronder is een tabel van de configuratie voor zowel router A als router B, die in vet is gemarkeerd, zijn parameters die het omgekeerde van de tegenoverliggende router zijn. Alle andere parameters blijven hetzelfde. In dit document zullen we de lokale router configureren met behulp van router A.

Velden	router A (lokaal) WAN IP-adres: 140.x.x Lokaal IP-adres: 192.168.2.0/24	router B (Remote) WAN IP-adres: 145.x.x Lokaal IP-adres: 10.1.1.0/24
Naam van verbinding	**VPNest**	**VPNestB**
IPsec-profiel	**HomeOffice (heeft dezelfde configuratie als RemoteOffice)**	**RemoteOffice (heeft dezelfde configuratie als HomeOffice)**
Interface	WAN	WAN
Remote-endpoint	**Statische IP: 145.x.x**	**Statische IP: 140.x.x**
IKE-verificatiemethode	Vooraf gedeelde sleutel Vooraf gedeelde sleutel: CiscoTest123!	Vooraf gedeelde sleutel Vooraf gedeelde sleutel: CiscoTest123!
Type lokale identificator	Lokale WAN IP	Lokale WAN IP
Lokale identificator	**140.x.x**	**145.x.x**
Lokaal IP-type	Subnet	Subnet
Lokaal IP-adres	**192.168.2.0**	**10.1.1.0**

Lokale subnetmasker	255.255.255.0	255.255.255.0
Type afstandsidentificatie	Remote WAN IP	Remote WAN IP
Afstandsidentificatie	**145.x.x**	**140.x.x**
Remote IP-type	Subnet	Subnet
Remote IP-adres	**10.1.1.0**	**192.168.2.0**
Remote-subnetmasker	255.255.255.0	255.255.255.0
Aggressief Mode	Uitgeschakeld	Uitgeschakeld

U kunt leren hoe u IPsec-profiel wilt configureren via het artikel op: IPsec-profielen configureren (Auto Keying Mode) op de RV160 en RV260.

Om site-to-Site VPN te configureren met behulp van de wizard, raadpleegt u het artikel op: VPN Setup-wizard configureren op RV160 en RV260.

Toepasselijke apparaten

RV160

RV260

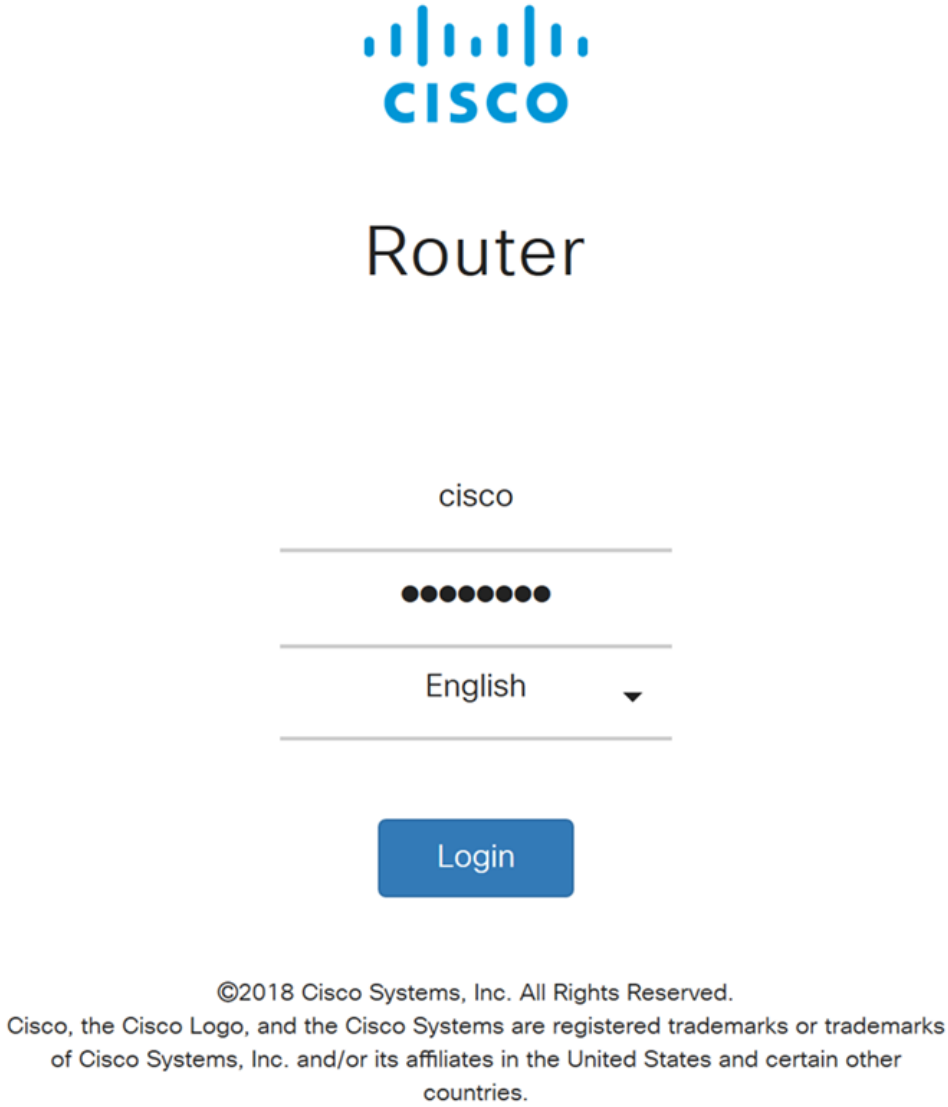
Softwareversie

·1.0.00.13

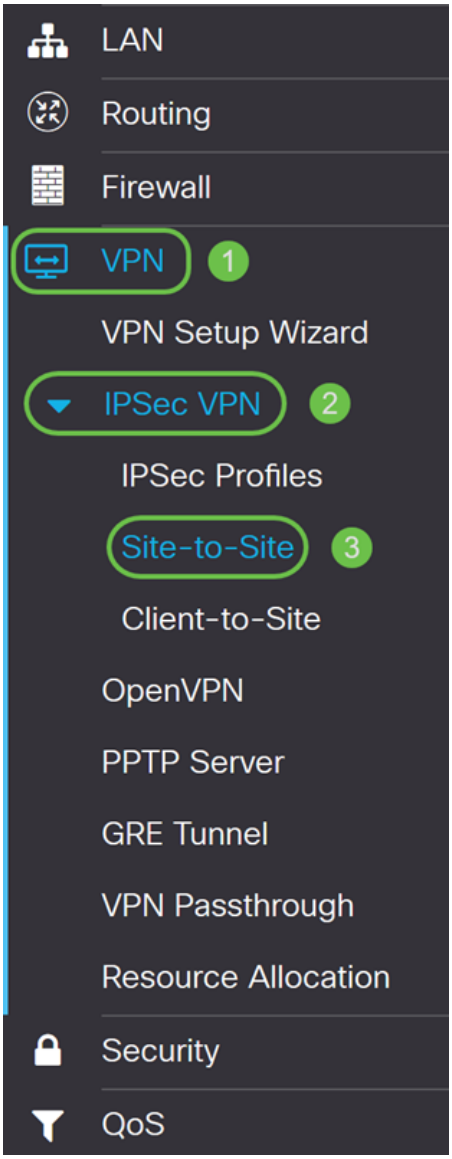
De verbinding van site-to-site VPN - router A

Stap 1. Meld u aan bij de webconfiguratie van uw router A.

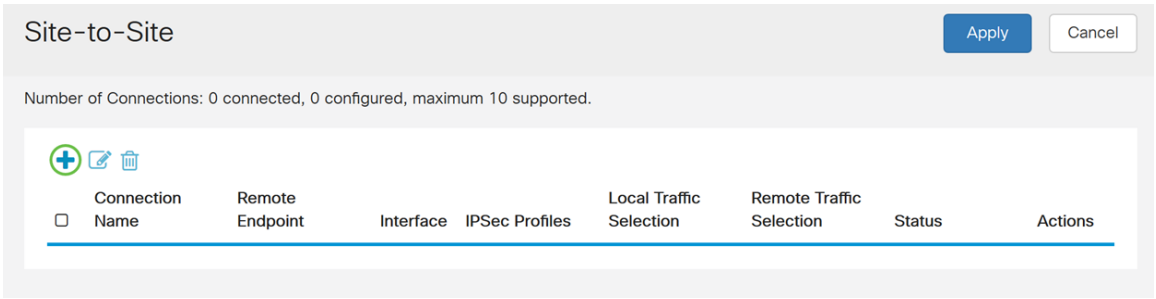
Opmerking: We zullen RV160 voor beide routers gebruiken.



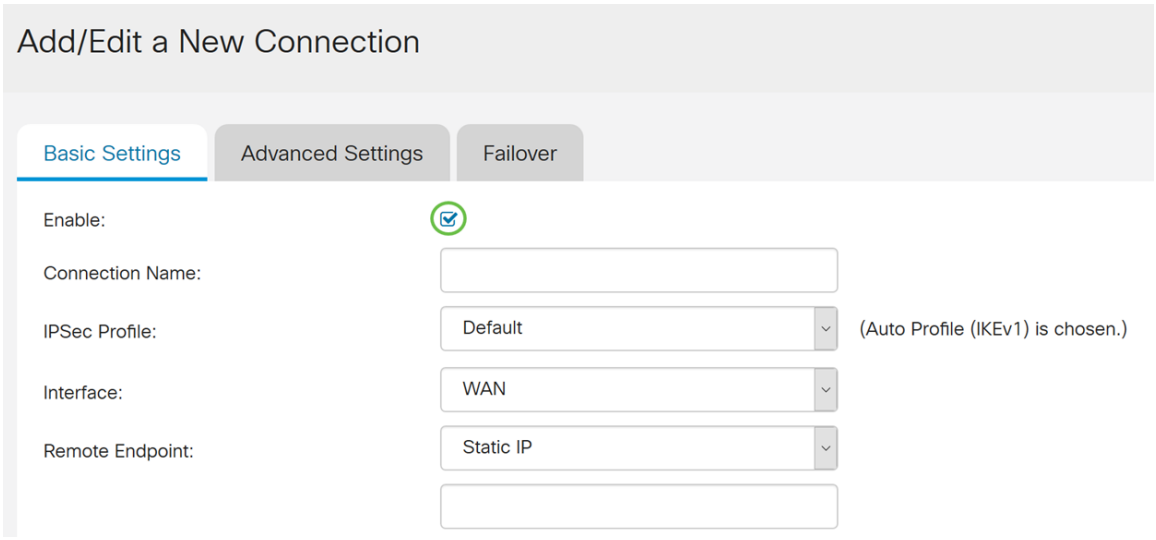
Stap 2. Navigeer naar **VPN > IPSec VPN > Site-to-Site**.



Stap 3. Klik op de knop Toevoegen om een nieuwe Site-to-Site VPN-verbinding toe te voegen.

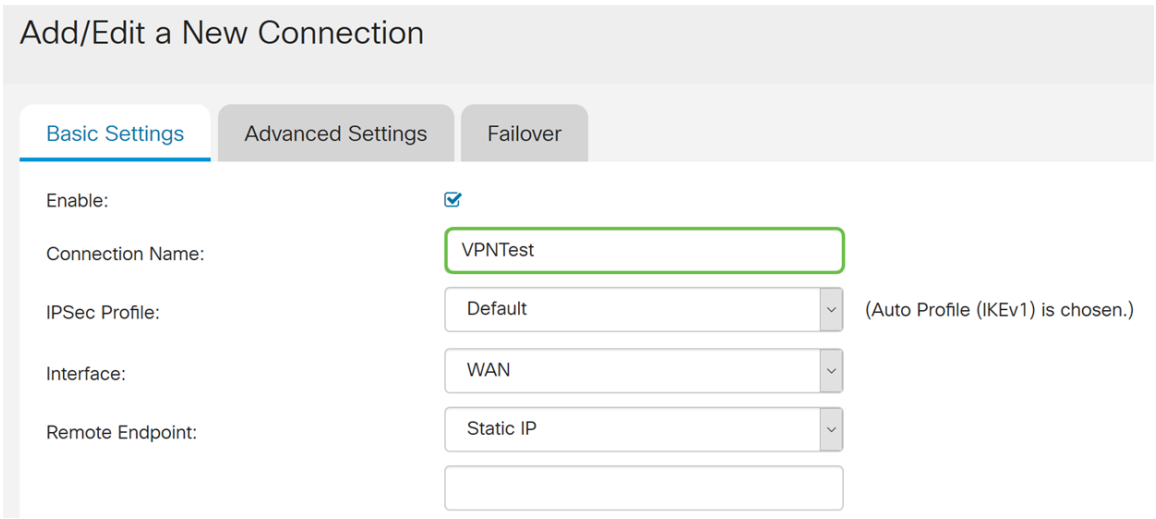


Stap 4. Controleer de configuratie inschakelen. Dit is standaard ingeschakeld.



Stap 5. Voer een verbindingsnaam in voor de VPN-tunnel. Deze beschrijving is bedoeld voor referentiedoeleinden en hoeft niet overeen te komen met de naam die aan het andere uiteinde van de tunnel wordt gebruikt.

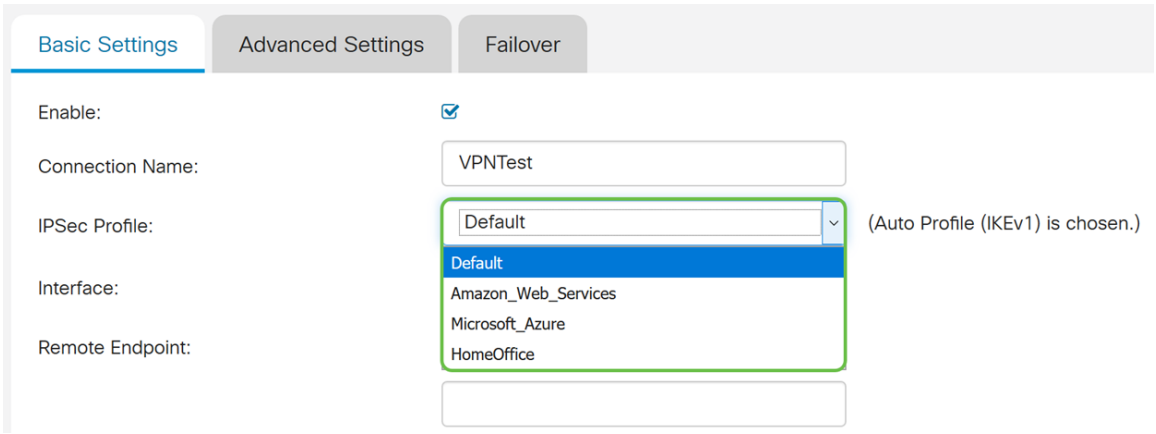
In dit voorbeeld gaan we **VPNTest** in als onze verbindingsnaam.



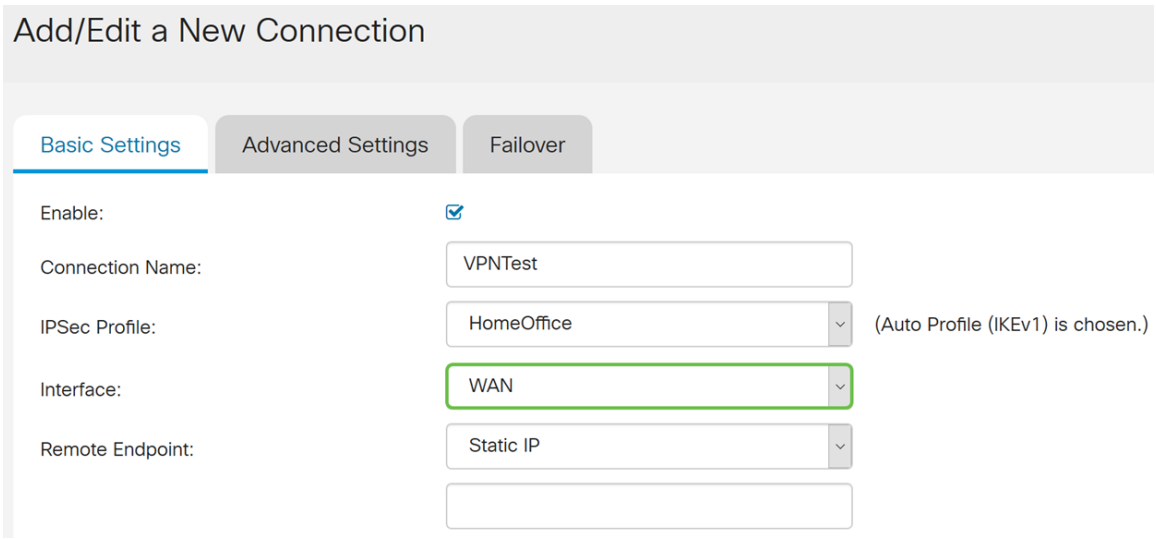
Stap 6. Als u een nieuw IPsec-profiel hebt gemaakt of u een vooraf gemaakt profiel wilt gebruiken (Amazon_Web_Services, Microsoft_Messenger), selecteert u het IPsec-profiel dat u voor VPN wilt gebruiken. De standaardinstelling - Het automatische profiel wordt standaard geselecteerd. IPsec-profiel is de centrale configuratie in IPsec die de algoritmen definieert zoals encryptie, verificatie en Diffie-Hellman (DH) voor fase I en fase II onderhandeling.

Bijvoorbeeld, zullen we **HomeOffice** selecteren als ons IPsec-profiel.

Opmerking: Als u meer wilt weten over het maken van een IPsec-profiel, raadpleegt u het artikel: IPsec-profielen configureren (Auto Keying Mode) op de RV160 en RV260.

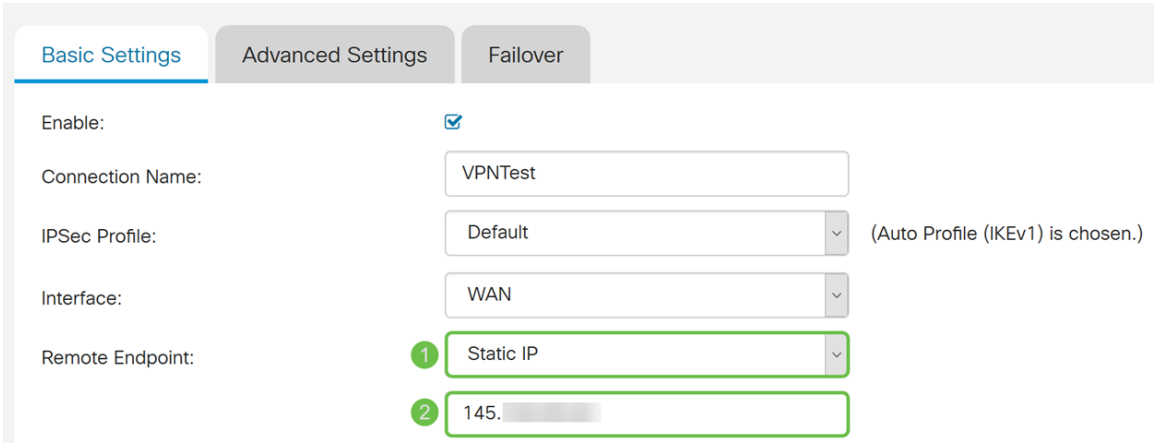


Stap 7. Selecteer in het veld *Interface* de interface die voor de tunnel wordt gebruikt. In dit voorbeeld zullen we **WAN** gebruiken als onze interface.



Stap 8. Selecteer ofwel **Statische IP**, **Full Qualified Domain Name (FQDN)** of **Dynamic IP** voor *Remote Endpoint*. Voer in het IP-adres of FQDN van het externe eindpunt in op basis van uw selectie.

We hebben **Statische IP** geselecteerd en in ons IP-adres van het externe eindpunt ingevoerd.



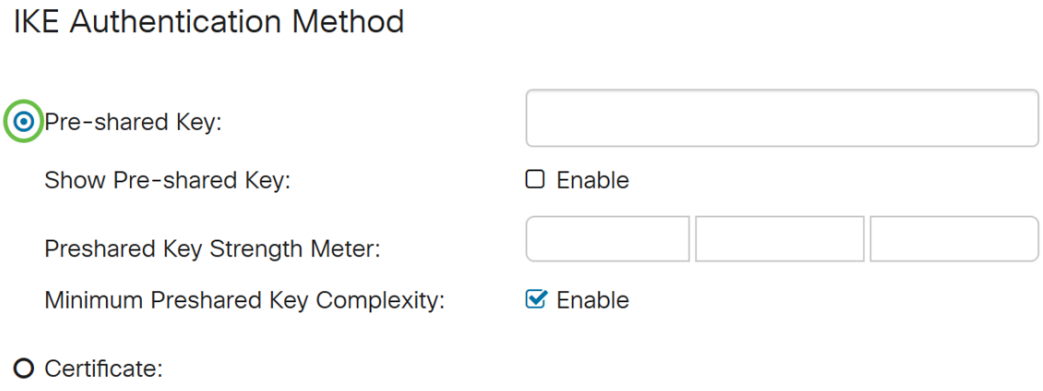
IKE-verificatiemethode configureren

Stap 1. Selecteer een **voorgedeelde sleutel** of een **certificaat**. Voor deze demonstratie zullen we **Pre-Shared Key** selecteren als onze IKE-authenticatiemethode.

IKE-peers authenticeren elkaar door keiharde data te berekenen en te verzenden die de vooraf gedeelde sleutel bevatten. Als het ontvangende peer in staat is om het zelfde hash

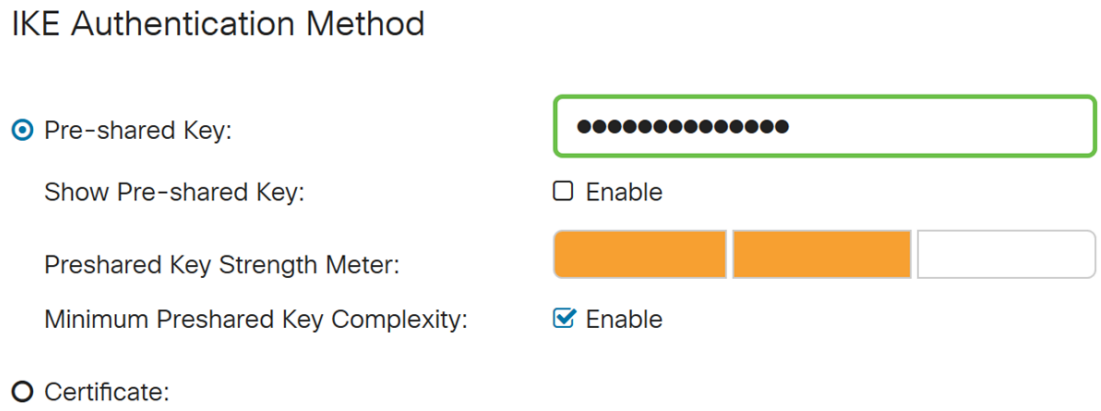
onafhankelijk te creëren met gebruik van zijn pre-gedeelde sleutel, weet het dat beide peers het zelfde geheim moeten delen en zo het andere peer authentiek te verklaren. Vooraf gedeelde toetsen schalen niet goed omdat elke IPsec-peer moet worden geconfigureerd met de voorgedeelde toets van elke andere peer waarmee deze een sessie vastlegt.

Het digitale certificaat is een pakket dat informatie bevat, zoals de identificatie van een certificaathouder: naam of IP-adres, het serienummer van het certificaat, de vervaldatum van het certificaat en een kopie van de openbare sleutel van de houder van het certificaat. De standaard digitale certificaatindeling is gedefinieerd in de X.509-specificatie. X.509 versie 3 definieert de gegevensstructuur voor certificaten. Als u **Certificaat** hebt geselecteerd, moet u ervoor zorgen dat uw ondertekende certificaat in **Beheer > Certificaat** wordt geïmporteerd. Selecteer het certificaat in de vervolgkeuzelijst voor zowel de lokale als de afstandsbediening.

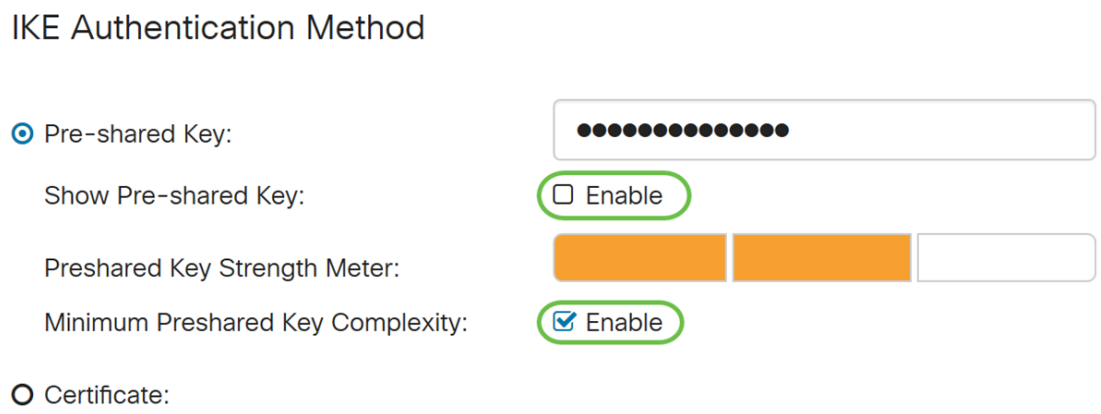


Stap 2. Voer in het veld *Voorgedeelde sleutel* in een vooraf gedeelde toets.

Opmerking: Zorg ervoor dat de externe router dezelfde pre-gedeelde sleutel gebruikt.

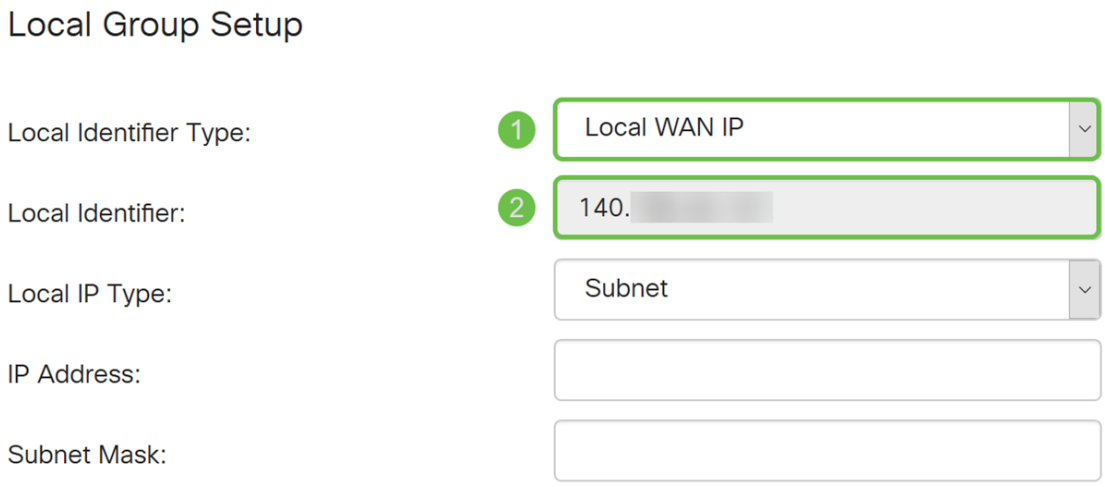


Stap 3. Controleer het selectieteken **Enable** (inschakelen) als u de voorgedeelde toets wilt weergeven. De *PreShared Key Sterker Meter* toont de kracht van de vooraf gedeelde toets door gekleurde staven. Controleer **Schakel** in om de minimale pre-gedeelde sleutelcomplexiteit mogelijk te maken. Sla vervolgens over naar *het* gedeelte *Local Group Setup*.



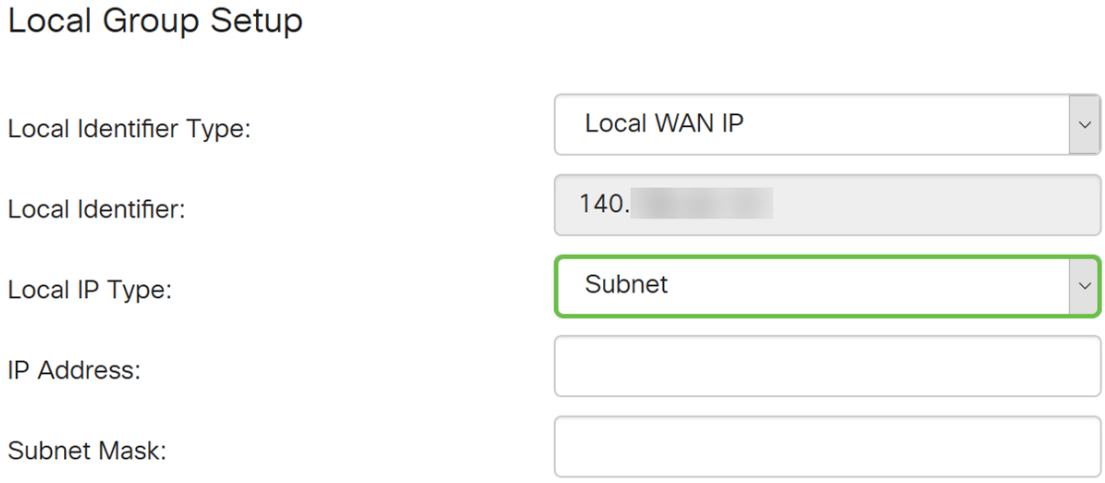
Instellen lokale groep

Stap 1. Selecteer **Lokale WAN-IP**, **IP-adres**, **Lokale FQDN**, of **Lokale gebruiker FQDN** in de vervolgkeuzelijst. Voer de identificatienaam of het IP-adres in op basis van uw selectie. Als u **Lokale WAN-IP** hebt geselecteerd, zal het WAN IP-adres van uw router automatisch worden ingevoerd.



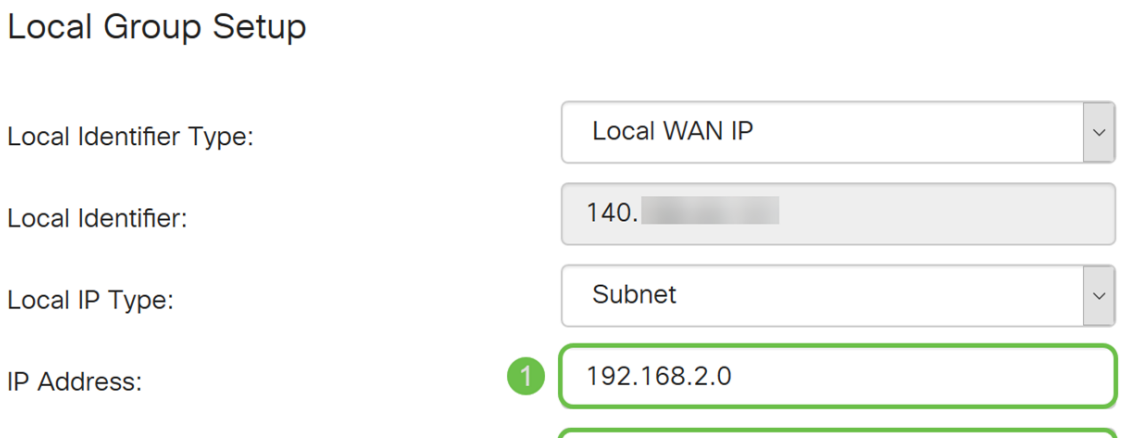
Stap 2. Voor het *lokale IP-type* selecteert u **Subnet**, **Single**, **Any**, **IP-groep of GRE-interface in de vervolgkeuzelijst.**

In dit voorbeeld werd **Subnet** gekozen.



Stap 3. Voer het IP-adres in van het apparaat dat deze tunnel kan gebruiken. Voer dan het subnetmasker in.

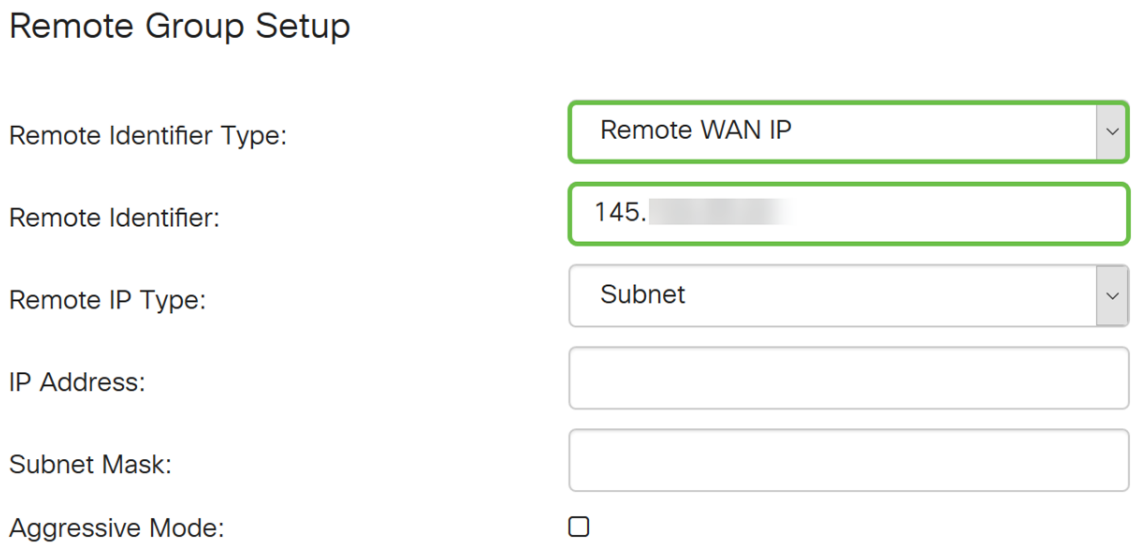
Voor deze demonstratie gaan we **192.168.2.0** in als ons lokale IP-adres en **255.255.255.0** voor het subnetmasker.



Instellen afstandsgroep

Stap 1. Selecteer **Remote WAN IP**, **Remote FQDN**, of **Remote User FQDN** in de vervolgkeuzelijst. Voer de identificatienaam of het IP-adres in op basis van uw selectie.

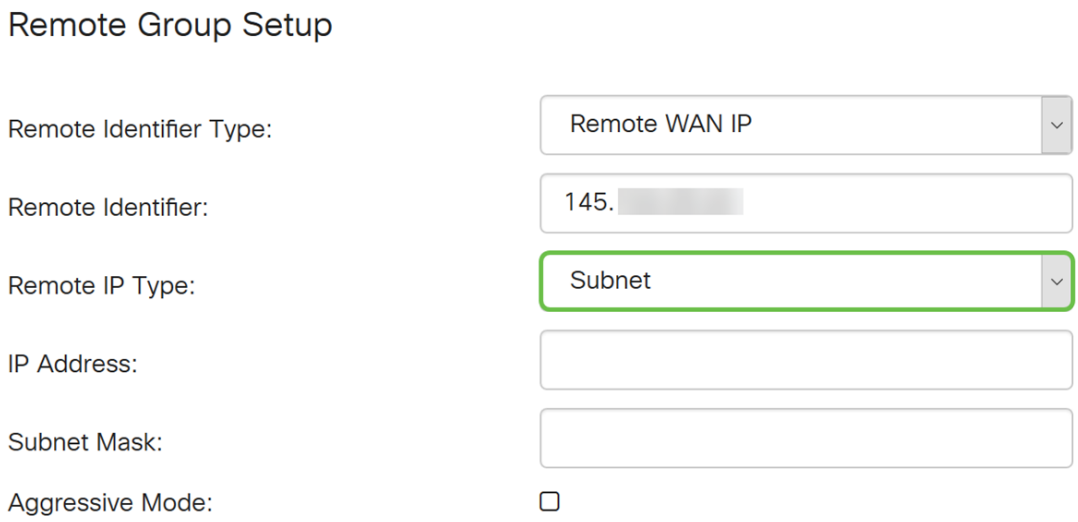
We hebben **Remote WAN IP** geselecteerd als ons *Remote Identifier-type* en zijn in het IP-adres van de externe router ingevoerd.



Stap 2. Selecteer **Subnet**, **Enkelvoudig**, **Any**, **IP-groep** in de *vervolgkeuzelijst Afgelegen IP-type.*

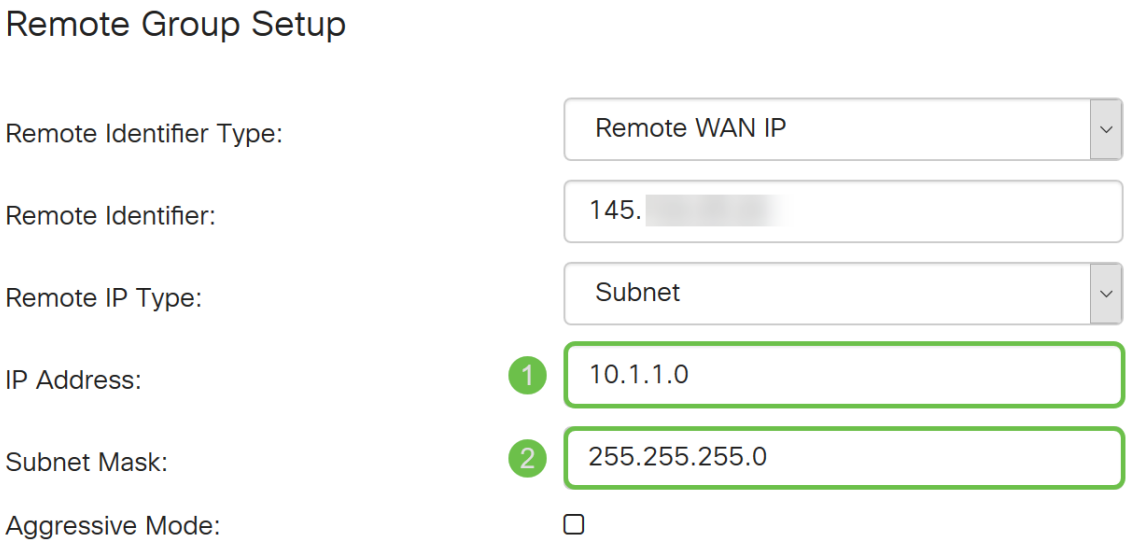
In dit voorbeeld selecteren we **Subnet**.

Opmerking: Als u IP Group als uw externe IP-type hebt geselecteerd, verschijnt een pop-upvenster om een nieuwe IP-groep te maken.



Stap 3. Voer het lokale IP-adres en het subnetmasker op afstand in van het apparaat dat deze tunnel kan gebruiken.

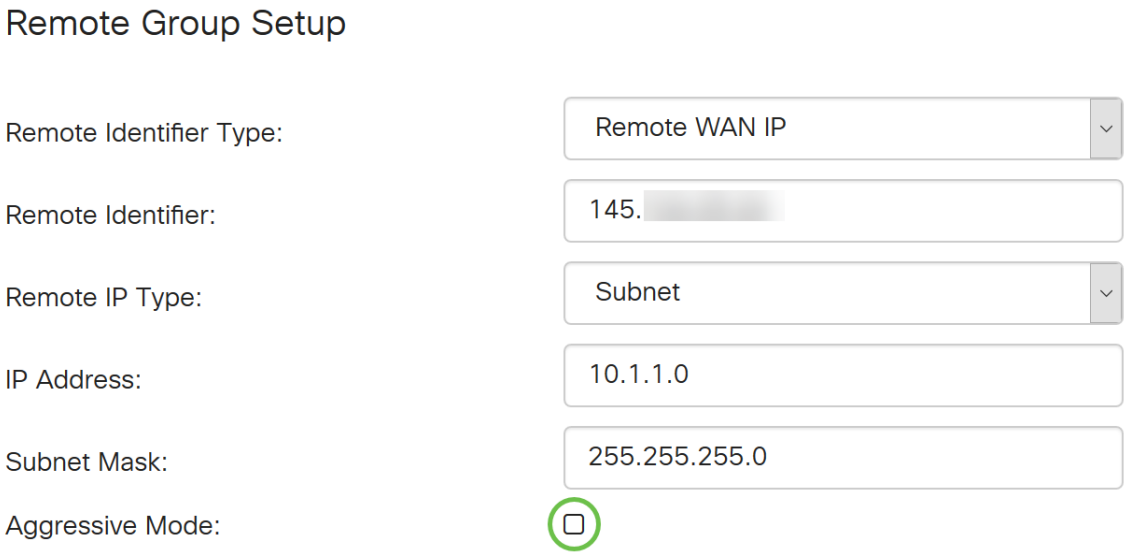
We zijn **10.1.1.0** ingevoerd voor het lokale IP-adres op afstand dat deze tunnel en het subnetmasker van **255.255.255.0** kan gebruiken.



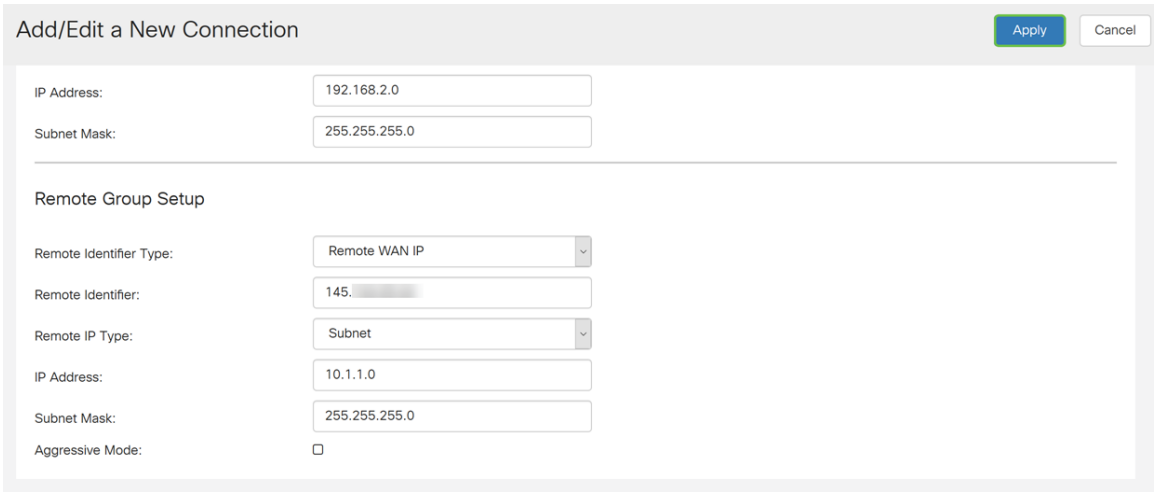
Stap 4. Controleer het vakje om de agressieve modus te activeren. De agressieve modus is wanneer de onderhandeling voor IKE SA gecomprimeerd is in drie pakketten met alle SA vereiste gegevens die door de initiatiefnemer moeten worden doorgegeven. De onderhandelingen verlopen sneller, maar hebben in duidelijke tekst een kwetsbaarheid voor uitwisselingsidentiteiten.

In dit voorbeeld laten we het ongecontroleerd.

Opmerking: Extra informatie voor hoofdmodus vs agressieve modus, zie: Hoofdmode VS Aggressief Mode



Stap 5. Klik op **Toepassen** om een nieuwe Site-to-Site VPN-verbinding te maken.

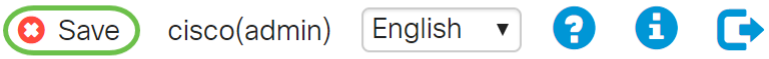


Conclusie

U zou nu met succes een nieuwe verbinding van Site-to-Site VPN voor uw lokale router moeten toevoegen. U zou uw afstandsrouter (router B) moeten configureren met behulp van de omgekeerde informatie.

Alle configuratie die de router momenteel gebruikt, bevindt zich in het configuratiebestand dat vluchtig is in de zin dat het niet tussen de herstart blijft behouden.

Stap 1. Klik boven op de pagina op de knop **Opslaan** om in het *Configuratiebeheer* te navigeren om de actieve configuratie in de opstartconfiguratie op te slaan. Dit is om de configuratie tussen de herstart te behouden.



Stap 2. *Controleer* in het *Configuratiebeheer* of de *bron* **de configuratie uitvoert** en *de bestemming* **de opstartconfiguratie** is**.** Druk vervolgens op **Toepassen** om de actieve configuratie op te slaan. Alle configuratie die de router momenteel gebruikt, bevindt zich in het configuratiebestand dat vluchtig is en niet tussen de herstart blijft behouden. Het kopiëren van het Configuration-bestand dat naar het opstartconfiguratiesbestand wordt uitgevoerd, behoudt alle configuratie tussen de herstart.