

VPN de sitio a sitio con Amazon Web Services

Objetivo

El objetivo de este artículo es guiarle a través de la configuración de una VPN de sitio a sitio entre los routers de la serie RV de Cisco y Amazon Web Services.

Dispositivos aplicables | Versión de software

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

Introducción

Una VPN de sitio a sitio permite una conexión a dos o más redes, lo que proporciona a las empresas y a los usuarios en general la capacidad de conectarse a diferentes redes. Amazon Web Services (AWS) proporciona muchas plataformas de Cloud Computing a demanda, incluidas VPNS de sitio a sitio que le permiten acceder a sus plataformas AWS. Esta guía le ayudará a configurar la VPN de sitio a sitio en los routers RV16X, RV26X y RV34X a Amazon Web Services.

Las dos partes son las siguientes:

[Configuración de VPN de sitio a sitio en Amazon Web Services](#)

[Configuración de VPN de sitio a sitio en un router RV16X/RV26X, RV34X](#)

Configuración de una VPN de sitio a sitio en Amazon Web Services

Paso 1

Cree un nuevo VPC, definiendo un **bloque CIDR IPv4**, en el cual definiremos posteriormente la LAN utilizada como nuestra *LAN AWS*. Seleccione *Crear*.

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 ⓘ

2 IPv4 CIDR block* ⓘ

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

Tenancy ⓘ

* Required

3

Paso 2

Al crear la subred, asegúrese de haber seleccionado el **VPC** creado anteriormente. Defina una subred dentro de la red /16 existente creada anteriormente. En este ejemplo, se utiliza 172.16.10.0/24.

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 ⓘ

1 VPC* ⓘ

Availability Zone ⓘ

VPC CIDRs	Status	Status Reason
172.16.0.0/16	associated	

2 IPv4 CIDR block* ⓘ

* Required

Paso 3

Cree una **gateway del cliente**, definiendo la **dirección IP** como la *dirección IP pública* del router Cisco RV.

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 ⓘ

Routing Dynamic
 Static

2 IP Address ⓘ

Certificate ARN ⓘ

Device ⓘ

* Required

Paso 4

Cree un **Virtual Private Gateway** - creando una *etiqueta Name* para ayudar a identificar más adelante.

Para **Opciones de ruteo**, asegúrese de seleccionar Estático. Ingrese cualquier **Prefijos IP** incluyendo la notación CIDR para cualquier red remota que espere atravesar la VPN. [Estas son las redes que existen en el router de Cisco.]

1 Routing Options Dynamic (requires BGP) Static

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

2

Add Another Rule

Paso 9

No trataremos ninguna de las **opciones de túnel** en esta guía: seleccione *Crear conexión 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

Paso 10

Cree una **tabla de rutas** y asocie el **VPC** creado anteriormente. Pulse **Crear**.

[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

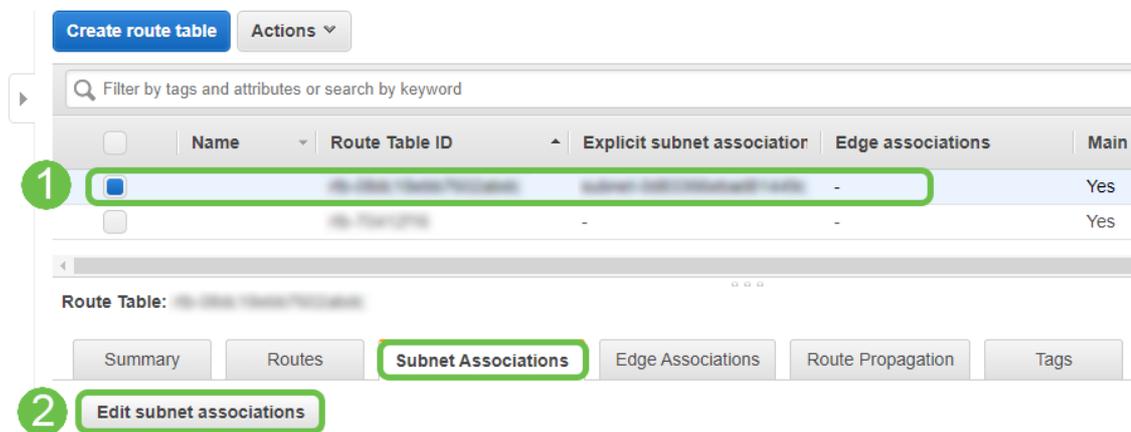
- vpc-0e3159af82f3ecfa4 Cisco_Lab
- vpc-791fec1f

* Required

Cancel

Paso 11

Seleccione la **tabla de rutas** creada anteriormente. En la pestaña **Asociaciones de subred**, elija **Editar asociaciones de subred**.

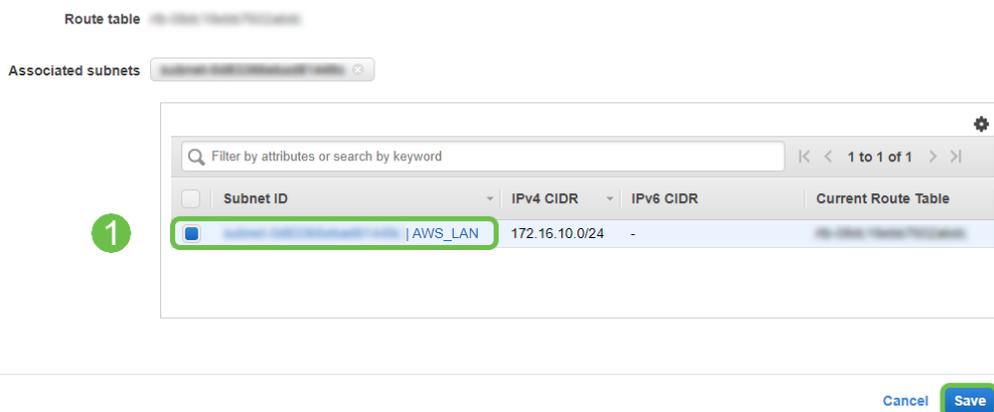


Paso 12

En la página **Editar asociaciones de subred**, seleccione la subred creada anteriormente. Seleccione la **tabla de rutas** creada anteriormente. A continuación, seleccione **guardar**.

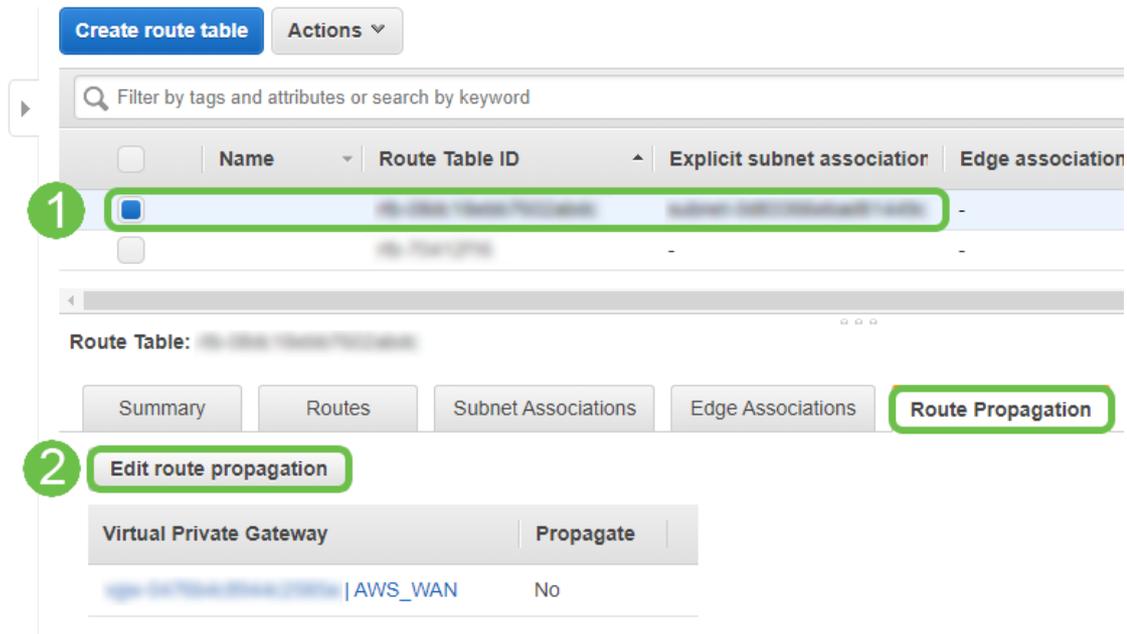
[Route Tables](#) > Edit subnet associations

Edit subnet associations



Paso 13

En la pestaña **Propagación de ruta**, elija *Editar propagación de ruta*.



Paso 14

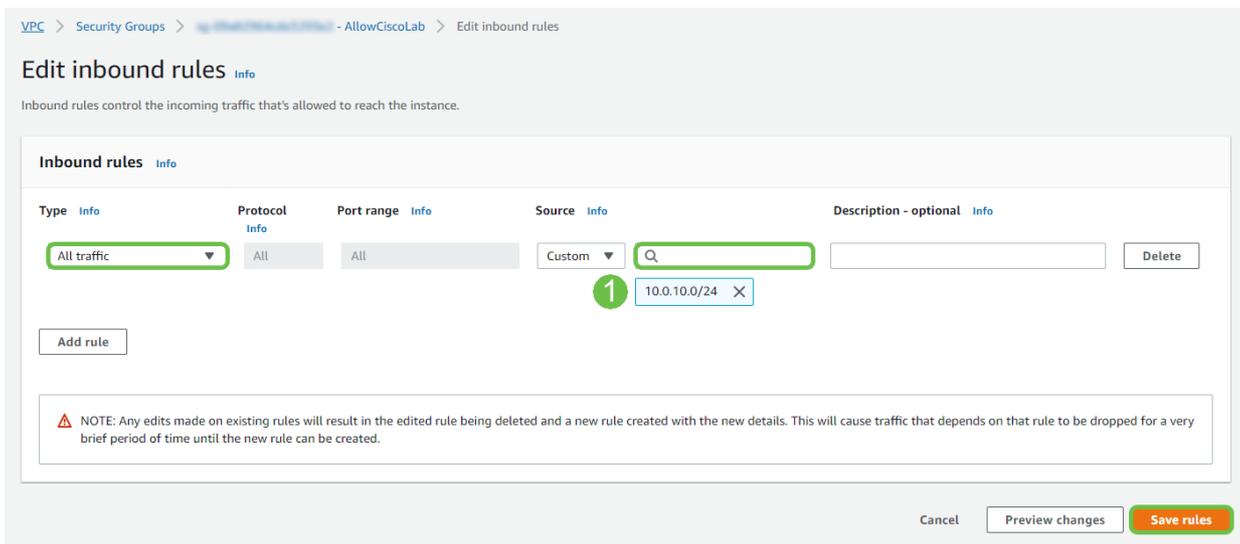
Seleccione el **Virtual Private Gateway** creado anteriormente.



Paso 15

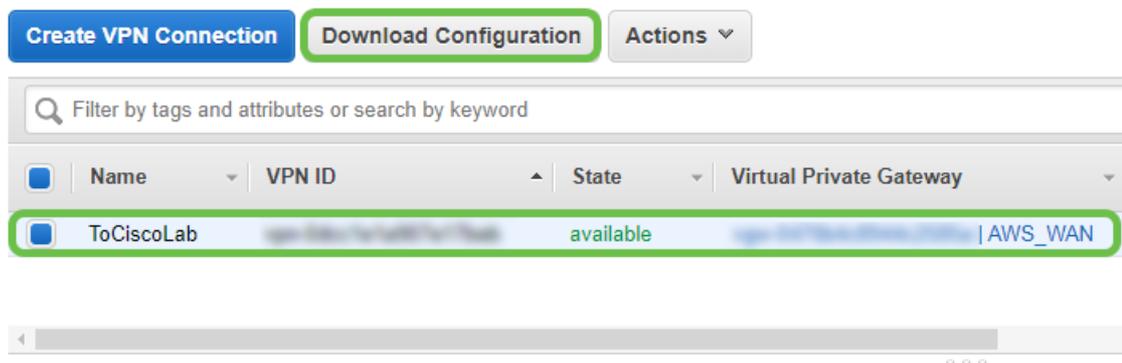
Desde **VPC > Security Groups**, asegúrese de que tiene una política creada para permitir el tráfico deseado.

Nota: En este ejemplo, estamos utilizando un origen de 10.0.10.0/24 - que corresponde a la subred en uso en nuestro router RV de ejemplo.



Paso 16

Seleccione la conexión VPN que ha creado anteriormente y elija *Descargar configuración*.



Configuración de sitio a sitio en un router RV16X/RV26X, RV34X

Paso 1

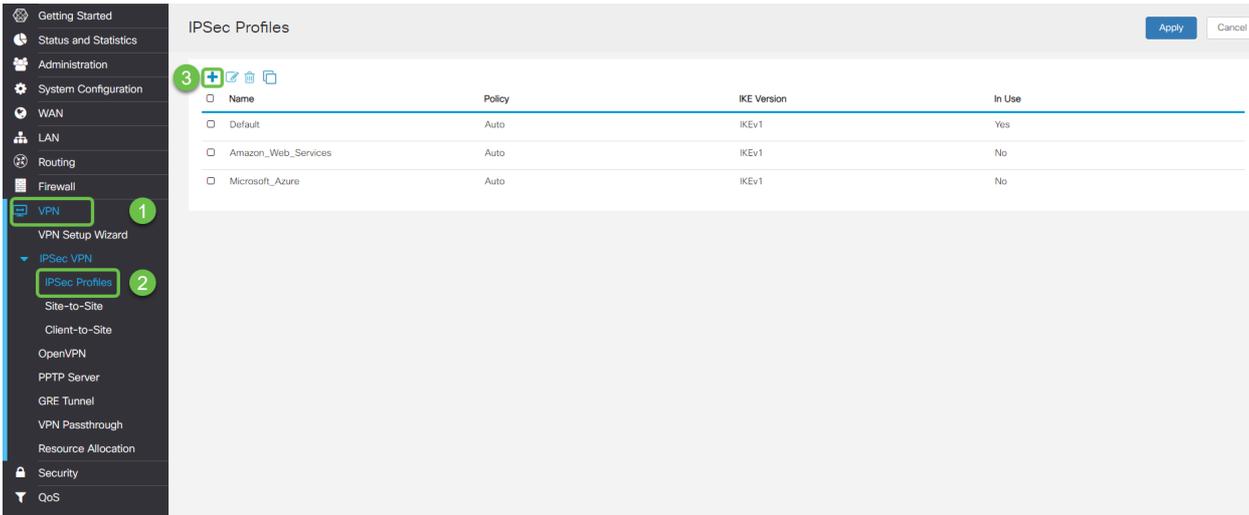
Inicie sesión en el router con credenciales válidas.



Paso 2

Navigate hasta **VPN > Perfiles Isec**. De este modo, accederá a la página Perfil de IPsec y pulse

el icono de agregar (+).



Paso 3

Ahora crearemos nuestro perfil IPSEC. Al crear el **perfil IPsec** en su router Small Business, asegúrese de que **DH Group 2** esté seleccionado para la Fase 1.

Nota: AWS admitirá niveles más bajos de cifrado y autenticación; en este ejemplo, se utilizan AES-256 y SHA2-256.

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)

Paso 4

Asegúrese de que las opciones de la fase dos coinciden con las de la fase uno. Para AWS DH Group 2 se debe utilizar.

Phase II Options

Protocol Selection:

Encryption:

Authentication:

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

Perfect Forward Secrecy: Enable

DH Group:

Paso 5

Pulse Aplicar y accederá a la página IPSEC; asegúrese de pulsar Aplicar una vez más.

IPSec Profiles Apply Cancel

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

Paso 6

Desplácese hasta VPN < Cliente a sitio y, en la página cliente a sitio, pulse el icono más (+).

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	

Paso 7

Al crear la conexión de sitio a sitio IPsec, asegúrese de seleccionar el **perfil IPsec** creado en los pasos anteriores. Utilice el tipo de **terminal remoto** de *IP estática* e introduzca la dirección proporcionada en la configuración de AWS exportada. Introduzca la **clave precompartida** proporcionada en la configuración exportada de AWS.

Paso 8

Introduzca el **identificador local** para el router Small Business; esta entrada debe coincidir con la **puerta de enlace del cliente** creada en AWS. Ingrese la **dirección IP** y la **máscara de subred** para su router Small Business; esta entrada debe coincidir con el **prefijo IP estático** agregado a la **conexión VPN** en AWS. Ingrese la **dirección IP** y la **máscara de subred** para su router Small Business; esta entrada debe coincidir con el **prefijo IP estático** agregado a la **conexión VPN** en AWS.

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:

Paso 9

Ingrese el **identificador remoto** para su conexión AWS - esto aparecerá en Detalles del Túnel de la **Conexión VPN de Sitio a Sitio AWS** . Ingrese la **dirección IP** y la **máscara de subred** para su conexión AWS, que se definió durante la configuración de AWS. A continuación, pulse **Aplicar** .

Remote Group Setup

Remote Identifier Type:

Remote Identifier: **1**

Remote IP Type:

IP Address: **2**

Subnet Mask:

Aggressive Mode:

Paso 10

Una vez en la página Sitio a Sitio de Ip, presione **Aplicar**.

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	

Conclusión

Ya ha creado correctamente una VPN de sitio a sitio entre el router de la serie RV y su AWS. Para los debates de la comunidad sobre VPN de sitio a sitio, vaya a la página [Cisco Small Business Support Community](#) y busque VPN de sitio a sitio.