# 使用Amazon Web Services的站点到站点VPN

## 目标

本文的目的是指导您在Cisco RV系列路由器和Amazon Web Services之间设置站点到站点VPN。

## 适用设备 |软件版本

RV160| 1.0.00.17

RV260|1.0.00.17

RV340| 1.0.03.18

RV345| 1.0.03.18

## 简介

站点到站点VPN允许连接到两个或多个网络，这使企业和一般用户能够连接到不同的网络。Amazon Web Services(AWS)提供许多按需云计算平台，包括站点到站点VPNS，让您能够访问AWS平台。本指南将帮助您在RV16X、RV26X、RV34X路由器上配置站点到站点VPN，以连接到Amazon Web Services。

这两部分如下：

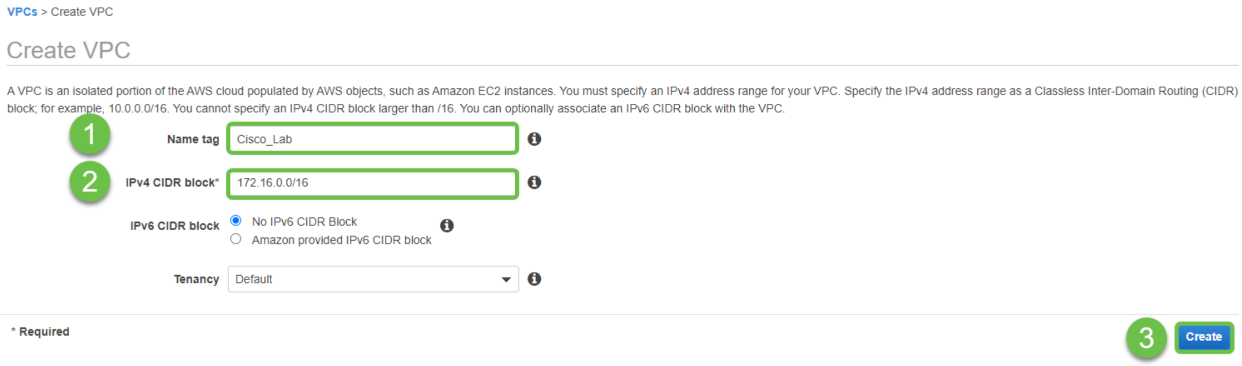
在Amazon Web Services上设置站点到站点VPN

在RV16X/RV26X、RV34X路由器上设置站点到站点VPN

## 在Amazon Web Services上设置站点到站点VPN

### 第 1 步

创建新的VPC，定义**IPv4 CIDR块**，稍后我们将在其中定义用作AWS LAN*的LAN*。选择“*创建*”。



VPCs > Create VPC

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

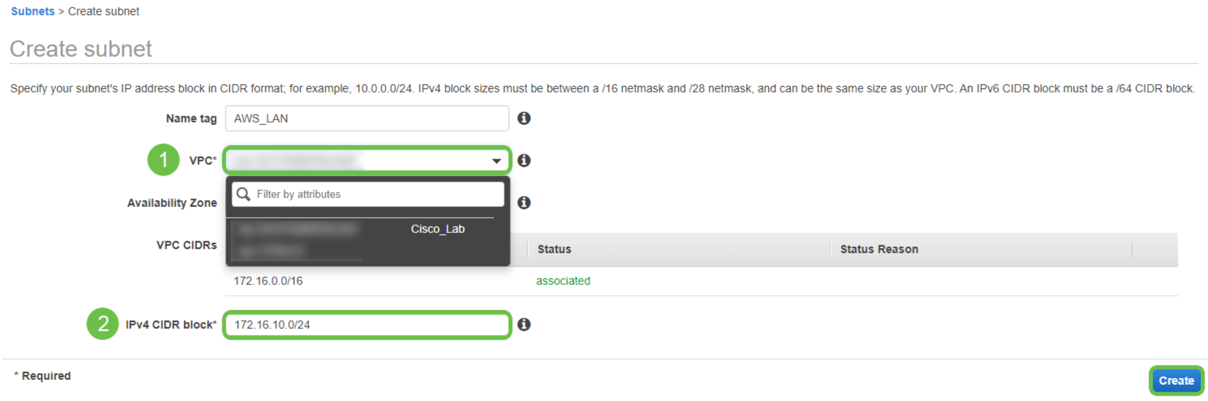
IPv6 CIDR block: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

Tenancy: Default

* Required

## 步骤 2

创建子网时，请确保您已选择之前**创建**的VPC。在之前创建的现有/16网络中定义子网。在本例中，使用172.16.10.0/24。



Subnets > Create subnet

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*: [redacted]

Filter by attributes

[redacted] Cisco_Lab

[redacted]

Availability Zone

VPC CIDRs

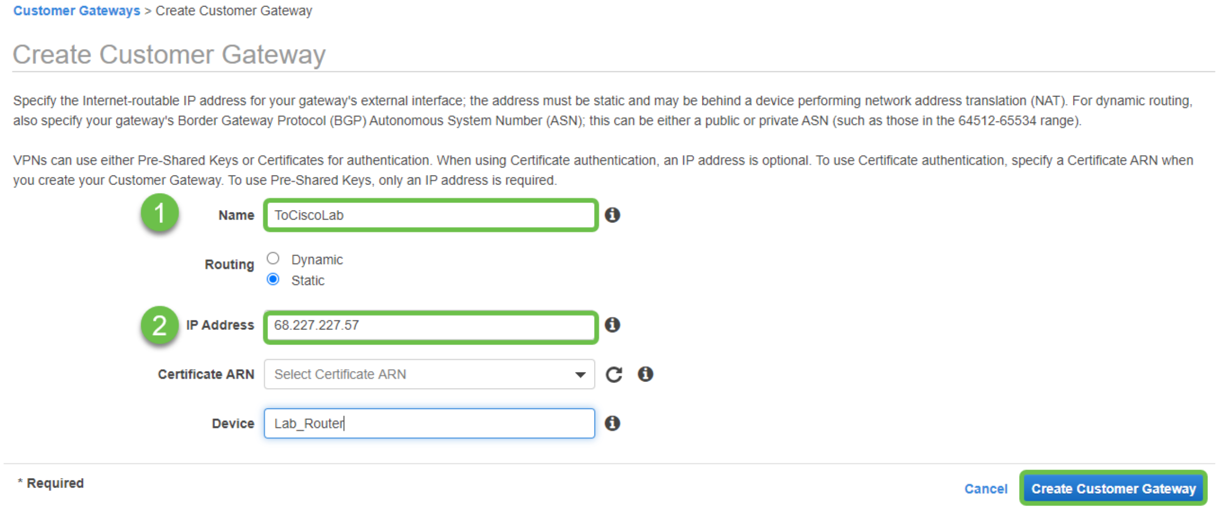
| CIDR | Status | Status Reason |
|---|---|---|
| 172.16.0.0/16 | associated | |

2 IPv4 CIDR block*: 172.16.10.0/24

* Required

## 步骤 3

创建**客户网**关，将**IP地址**定义为*Cisco RV路*由器的公有IP地址。



Customer Gateways > Create Customer Gateway

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

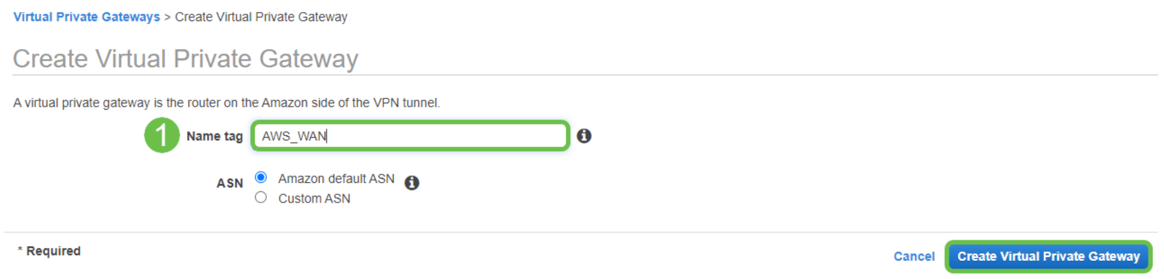
Certificate ARN: Select Certificate ARN

Device: Lab_Router

* Required

## 步骤 4

创建虚**拟专用网**关 — 创*建Name*标记以帮助稍后识别。



Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

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

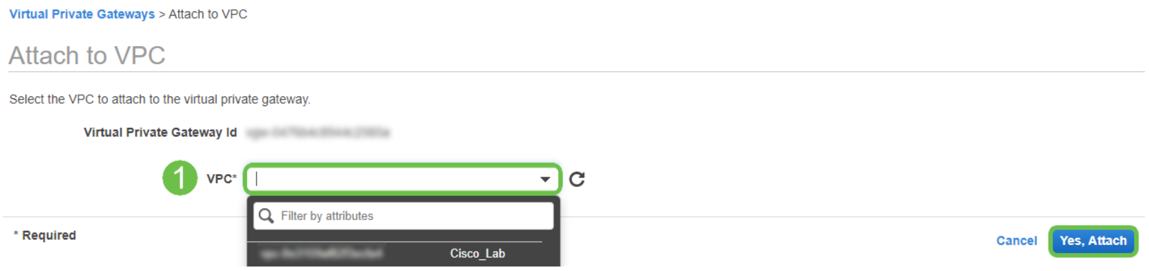
1 Name tag: AWS_WAN

ASN: ● Amazon default ASN ○ Custom ASN

* Required

## 步骤 5

将虚拟**专用网关连**接到以**前创**建的VPC。



Virtual Private Gateways > Attach to VPC

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id: [redacted]

1 VPC*: |

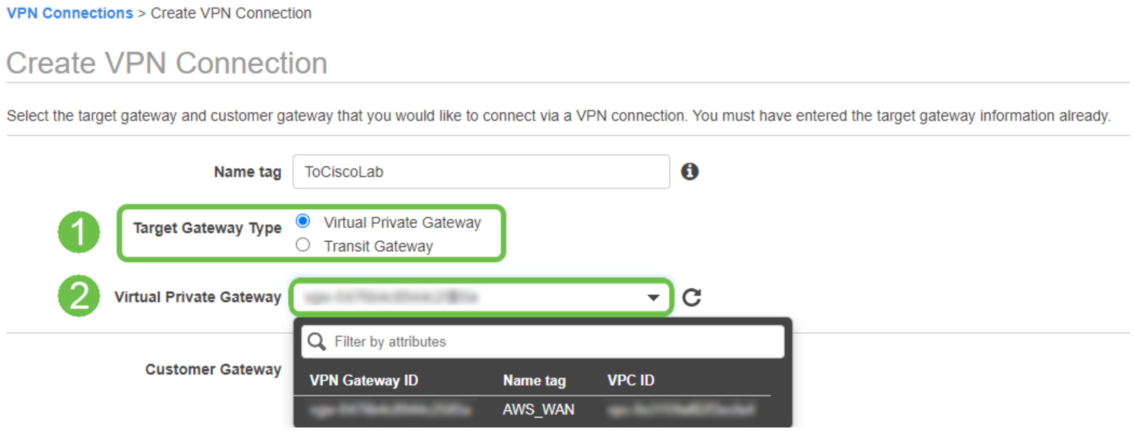
Filter by attributes

| | |
|---|---|
| [redacted] | Cisco_Lab |

* Required

## 第 6 步

创建新的**VPN连接**，选择**目标网关类***型虚拟专用网关*。将VPN连**接与之**前创建**的虚拟专**用网关关联
。



VPN Connections > Create VPN Connection

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: ToCiscoLab

1 Target Gateway Type: ● Virtual Private Gateway ○ Transit Gateway

2 Virtual Private Gateway: [redacted]

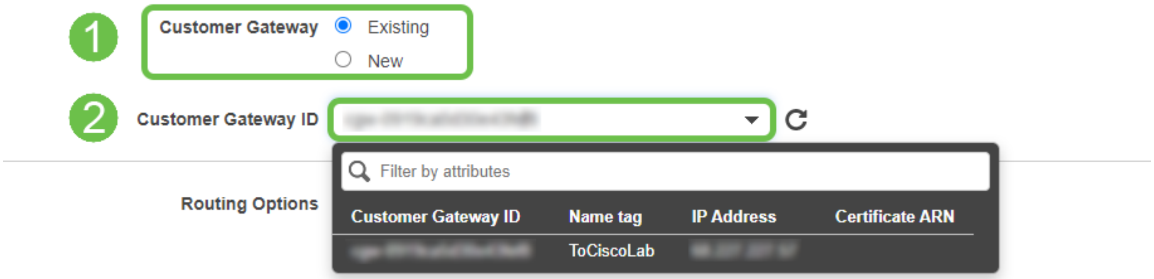
Customer Gateway

Filter by attributes

| VPN Gateway ID | Name tag | VPC ID |
|---|---|---|
| [redacted] | AWS_WAN | [redacted] |

## 步骤 7

选择*Existing* **Customer Gateway**。选择之前**创建的**客户网关。



1 Customer Gateway: ● Existing ○ New

2 Customer Gateway ID: [redacted]

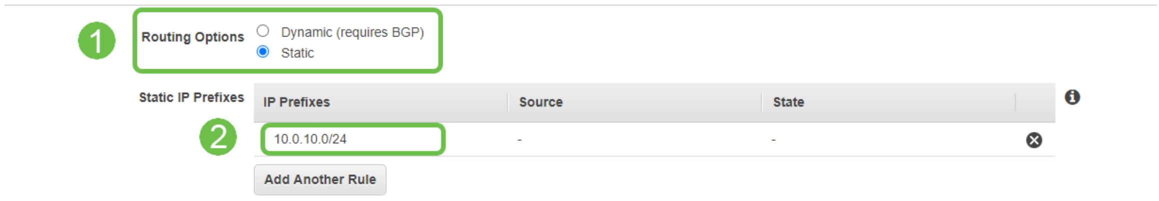
Routing Options

Filter by attributes

| Customer Gateway ID | Name tag | IP Address | Certificate ARN |
|---|---|---|---|
| [redacted] | ToCiscoLab | [redacted] | |

## 步骤 8

对于“**路由选**项”，请确保选择“静态”。输入任**何IP前**缀，包括您期望通过VPN的任何远程网络的CIDR表示法。[这些是您的Cisco路由器上存在的网络。]



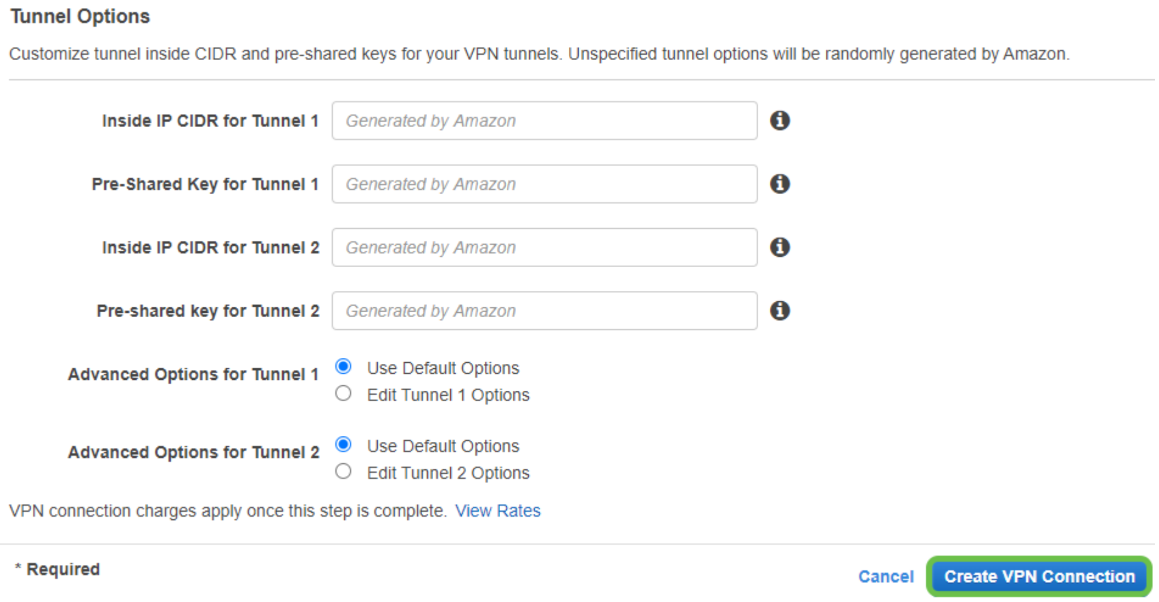
1 Routing Options ○ Dynamic (requires BGP) ● Static

Static IP Prefixes

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

## 步骤 9

我们不会介绍本指南中的**任何隧**道选项 — 选择创*建VPN连接*。



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

Pre-Shared Key for Tunnel 1: Generated by Amazon

Inside IP CIDR for Tunnel 2: Generated by Amazon

Pre-shared key for Tunnel 2: Generated by Amazon

Advanced Options for Tunnel 1: ● Use Default Options ○ Edit Tunnel 1 Options

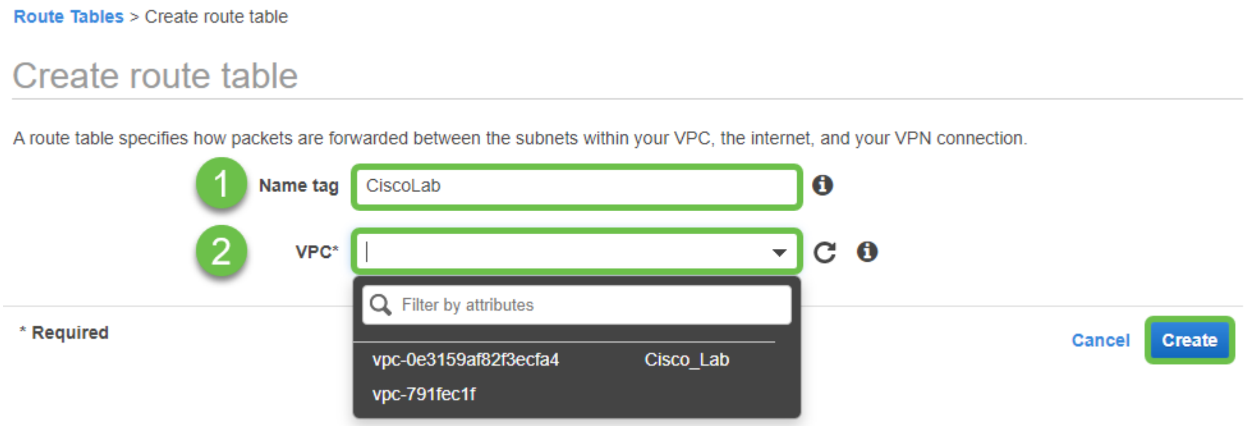
Advanced Options for Tunnel 2: ● Use Default Options ○ Edit Tunnel 2 Options

VPN connection charges apply once this step is complete. View Rates

* Required

## 步骤 10

创建路**由表**并关联之前**创**建的VPC。按创**建**。



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: CiscoLab

2 VPC*:

Filter by attributes

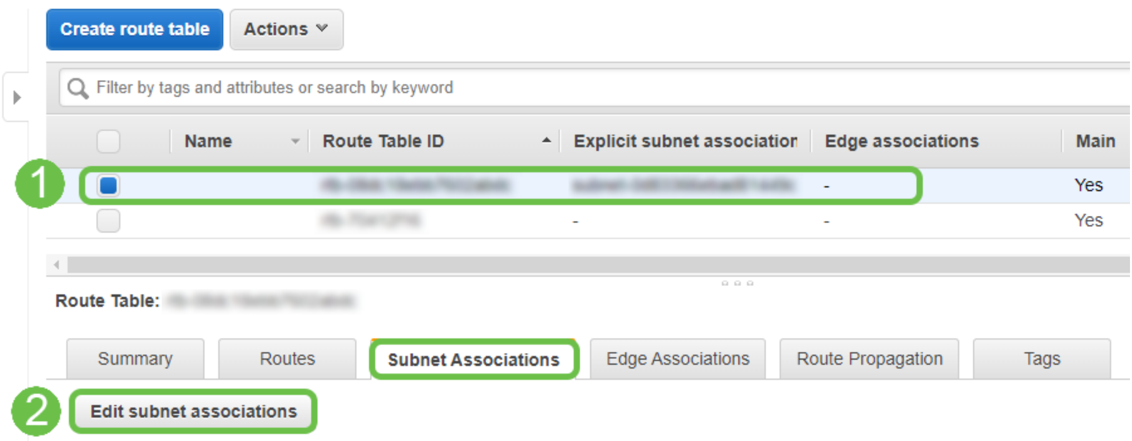
vpc-0e3159af82f3ecfa4 Cisco_Lab

vpc-791fec1f

* Required

## 步骤 11

选择之前**创建的**路由表。从子网关**联选项卡**中，选择编***辑子网关联***。

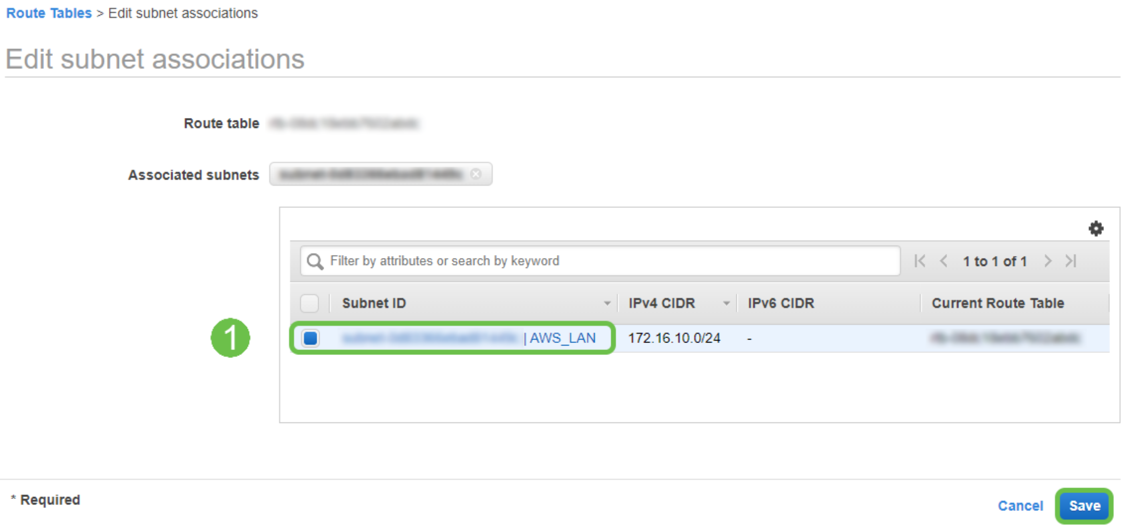


| ☐ | Name | Route Table ID | Explicit subnet association | Edge associations | Main |
|---|---|---|---|---|---|
| ☑ |  | [redacted] | [redacted] | - | Yes |
| ☐ |  | [redacted] | - | - | Yes |

Route Table: [redacted]

## 步骤 12

从“编**辑子网关联**”页中，选择之前创建的子网。选择之前**创建的**路由表。然后选择**保存。**


Route Tables > Edit subnet associations
Edit subnet associations
Filter by attributes or search by keyword
1 to 1 of 1
1
Cancel
Save

Route table [redacted]

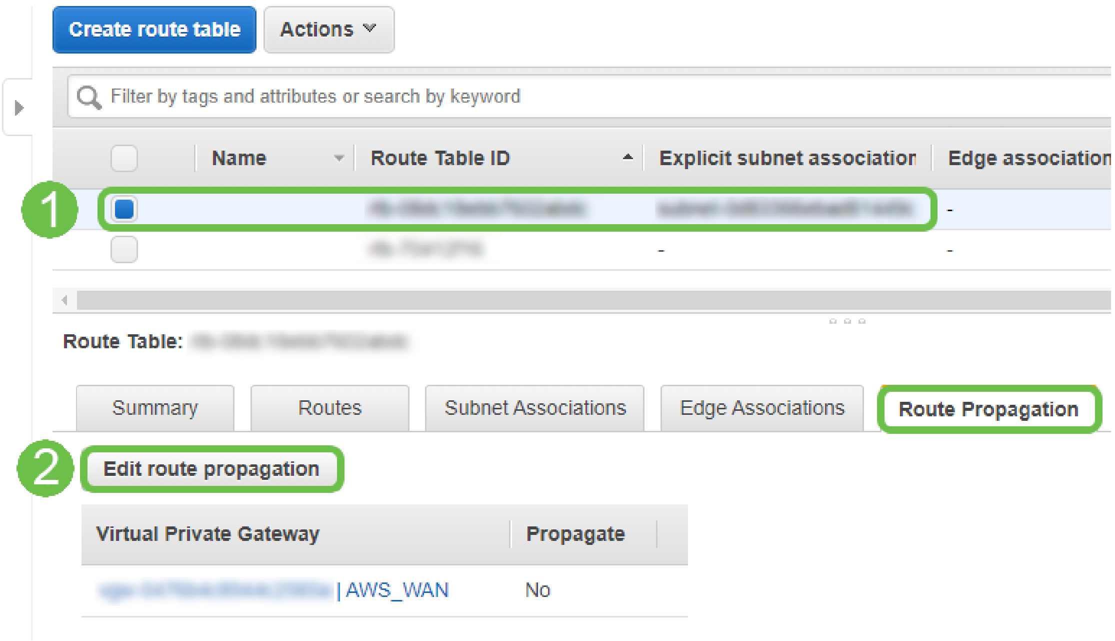
Associated subnets [redacted]

| ☐ | Subnet ID | IPv4 CIDR | IPv6 CIDR | Current Route Table |
|---|---|---|---|---|
| ☑ | [redacted] \| AWS_LAN | 172.16.10.0/24 | - | [redacted] |

* Required

## 步骤 13

**从路由传播选项卡中，选择编*辑路由传播*。**



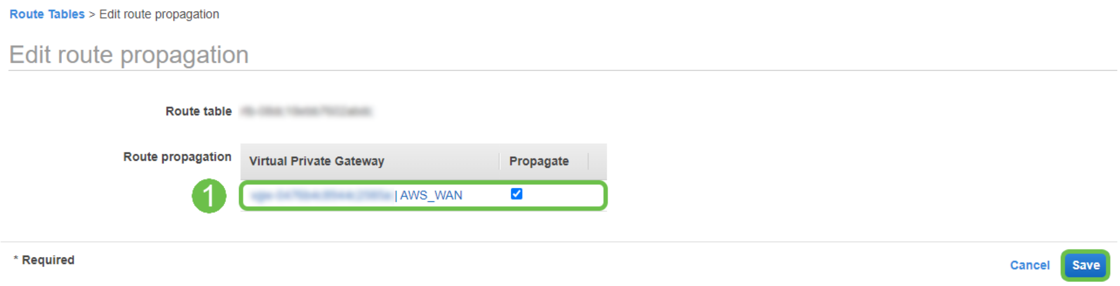
| ☐ | Name | Route Table ID | Explicit subnet association | Edge association |
|---|---|---|---|---|
| ☑ |  | [redacted] | [redacted] | - |
| ☐ |  | [redacted] | - | - |

Route Table: [redacted]

| Virtual Private Gateway | Propagate |
|---|---|
| [redacted] \| AWS_WAN | No |

### 步骤 14

选择之前**创建的虚拟**专用网关。



Route Tables > Edit route propagation

Edit route propagation

Route table [redacted]

Route propagation

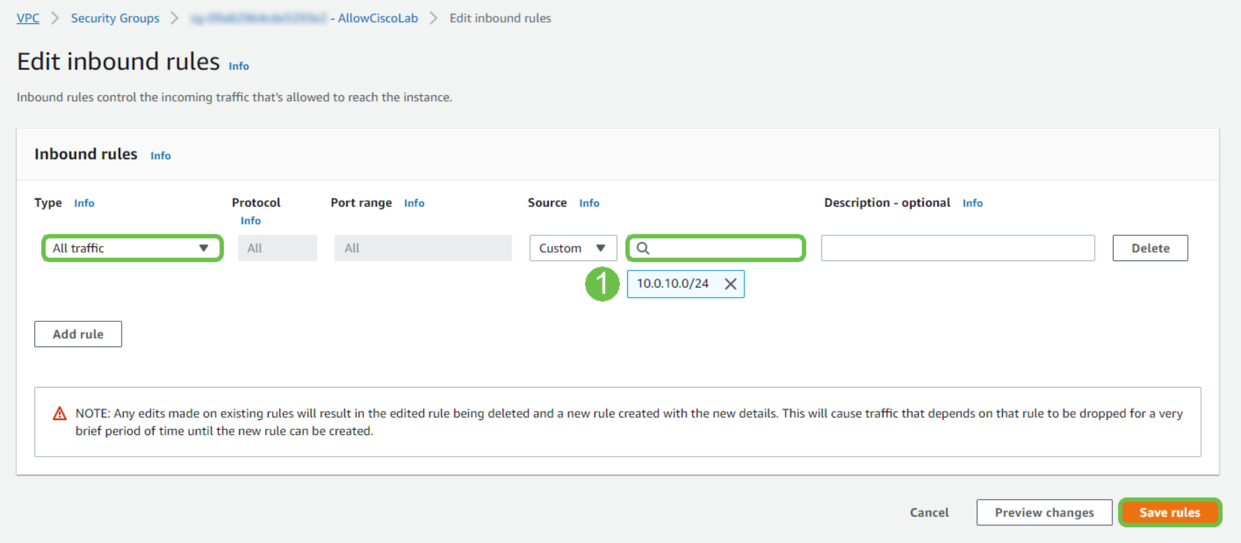
| Virtual Private Gateway | Propagate |
|---|---|
| [redacted] \| AWS_WAN | ☑ |

* Required

### 步骤 15

从VPC > Security Groups，确保已创建允许所需流量的策略。

***注意：***在本例中，我们使用源10.0.10.0/24，该源与我们的RV路由器示例中使用的子网对应。



VPC > Security Groups > [redacted] - AllowCiscoLab > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

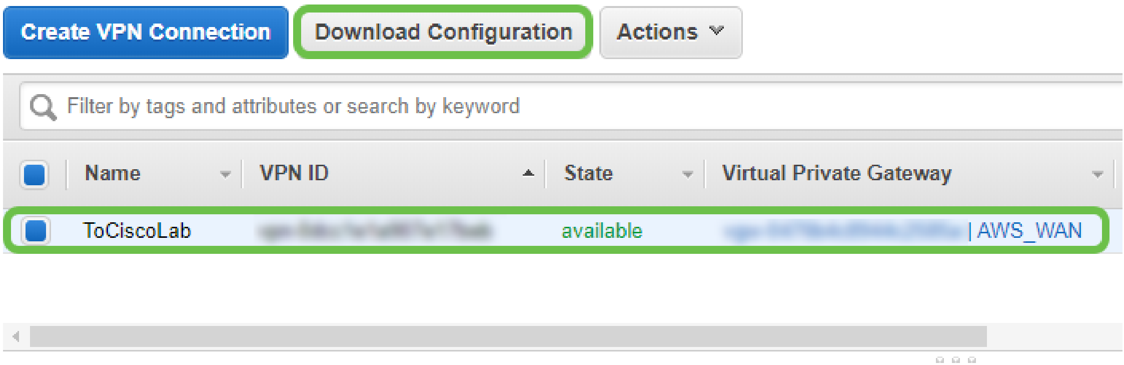
Inbound rules Info

| Type Info | Protocol Info | Port range Info | Source Info | | Description - optional Info | |
|---|---|---|---|---|---|---|
| All traffic | All | All | Custom | 10.0.10.0/24 | | Delete |

⚠ NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

### 步骤 16

选择您之前创建的VPN连接，然后选择“下载*配置*”。



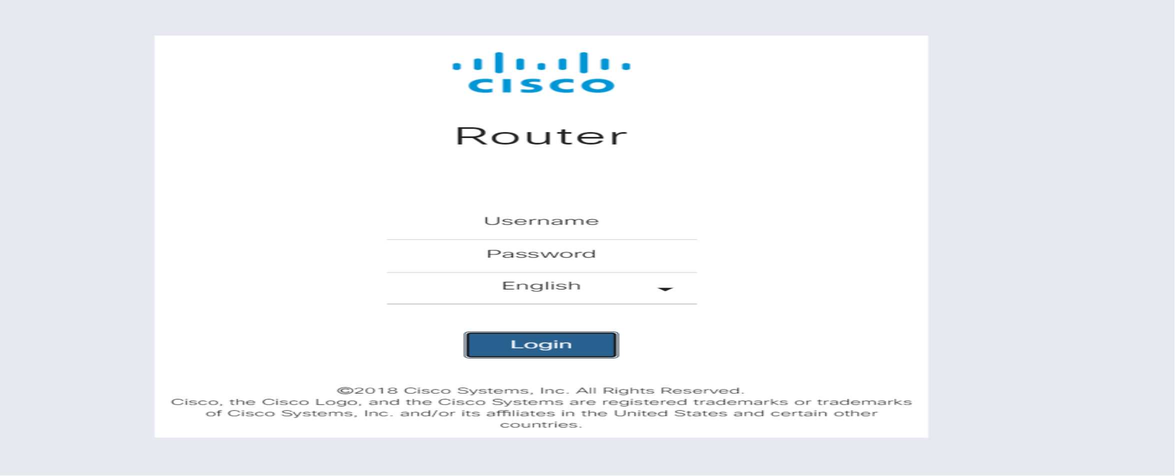
Filter by tags and attributes or search by keyword

| □ | Name | VPN ID | State | Virtual Private Gateway |
|---|---|---|---|---|
| ☑ | ToCiscoLab | [redacted] | available | [redacted] \| AWS_WAN |

## 在RV16X/RV26X、RV34X路由器上设置站点到站点

### 第 1 步

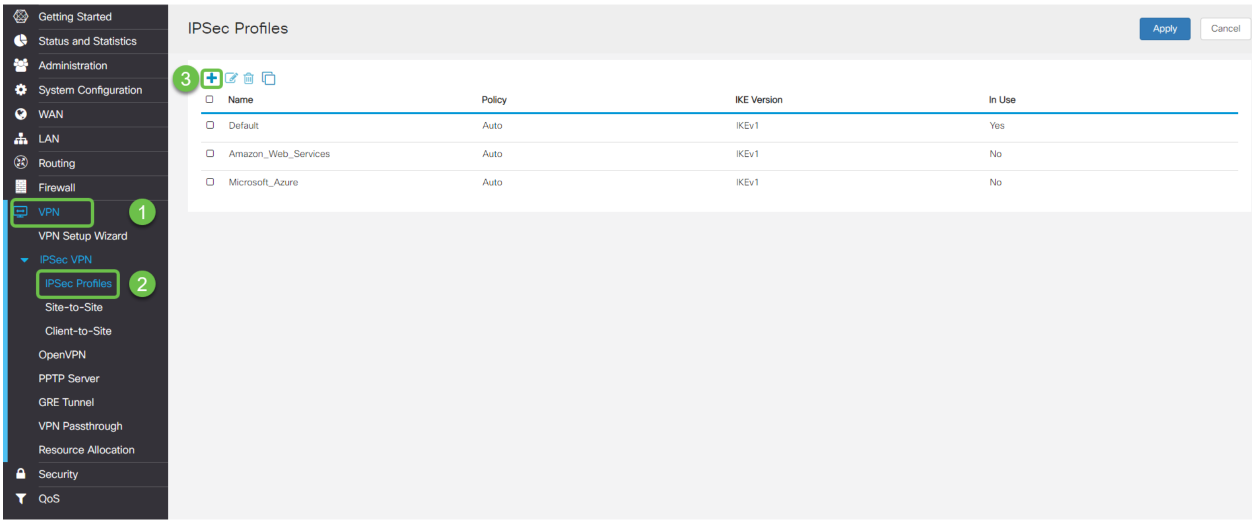
使用有效凭证登录路由器。



©2018 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

## 步骤 2

导航至**VPN > Ipsec Profiles**。这将带您进入Ipsec配置文件页面，按添加图标(+)。

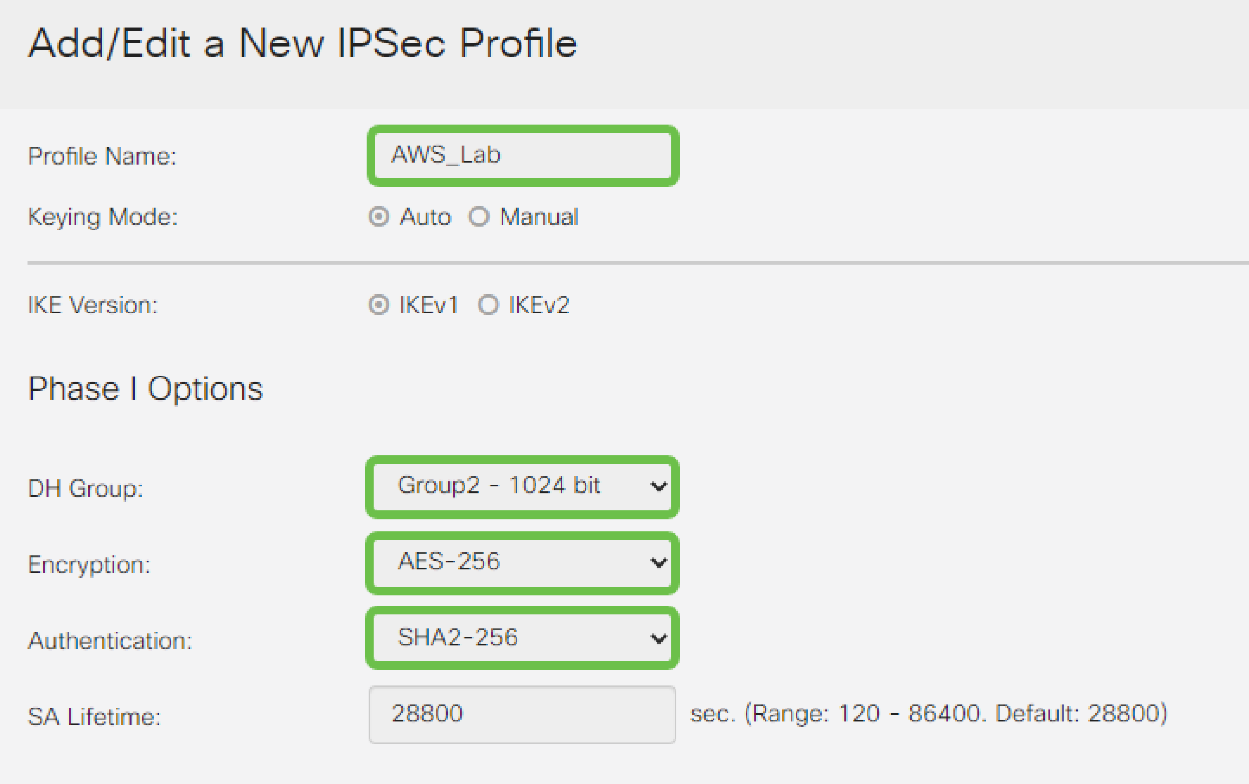


| □ | Name | Policy | IKE Version | In Use |
|---|---|---|---|---|
| □ | Default | Auto | IKEv1 | Yes |
| □ | Amazon_Web_Services | Auto | IKEv1 | No |
| □ | Microsoft_Azure | Auto | IKEv1 | No |

## 步骤 3

我们现在将创建IPSEC配置文件。在S系列路**由器上**创建IPsec配置文件时，请确**保为第1**阶段选择DH组2。

**注意**：AWS将支持较低级别的加密和身份验证 — 在本例中，使用AES-256和SHA2-256。



Add/Edit a New IPSec Profile

Profile Name: AWS_Lab

Keying Mode: ● Auto ○ Manual

IKE Version: ● IKEv1 ○ IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

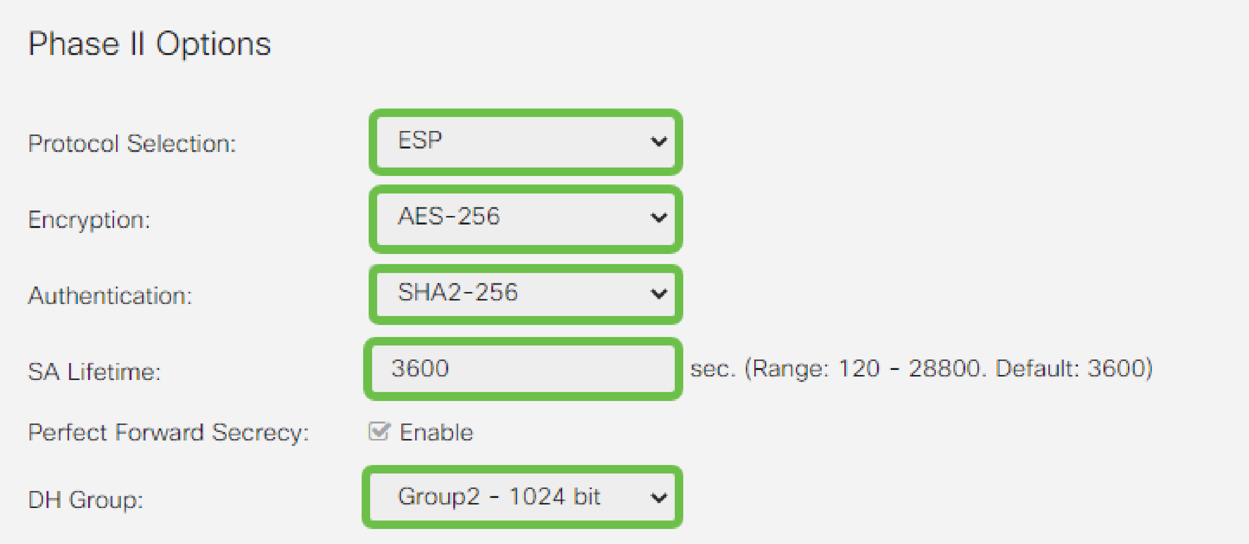
Encryption: AES-256

Authentication: SHA2-256

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

### 步骤 4

确保您的阶段2选项与阶段1中的选项相匹配。对于AWS DH组2，必须使用。



Phase II Options

Protocol Selection: ESP

Encryption: AES-256

Authentication: SHA2-256

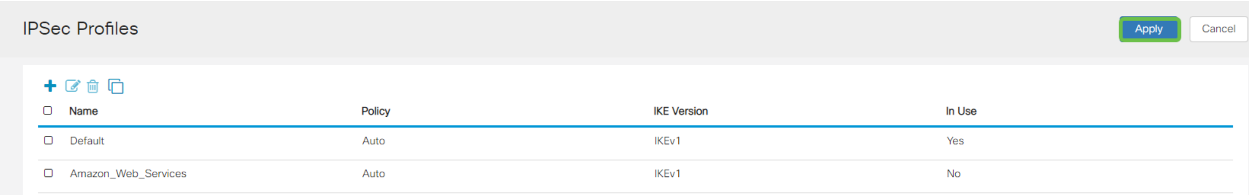
SA Lifetime: 3600 sec. (Range: 120 - 28800. Default: 3600)

Perfect Forward Secrecy: ☑ Enable

DH Group: Group2 - 1024 bit

### 步骤 5

按Apply键，系统会将您导航到IPSEC页面，请确保再次按Apply键。

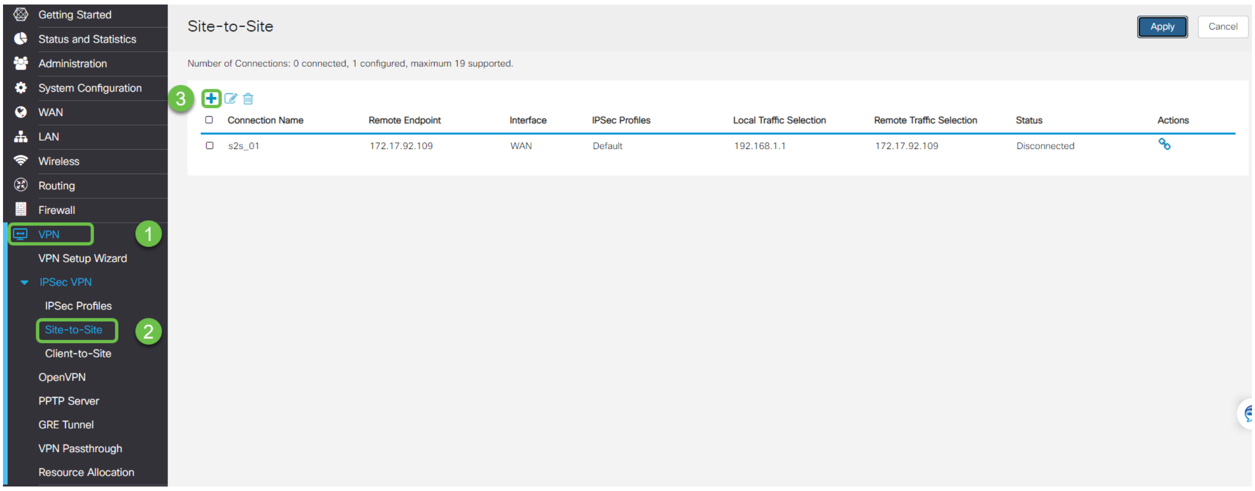


IPSec Profiles

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

### 步骤 6

导航至VPN< Client to site，在Client to site页面上按加号图标(+)。



Site-to-Site

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

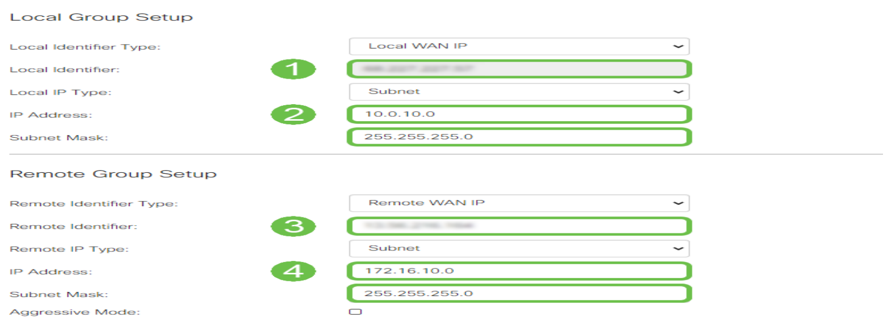
| □ | Connection Name | Remote Endpoint | Interface | IPSec Profiles | Local Traffic Selection | Remote Traffic Selection | Status | Actions |
|---|---|---|---|---|---|---|---|---|
| □ | s2s_01 | 172.17.92.109 | WAN | Default | 192.168.1.1 | 172.17.92.109 | Disconnected | |

## 步骤 7

创建IPsec站点到站点连接时，请确保选择在前面**步骤中**创建的IPsec配置文件。使用**Remote Endpoint**类型*的Static IP*并输入导出的AWS配置中提供的地址。输入**AWS导出配**置中提供的预共享密钥。

## 步骤 8

输入S系列**路由器**的本地标识符 — 此条目应与AWS中创建**的客户**网关匹配。输入S系列**路由器的IP地址**和**子网掩码** — 此条目应与AWS中添加到**VPN连接**的**静态IP前缀**匹配。输入S系列**路由器的IP地址**和**子网掩码** — 此条目应与AWS中添加到**VPN连接**的**静态IP前缀**匹配。



Local Group Setup

Local Identifier Type: Local WAN IP

Local Identifier: [redacted]

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: [redacted]

Remote IP Type: Subnet

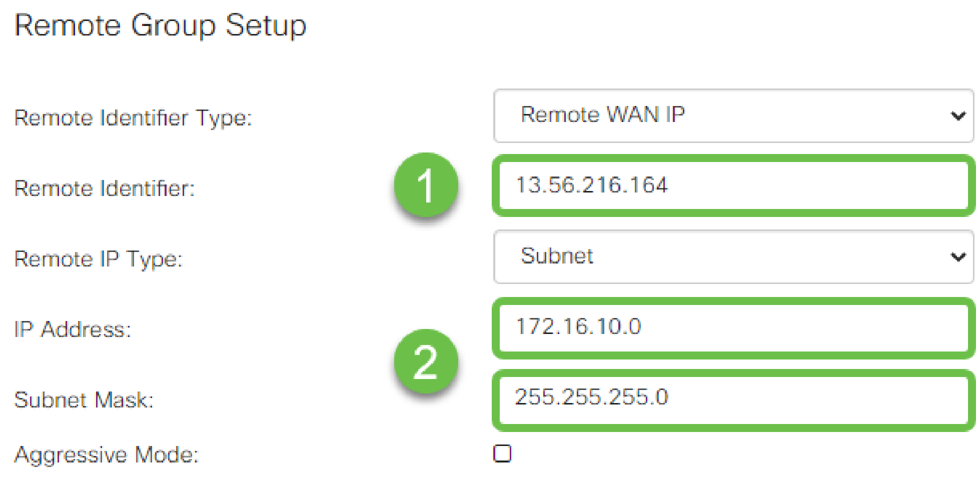
IP Address: 172.16.10.0

Subnet Mask: 255.255.255.0

Aggressive Mode: □

## 步骤 9

输入AWS**连接的**远程标识符 — 此标识符将列在AWS站点到站点VPN连接的**隧道详细信息下。**输入AWS**连接的IP**地址**和子**网掩码 — 在AWS配置期间定义。然后按应**用。**



Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 13.56.216.164

Remote IP Type: Subnet

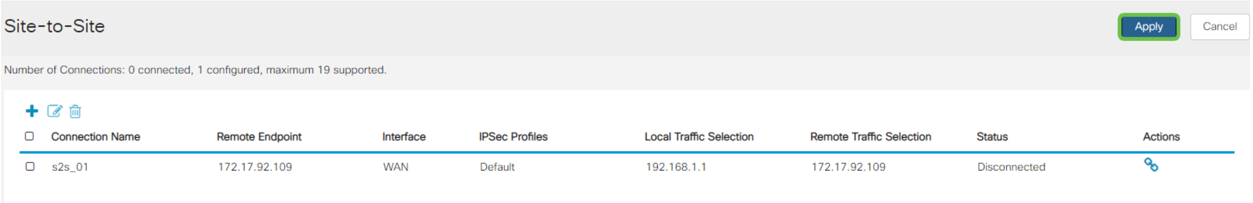
IP Address: 172.16.10.0

Subnet Mask: 255.255.255.0

Aggressive Mode: □

## 步骤 10

进入"IP站点到站点"页面后，按**"应用**"。



Site-to-Site

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 | |

# 结论

您现在已成功在RV系列路由器和AWS之间创建站点到站点VPN。有关站点到站点VPN的社区讨论，请转至Cisco S系列支持社区页面并搜索站点到站点VPN。