

Configuratie van een site-to-site Virtual Private Network (VPN)-verbinding op een RV340 of RV345-router

Doel

Een Virtual Private Network (VPN) is de verbinding tussen het lokale netwerk en een externe host via het internet. De lokale en externe hosts kunnen een computer zijn, of een ander netwerk waarvan de instellingen gesynchroniseerd zijn om te kunnen communiceren. Dit geldt voor alle typen VPN. Meestal geeft het beide netwerken toegang tot de resources aan beide zijden van de verbinding. Een VPN-verbinding wordt meestal gebruikt bij het aansluiten van een tweede kantoor op het hoofdkantoor of bij het aansluiten van een externe werknemer op een computernetwerk van het kantoor, ook al is hij niet fysiek verbonden met de netwerkinfrastructuur. Afstandsarbeiders verbinden zich doorgaans via een VPN-softwareclient zoals AnyConnect, Shrew Soft, GreenBow en vele anderen.

Dit artikel heeft als doel u te tonen hoe u een site-to-site VPN-verbinding tussen een RV340 en een RV345-router kunt configureren. Het zal de primaire router de lokale router roepen, en de secundaire router zal de afstandsrouter worden genoemd. Zorg ervoor dat u externe of fysieke toegang hebt tot de secundaire router.

LAN-netwerken moeten op verschillende subnetwerken (bijvoorbeeld 192.168.1.x en 192.168.2.x) of op totaal verschillende netwerken zijn gericht (bijvoorbeeld 192.168.1.x en 10.10.1.x). Als beide netwerken op zelfde subnet waren, zouden de routers nooit proberen pakketten over VPN te verzenden.

Toepasselijke apparaten

- RV340
- RV340 W
- RV345
- RV345P router

Softwareversie

- 1.0.03.15

Bijzondere opmerking: Licentiestructuur - Firmware versies 1.0.3.15 en hoger. AnyConnect brengt *alleen* kosten in rekening voor licenties aan klanten.

U moet een of meer clientlicenties aanschaffen bij een partner als CDW of via de aanschaf van apparatuur van uw bedrijf. Er zijn opties voor 1 gebruiker (L-AC-PLS-3Y-S5) of pakketten licenties inclusief één jaar voor 25 gebruikers (AC-PLS-P-25-S). Ook andere licentieopties zijn beschikbaar, inclusief permanente licenties. Bekijk de koppelingen in het onderstaande gedeelte *Licentie-informatie* voor meer informatie over licenties.

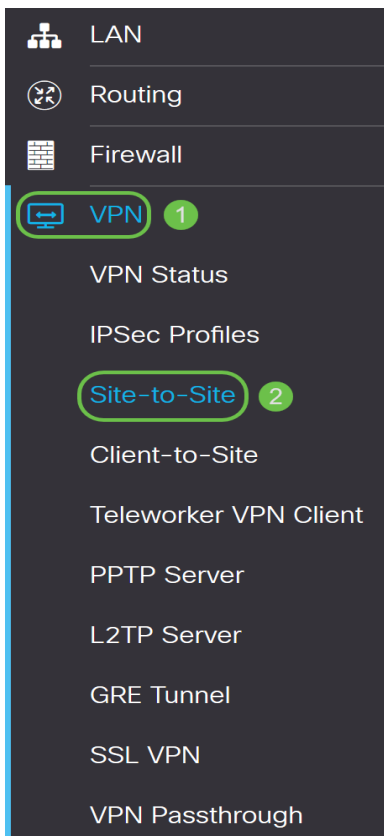
Ga voor extra informatie over AnyConnect-licenties op de RV340-Series routers naar het artikel [AnyConnect-licenties voor de RV340 Series routers](#).

Een VPN-verbinding configureren

Lokale router

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van de lokale router en kies **VPN > Site-to-Site**.

Opmerking: In dit voorbeeld wordt een RV340 gebruikt.



Stap 2. Klik op het pictogram **plus**.

Site to Site Table ^



Connection Name ⌵ Remote Endpoint ⌵ Interface ⌵ IPSec Profile ⌵ Local Traffic Selection ⌵ Remote Traffic Selection ⌵ Stat

Stap 3. Zorg ervoor dat het vakje **Enable** aangevinkt is. Standaard wordt het programma afgevinkt.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 4. Voer de naam van de verbinding in het veld *Connection Name*.

Opmerking: In dit voorbeeld is de naam TestVPN1.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 5. Kies de beveiligingsinstellingen van de verbinding in de vervolgkeuzelijst IPsec Profile. De opties zullen afhangen van de gemaakte IPsec-profielen. Voor instructies hoe u een IPsec Profile kunt maken, klik [hier](#).

Opmerking: In dit voorbeeld wordt CiscoTestVPN geselecteerd.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 6. Kies de interface die door de lokale router moet worden gebruikt. De opties zijn:

- WAN1 - Deze optie gebruikt het IP-adres van de WAN-interface (Wide Area Network 1) van de lokale router voor de VPN-verbinding.
- WAN2 - Deze optie zal het IP-adres van de WAN2-interface van de lokale router voor de VPN-verbinding gebruiken. WAN2 is niet beschikbaar in routers met één WAN.
- USB1 — Deze optie gebruikt het IP-adres van de Universal Serial Bus 1 (USB1) interface van de lokale router voor de VPN-verbinding.

- USB2 — Deze optie zal het IP-adres van de USB2-interface van de lokale router voor de VPN-verbinding gebruiken. USB2 is niet beschikbaar op USB-routers.

Opmerking: In dit voorbeeld wordt WAN1 geselecteerd.

The screenshot shows a configuration interface with three tabs: 'Basic Settings' (active), 'Advanced Settings', and 'Failover'. The 'Enable' checkbox is checked. The 'Connection Name' field contains 'TestVPN1'. The 'IPsec Profile' dropdown is set to 'CiscoTestVPN', with a note 'Auto (IKEv1) Profile is Chosen.' The 'Interface' dropdown is set to 'WAN1' and is highlighted with a green border. The 'Remote Endpoint' dropdown is set to 'Static IP' and is highlighted with a red border. Below the dropdown is an empty text input field.

Stap 7. Kies de id van de WAN-interface van de externe router. De opties zijn:

- Statische IP — Deze optie zal de lokale router het statische IP-adres van de afstandsrouter laten gebruiken wanneer u een VPN-verbinding maakt. Als deze optie op de lokale router is geselecteerd, moet de externe router ook met dezelfde optie zijn geconfigureerd.
- FQDN - Deze optie zal de Full Qualified Domain Name (FQDN) van de afstandsrouter gebruiken wanneer het opzetten van de VPN-verbinding.
- Dynamische IP — Deze optie zal het dynamische IP-adres van de afstandsrouter gebruiken wanneer er een VPN-verbinding wordt gemaakt.

Opmerking: Interface identifieer op de externe router dient hetzelfde te zijn als de interfaceid van de lokale router. In dit voorbeeld wordt er voor statische IP gekozen.

The screenshot shows the same configuration interface as before, but the 'Remote Endpoint' dropdown menu is open, showing three options: 'Static IP' (highlighted in blue), 'FQDN', and 'Dynamic IP'. The 'Static IP' option is selected.

Stap 8. Voer het IP-adres van de WAN-interface van de externe router in.

Opmerking: In dit voorbeeld wordt 124.123.122.123 gebruikt.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

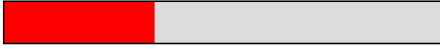
Stap 9. Klik het radioknop voor de Internet Key Exchange (IKE)-verificatiemethode die u nodig hebt. De opties zijn:

- Voorgedeelde sleutel — Deze optie betekent dat de verbinding een wachtwoord nodig heeft om de verbinding te voltooien. De vooraf gedeelde toets zou hetzelfde moeten zijn aan beide uiteinden van de VPN-verbinding.
- Certificaat - Deze optie betekent dat de authenticatiemethode een certificaat gebruikt dat door de router gegenereerd is in plaats van een wachtwoord bij de verbinding.

Opmerking: In dit voorbeeld wordt PreShared Key gekozen.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Stap 10. Voer de vooraf gedeelde sleutel voor de VPN-verbinding in het veld *PreShared Key*.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Stap 1. (Optioneel) Schakel het vakje Minimale gedeelde sleutel uit om een eenvoudig wachtwoord voor de VPN-verbinding te gebruiken. Dit wordt standaard gecontroleerd.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Stap 12. (Optioneel) Controleer de onbewerkte tekst tonen wanneer u het vakje Inschakelen bewerkt om de voorgedeelde toets in onbewerkte tekst weer te geven. Dit wordt standaard niet gecontroleerd.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Stap 13. Kies het herkenningstype van het lokale netwerk in de vervolgkeuzelijst Local Identifier Type. De opties zijn:

- IP van lokaal WAN - Deze optie zal het lokale netwerk door WAN IP van de interface identificeren.
- IP-adres - Met deze optie identificeert u het lokale netwerk via het lokale IP-adres.
- Lokale FQDN - Deze optie identificeert het lokale netwerk via de FQDN, als het een heeft.
- Lokale gebruiker FQDN - Deze optie identificeert het lokale netwerk via de FQDN van de gebruiker, wat zijn e-mailadres kan zijn.

Opmerking: In dit voorbeeld, wordt het IP Adres gekozen.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Stap 14. Voer de identicator van het lokale netwerk in het veld *Local Identifier*.

Opmerking: In dit voorbeeld wordt 124.123.122.121 opgenomen.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Stap 15. Kies het IP-adrestype dat door de VPN-client benaderd kan worden, in de vervolgkeuzelijst Local IP Type. De opties zijn:

- Subnet - Deze optie staat de verre kant van VPN toe om tot de lokale gastheren in gespecificeerde netto toegang te hebben.
- IP-adres - Met deze optie krijgt de externe kant van VPN toegang tot de lokale host met het opgegeven IP-adres.
- Elk — Deze optie geeft de externe kant van VPN toegang tot een van de lokale hosts.

Opmerking: In dit voorbeeld wordt Subnet geselecteerd.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Subnet

IP Address

IP Group

GRE Interface

Any

Stap 16. Voer het IP-adres in van het netwerk of de host die door de VPN-client moet worden benaderd in het veld *IP-adres*.

Opmerking: In dit voorbeeld is het IP-adres 10.10.10.1.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text"/>

Stap 17. Voer het subnetmasker van het IP-adres in het veld *Subnetmasker in*.

Opmerking: In dit voorbeeld, is het netto masker 255.255.255.0.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.121"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="10.10.10.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Stap 18. Kies het type afstands aanduiding in de vervolgkeuzelijst. De opties zijn:

- IP op afstand van WAN - Deze optie zal het externe netwerk via WAN IP van de interface identificeren.
- Remote FQDN - Deze optie identificeert het externe netwerk via de FQDN, als het een heeft.
- Afstandsgebruiker FQDN - Deze optie zal het afgelegen netwerk via de FQDN van de gebruiker identificeren, wat zijn e-mailadres kan zijn.

Opmerking: In dit voorbeeld wordt IP op Remote WAN geselecteerd.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="Remote WAN IP"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Stap 19. Voer het WAN IP-adres van de externe router in het veld *Remote Identifier*.

Opmerking: In dit voorbeeld is de identificator op afstand 124.123.122.123.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.123"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

Stap 20. Kies het netwerktype waarop het lokale netwerk toegang nodig heeft, uit de vervolgkeuzelijst Remote IP-type. De opties zijn:

- IP Address - Deze optie geeft de lokale hosts toegang tot de externe host met het opgegeven IP-adres.

- Subnet - Deze optie laat de lokale gastheren toegang hebben tot de middelen op de afstandsbediening met het gespecificeerde net.
- Enig — Deze optie laat de lokale gastheren toegang tot de middelen op de afstandsbediening met om het even welk IP adres.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.123"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="Subnet"/>
Subnet Mask:	<input type="text" value="IP Address"/>
	<input type="text" value="IP Group"/>
	<input type="text" value="Any"/>

Stap 21. Voer het LAN IP-adres van het externe netwerk in het veld *IP-adres*.

Opmerking: In dit voorbeeld is het IP-adres 192.168.2.1.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.123"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value=""/>

Stap 2. Voer het subnetmasker van het externe netwerk in het veld *Subnetmasker in*.

Opmerking: In dit voorbeeld, is het netto masker 255.255.255.0.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="124.123.122.123"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Stap 23. Klik op **Toepassen**.

Add/Edit a New Connection Apply Cancel

Local IP Type: Subnet

IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.123

Remote IP Type: Subnet

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Stap 24. Klik op **Opslaan**.



cisco (admin)

English



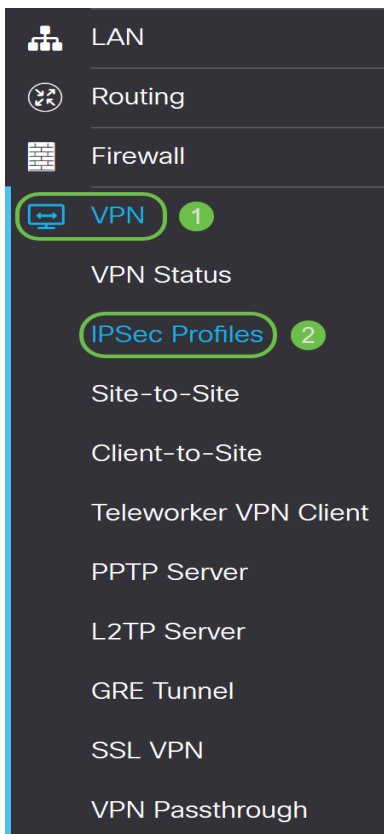
U had nu de VPN-instellingen op de lokale router moeten configureren.

Remote-router

Stap 1. Bepaal de VPN-instellingen van de lokale router zoals:

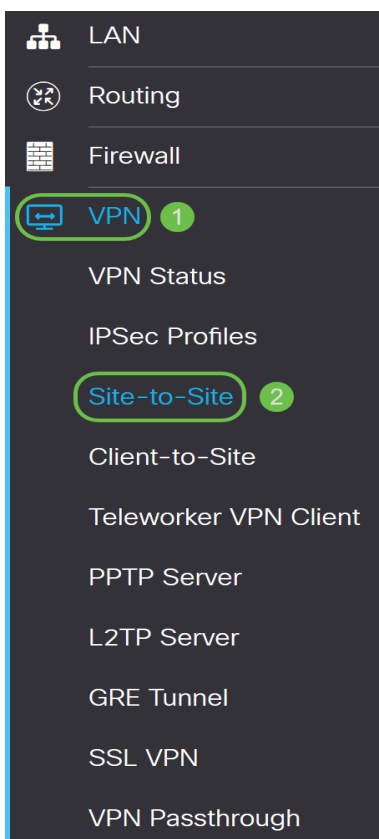
- Interface van de lokale en externe router die voor de VPN-verbinding wordt gebruikt.
- Wide Area Network (WAN) Internet Protocol (IP)-adres van de lokale en externe router.
- LAN-adres (Local Area Network) en subnetmasker van het lokale en externe netwerk.
- Eerder gedeelde sleutel, wachtwoord of certificaat voor de VPN-verbinding.
- Beveiligingsinstellingen van de lokale router.
- Firewallvrijstelling voor de VPN-verbinding.

Stap 2. Meld u aan bij het webgebaseerde hulpprogramma van de router en kies **VPN > IPSec-profielen**.



Stap 3. Het configureren van de VPN-beveiligingsinstellingen van de externe router, waarbij de VPN-beveiligingsinstellingen van de lokale router worden aangepast. Klik [hier](#) voor meer informatie.

Stap 4. Kies op het web-based hulpprogramma van de lokale router **VPN > Site-to-Site**.



Stap 5. Klik op het pictogram **plus**.



Connection Name **◆** Remote Endpoint **◆** Interface **◆** IPsec Profile **◆** Local Traffic Selection **◆** Remote Traffic Selection **◆** Sta

Stap 6. Zorg ervoor dat het vakje **Enable** aangevinkt is. Standaard wordt het programma afgevinkt.

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 7. Voer de naam van de VPN-verbinding in het veld *Connection Name*. De verbindingsnaam van de afstandsrouter kan verschillen van de verbindingsnaam die in de lokale router gespecificeerd is.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Opmerking: In dit voorbeeld is de verbindingsnaam TestVPN.

Stap 8. Kies het IPsec Profile van de vervolgkeuzelijst. De opties zullen afhangen van de gemaakte IPsec-profielen. Klik [hier](#) voor instructies voor het maken van een IPsec-profiel.

Opmerking: In dit voorbeeld wordt CiscoTestVPN geselecteerd.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 9. Kies de interface die de externe router voor de VPN-verbinding zal gebruiken in de vervolgkeuzelijst. De opties zijn:

- WAN1 - Deze optie gebruikt het IP-adres van de WAN-interface (Wide Area Network 1) van de externe router voor de VPN-verbinding.
- WAN2 - Deze optie zal het IP-adres van de WAN2-interface van de externe router voor de VPN-verbinding gebruiken. WAN2 is niet beschikbaar in routers met één WAN.
- USB1 — Deze optie gebruikt het IP-adres van de Universal Serial Bus 1 (USB1) interface van de afstandsrouter voor de VPN-verbinding.
- USB2 — Deze optie zal het IP-adres van de USB2-interface van de externe router voor de VPN-verbinding gebruiken. USB2 is niet beschikbaar op USB-routers.

Opmerking: In dit voorbeeld wordt WAN1 geselecteerd.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 10. Kies de identificatie van de WAN-interface van de lokale router in de vervolgkeuzelijst Remote Endpoint. De opties zijn:

- Statische IP — Deze optie zal de externe router het statische IP-adres van de lokale router laten gebruiken wanneer u een VPN-verbinding maakt. Als deze optie op de lokale router is geselecteerd, moet de externe router ook met dezelfde optie zijn geconfigureerd.
- FQDN - Deze optie gebruikt de Full Qualified Domain Name (FQDN) van de lokale route wanneer het opzetten van de VPN-verbinding.
- Dynamische IP — Deze optie zal het dynamische IP-adres van de lokale router gebruiken wanneer er een VPN-verbinding wordt gemaakt.

Opmerking: Interface identifier op de externe router dient hetzelfde te zijn als de interfaceid van de

lokale router. In dit voorbeeld wordt er voor statische IP gekozen.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

Stap 1. Voer het WAN IP-adres van de lokale router in.

Opmerking: In dit voorbeeld is het IP-adres 124.123.122.121.

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

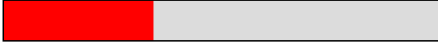
Stap 12. Klik het radioknop voor de Internet Key Exchange (IKE)-verificatiemethode die u nodig hebt. De opties zijn:

- Voorgedeelde sleutel — Deze optie betekent dat de verbinding een wachtwoord nodig heeft om de verbinding te voltooien. De vooraf gedeelde toets zou hetzelfde moeten zijn aan beide uiteinden van de VPN-verbinding.
- Certificaat - Deze optie betekent dat de authenticatiemethode een certificaat gebruikt dat door de router gegenereerd is in plaats van een wachtwoord bij de verbinding.

Opmerking: In dit voorbeeld wordt PreShared Key gekozen.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Step 13. Voer de vooraf gedeelde sleutel voor de VPN-verbinding in het veld *PreShared Key*.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Step 14. (Optioneel) Schakel de optie Minimale gedeelde sleutel uit Complexiteit inschakelen uit als u een eenvoudig wachtwoord voor de VPN-verbinding wilt gebruiken. Dit wordt standaard gecontroleerd.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

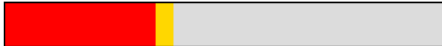
Show Pre-shared Key: Enable

Certificate:

Step 15. (Optioneel) Controleer de onbewerkte tekst tonen wanneer u het vakje Inschakelen bewerkt om de voorgedeelde toets in onbewerkte tekst weer te geven. Dit wordt standaard niet gecontroleerd.

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Step 16. Kies het herkenningstype van het externe netwerk van de vervolgkeuzelijst Local Identifier Type van de afstandsrouter. De opties zijn:

- IP van lokaal WAN - Deze optie zal het externe netwerk via WAN IP van de interface identificeren.
- IP-adres - Met deze optie identificeert u het externe netwerk via het lokale IP-adres.
- Lokale FQDN - Deze optie identificeert het externe netwerk via de FQDN, als het een heeft.
- Lokale gebruiker FQDN - Deze optie identificeert het externe netwerk via de FQDN van de gebruiker, wat zijn e-mailadres kan zijn.

Opmerking: In dit voorbeeld, wordt het IP Adres gekozen.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Stap 17. Voer de identicator van het externe netwerk in het veld *Local Identifier* van de afstandsrouter in.

Opmerking: In dit voorbeeld wordt 124.123.122.123 opgenomen.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Stap 18. Kies het IP-adrestype dat door de VPN-client benaderd kan worden, in de vervolgkeuzelijst Local IP Type. De opties zijn:

- Subnet - Deze optie staat de lokale kant van VPN toe om tot de afstandsbediening van hosts in het gespecificeerde net toegang te hebben.
- IP-adres - Met deze optie krijgt de lokale zijde van VPN toegang tot de externe host met het opgegeven IP-adres.
- Any — Met deze optie krijgt de lokale zijde van VPN toegang tot een van de externe hosts.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Opmerking: In dit voorbeeld wordt Subnet geselecteerd.

Stap 19. Voer het IP-adres in van het netwerk of de host die door de VPN-client moet worden benaderd in het veld *IP-adres*.

Opmerking: In dit voorbeeld is het IP-adres 192.168.2.1.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text"/>

Stap 20. Voer het subnetmasker van het IP-adres in het veld *Subnetmasker in*.

Opmerking: In dit voorbeeld, is het netto masker 255.255.255.0.

Local Group Setup

Local Identifier Type:	<input type="text" value="IP Address"/>
Local Identifier:	<input type="text" value="124.123.122.123"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Stap 21. Kies het lokale identificatienummer in de vervolgkeuzelijst. De opties zijn:

- IP op afstand van WAN - Deze optie zal het lokale netwerk via WAN IP van de interface identificeren.
- Remote FQDN - Deze optie identificeert het lokale netwerk via de FQDN, als het een heeft.
- Remote User FQDN - Deze optie zal het lokale netwerk via de FQDN van de gebruiker identificeren, wat zijn e-mailadres kan zijn.

Opmerking: In dit voorbeeld wordt IP op Remote WAN geselecteerd.

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.121

Remote IP Type:

Subnet

IP Address:

10.10.10.1

Subnet Mask:

255.255.255.0

Stap 2. Klik op **Toepassen**.

Add/Edit a New Connection Apply Cancel

Local IP Type: Subnet

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 124.123.122.121

Remote IP Type: Subnet

IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0

Stap 23. Klik op **Opslaan**.



cisco (admin)

English



U had nu de VPN-instellingen op de externe router moeten configureren.

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)