

使用Amazon Web Services的站點到站點VPN

目標

本文的目的是指導您在Cisco RV系列路由器和Amazon Web Services之間設定站點到站點VPN。

適用裝置 | 軟體版本

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

簡介

站點到站點VPN允許連線到兩個或多個網路，這使企業和一般使用者能夠連線到不同的網路。Amazon Web Services(AWS)提供許多按需雲端計算平台，包括站點到站點VPN，使您能夠訪問您的AWS平台。本指南將幫助您將RV16X、RV26X、RV34X路由器上的站點到站點VPN配置到Amazon Web Services。

這兩個部分如下：

[在Amazon Web Services上設定站點到站點VPN](#)

[在RV16X/RV26X、RV34X路由器上設定站點到站點VPN](#)

在Amazon Web Services上設定站點到站點VPN

步驟1

建立一個新的VPC，定義一個IPv4 CIDR塊，之後我們將在該塊中定義用作我們的AWS LAN的LAN。選擇建立。

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

步驟2

建立子網時，請確保您已選擇先前創建的VPC。在先前建立的現有/16網路中定義子網。本示例使用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 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

步驟3

建立客戶網關，將IP地址定義為Cisco RV路由器的公共IP地址。

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

步驟4

建立虛擬專用網關 — 建立Name標籤以幫助稍後識別。

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

步驟5

將**虛擬專用網關**連線到先前建立的**VPC**。

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC ⓘ

Filter by attributes

VPC ID	Name tag
vpc-1234567890123456	Cisco_Lab

* Required

Cancel

步驟6

建立新的**VPN連線**，選擇**目標網關型別**為**虛擬專用網關**。將**VPN連線**與先前建立的**虛擬專用網關**相關聯。

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	vpc-1234567890123456

第7步

選擇**Existing Customer Gateway**。選擇之前建立的**客戶網關**。

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	10.0.0.0/16	

步驟8

對於**路由選項**，請確保選擇Static。輸入任何IP字首，包括您預計通過VPN的任何遠端網路的CIDR表示法。[這些網路存在於您的Cisco路由器上。]

1 Routing Options Dynamic (requires BGP) Static

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

Add Another Rule

步驟9

我們不會在本指南中介紹任何**Tunnel Options** — 選擇 *Create VPN Connection*。

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

步驟10

建立**路由表**並關聯先前建立的VPC。按**Create**。

[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

步驟11

選擇**先前建立**的路由表。在**Subnet Associations**頁籤中選擇 *Edit subnet associations*。

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

步驟12

在編輯子網關聯頁中，選擇以前建立的子網。選擇先前建立的路由表。然後選擇save。

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table [Route Table ID](#)

Associated subnets [Subnet ID](#)

1

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

* Required Cancel Save

步驟13

在Route Propagation頁籤中，選擇Edit route propagation。

Create route table Actions

Filter by tags and attributes or search by keyword

	Name	Route Table ID	Explicit subnet association	Edge association
1				

Route Table: [Route Table ID](#)

Summary Routes Subnet Associations Edge Associations Route Propagation

2 Edit route propagation

Virtual Private Gateway	Propagate
Subnet ID AWS_WAN	No

步驟14

選擇之前建立的虛擬專用網關。

[Route Tables](#) > [Edit route propagation](#)

Edit route propagation

Route table [\[ID\]](#)

Route propagation **Virtual Private Gateway** Propagate

1

* Required Cancel **Save**

步驟15

在VPC > Security Groups中，確保已建立策略以允許所需的流量。

附註：在本例中，我們使用源10.0.10.0/24，該源與示例RV路由器上使用的子網相對應。

VPC > Security Groups > [\[ID\]](#) - 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 <input type="text" value="10.0.10.0/24"/>	

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.

Cancel **Save rules**

步驟16

選擇您之前建立的VPN連線，然後選擇*Download Configuration*。

Create VPN Connection **Download Configuration** Actions ▾

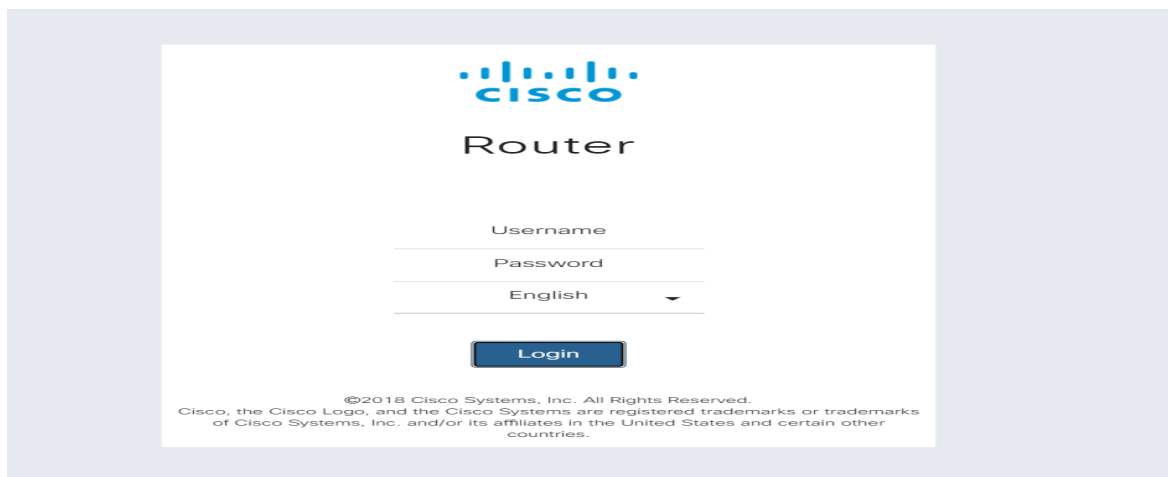
Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	VPN ID	State	Virtual Private Gateway
<input checked="" type="checkbox"/>	ToCiscoLab	[ID]	available	[ID] AWS_WAN

在RV16X/RV26X、RV34X路由器上設定站點到站點

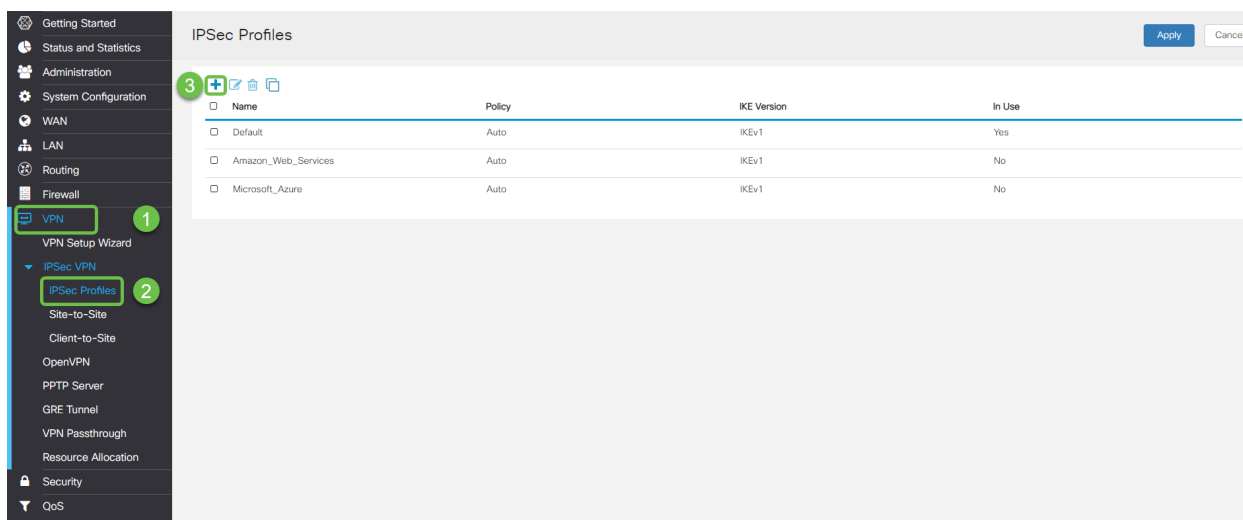
步驟1

使用有效憑證登入到路由器。



步驟2

導航到VPN > Ipsec Profiles。這會將您帶到Ipsec配置檔案頁面，按新增圖示(+)



步驟3

我們現在建立我們的IPSEC配置檔案。在小型企業路由器上建立IPsec Profile時，請確保為階段1選擇DH Group 2。

附註：AWS將支援較低級別的加密和身份驗證 — 在本示例中，使用了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)

步驟4

確保您的第二階段選項與第一階段中提供的選項匹配。對於AWS DH組2，必須使用。

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

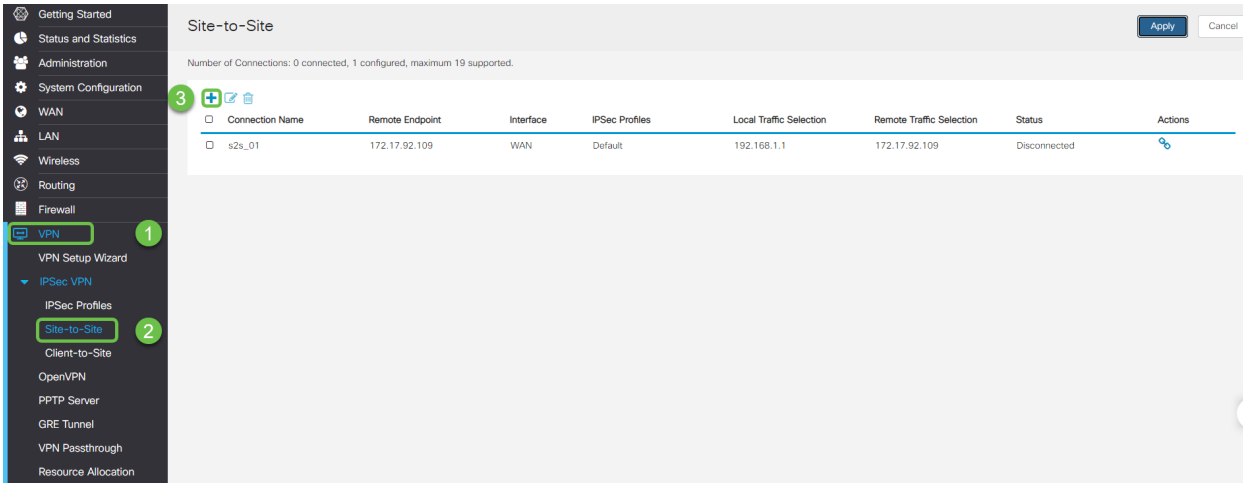
步驟5

按Apply後，您將導航到IPSEC頁面，一定要再次按Apply。

IPsec Profiles				Apply	Cancel
Name	Policy	IKE Version	In Use		
Default	Auto	IKEv1	Yes		
Amazon_Web_Services	Auto	IKEv1	No		

步驟6

導航到VPN < Client to site，然後在客戶端到站點頁面上按加號圖示(+)



第7步

建立IPsec站點到站點連線時，請確保選擇在上面的步驟中建立的IPsec配置檔案。使用Static IP的Remote Endpoint型別，並輸入匯出的AWS配置中提供的地址。輸入從AWS匯出的配置中提供的預共用金鑰。

步驟8

輸入Local Identifier for your Small Business router — 此條目應與AWS中建立的Customer Gateway匹配。輸入您的小型企業路由器的IP地址和子網掩碼 — 此條目應與AWS中新增到VPN連線的靜態IP字首匹配。輸入您的小型企業路由器的IP地址和子網掩碼 — 此條目應與AWS中新增到VPN連線的靜態IP字首匹配。

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:

步驟9

輸入AWS連線的遠端識別符號 — 這將列在AWS站點到站點VPN連線的隧道詳細資訊下。輸入您的AWS連線的IP地址和子網掩碼 (在AWS配置過程中定義)。然後按應用鍵。

Remote Group Setup

Remote Identifier Type:

Remote Identifier: **1**

Remote IP Type:

IP Address: **2**

Subnet Mask:

Aggressive Mode:

步驟10

進入Ip Site to Site (Ip站點到站點) 頁面後，按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	

結論

現在，您已成功在RV系列路由器和AWS之間建立站點到站點VPN。有關站點到站點VPN的社群討論，請轉至[思科小型企業支援社群](#)頁面，然後搜尋站點到站點VPN。