

アマゾンウェブサービスを使用したサイト間VPN

目的

この記事の目的は、Cisco RVシリーズルータとAmazon Web Servicesの間でサイト間VPNをセットアップする方法を説明することです。

該当するデバイス | ソフトウェアバージョン

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

概要

サイト間VPNでは、複数のネットワークに接続できます。これにより、企業および一般ユーザは異なるネットワークに接続できます。Amazon Web Services(AWS)は、AWSプラットフォームにアクセスできるサイト間VPNなど、多くのオンデマンドクラウドコンピューティングプラットフォームを提供します。このガイドは、RV16X、RV26X、RV34Xルータのサイト間VPNをAmazon Web Servicesに設定する際に役立ちます。

次の2つの部分があります。

[アマゾンウェブサービスでのサイト間VPNのセットアップ](#)

[RV16X/RV26X、RV34Xルータでのサイト間VPNの設定](#)

アマゾンウェブサービスでのサイト間VPNのセットアップ

手順 1

IPv4 CIDRブロックを定義する新しいVPCを作成し、後でAWS LANとして使用するLANを定義します。「作成」を選択します。

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

手順 2

サブネットを作成する場合は、以前に作成したVPCを選択していることを確認します。前に作成した既存の/16ネットワーク内のサブネットを定義します。この例では、172.16.10.0/24が使用されています。

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

手順 3

お客様のゲートウェイを作成し、IPアドレスをCisco RVルータのパブリックIPアドレスとして定義します。

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

手順 4

バーチャルプライベートゲートウェイの作成 – 後で識別するのに役立つ名前タグの作成

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

手順 5

仮想プライベートゲートウェイを前に作成したVPCに接続してください。

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC ⓘ

Filter by attributes

vpn-gw-01234567890123456	Cisco_Lab
--------------------------	-----------

* Required

Cancel

手順 6

新しいVPN接続を作成し、[Target Gateway Type Virtual Private Gateway]を選択します。VPN接続を前に作成した仮想プライベートゲートウェイに関連付けます。

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-01234567890123456	AWS_WAN	vpn-gw-01234567890123456

ステップ7

「既存の顧客ゲートウェイ」を選択します。以前に作成したカスタマーゲートウェイを選択します。

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-01234567890123456	ToCiscoLab	vpn-gw-01234567890123456	vpn-gw-01234567890123456

手順 8

[ルーティングオプション]で、[静的]を必ず選択してください。VPNを通過する予定のリモートネットワークのCIDR表記を含む任意のIPプレフィックスを入力します。[これらはCiscoルータに存在するネットワークです。]

1 Routing Options Dynamic (requires BGP) Static

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

Add Another Rule

手順 9

このガイドのトンネルオプションは取り上げません。Create VPN Connectionを選択してください。

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	i
Pre-Shared Key for Tunnel 1	Generated by Amazon	i
Inside IP CIDR for Tunnel 2	Generated by Amazon	i
Pre-shared key for Tunnel 2	Generated by Amazon	i
Advanced Options for Tunnel 1	<input checked="" type="radio"/> Use Default Options <input type="radio"/> Edit Tunnel 1 Options	
Advanced Options for Tunnel 2	<input checked="" type="radio"/> Use Default Options <input type="radio"/> Edit Tunnel 2 Options	

VPN connection charges apply once this step is complete. [View Rates](#)

* Required

Cancel [Create VPN Connection](#)

手順 10

ルートテーブルを作成し、以前に作成したVPCを関連付けます。[作成]を押します。

[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 i

2 VPC* i

Filter by attributes

vpc-0e3159af82f3ecfa4	Cisco_Lab
vpc-791fec1f	

* Required

Cancel [Create](#)

手順 11

前に作成したルートテーブルを選択します。[サブネットアソシオン]タブで、[サブネットアソシ

エーションの編集]を選択します。

1

Name	Route Table ID	Explicit subnet association	Edge associations	Main
[Route Table Name]	[Route Table ID]	-	-	Yes
[Route Table Name]	[Route Table ID]	-	-	Yes

Route Table: [Route Table Name]

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

2 Edit subnet associations

ステップ 12

[サブネットの関連付けを編集]ページで、以前に作成したサブネットを選択します。前に作成したルートテーブルを選択します。次に、[保存]を選択します。

Route Tables > Edit subnet associations

Edit subnet associations

Route table [Route Table Name]

Associated subnets [Subnet ID]

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

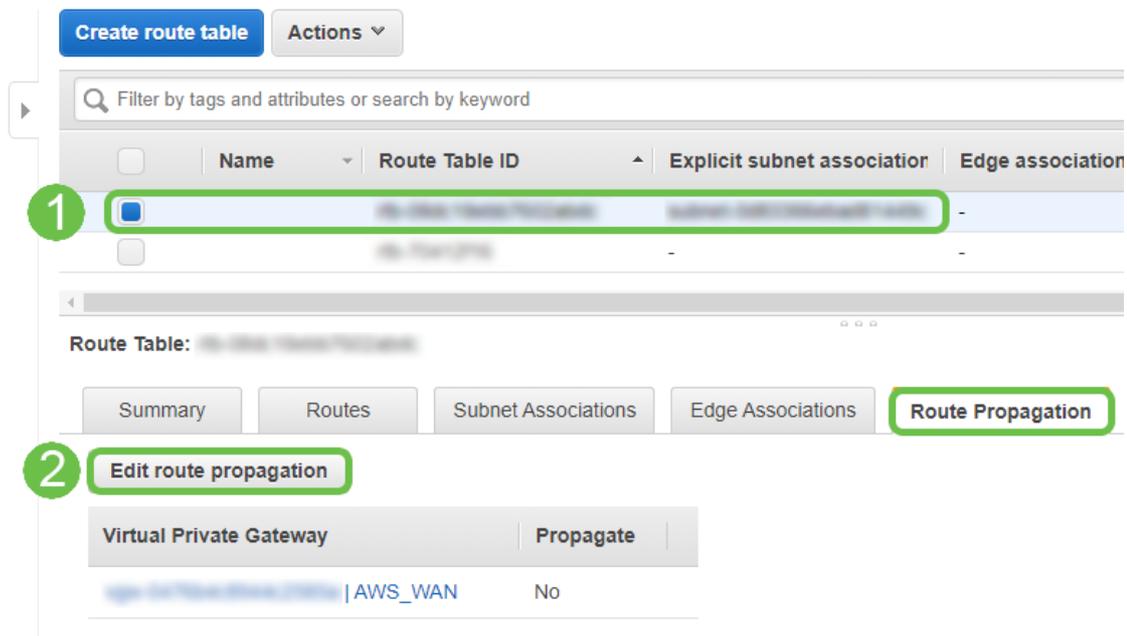
1

* Required

Cancel Save

手順 13

[Route Propagation]タブで、[Edit route propagation]を選択します。



ステップ 14

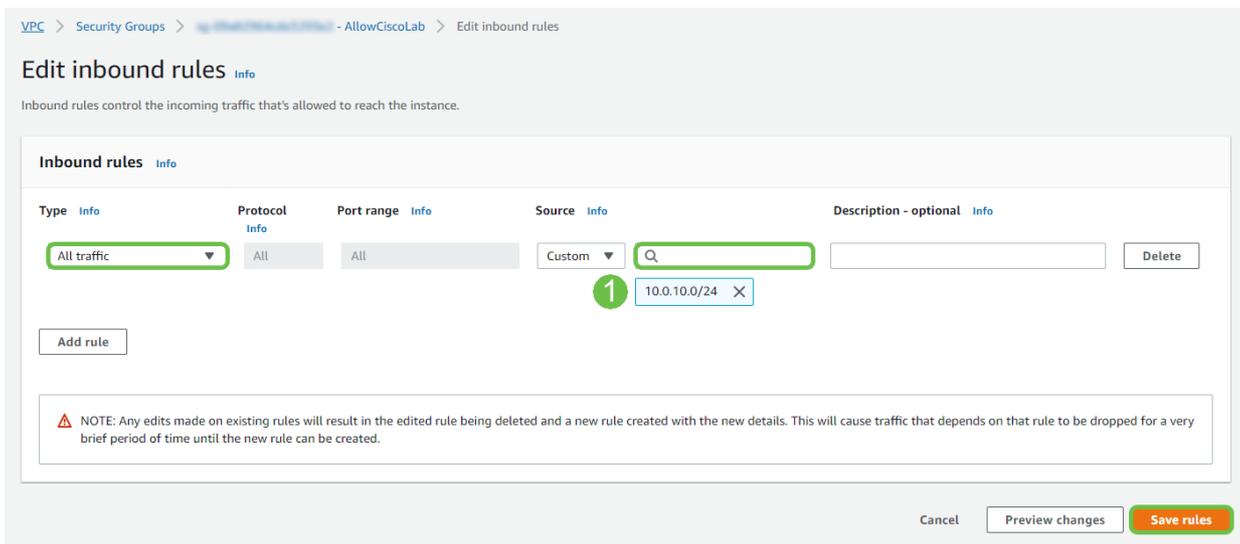
以前に作成したVirtual Private Gatewayを選択します。



ステップ 15

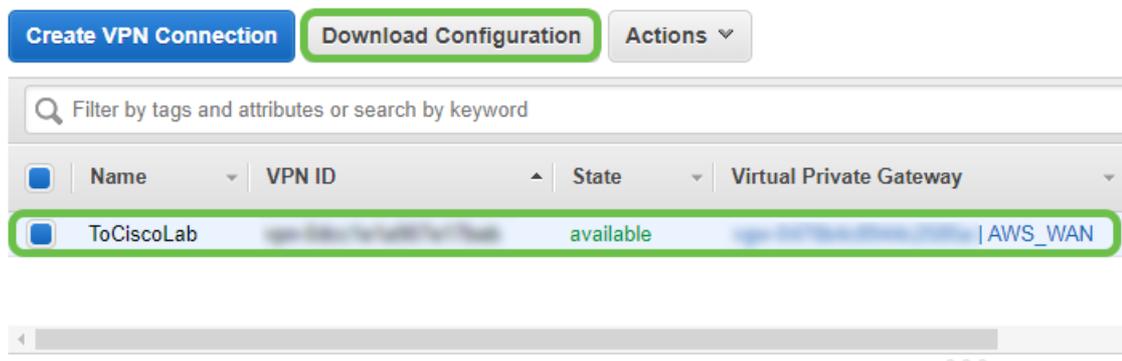
[VPC] > [セキュリティグループ]で、目的のトラフィックを許可するポリシーが作成されていることを確認します。

注：この例では、10.0.10.0/24の送信元を使用しています。これは、この例のRVルータで使用されているサブネットに対応しています。



ステップ 16

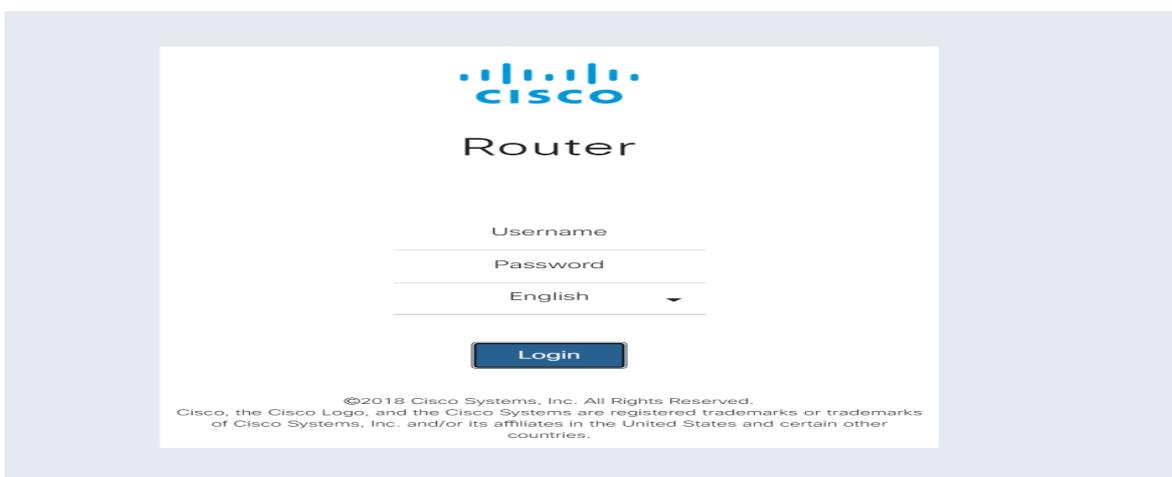
以前に作成したVPN接続を選択し、[Download Configuration]を選択します。



RV16X/RV26X、RV34Xルータでのサイト間の設定

手順 1

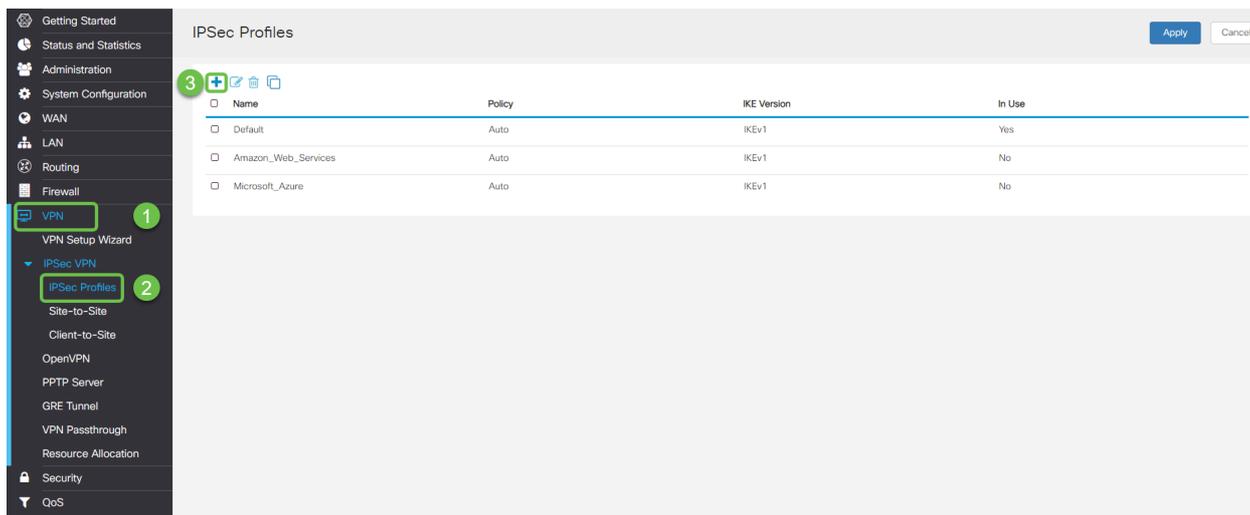
有効なクレデンシャルを使用してルータにログインします。



手順 2

[VPN] > [Ipsec Profiles]に移動します。これにより、Ipsecプロファイルページが表示され、追加

アイコン(+)を押します。



手順 3

次に、IPSECプロファイルを作成します。Small BusinessルータでIPsecプロファイルを作成する場合は、フェーズ1に対して[DHグループ2]が選択されていることを確認します。

注：AWSでは、低レベルの暗号化と認証がサポートされます。この例では、AES-256とSHA2-256が使用されます。

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)

手順 4

フェーズ2のオプションが、フェーズ1で行ったオプションと一致していることを確認します。AWSの場合、DHグループ2を使用する必要があります。

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

手順 5

[適用]を押すと、IPSECページに移動します。必ず[適用]をもう一度押してください。

IPSec Profiles Apply Cancel

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

手順 6

[VPN< Client to site]に移動し、クライアントからサイトへのページでプラス(+)アイコンを押します。

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	

ステップ7

IPsecサイト間接続を作成する場合は、前の手順で作成したIPsecプロファイルを選択してください。リモートエンドポイントのタイプを[静的IP]に設定し、エクスポートされたAWS構成で指定されたアドレスを入力します。AWSからエクスポートされた構成で提供される事前共有キーを入力します。

手順 8

Small Businessルータのローカル識別子を入力します。このエントリは、AWSで作成された **Customer Gateway**と一致する必要があります。Small BusinessルータのIPアドレスとサブネットマスクを入力します。このエントリは、AWSのVPN Connectionに追加された静的IPプレフィクスと一致する必要があります。Small BusinessルータのIPアドレスとサブネットマスクを入力します。このエントリは、AWSのVPN Connectionに追加された静的IPプレフィクスと一致する必要があります。

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"/>

手順 9

AWS接続のリモート識別子を入力します。これは、AWSサイト間VPN接続のトンネルの詳細の下に表示されます。AWS接続のIPアドレスとサブネットマスクを入力します。AWS接続はAWSの設定中に定義されました。次に、[Apply]を押します。

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:

手順 10

[Ip Site to Site]ページで、[Apply]を押します。

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	

結論

これで、RVシリーズルータとAWS間にサイト間VPNが正常に作成されました。サイト間VPNに関するコミュニティディスカッションについては、[Cisco Small Business Support Communityページに移動](#)し、サイト間VPNを検索してください。