

Site-to-Site VPN configureren op de RV34x

Doel

Het doel van dit document is om een site-to-site VPN op RV34x Series routers te maken.

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 de industrie-standaard encryptie en authenticatietechnieken te gebruiken om gegevens te beveiligen die worden verzonden.

Configuratie van een site-to-site VPN houdt in dat het IPsec-profiel en de configuratie van de site-to-site VPN op de twee routers worden ingesteld. Het IPsec-profiel is al ingesteld om het makkelijk te maken om site-to-site VPN in te stellen, zelfs bij een derde partij (zoals AWS of AWS). Het IPsec-profiel bevat alle benodigde encryptie voor de tunnel. Site-to-site VPN is de configuratie zodat de router weet met welke andere site u verbinding wilt maken. Als u ervoor kiest het vooraf ingestelde IPsec-profiel niet te gebruiken, hebt u de optie om een ander profiel te maken.

Wanneer u site-to-site VPN configureren kan LAN (Local Area Network) subnetten aan beide zijden van de tunnel niet op hetzelfde netwerk 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 ander net 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 vet gemarkeerd is, zijn parameters die het omgekeerde van de tegenoverliggende router zijn. Alle andere parameters zijn hetzelfde ingesteld. In dit document zullen we de lokale router, router A. configureren.

Veld	Lokale router (router A)	Remote-router (router B)
	WAN IP-adres: 140.x.x	WAN IP-adres: 145.x.x
	Private IP-adres (lokaal): 192.168.2.0/24	Private IP-adres (lokaal): 10.1.1.0/24
Naam van verbinding	VPNest	VPNestRemote
IPsec-profiel	TestProfile	TestProfile
Interface	WAN1	WAN1

Remote-endpoint	Statische IP	Statische IP
Remote Endpoint IP-adres	145.x.x	140.x.x
Vooraf gedeelde sleutel	CiscoTest123!	CiscoTest123!
Type lokale identificateur	Lokale WAN IP	Lokale WAN IP
Lokale identificateur	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

Toepasselijke apparaten

RV34x

Softwareversie

·1.0.02.16

De site-to-site VPN-verbinding configureren

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



Router

cisco



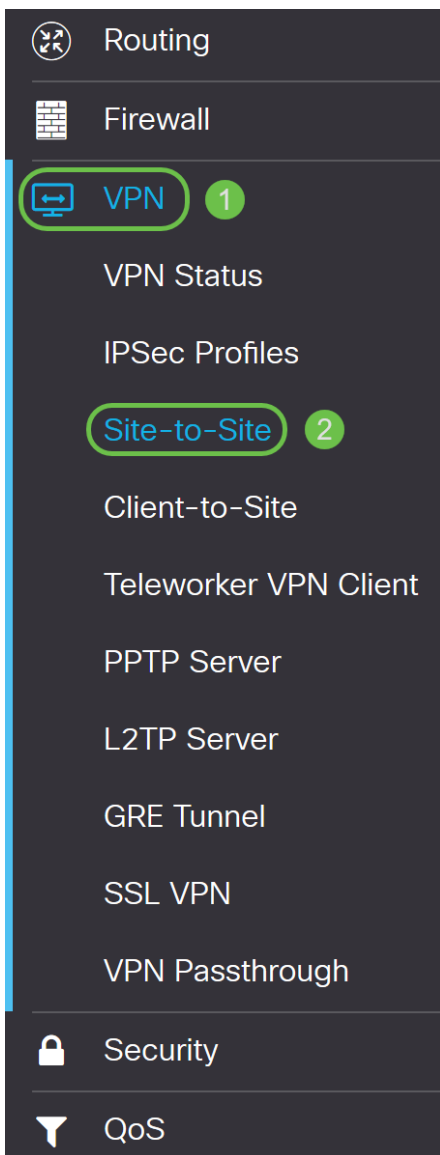
English ▼

Login

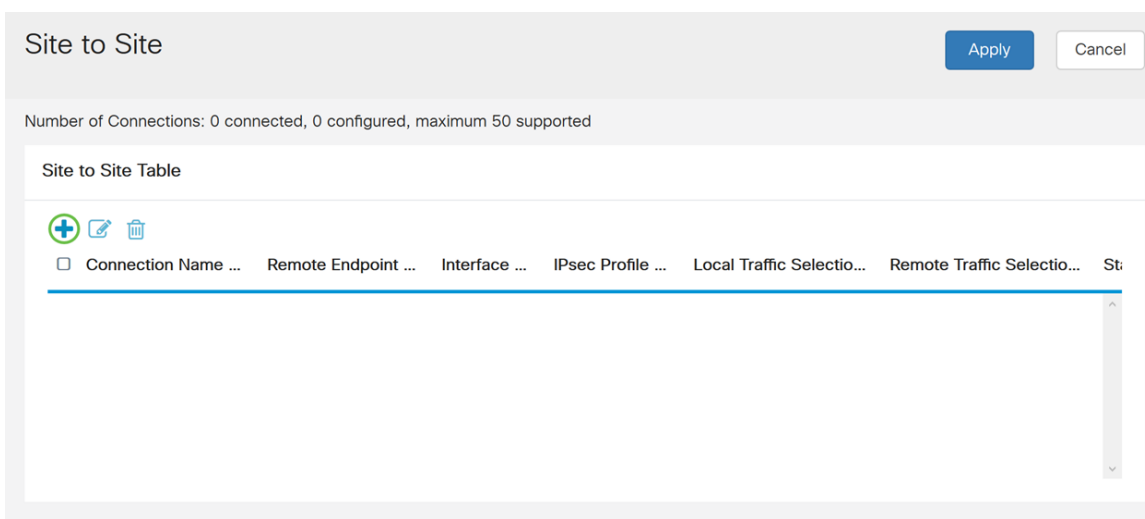
©2017-2018 Cisco Systems, Inc. All rights reserved.

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

Stap 2. Navigeer naar **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.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Default Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

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 **VPNTTest** in als onze verbindingsnaam.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name: VPNTTest

IPsec Profile: Default Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

Stap 6. Selecteer het IPsec-profiel dat u voor VPN wilt gebruiken. 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.

Klik op de link om te leren hoe u IPsec-profiel wilt configureren met IKEv2: [IPsec-profiel configureren met IKEv2 op de RV34x](#).

Opmerking: De optie om een 3^e partij (Amazon Web Services of Microsoft Messenger) te gebruiken voor IPsec-profiel is beschikbaar. Dit IPsec-profiel is al geconfigureerd met alle benodigde selecties die geconfigureerd moeten worden voor Amazon Web Services of Microsoft arek zodat u het niet hoeft te configureren. Als u probeert om site-to-site VPN tussen AWS of Kouk aan uw website te configureren, dan moet u de informatie gebruiken die AWS of Kuurarm u aan hun kant geeft en het vooraf ingestelde IPsec-profiel gebruiken bij het configureren van site-to-site VPN aan deze kant.

Dit voorbeeld, we zullen **TestProfile** selecteren als ons IPsec-profiel.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface: (Dropdown menu open with options: Amazon_Web_Services, Default, Microsoft_Azure, TestProfile)

Remote Endpoint:

Stap 7. Selecteer in het veld *Interface* de interface die voor de tunnel wordt gebruikt. In dit voorbeeld zullen we **WAN1** gebruiken als onze interface.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface: (Dropdown menu open with options: WAN1, WAN2, USB1, USB2)

Remote Endpoint:

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.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name:

IPsec Profile: Auto (IKEv1) Profile is Chosen.

Interface:

Remote Endpoint:

IKE-verificatiemethode configureren

Stap 1. Selecteer een **voorgedeelde sleutel** of een **certificaat**.


Vooraf gedeelde sleutel: IKE-peers authenticeren elkaar door gegevens te berekenen en te verzenden die de vooraf gedeelde sleutel bevatten. Beide peers moeten dezelfde geheime sleutel delen. Als het ontvangende peer in staat is om het zelfde hash onafhankelijk te creëren met gebruik van zijn pre-gedeelde sleutel, authenticceert het de andere peer. 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.

Certificaat: Het digitale certificaat is een pakket dat informatie bevat zoals de identiteit van de certificaathouder, waaronder een naam of IP-adres, het serienummer van het certificaat, de vervaldatum van het certificaat en een kopie van de openbare sleutel van de certificaathouder. 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.

Voor deze demonstratie selecteren we **een vooraf gedeelde sleutel** als onze IKE-authenticatiemethode.

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable


Certificate:

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.

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Stap 3. De *Vooraf gedeelde toetsuitbreidingsmeter* toont de kracht van de voorgedeelde toets door middel van gekleurde staven. Controleer **Schakel** in om de minimale pre-gedeelde sleutelcomplexiteit mogelijk te maken. De vooraf gedeelde complexiteit wordt standaard gecontroleerd. Als u de voorgedeelde toets wilt weergeven, controleert u het selectieteken **Inschakelen**.

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: 1 Enable

Show Pre-shared Key: 2 Enable

Certificate:

Local Group Setup

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.

Local Group Setup

Local Identifier Type: 1

Local Identifier: 2

Local IP Type:

IP Address:

Subnet Mask:

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.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

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.

Local Group Setup

Local Identifier Type:	<input type="text" value="Local WAN IP"/>
Local Identifier:	<input type="text" value="140."/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.0"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

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.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="145."/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

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.

Remote Group Setup

Remote Identifier Type:

Remote Identifier:

Remote IP Type:

IP Address:

Subnet Mask:

Stap 3. Voer het IP-adres en het subnetmasker 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.

Remote Group Setup

Remote Identifier Type:

Remote Identifier:

Remote IP Type:

IP Address: **1**

Subnet Mask: **2**

Stap 4. Klik op **Toepassen** om een nieuwe Site-to-Site VPN-verbinding te maken.

Add/Edit a New Connection Apply Cancel

Local IP Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Identifier Type:

Remote Identifier:

Remote IP Type:

IP Address:

Subnet Mask:

Alle configuraties die u op de router hebt ingevoerd, zijn in het bestand Configuration

uitvoeren dat vluchtig is en niet tussen de herstart blijft behouden.

Stap 5. 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 na een herstart te behouden.



Stap 6. *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. Het opstartconfiguratiebestand behoudt nu alle configuraties na een herstart.

Configuration Management 3 Apply Cancel Disabled Save Icon Blinking

Configuration File Name

Last Change Time

Running Configuration: 2018-Dec-11, 17:07:01 GMT

Startup Configuration: 2018-Dec-07, 21:54:43 GMT

Mirror Configuration: 2018-Dec-12, 18:00:03 GMT

Backup Configuration: N/A

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source: 1

Destination: 2

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.