

VPN-setup-wizard configureren op de RV160 en RV260

Doel

Dit document toont u hoe u de Wizard VPN Setup op de RV160 en RV260 kunt configureren.

Inleiding

De technologie is geëvolueerd en er wordt vaak buiten het kantoor gehandeld. Apparaten zijn mobieler en werknemers werken vaak vanuit hun huis of tijdens hun reis. Dit kan enige veiligheidskwetsbaarheden veroorzaken. Een Virtual Private Network (VPN) is een goede manier om externe medewerkers aan een beveiligd netwerk te verbinden. Een VPN kan een externe host inschakelen om op te treden alsof ze was verbonden met het beveiligde onsite netwerk.

VPN voert een versleutelde verbinding in via een minder beveiligd netwerk zoals het internet. Het waarborgt het juiste beveiligingsniveau voor de aangesloten systemen. Een tunnel wordt opgericht als een privaat netwerk dat gegevens veilig kan verzenden door middel van industriestandaard encryptie- en authenticatietechnieken om de verzonden gegevens te beveiligen. Een VPN dat op afstand toegang heeft, is meestal afhankelijk van Internet Protocol Security (IPsec) of Secure Socket Layer (SSL) om de verbinding te beveiligen.

VPN's bieden Layer 2-toegang tot het doelnetwerk; Hiervoor is een tunneling-protocol nodig, zoals Point-to-Point Tunneling Protocol (PPTP) of Layer 2 Tunneling Protocol (L2TP), dat over de basisverbinding van IPsec loopt. IPsec VPN ondersteunt site-to-site VPN voor een gateway-naar-gateway-tunnel. Bijvoorbeeld, kan een gebruiker VPN tunnel op een tak-plaats vormen om aan de router op bedrijfsplaats te verbinden, zodat de kantorsite veilig tot het bedrijfsnetwerk kan toegang hebben. IPsec VPN ondersteunt client-to-server VPN voor host-naar-gateway-tunnel. De client-naar-server-VPN is handig bij de verbinding van Laptop/PC van thuis naar een bedrijfsnetwerk via VPN-server.

De RV160 Series router ondersteunt 10 tunnels en de RV260 Series router ondersteunt 20 tunnels. De Wizard VPN-installatie begeleidt de gebruiker bij het configureren van een beveiligde verbinding voor een site-to-site IPsec-tunnel. Dit vereenvoudigt de configuratie door complexe en optionele parameters te vermijden, zodat elke gebruiker de IPsec-tunnel snel en efficiënt kan opzetten.

Toepasselijke apparaten

RV160

RV260

Softwareversie

1.0.0.13

VPN Setup Wizard Configuratie van lokale router

Stap 1. Meld u aan bij de webconfiguratie op uw lokale router.

Opmerking: Wij zullen de lokale router als router A en de verre router als router B verwijzen. In dit document worden we twee RV160 gebruikt om de VPN Setup-wizard te tonen.



Router

cisco

●●●●●●●●

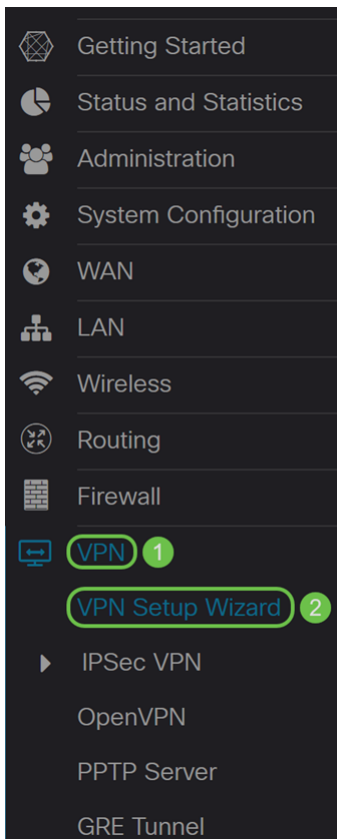
English ▼

Login

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Stap 2. Navigeer naar **VPN > VPN Setup Wizard**.



Stap 3. Voer in het gedeelte *Introductie* een verbindingsnaam in in het veld **Voer een verbindingsnaam in**. We gingen in **HomeOffice** als verbindingsnaam in.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name:

4. Profile

Interface: WAN

5. Summary

Next

Cancel

Stap 4. In het veld *Interface* selecteert u een interface uit de vervolgkeuzelijst als u een RV260 gebruikt. De RV160 heeft alleen een WAN-link, zodat u geen interface uit de vervolgkeuzelijst kunt selecteren. Klik op **Next** om naar de sectie *Remote Router Instellingen* te gaan.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name:  HomeOffice

4. Profile

Interface: WAN

5. Summary

Next

Cancel

Stap 5. Selecteer een *type afstandsbediening* in de vervolgkeuzelijst. Selecteer of **Static IP** of **FQDN** (Full Qualified Domain Name) en voer vervolgens het WAN IP-adres of de FQDN van de gateway in die u in het *Remote Address* veld wilt aansluiten. In dit voorbeeld werd **Statische IP** geselecteerd en werd het IP-adres van de externe router (router B) ingevoerd. Klik vervolgens op **Volgende** om naar de volgende sectie te gaan.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Remote Connection Type :

Static IP

1

2. Remote Router Settings

Remote Address : ?

145.

2

3. Local and Remote Networks

4. Profile

5. Summary

3

Back

Next

Cancel

Stap 6. Selecteer in het gedeelte *Local and Remote Network* onder de *selectie Local Traffic*, de optie Local IP (**Subnet**, **Single** of **Any**) in de **vervolgkeuzelijst**. Als u **Subnet** selecteert, voer het netto IP adres en het Subnet masker in. Als u **Single** selecteert, voer dan een IP-adres in. Als **Any** geselecteerd is, gaat u naar de volgende stap om de *selectie van het afstandsverkeer* te configureren.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

Subnet Mask:

Back

Next

Cancel

Stap 7. *Selecteer in de selectie van het afstandsverkeer de externe IP (Subnet, Enkelvoudig of Any) in de vervolgkeuzelijst. Als u Subnet selecteert, voer het netto IP adres en het subnetmasker van de verre router (router B) in. Als u Enkelvoudig selecteert, voer het IP-adres in. Klik vervolgens op **Volgende** om de sectie van het profiel te configureren.*

Opmerking: Als u **Any** hebt geselecteerd voor *selectie van het lokale verkeer*, moet u ofwel **Subnet** ofwel **Single** selecteren voor *de selectie van het afstandsverkeer*.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

10.1.1.0

Subnet Mask:

255.255.255.0

4

Back

Next

Cancel

Stap 8. Selecteer in het gedeelte *Profile* een naam voor IPsec-profiel in de vervolgkeuzelijst. Voor deze demonstratie is **een nieuw profiel** geselecteerd als het IPsec-profiel.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile:

IKE Version:

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime (sec.):

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 9. Kies **IKEv1** (Internet Key Exchange versie 1) of **IKEv2** (Internet Key Exchange versie 2) als uw *IKE-versie*. IKE is een hybride protocol ter uitvoering van de Oakley-uitwisseling en de Skeme-sleuteluitwisseling binnen het kader van Internet Security Association en Key Management Protocol (ISAKMP). IKE biedt verificatie van de IPsec-peers, onderhandelt over IPsec-toetsen en onderhandelt over IPsec-beveiligingsassociaties. IKEv2 is efficiënter omdat het minder pakketten nodig heeft om de belangrijke uitwisseling te doen en meer authenticatieopties ondersteunt, terwijl IKEv1 alleen gedeelde sleutel en op certificaat gebaseerde authenticatie doet. In dit voorbeeld is **IKEv1** geselecteerd als onze IKE-versie.

Opmerking: Als uw apparaat IKEv2 ondersteunt, wordt het aanbevolen IKEv2 te gebruiken. Als uw apparaten IKEv2 niet ondersteunen, dan moet u IKEv1 gebruiken. Beide routers (lokaal en extern) moeten dezelfde IKE versie en beveiligingsinstellingen gebruiken.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 10. Selecteer in het gedeelte *Fase 1 Opties* een DH (Diffie-Hellman) groep (**Groep 2 - 1024 bit** of **Groep 5 - 1536 bit**) in de vervolgkeuzelijst. DH is een belangrijk uitwisselingsprotocol, met twee groepen van verschillende priemlengte: Groep 2 heeft tot 1.024 bits en Groep 5 heeft tot 1.536 bits. We zullen **groep 2 - 1024 bit** gebruiken voor deze demonstratie.

Opmerking: Voor snellere en lagere veiligheid, kies Groep 2. Voor langzamere snelheid en hogere veiligheid, kies Groep 5. Groep 2 wordt door standaard geselecteerd.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back

Next

Cancel

Stap 1. Selecteer een coderingsoptie (**3DES, AES-128, AES-192** of **AES-256**) in de vervolgkeuzelijst. Deze methode bepaalt het algoritme dat wordt gebruikt om de pakketten Security Payload (ESP)/Internet Security Association en Key Management Protocol (ISAKMP) te versleutelen of te decrypteren. Triple Data Encryption Standard (3DES) gebruikt DES-encryptie drie keer, maar is nu een legacy-algoritme. Dit betekent dat het alleen gebruikt mag worden als er geen betere alternatieven zijn, aangezien het nog steeds een marginaal maar aanvaardbaar veiligheidsniveau biedt. Gebruikers mogen het alleen gebruiken als het vereist is voor achterwaartse compatibiliteit omdat het kwetsbaar is voor een of andere "blokbotsing"-aanvallen. Advanced Encryption Standard (AES) is een cryptografisch algoritme dat ontworpen is om veiliger te zijn dan DES. AES gebruikt een grotere key size die ervoor zorgt dat de enige bekende benadering om een bericht te decrypteren voor een indringer is om elke mogelijke sleutel te proberen. Aanbevolen wordt AES in plaats van 3DES te gebruiken. In dit voorbeeld zullen we **AES-192** gebruiken als onze encryptie optie.

Opmerking: Hier zijn een paar extra hulpmiddelen die kunnen helpen: [Het configureren van beveiliging voor VPN's met IPSec](#) en [encryptie van de volgende generatie](#).

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 12. De verificatiemethode bepaalt hoe de ESP-headerpakketten (Encapsulation Security Payload Protocol) worden gevalideerd. De MD5 is een one-way hashing algoritme dat een 128-bits resumé produceert. SHA1 is een one-way hashing algoritme dat een 160 bit digest produceert terwijl SHA2-256 een 256-bits digest produceert. SHA2-256 wordt aanbevolen omdat het veiliger is. Zorg ervoor dat beide uiteinden van de VPN-tunnel dezelfde authenticatiemethode gebruiken. Selecteer een verificatie (**MD5, SHA1 of SHA2-256**). **SHA2-256** is voor dit voorbeeld geselecteerd.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 13. De *SA Lifetime (SEC)* vertelt u de hoeveelheid tijd, in seconden, is een IKE SA actief in deze fase. Er is onderhandeld over een nieuwe Security Association (SA) voordat de levensduur verstrijkt om te verzekeren dat een nieuwe SA klaar is om te worden gebruikt als de oude verstrijkt. De standaard is 28800 en het bereik loopt van 120 tot 86400. We gebruiken de standaardwaarde van **28800** seconden als onze SA-levensduur voor fase I.

Opmerking: Aanbevolen wordt dat uw SA-levensduur in fase I langer is dan uw fase II SA-levensduur. Als je fase I korter maakt dan fase II, dan moet je regelmatig opnieuw onderhandelen over de tunnel dan vaak in tegenstelling tot de datunnel. Gegevenstunnel is wat meer veiligheid nodig heeft, zodat het beter is om de levensduur in fase II korter te hebben dan fase I.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 14. Voer in de **Voorgedeelde sleutel** in om de externe IKE-peer te authentifieren. U kunt maximaal 30 toetsenbordtekens of hexadecimale waarden opgeven, zoals My_@123 of 4d795f40313233. Beide uiteinden van de VPN-tunnel moeten dezelfde voorgedeelde sleutel gebruiken.

Opmerking: We raden u aan de voorgedeelde sleutel regelmatig te wijzigen om de VPN-beveiliging te maximaliseren.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 28800

Pre-shared Key: ●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Stap 15. Selecteer in het gedeelte *Fase II Opties* een protocol in de vervolgkeuzelijst.

ESP - Selecteer ESP voor gegevenscodering en voer de codering in.

AH - Selecteer dit voor gegevensintegriteit in situaties waarin gegevens niet geheim zijn, maar voor authenticatie geschikt zijn.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Stap 16. Selecteer een coderingsoptie (**3DES, AES-128, AES-192** of **AES-256**) in de vervolgkeuzelijst. Deze methode bepaalt het algoritme dat wordt gebruikt om de pakketten Security Payload (ESP)/Internet Security Association en Key Management Protocol (ISAKMP) te versleutelen of te decrypteren. Triple Data Encryption Standard (3DES) gebruikt DES-encryptie drie keer, maar is nu een legacy-algoritme. Dit betekent dat het alleen gebruikt mag worden als er geen betere alternatieven zijn, aangezien het nog steeds een marginaal maar aanvaardbaar veiligheidsniveau biedt. Gebruikers mogen het alleen gebruiken als het vereist is voor achterwaartse compatibiliteit omdat het kwetsbaar is voor een of andere "blokbotsing"-aanvallen. Advanced Encryption Standard (AES) is een cryptografisch algoritme dat ontworpen is om veiliger te zijn dan DES. AES gebruikt een grotere key size die ervoor zorgt dat de enige bekende benadering om een bericht te decrypteren voor een indringer is om elke mogelijke sleutel te proberen. Aanbevolen wordt AES in plaats van 3DES te gebruiken. In dit voorbeeld zullen we **AES-192** gebruiken als onze encryptie optie.

Opmerking: Hier zijn een paar extra hulpmiddelen die kunnen helpen: [Het configureren van beveiliging voor VPN's met IPSec](#) en [encryptie van de volgende generatie](#).

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Stap 17. De authenticatiemethode bepaalt hoe de Encapsulation Security Payload Protocol (ESP)-headerpakketten worden gevalideerd. De MD5 is een one-way hashing algoritme dat een 128-bits resumé produceert. SHA1 is een one-way hashing algoritme dat een 160 bit digest produceert terwijl SHA2-256 een 256-bits digest produceert. SHA2-256 wordt aanbevolen omdat het veiliger is. Zorg ervoor dat beide uiteinden van de VPN-tunnel dezelfde authenticatiemethode gebruiken. Selecteer een verificatie (**MD5, SHA1 of SHA2-256**). **SHA2-256** is voor dit voorbeeld geselecteerd.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.):

3600

Pre-shared Key:

●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.):

3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back

Next

Cancel

Stap 18. Voer in de *SA Lifetime (SEC)* in die de hoeveelheid tijd, in seconden, is dat een VPN-tunnel (IPsec SA) in deze fase actief is. De standaardwaarde voor fase 2 is 3600 seconden.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Stap 19. Wanneer Perfect Forward Security (PFS) is ingeschakeld, genereert IKE Fase 2-onderhandeling nieuw essentieel materiaal voor IPsec-verkeersencryptie en -verificatie. Perfect voorwaartse geheimhouding wordt gebruikt om de beveiliging van communicatie via het internet te verbeteren door middel van openbare sleutelcryptografie. Schakel dit vakje in om deze optie in te schakelen, of trek het vakje uit om deze optie uit te schakelen. Deze optie wordt aanbevolen. Selecteer desgewenst een *drooggroep*. In dit voorbeeld wordt **Group2 - 1024 bit** gebruikt.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

Show Pre-shared Key:


 Enable

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime (sec.): 

Perfect Forward Secrecy: Enable 1

DH Group: 2

Save as a new profile

Back

Next

Cancel

Stap 20. Voer in het *gedeelte Opslaan als een nieuw profiel* een naam in voor het nieuwe profiel dat u zojuist hebt gemaakt. Klik op **Next** om de samenvatting van uw VPN-configuratie te zien.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime (sec.): ?

Perfect Forward Secrecy: Enable

DH Group:

Save as a new profile 1

Back

2 Next

Cancel

Stap 21. Controleer de informatie en klik vervolgens op **Inzenden**.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started	(sec.):	-----	
✓ 2. Remote Router Settings	Pre-shared Key:	Test123	
✓ 3. Local and Remote Networks	Phase II Options		Remote Group
✓ 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
5. Summary	Encryption:	AES-192	IP Address: 10.1.1.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

Back

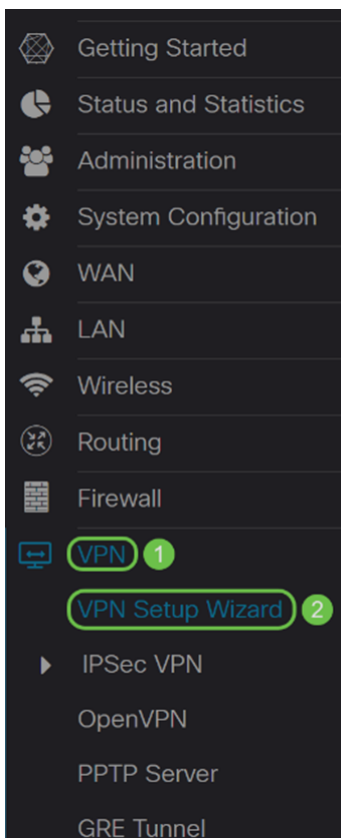
Submit

Cancel

VPN Setup Wizard Configuration voor Remote-router

Op de verre router, zou u de zelfde veiligheidsinstellingen moeten vormen zoals uw lokale router maar gebruik het lokale IP adres van de router als het verre verkeer.

Stap 1. Meld u aan bij de webconfiguratie op uw afstandsrouter (router B) en navigeer naar **VPN > VPN Setup Wizard**.



Stap 2. Voer een verbindingsnaam in en kies de interface die voor VPN wordt gebruikt als u een RV260 gebruikt. De RV160 heeft alleen een WAN-link zodat u geen interface uit de vervolgkeuzelijst kunt selecteren. Klik vervolgens op **Volgende** om verder te gaan

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name:

4. Profile

Interface: WAN

5. Summary

Next

Cancel

Stap 3. In de *Instellingen* van de *Remote-router* selecteert u het *type* afstandsbediening en voert u vervolgens het WAN IP-adres van router A in. Klik vervolgens op **Volgende** om

verder te gaan naar de volgende sectie.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Remote Connection Type :

Static IP

1

2. Remote Router Settings

Remote Address : ?

140.

2

3. Local and Remote Networks

4. Profile

5. Summary

3

Back

Next

Cancel

Stap 4. Selecteer het lokale en externe verkeer. Als u **Subnet** in het veld *Selectie* van het *Afstandsverkeer* hebt geselecteerd, voer dan in de privé IP adressubster van router A in. Klik vervolgens op **Volgende** om de sectie van het *profiel* te configureren.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Local Traffic Selection:

Any

1

✓ 2. Remote Router Settings

Remote Traffic Selection:

Subnet

2

3. Local and Remote Networks

IP Address:

192.168.2.0

3

Subnet Mask:

255.255.255.0

4

4. Profile

5. Summary

5

Back

Next

Cancel

Stap 5. Selecteer in het gedeelte *Profiel* dezelfde beveiligingsinstellingen als router A. We hebben ook dezelfde pre-gedeeld sleutel ingevoerd als router A. Klik vervolgens op **Volgende** om naar de pagina *Samenvatting te gaan*.

Mogelijkheden fase I:

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile:

1 new-profile

IKE Version:

2 IKEv1 IKEv2

Phase I Options

DH Group:

3 Group2 - 1024 bit

Encryption:

4 AES-192

Authentication:

5 SHA2-256

SA Lifetime (sec.):

? 6 28800

Pre-shared Key:

7 ●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Back

Next

Cancel

Fase II-opties:

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared key:

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection:

1 ESP

Encryption:

2 AES-192

Authentication:

3 SHA2-256

SA Lifetime (sec.):

4 3600

Perfect Forward Secrecy:

5 Enable

DH Group:

6 Group2 - 1024 bit

Save as a new profile

7 RemoteOffice

8

Back

Next

Cancel

Stap 6. In de overzichtspagina controleert u of de informatie die u zojuist hebt ingesteld, juist is. Klik vervolgens op **Inzenden** om uw site-to-site VPN te maken.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started	(sec.):	-----	
✓ 2. Remote Router Settings	Pre-shared Key:	Test123	
✓ 3. Local and Remote Networks	Phase II Options	Remote Group	
✓ 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
5. Summary	Encryption:	AES-192	IP Address: 192.168.2.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

[Back](#) [Submit](#) [Cancel](#)

Opmerking: Alle configuraties die de router momenteel gebruikt zijn in het bestand Configuration uitvoeren dat vluchtig is en niet tussen de herstart blijft behouden. Als u de configuratie tussen de herstart wilt behouden, moet u het Configuratiebestand uitvoeren naar het Opstartbestand kopiëren nadat u alle wijzigingen hebt uitgevoerd. Klik hiervoor op de knop **Opslaan** boven op de pagina of navigeer naar **Beheer > Configuration Management**. Controleer vervolgens of de *bron Configuratie* is **uitgevoerd** en de *bestemming opstartconfiguratie* is. Klik op **Toepassen**.

Conclusie

U had een site-to-site VPN met succes moeten configureren met behulp van de VPN Setup-wizard. Volg de onderstaande stappen om te controleren of uw Site-to-Site VPN is aangesloten.

Stap 1. Om te verifiëren dat uw verbinding is gerealiseerd, moet u een *Connected* status zien wanneer u **VPN > IPSec VPN > Site-to-Site**.

Site-to-Site								Apply	Cancel
Number of Connections: 1 connected, 1 configured, maximum 10 supported.									
+	+	+							
Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions		
<input type="checkbox"/>	RemoteOffice	140. [redacted]	WAN	VPNTest	0.0.0.0/0	192.168.2.0/24	Connected		

Stap 2. navigeren naar **Status en Statistieken > VPN Status** en zorg ervoor dat de site-to-Site tunnel *ingeschakeld* is en *omhoog*.

VPN Status

Site-to-Site Tunnel Status

1 Tunnel(s) Used 9 Tunnel(s) Available
1 Tunnel(s) Enabled 1 Tunnel(s) Defined

Connection Table



Column Display Selection

<input type="checkbox"/>	No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
<input type="checkbox"/>	1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140. [REDACTED]	