

Site-to-Site VPN met Amazon Web Services

Doel

Het doel van dit artikel is om u door het opzetten van een Site-to-Site VPN tussen Cisco RV Series routers en Amazone Web Services te begeleiden.

Toepasselijke apparaten | Software versie

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

Inleiding

Een site-to-site VPN maakt een verbinding met twee of meer netwerken mogelijk, waardoor bedrijven en algemene gebruikers de mogelijkheid krijgen om verbinding te maken met verschillende netwerken. Amazon Web Services (AWS) biedt veel on demand cloud computing platforms, waaronder site om VPN's te plaatsen, die u toegang geven tot uw AWS-platforms. Deze gids zal u helpen om de site aan site VPN te configureren op zowel de RV16X, RV26X, RV34X router naar de Amazone Web Services.

De twee delen zijn:

[Site-to-Site VPN instellen op Amazon Web Services](#)

[Site-to-Site VPN-via een RV16X/RV26X, RV34X router](#)

Installatie van een Site-to-Site VPN op Amazon Web Services

Stap 1

Maak een nieuwe VPC, die een IPv4 CIDR-blok definieert, waarin we later het LAN definiëren als ons AWS LAN. Selecteer *Maken*.

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

1 Name tag Cisco_Lab ⓘ

2 IPv4 CIDR block* 172.16.0.0/16 ⓘ

IPv6 CIDR block No IPv6 CIDR Block ⓘ
 Amazon provided IPv6 CIDR block

Tenancy Default ⓘ

* Required

3 Create

Step 2

Wanneer u het subprogramma maakt, zorg er dan voor dat u de **VPC** hebt geselecteerd die eerder is gemaakt. Definieer een subtype binnen het bestaande /16 netwerk dat eerder gecreëerd is. In dit voorbeeld wordt 172.16.10.0/24 gebruikt.

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag AWS_LAN ⓘ

1 VPC* ⓘ

Availability Zone Filter by attributes ⓘ

VPC CIDRs

VPC CIDRs	Status	Status Reason
172.16.0.0/16	associated	

2 IPv4 CIDR block* 172.16.10.0/24 ⓘ

* Required

Create

Step 3

Maak een **gateway van de klant**, die het **IP-adres** als het *openbare IP-adres* van uw Cisco RV-router definieert.

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

1 Name ToCiscoLab ⓘ

Routing Dynamic
 Static

2 IP Address 68.227.227.57 ⓘ

Certificate ARN Select Certificate ARN ⓘ ⓘ

Device Lab_Router ⓘ

* Required

Cancel Create Customer Gateway

Step 4

Maak een **Virtual Private Gateway** - waarbij u een *naamp/laatje* maakt om later te helpen identificeren.

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

1 Name tag ⓘ

ASN Amazon default ASN ⓘ
 Custom ASN

* Required

Cancel

Step 5

Sluit de **Virtual Private Gateway** aan op de **VPC** die eerder is gemaakt.

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC ⓘ

Filter by attributes

vpn-gw-1234567890123456	Cisco_Lab
-------------------------	-----------

* Required

Cancel

step 6

Maak een nieuwe **VPN-verbinding**, door het **type** Virtual Private Gateway van **Target Gateway** te selecteren. Associeer de **VPN-verbinding** met de **Virtual Private Gateway** die eerder is gemaakt.

Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the target gateway information already.

Name tag ⓘ

1 Target Gateway Type Virtual Private Gateway
 Transit Gateway

2 Virtual Private Gateway ⓘ

Customer Gateway

Filter by attributes

VPN Gateway ID	Name tag	VPC ID
vpn-gw-1234567890123456	AWS_WAN	vpn-gw-1234567890123456

Step 7

Selecteer **Bestaande klantgateway**. Selecteer de eerder gemaakte **klantgateway**.

1 Customer Gateway Existing
 New

2 Customer Gateway ID ⓘ

Routing Options

Filter by attributes

Customer Gateway ID	Name tag	IP Address	Certificate ARN
vpn-gw-1234567890123456	ToCiscoLab	192.168.1.1	

Step 8

Voor **Routing Opties** dient u de optie Static te selecteren. Voer elke **IP-voorvoegsel in**, inclusief CIDR-notatie voor externe netwerken die u verwacht door VPN te verplaatsen. [Dit zijn de netwerken die op uw Cisco-router bestaan.]

1 Routing Options Dynamic (requires BGP) Static

Static IP Prefixes	IP Prefixes	Source	State
2	10.0.10.0/24	-	-

Add Another Rule

Stap 9

We zullen geen van de **tunnelopties** in deze handleiding bestrijken - selecteer *VPN-verbinding maken*.

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1 ⓘ

Pre-Shared Key for Tunnel 1 ⓘ

Inside IP CIDR for Tunnel 2 ⓘ

Pre-shared key for Tunnel 2 ⓘ

Advanced Options for Tunnel 1 Use Default Options
 Edit Tunnel 1 Options

Advanced Options for Tunnel 2 Use Default Options
 Edit Tunnel 2 Options

VPN connection charges apply once this step is complete. [View Rates](#)

* Required

Cancel

Stap 10

Maak een **routeswitch-tabel** en associeer de **VPC** die eerder is gemaakt. Druk op **Maken**.

[Route Tables](#) > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

1 Name tag ⓘ

2 VPC* ⓘ

Filter by attributes

- vpc-0e3159af82f3ecfa4 Cisco_Lab
- vpc-791fec1f

* Required

Cancel

Stap 11

Selecteer de eerder gemaakte **routekaart**. Kies op het tabblad **Subnet Associations** de

subnetverenigingen bewerken.

1

Name	Route Table ID	Explicit subnet association	Edge associations	Main
Subnet-1	rt-12345678	-	-	Yes
Subnet-2	rt-12345678	-	-	Yes

2 Edit subnet associations

Stap 12

Van de pagina **Bewerken** van **Subnet** associaties, selecteer het eerder gemaakte type. Selecteer de eerder gemaakte **routekaart**. Selecteer vervolgens **Opslaan**.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table: rt-12345678

Associated subnets: subnet-12345678-1

1

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-12345678-1 AWS_LAN	172.16.10.0/24	-	rt-12345678

* Required Cancel Save

Stap 13

Kies in het tabblad **Route Propagation**, *routepropagatie bewerken*.

[Create route table](#) Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge association
<input checked="" type="checkbox"/>	-	-
<input type="checkbox"/>	-	-

1

Route Table: ...

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)

2 [Edit route propagation](#)

Virtual Private Gateway	Propagate
... AWS_WAN	No

Stap 14

Selecteer de eerder gemaakte **Virtual Private Gateway**.

[Route Tables](#) > Edit route propagation

Edit route propagation

Route table: ...

Virtual Private Gateway	Propagate
... AWS_WAN	<input checked="" type="checkbox"/>

1

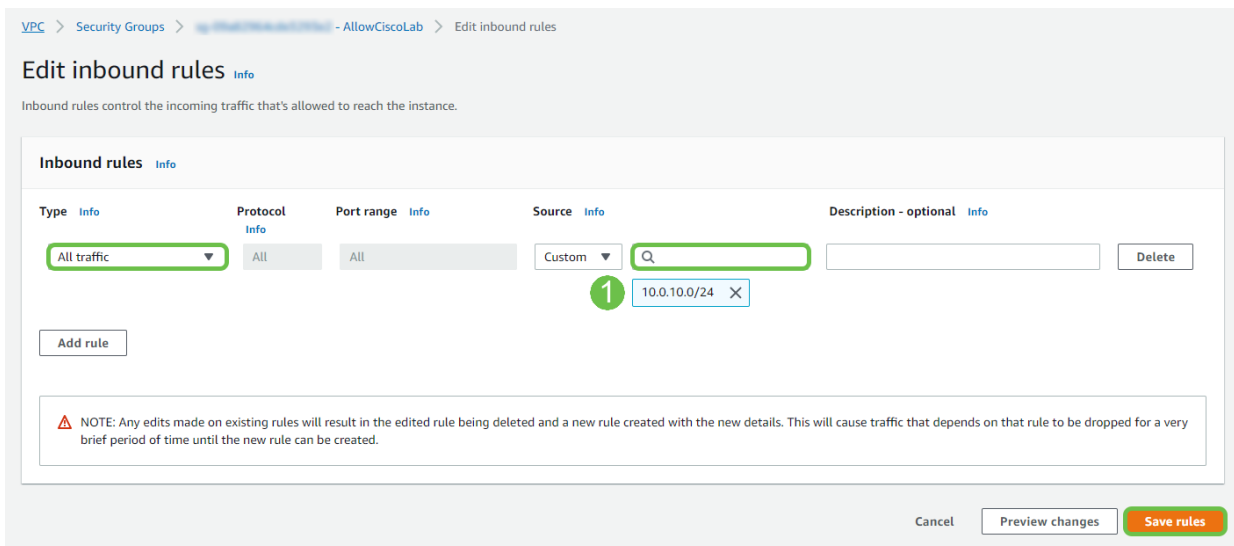
* Required

Cancel [Save](#)

Stap 15

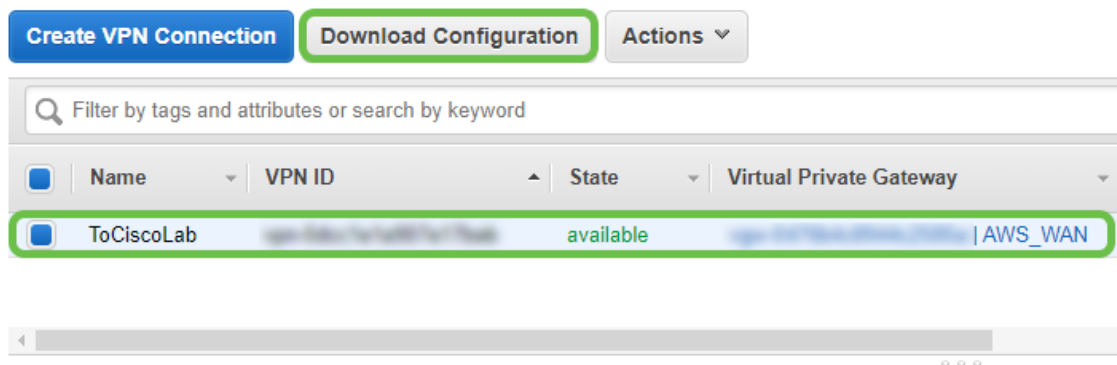
Zorg er bij VPC > Security Group voor dat u een beleid hebt gestart om het gewenste verkeer mogelijk te maken.

Opmerking: In dit voorbeeld gebruiken we een bron van 10.0.10.0/24 - wat overeenkomt met het subtype in gebruik op onze voorbeeld-RV-router.



Stap 16

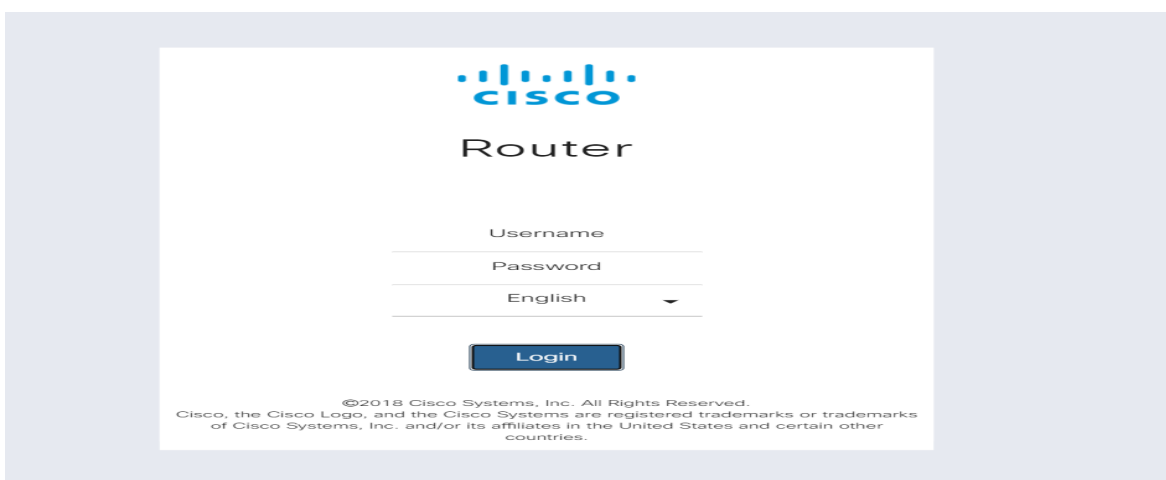
Selecteer de VPN-verbinding die u eerder hebt gemaakt en kies *Downloadconfiguratie*.



Site-to-Site op een RV16X/RV26X, RV34X router

Stap 1

Meld u aan bij de router met geldige aanmeldingsgegevens.



Stap 2

Navigeer naar **VPN > IPsec profielen**. Dit brengt u naar de pagina met het IPsec-profiel en druk op

het pictogram toevoegen (+).

Name	Policy	IKE Version	In Use
Default	Auto	IKEv1	Yes
Amazon_Web_Services	Auto	IKEv1	No
Microsoft_Azure	Auto	IKEv1	No

Step 3

We zullen nu ons IPSEC-profiel creëren. Wanneer u het **IPsec-profiel** maakt op uw Small Business-router, zorg er dan voor dat **DH Group 2** voor fase 1 is geselecteerd.

Opmerking: AWS zal lagere niveaus van encryptie en authenticatie ondersteunen - in dit voorbeeld worden AES-256 en SHA2-256 gebruikt.

Add/Edit a New IPsec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 86400. Default: 28800)

Step 4

Zorg ervoor dat uw fase twee opties overeenkomen met de opties die in fase één zijn gemaakt. Voor AWS moet DH Group 2 worden gebruikt.

Phase II Options

Protocol Selection: ESP

Encryption: AES-256

Authentication: SHA2-256

SA Lifetime: 3600 sec. (Range: 120 - 28800. Default: 3600)

Perfect Forward Secrecy: Enable

DH Group: Group2 - 1024 bit

Stap 5

Druk op Toepassen en u gaat naar de pagina IPSEC (Toepassen). Druk nogmaals op Toepassen.

IPSec Profiles Apply Cancel

Name	Policy	IKE Version	In Use
Default	Auto	IKEv1	Yes
Amazon_Web_Services	Auto	IKEv1	No

Stap 6

Navigeren naar VPN > Client om te site en op de client om pagina te plaatsen drukt u op het plus-pictogram (+).

Site-to-Site Apply Cancel

Number of Connections: 0 connected, 1 configured, maximum 19 supported.

Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
s2s_01	172.17.92.109	WAN	Default	192.168.1.1	172.17.92.109	Disconnected	

Stap 7

Wanneer u de IPsec Site-to-Site Connection maakt, dient u het **IPsec-profiel** te selecteren dat in de voorgaande stappen is gemaakt. Gebruik het type **Remote Endpoint** van *statische IP* en voer het adres in dat in de geëxporteerde AWS-configuratie is meegeleverd. Voer de **voorgedeelde sleutel** in die in de geëxporteerde configuratie van AWS is meegeleverd.

Stap 8

Voer de **lokale identificatiecode** in voor uw router voor kleine bedrijven - deze ingang moet overeenkomen met de **klantgateway** die in AWS is gemaakt. Voer het **IP-adres** en het **subnetmasker** in voor uw router voor kleine bedrijven - deze ingang moet overeenkomen met de **statische IP-prefixatie** die aan de **VPN-verbinding** in AWS is toegevoegd. Voer het **IP-adres** en het **subnetmasker** in voor uw router voor kleine bedrijven - deze ingang moet overeenkomen met de **statische IP-prefixatie** die aan de **VPN-verbinding** in AWS is toegevoegd.

Local Group Setup

Local Identifier Type:

Local Identifier: **1**

Local IP Type:

IP Address: **2**

Subnet Mask:

Remote Group Setup

Remote Identifier Type:

Remote Identifier: **3**

Remote IP Type:

IP Address: **4**

Subnet Mask:

Aggressive Mode:

Stap 9

Voer het **Remote Identifier** in voor uw AWS-verbinding - dit wordt weergegeven onder Tunneldetails van de AWS **Site-to-Site VPN-verbinding**. Voer het **IP-adres** en het **subnetmasker** in voor uw AWS-verbinding, dat tijdens de AWS-configuratie is gedefinieerd. Druk vervolgens op **Toepassen**.

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 1 13.56.216.164

Remote IP Type: Subnet

IP Address: 2 172.16.10.0

Subnet Mask: 255.255.255.0

Aggressive Mode:

Stap 10

Enmaail op de IP Site op Site drukken op Toepassen.

Site-to-Site Apply Cancel

Number of Connections: 0 connected, 1 configured, maximum 19 supported.

Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
s2s_01	172.17.92.109	WAN	Default	192.168.1.1	172.17.92.109	Disconnected	

Conclusie

U hebt nu met succes een Site to Site VPN gemaakt tussen uw RV Series-router en uw AWS. Ga voor community-discussies op Site-to-Site VPN naar de [Cisco Small Business Support Community](#)-pagina en zoek naar Site-to-Site VPN.