

VPN site à site avec services Web Amazon

Objectif

L'objectif de cet article est de vous guider dans la configuration d'un VPN site à site entre les routeurs de la gamme Cisco RV et les services Web Amazon.

Périphériques pertinents | Version du logiciel

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

Introduction

Un VPN site à site permet une connexion à deux réseaux ou plus, ce qui donne aux entreprises et aux utilisateurs généraux la possibilité de se connecter à différents réseaux. Amazon Web Services (AWS) fournit de nombreuses plates-formes de cloud computing à la demande, y compris des VPN site à site, qui vous permettent d'accéder à vos plates-formes AWS. Ce guide vous aidera à configurer le VPN site à site sur les routeurs RV16X, RV26X et RV34X sur les services Web Amazon.

Les deux parties sont les suivantes :

[Configuration du VPN site à site sur les services Web Amazon](#)

[Configuration d'un VPN site à site sur un routeur RV16X/RV26X, RV34X](#)

Configuration d'un VPN site à site sur les services Web Amazon

Étape 1

Créez un VPC, définissant un **bloc CIDR IPv4**, dans lequel nous définirons plus tard le LAN utilisé comme notre *LAN AWS*. Sélectionnez *Créer*.

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

Étape 2

Lors de la création du sous-réseau, assurez-vous que vous avez sélectionné le VPC créé précédemment. Définissez un sous-réseau dans le réseau /16 existant créé précédemment. Dans cet exemple, 172.16.10.0/24 est utilisé.

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 ⓘ

VPC CIDRs

VPC CIDRs	Status	Status Reason
172.16.0.0/16	associated	

2 IPv4 CIDR block* 172.16.10.0/24 ⓘ

* Required

Create

Étape 3

Créez une **passerelle client**, en définissant l'**adresse IP** comme *adresse IP publique* de votre routeur RV Cisco.

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

Étape 4

Créer une **passerelle privée virtuelle** : création d'une *balise Name* pour vous aider à vous identifier ultérieurement.

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

Étape 5

Connectez la passerelle privée virtuelle au VPC créé précédemment.

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC

Cisco_Lab

* Required

Cancel

étape 6

Créez une nouvelle connexion VPN, en sélectionnant le type de passerelle cible *Passerelle privée virtuelle*. Associez la connexion VPN à la passerelle privée virtuelle créée précédemment.

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

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

Étape 7

Sélectionnez *Existant Customer Gateway*. Sélectionnez la passerelle client créée précédemment.

1 Customer Gateway Existing
 New

2 Customer Gateway ID

Routing Options

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

Étape 8

Pour **Options de routage**, assurez-vous de sélectionner Statique. Entrez les **préfixes IP** y compris la notation CIDR pour tous les réseaux distants que vous prévoyez de traverser le VPN. [Voici les réseaux qui existent sur votre routeur Cisco.]

1 Routing Options Dynamic (requires BGP) Static

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

Add Another Rule

Étape 9

Nous ne couvrirons aucune des **options de tunnel** dans ce guide - sélectionnez *Créer une connexion VPN*.

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

Étape 10

Créez une **table de routage** et associez le **VPC** créé précédemment. Appuyez sur **Créer**.

[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	

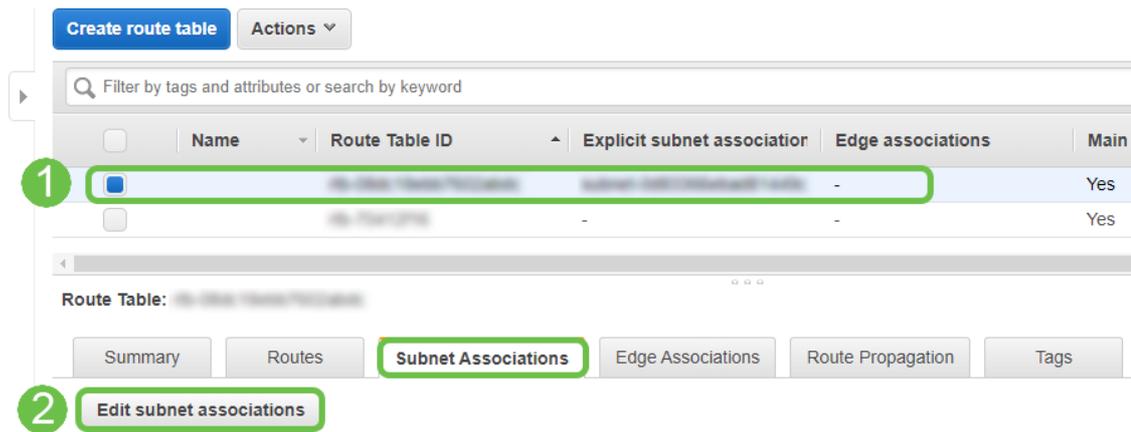
* Required

Cancel

Étape 11

Sélectionnez la **table de routage** créée précédemment. Dans l'onglet **Associations de sous-**

réseaux, sélectionnez **Modifier les associations de sous-réseaux**.

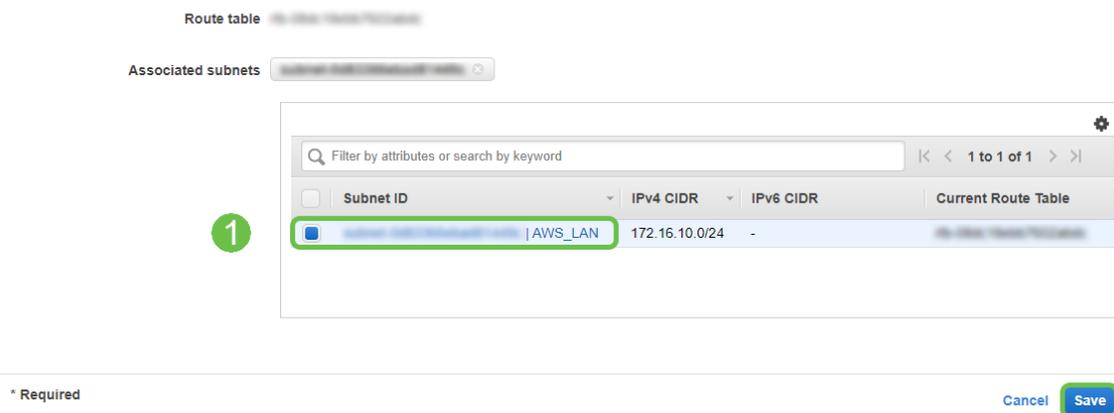


Étape 12

Dans la page **Modifier les associations de sous-réseaux**, sélectionnez le sous-réseau créé précédemment. Sélectionnez la **table de routage** créée précédemment. Sélectionnez ensuite **Enregistrer**.

[Route Tables](#) > Edit subnet associations

Edit subnet associations



Étape 13

Dans l'onglet **Propagation de route**, sélectionnez **Modifier la propagation de route**.

[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"/>	rt-1234567890	rt-1234567890	-	-
<input type="checkbox"/>	rt-1234567890	rt-1234567890	-	-

1

Route Table: rt-1234567890

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

2 [Edit route propagation](#)

Virtual Private Gateway	Propagate
vpn-1234567890 AWS_WAN	No

Étape 14

Sélectionnez la **passerelle privée virtuelle** créée précédemment.

[Route Tables](#) > Edit route propagation

Edit route propagation

Route table: rt-1234567890

Route propagation	Virtual Private Gateway	Propagate
1	vpn-1234567890 AWS_WAN	<input checked="" type="checkbox"/>

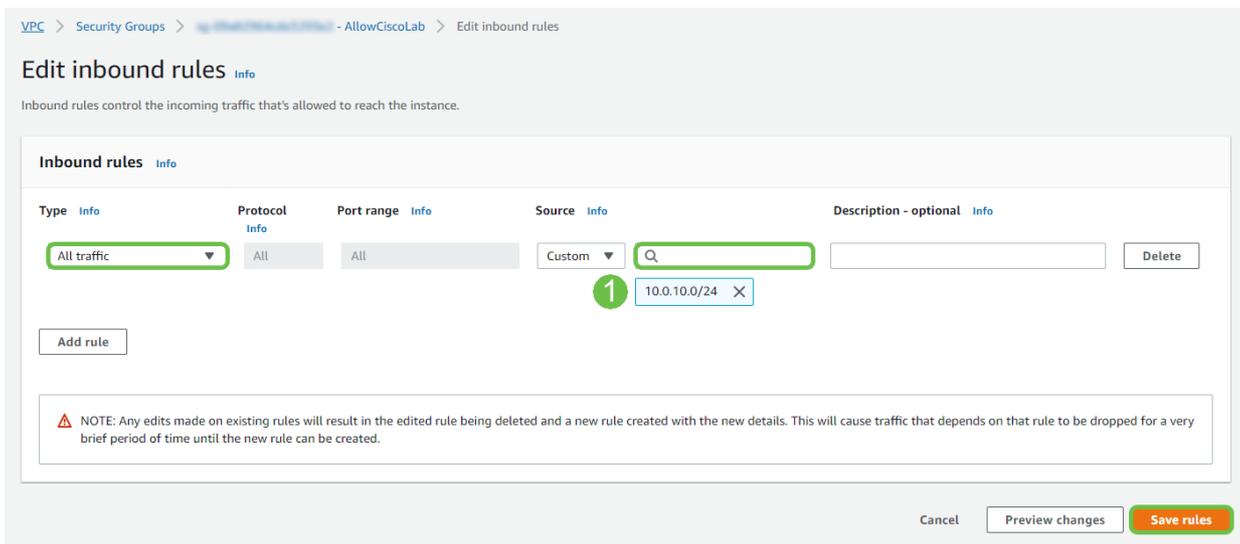
* Required

Cancel [Save](#)

Étape 15

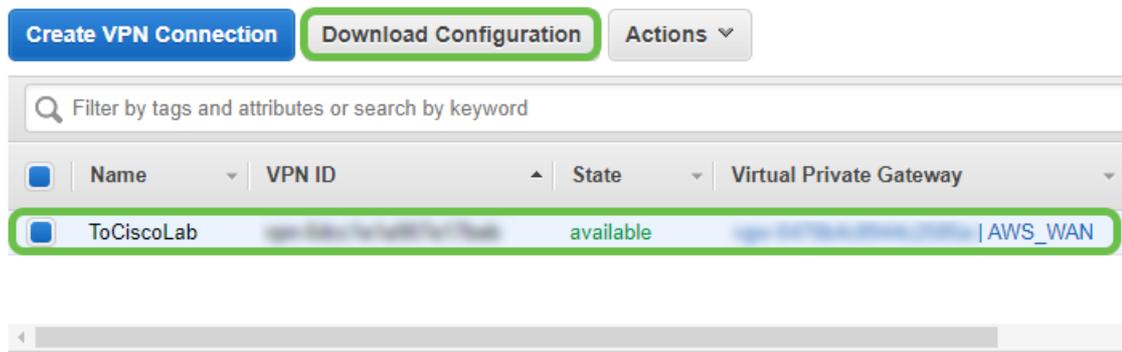
À partir de **VPC > Groupes de sécurité**, assurez-vous qu'une stratégie a été créée pour autoriser le trafic souhaité.

Note: Dans cet exemple, nous utilisons une source de 10.0.10.0/24 qui correspond au sous-réseau utilisé sur notre exemple de routeur RV.



Étape 16

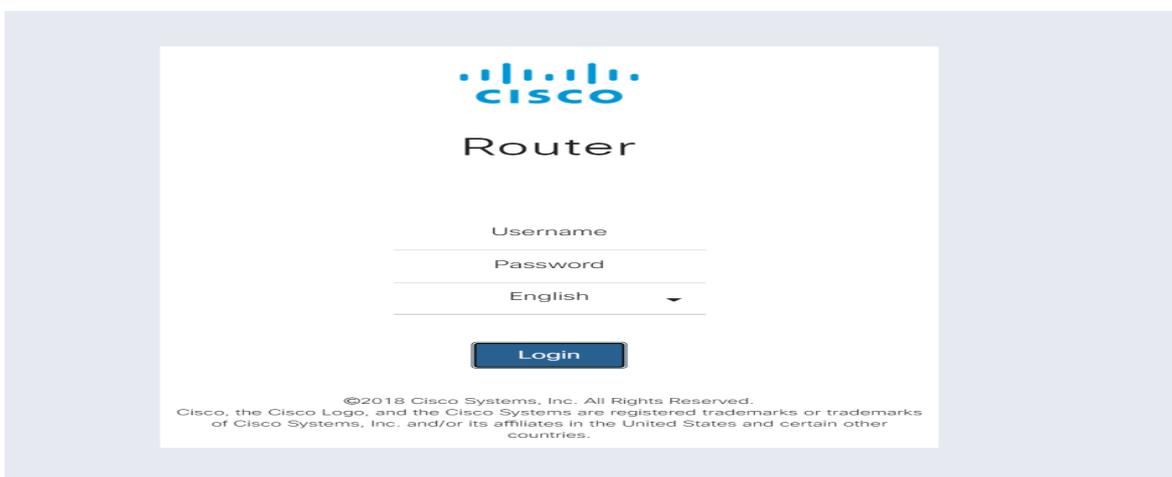
Sélectionnez la connexion VPN que vous avez créée précédemment et choisissez *Télécharger la configuration*.



Configuration de site à site sur un routeur RV16X/RV26X, RV34X

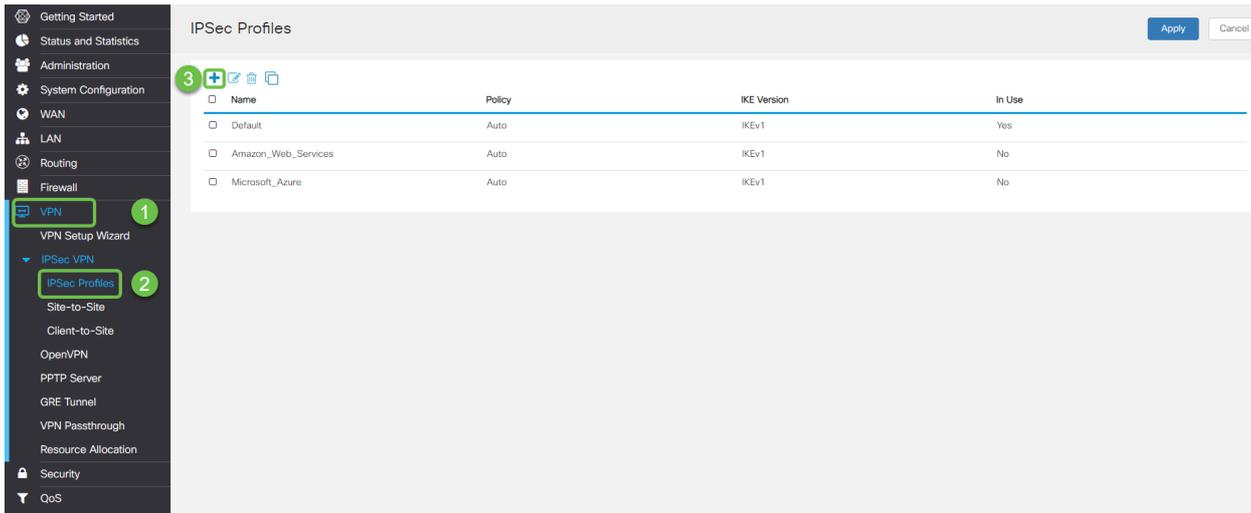
Étape 1

Connectez-vous au routeur à l'aide d'informations d'identification valides.



Étape 2

Accédez à **VPN > Profils Ipsec**. Vous accédez alors à la page de profil Ipsec, puis appuyez sur l'icône d'ajout (+).



Étape 3

Nous allons maintenant créer notre profil IPSEC. Lors de la création du **profil IPsec** sur votre routeur Small Business, assurez-vous que **DH Group 2** est sélectionné pour la phase 1.

Note: AWS prend en charge des niveaux de chiffrement et d'authentification inférieurs. Dans cet exemple, AES-256 et SHA2-256 sont utilisés.

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)

Étape 4

Assurez-vous que les options de la phase deux correspondent à celles de la phase un. Pour AWS DH Group 2 doit être utilisé.

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

Étape 5

Appuyez sur Apply (Appliquer) et vous accédez à la page IPSEC. Veillez à appuyer à nouveau sur Apply (Appliquer).

IPSec Profiles Apply Cancel

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

Étape 6

Accédez à VPN < Client to site et sur la page client to site, appuyez sur l'icône plus (+).

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	

Étape 7

Lors de la création de la connexion de site à site IPsec, assurez-vous de sélectionner le **profil IPsec** créé au cours des étapes précédentes. Utilisez le type **Remote Endpoint** de *Static IP* et saisissez l'adresse fournie dans la configuration AWS exportée. Entrez la **clé prépartagée** fournie dans la configuration exportée à partir d'AWS.

Étape 8

Entrez l'**identificateur local** de votre routeur Small Business. Cette entrée doit correspondre à la **passerelle du client** créée dans AWS. Entrez l'**adresse IP** et le **masque de sous-réseau** de votre routeur Small Business. Cette entrée doit correspondre au **préfixe IP statique** ajouté à la **connexion VPN** dans AWS. Entrez l'**adresse IP** et le **masque de sous-réseau** de votre routeur Small Business. Cette entrée doit correspondre au **préfixe IP statique** ajouté à la **connexion VPN** dans AWS.

Local Group Setup

Local Identifier Type:	<input type="text" value="Local WAN IP"/>
Local Identifier:	<input type="text" value="1"/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="2 10.0.10.0"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="3"/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="4 172.16.10.0"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Aggressive Mode:	<input type="checkbox"/>

Étape 9

Entrez l'**identificateur distant** de votre connexion AWS - cette liste sera affichée sous Tunnel Details de la **connexion VPN site à site AWS** . Entrez l'**adresse IP** et le **masque de sous-réseau** pour votre connexion AWS, qui a été définie lors de la configuration AWS. Appuyez ensuite sur **Appliquer**.

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:

Étape 10

Une fois sur la page Ip Site to Site, appuyez sur **Apply**.

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	

Conclusion

Vous avez maintenant créé un VPN site à site entre votre routeur RV et votre AWS. Pour les discussions de communauté sur le VPN site à site, accédez à la page [Communauté d'assistance Cisco Small Business](#) et recherchez le VPN site à site.