# 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 <u>1.0.00.17</u>

RV260|<u>1.0.00.17</u>

RV340| <u>1.0.03.18</u>

RV345| <u>1.0.03.18</u>

# 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*.

VPCs >	Create	VPC
--------	--------	-----

Create VPC

A VPC is an isolated portion of the AWS c block; for example, 10.0.0.0/16. You cannot	oud populated by AWS objects, such as Amazon EC2 in to specify an IPv4 CIDR block larger than /16. You can o	stances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CID ptionally associate an IPv6 CIDR block with the VPC.	२)
Name tag	Cisco_Lab	0	
IPv4 CIDR block*	172.16.0.0/16	0	
IPv6 CIDR block	<ul> <li>No IPv6 CIDR Block</li> <li>Amazon provided IPv6 CIDR block</li> </ul>		
Tenancy	Default	0	
* Required		3 Create	

#### 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.

Subnets > Create subnet			
Create subnet			
Specify your subnet's IP address block in C	CIDR format; for example, 10.0.0.0/24. IPv4 block sizes i	must be between a /16 netmask and /28 netmask, and can be th	e same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.
Name tag	AWS_LAN	0	
		0	
Availability Zone	<b>Q</b> Filter by attributes	0	
VPC CIDRs	Cisco_Lab	Status	Status Reason
	172.16.0.0/16	associated	
2 IPv4 CIDR block*	172.16.10.0/24	) ⊕	
* Required			Create

### Paso 3

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

Customer Gateways > Create Customer	Gateway		
Create Customer Gat	eway		
Specify the Internet-routable IP address fo also specify your gateway's Border Gateway	r your gateway's external interface; the address must be ay Protocol (BGP) Autonomous System Number (ASN); ti	static and may be behind a device performing network address his can be either a public or private ASN (such as those in the	s translation (NAT). For dynamic routing, 64512-65534 range).
VPNs can use either Pre-Shared Keys or ( you create your Customer Gateway. To use	Certificates for authentication. When using Certificate auth Pre-Shared Keys, only an IP address is required.	hentication, an IP address is optional. To use Certificate auther	ntication, specify a Certificate ARN when
1 Name	ToCiscoLab	Ð	
Routing	<ul><li>Dynamic</li><li>Static</li></ul>		
2 IP Address	68.227.227.57	Ð	
Certificate ARN	Select Certificate ARN	CO	
Device	Lab_Router	0	
* Required			Cancel Create Customer Gateway

#### Paso 4

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

Virtual Private Gateways > Create Virtua	I Private Gateway							
Create Virtual Private	Create Virtual Private Gateway							
A virtual private gateway is the router on the	e Amazon side of the VPN tunnel.							
1 Name tag	AWS_WAN	0						
ASN	Amazon default ASN     Custom ASN							
* Required		Cancel	Create Virtual Private Gateway					

#### Conecte el Virtual Private Gateway al VPC creado anteriormente.

Virtual Private Gateways > Attach to VPC	
Attach to VPC	
Select the VPC to attach to the virtual private gateway.	
Virtual Private Gateway Id	
	-) c
* Required Cisco_Lab	Cancel Yes, Attach

#### paso 6

Cree una nueva **conexión VPN**, seleccionando el **tipo de gateway de destino** *Virtual Private Gateway*. Asocie la **conexión VPN** con la **Virtual Private Gateway** creada anteriormente.



#### Paso 7

Seleccione *Gateway* del cliente *existente*. Seleccione la **puerta de enlace del cliente** creada anteriormente.



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	<ul><li>Dynamic (requires BGP)</li><li>Static</li></ul>	]			
	Static IP Prefixes	IP Prefixes	Source	State		0
	2	10.0.10.0/24	) -	-	8	
		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	Generated by Amazon	0	
Pre-Shared Key for Tunnel 1	Generated by Amazon	0	
Inside IP CIDR for Tunnel 2	Generated by Amazon	0	
Pre-shared key for Tunnel 2	Generated by Amazon	0	
Advanced Options for Tunnel 1	<ul> <li>Use Default Options</li> <li>Edit Tunnel 1 Options</li> </ul>		
Advanced Options for Tunnel 2	<ul> <li>Use Default Options</li> <li>Edit Tunnel 2 Options</li> </ul>		
VPN connection charges apply once this s	tep is complete. View Rates		
* Required		Can	cel Create VPN Connection

### 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. Name tag CiscoLab VPC\* Filter by attributes vpc-0e3159af82f3ecfa4 Vpc-791fec1f Cancel Create

#### Paso 11

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

<b>Q</b> Filter by tags and	attributes or searc	h by keyword			
Nam	e - Rou	te Table ID 🔶 E	Explicit subnet associat	on Edge association	s Mai
	- 6-1	to the YOAR I	and the state of the	-	Yes
	19.7	541276		-	Yes
4					
Route Table:	10400 To 2400		000		
Summary	Routes	Subnet Associations	Edge Associations	Route Propagation	Tags
Edit subnet ass	ociations				

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

Route table	0113	
Associated subnets		
	Q Filter by attributes or search by keyword	K < 1 to 1 of 1 > X
1	AWS_LAN 172.16.10.0/24 -	Current Route Table
equired		Cancel Sav

### Paso 13

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

Create route t	able Actions 👻			
► Filter by tag	gs and attributes or sear	ch by keyword		
	Name - Ros	ute Table ID	Explicit subnet associ	ation Edge association
		Interface Property	salest introduced in	-
	-	7541 (214)	-	-
4				
Route Table:	No. No. No. No.		52 53 53	
Summary	Routes	Subnet Associations	Edge Associations	Route Propagation
2 Edit route	propagation			
Virtual Priv	ate Gateway	Propagate		
194 DC704	AWS_	WAN No		

Seleccione el Virtual Private Gateway creado anteriormente.

Route Tables > Edit route propagation			
Edit route propagatio	n		
Route table	0.00.00070344		
Route propagation	Virtual Private Gateway	Propagate	
* Required			Cancel Save

# 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.

VPC > Security Groups >	40764-040205	- AllowCiscoLab > Edit i	nbound rules		
Edit inbound rules	Info				
Inbound rules control the incoming to	raffic that's allow	ed to reach the instance.			
Inbound rules Info					
Type Info	Protocol	Port range Info	Source Info	Description - optional Info	
All traffic 🔹	All	All	Custom 🔻 🔍		Delete
			10.0.10.0/2	24 🗙	
Add rule					
NOTE: Any edits made on e brief period of time until the second s	existing rules will he new rule can b	result in the edited rule bein be created.	g deleted and a new rule created with th	he new details. This will cause traffic that depends on that rule to be d	lropped for a very
				Cancel Preview change	es Save rules

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

Create VPN Connection Downlo	ad Configuration Actions 👻	
Q Filter by tags and attributes or search	ch by keyword	
Name - VPN ID	▲ State → Virtual	Private Gateway -
ToCiscoLab	available	AWS_WAN
		0.0.0

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

### Paso 1

Inicie sesión en el router con credenciales válidas.

1		
F	Router	
	Username	
	Password	
	English 🗸	
	Login	
©2018 Cisco Sy Cisco, the Cisco Logo, and the Cisc of Cisco Systems, Inc. and/or its	stems, Inc. All Rights Rese o Systems are registered s a affiliates in the United Sta countries.	erved. trademarks or trademarks ates and certain other

## Paso 2

Navegue hasta VPN > Perfiles Ipsec. De este modo, accederá a la página Perfil de IPSec y pulse

el icono de agregar (+).

-	Getting Started	IF	000	Drofiles				Annalus	Ormani
•	Status and Statistics	IP							Cancer
**	Administration	0	ш	R A B					
٠	System Configuration	ి		Name	Policy	IKE Version	In Use		
۲	WAN		-	Default	Auto	IKEv1	Yes		
#	LAN						No.		
8	Routing			Amazon_web_Services	Auto	IKEV I	ND		
	Firewall			Microsoft_Azure	Auto	IKEv1	No		
₽	VPN 1								
	VPN Setup Wizard								
·	IPSec VPN IPSec Profiles 2								
	Site-to-Site								
	Client-to-Site								
	OpenVPN								
	PPTP Server								
	GRE Tunnel								
	VPN Passthrough								
	Resource Allocation								
<b></b>	Security								
T	QoS								

#### 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:	AWS_Lab					
IKE Version:	<ul> <li>KEv1 O IKEv2</li> </ul>					
Phase I Options						
DH Group:	Group2 - 1024 bit 🗸					
Encryption:	AES-256					
Authentication:	SHA2-256					
SA Lifetime:	28800 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:	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	~

#### Paso 5

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

IPSec Profiles				Apply Cancel
+ 🕜 🖮 🗋 D 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 (+).

8	Getting Started	0.0	a ta Sita								and a
G	Status and Statistics	31	te-to-Site								
*	Administration	Nun	nber of Connections: 0 connec	ted, 1 configured, maximum 19 su	pported.						
٠	System Configuration	2									
۲	WAN	2	Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions	
4	LAN	1.1	□ s2s 01	172.17.92.109	WAN	Default	192,168,1,1	172.17.92.109	Disconnected	<i>6</i> 0	- 1
<b>?</b>	Wireless										
8	Routing										
	Firewall										
•	VPN 1										
	VPN Setup Wizard										
-	IPSec VPN										
	IPSec Profiles										
	Site-to-Site 2										
	Client-to-Site										
	OpenVPN										
	PPTP Server										6
	GRE Tunnel										2
	VPN Passthrough										
	Resource Allocation										

#### 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.

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. 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 AWS.

Local Group Setup		
Local Identifier Type:	Local WAN IP	~
Local Identifier:		
Local IP Type:	Subnet	~
IP Address:	10.0.10.0	
Subnet Mask:	255.255.255.0	
Remote Group Setup Remote Identifier Type:	Remote WAN IP	~
Remote Identifier:	112 (M. 216) (M.	
Remote IP Type:	Subnet	~
IP Address:	172.16.10.0	
Subnet Mask:	255.255.255.0	
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 WAN IP	~
Remote Identifier:	1	13.56.216.164	]
Remote IP Type:	_	Subnet	~
IP Address:		172.16.10.0	כ
Subnet Mask:	2	255.255.255.0	]
Aggressive Mode:	I		

# Paso 10

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

Site-to-Site										
Numbe	Number of Connections: 0 connected, 1 configured, maximum 19 supported.									
+	<b>e</b>									
D	Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions		
0	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 <u>Cisco Small</u> <u>Business Support Community</u> y busque VPN de sitio a sitio.