

VPN site a site com serviços da Web da Amazon

Objetivo

O objetivo deste artigo é guiá-lo na configuração de uma VPN site a site entre os roteadores Cisco RV Series e os serviços da Web da Amazon.

Dispositivos aplicáveis | Versão do software

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

Introduction

Uma VPN site a site permite uma conexão a duas ou mais redes, o que dá às empresas e aos usuários em geral a capacidade de se conectarem a redes diferentes. O Amazon Web Services (AWS) oferece muitas plataformas de computação em nuvem sob demanda, incluindo VPNS site a site, que permitem acessar suas plataformas AWS. Este guia o ajudará a configurar a VPN de site a site nos roteadores RV16X, RV26X e RV34X para os Serviços Web da Amazon.

As duas partes são as seguintes:

[Configurando a VPN site a site nos serviços da Web da Amazon](#)

[Configuração de VPN site a site em um roteador RV16X/RV26X, RV34X](#)

Configurando uma VPN site a site nos serviços da Web da Amazon

Passo 1

Crie um novo VPC, definindo um **bloco CIDR IPv4**, no qual posteriormente definiremos a LAN usada como nossa *LAN AWS*. Selecione *Criar*.

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

Passo 2

Ao criar a sub-rede, certifique-se de ter selecionado o **VPC** criado anteriormente. Defina uma sub-rede dentro da rede /16 existente criada anteriormente. Neste exemplo, 172.16.10.0/24 é usado.

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

Etapa 3

Crie um **Gateway do cliente**, definindo o **Endereço IP** como o *Endereço IP Público* do Roteador 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 ToCiscoLab ⓘ

Routing Dynamic
 Static

2 IP Address 68.227.227.57 ⓘ

Certificate ARN Select Certificate ARN ⓘ

Device Lab_Router ⓘ

* Required

Cancel Create Customer Gateway

Passo 4

Criar um **Virtual Private Gateway** - criar uma *tag Name* para ajudar a identificar mais tarde.

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

Etapa 5

Conecte o **Virtual Private Gateway** ao **VPC** criado anteriormente.

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

etapa 6

Crie uma nova **conexão VPN**, selecionando o **tipo de gateway de destino Virtual Private Gateway**. Associe a **conexão VPN** ao **Virtual Private Gateway** criado anteriormente.

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

Etapa 7

Selecione **Existente Customer Gateway**. Selecione o **Gateway do cliente** criado anteriormente.

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	

Passo 8

Para **opções de roteamento**, selecione Estático. Insira qualquer **prefixo IP** incluindo a notação CIDR para qualquer rede remota que você espera atravessar a VPN. [Essas são as redes que existem no roteador Cisco.]

1 Routing Options Dynamic (requires BGP) Static

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

Add Another Rule

Passo 9

Não cobriremos nenhuma das **Opções de Túnel** neste guia - selecione *Criar conexão 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

Passo 10

Crie uma **Tabela de Rotas** e associe o **VPC** criado anteriormente. Pressione **Criar**.

[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

Passo 11

Selecione a **tabela de rotas** criada anteriormente. Na guia **Associações de Sub-Rede**, escolha **Editar associações de sub-rede**.

Create route table Actions

Filter by tags and attributes or search by keyword

	Name	Route Table ID	Explicit subnet association	Edge associations	Main
1					Yes
					Yes

Route Table: **Route Table ID**

Summary Routes **Subnet Associations** Edge Associations Route Propagation Tags

2 Edit subnet associations

Etapa 12

Na página **Editar associações de sub-rede**, selecione a sub-rede criada anteriormente. Selecione a **tabela de rotas** criada anteriormente. Em seguida, selecione **salvar**.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table **Route Table ID**

Associated subnets **Subnet ID**

1

Filter by attributes or search by keyword

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
Subnet ID AWS_LAN	172.16.10.0/24	-	Route Table ID

* Required

Cancel **Save**

Passo 13

Na guia **Route Propagation (Propagação de Rota)**, escolha **Edit route propagation (Editar propagação de rota)**.

The screenshot shows the AWS Management Console interface for configuring a route table. At the top, there is a 'Create route table' button and an 'Actions' dropdown menu. Below this is a search bar labeled 'Filter by tags and attributes or search by keyword'. A table lists route tables with columns for 'Name', 'Route Table ID', 'Explicit subnet association', and 'Edge association'. A green circle with the number '1' highlights the first row of the table. Below the table, the selected route table is shown with tabs for 'Summary', 'Routes', 'Subnet Associations', 'Edge Associations', and 'Route Propagation'. The 'Route Propagation' tab is highlighted with a green box. Below the tabs, there is a table for route propagation settings. A green circle with the number '2' highlights the 'Edit route propagation' button. The table below shows a 'Virtual Private Gateway' with a 'Propagate' checkbox that is currently unchecked.

Passo 14

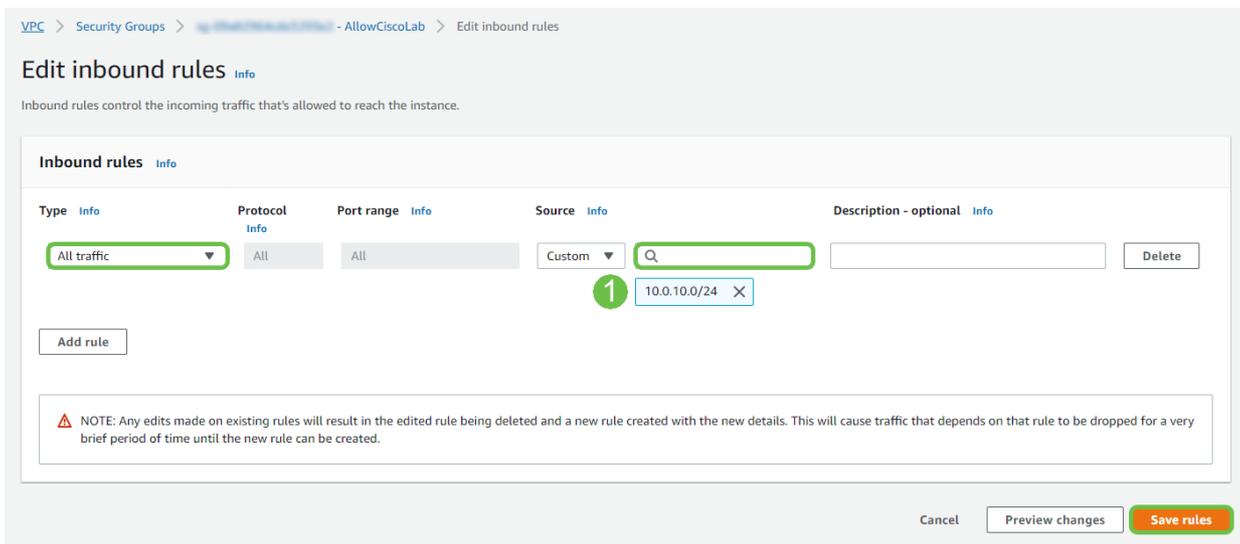
Selecione o **Virtual Private Gateway** criado anteriormente.

The screenshot shows the 'Edit route propagation' page in the AWS Management Console. The page title is 'Edit route propagation'. Below the title, the 'Route table' is identified. The 'Route propagation' section shows a table with two columns: 'Virtual Private Gateway' and 'Propagate'. A green circle with the number '1' highlights the first row of the table, where the 'Propagate' checkbox is checked. At the bottom of the page, there is a '* Required' label and two buttons: 'Cancel' and 'Save'.

Etapa 15

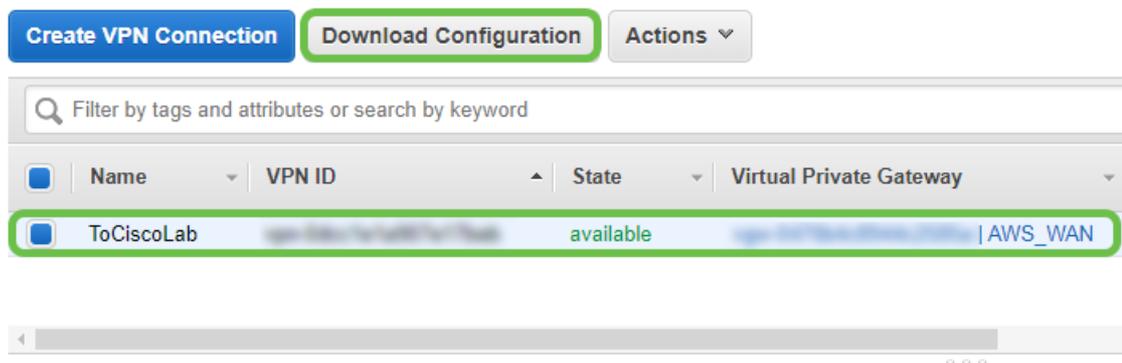
Em **VPC > Security Groups**, certifique-se de que tenha uma política criada para permitir o tráfego desejado.

Note: Neste exemplo, estamos usando uma origem de 10.0.10.0/24 - que corresponde à sub-rede em uso em nosso exemplo de roteador RV.



Passo 16

Selecione a conexão VPN que você criou anteriormente e escolha *Download Configuration*.



Configurando site a site em um roteador RV16X/RV26X, RV34X

Passo 1

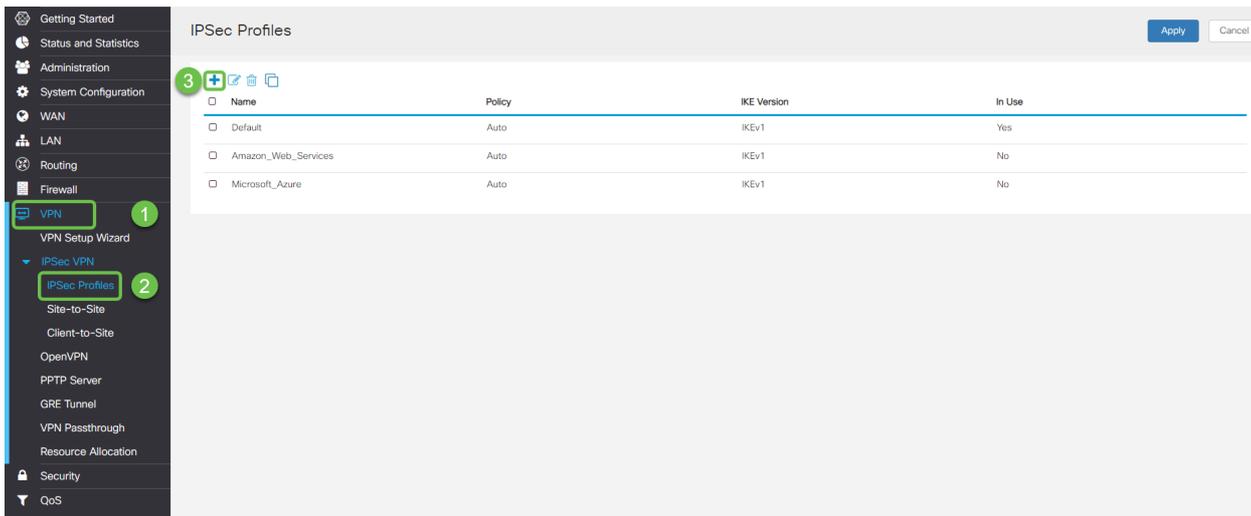
Faça login no roteador usando credenciais válidas.



Passo 2

Navegue até **VPN > Perfis Ipsec**. Isso o levará até a página de perfil Ipsec e pressione o ícone de

adição (+).



Etapa 3

Agora, criaremos nosso perfil IPSEC. Ao criar o **perfil IPsec** no roteador Small Business, verifique se **DH Group 2** está selecionado para a Fase 1.

Note: O AWS suportará níveis mais baixos de criptografia e autenticação - neste exemplo, AES-256 e SHA2-256 são usados.

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)

Passo 4

Certifique-se de que as opções da Fase dois correspondam às da Fase um. Para o AWS DH Group 2 deve ser usado.

Phase II Options

Protocol Selection:

Encryption:

Authentication:

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

Perfect Forward Secrecy: Enable

DH Group:

Etapa 5

Pressione Aplicar e você será direcionado para a página IPSEC. Pressione Aplicar novamente.

IPSec Profiles Apply Cancel

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

Etapa 6

Navegue até VPN < Cliente para site e, na página cliente para site, pressione o ícone de adição (+).

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	

Etapa 7

Ao criar a conexão de site a site IPsec, selecione o **perfil IPsec** criado nas etapas anteriores. Use o tipo de **endpoint remoto de IP estático** e insira o endereço fornecido na configuração de AWS exportada. Insira a **chave pré-compartilhada** fornecida na configuração exportada do AWS.

Passo 8

Insira o **Identificador local** para seu roteador Small Business - essa entrada deve corresponder ao **Gateway do cliente** criado no AWS. Insira o **endereço IP** e a **máscara de sub-rede** para seu roteador Small Business - essa entrada deve corresponder ao **prefixo IP estático** adicionado à **conexão VPN** no AWS. Insira o **endereço IP** e a **máscara de sub-rede** para seu roteador Small Business - essa entrada deve corresponder ao **prefixo IP estático** adicionado à **conexão VPN** no 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:

Passo 9

Insira o **Identificador remoto** para sua conexão AWS - isso será listado em Detalhes do túnel da **Conexão VPN Site-to-Site AWS** . Insira o **endereço IP** e a **máscara de sub-rede** para sua conexão AWS - que foi definida durante a configuração AWS. Em seguida, pressione **Apply (Aplicar)** .

Remote Group Setup

Remote Identifier Type:

Remote Identifier: **1**

Remote IP Type:

IP Address: **2**

Subnet Mask:

Aggressive Mode:

Passo 10

Uma vez na página Site a Site do Ip, pressione **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	

Conclusão

Agora você criou com êxito uma VPN de site para site entre seu roteador série RV e seu AWS. Para discussões da comunidade sobre VPN site a site, vá para a página [Comunidade de Suporte Cisco Small Business](#) e faça uma busca por VPN site a site.