

# VPN da sito a sito con servizi Web Amazon

## Obiettivo

L'obiettivo di questo articolo è guidare l'utente nella configurazione di una VPN da sito a sito tra i router Cisco serie RV e i servizi Web Amazon.

## Dispositivi interessati | Versione software

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

## Introduzione

Una VPN da sito a sito consente la connessione a due o più reti, consentendo ad aziende e utenti generici di connettersi a reti diverse. Amazon Web Services (AWS) fornisce molte piattaforme di cloud computing su richiesta, tra cui VPN da sito a sito, che consentono di accedere alle piattaforme AWS. Questa guida consente di configurare la VPN da sito a sito su router RV16X, RV26X e RV34X per Amazon Web Services.

Le due parti sono le seguenti:

[Configurazione della VPN da sito a sito sui servizi Web Amazon](#)

[Configurazione di una VPN da sito a sito su un router RV16X/RV26X e RV34X](#)

## Configurazione di una VPN da sito a sito sui servizi Web Amazon

### Passaggio 1

Creare un nuovo VPC, definendo un **blocco CIDR IPv4**, in cui definire successivamente la LAN utilizzata come *LAN AWS*. Selezionare *Crea*.

## 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

## Passaggio 2

Quando si crea la subnet, assicurarsi di aver selezionato il **VPC** creato in precedenza. Definire una subnet all'interno della rete /16 esistente creata in precedenza. Nell'esempio viene utilizzato 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 Filter by attributes ⓘ

VPC CIDRs	Status	Status Reason
172.16.0.0/16	associated	

2 IPv4 CIDR block\* 172.16.10.0/24 ⓘ

\* Required

Create

## Passaggio 3

Creare un **gateway cliente**, definendo l'indirizzo IP come *indirizzo IP pubblico* del router 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

## Passaggio 4

Creazione di un **gateway privato virtuale** - creazione di un *tag Name* per una successiva identificazione.

## 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

## Passaggio 5

Collegare il **gateway privato virtuale** al **VPC** creato in precedenza.

## Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC  ⓘ

Filter by attributes

vpn-gw-0123456789012345	Cisco_Lab
-------------------------	-----------

\* Required

Cancel

## passaggio 6

Creare una nuova **connessione VPN**, selezionando il tipo di **gateway di destinazione Gateway privato virtuale**. Associare la **connessione VPN** al **gateway privato virtuale** creato in precedenza.

## 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-0123456789012345	AWS_WAN	vpn-gw-0123456789012345

## Passaggio 7

Selezionare **Existing Customer Gateway**. Selezionare il **Gateway clienti** creato in precedenza.

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-0123456789012345	ToCiscoLab	192.168.1.1	

## Passaggio 8

Per **Opzioni di instradamento**, selezionare Statico. Immettere eventuali **prefissi IP**, inclusa la notazione CIDR, per le reti remote che si prevede di attraversare la VPN. [Queste sono le reti che esistono sul router Cisco.]

1 Routing Options  Dynamic (requires BGP)  Static

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

Add Another Rule

## Passaggio 9

In questa guida non illustreremo alcuna delle **opzioni tunnel** - selezionare *Crea connessione 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

## Passaggio 10

Creare una **tabella di route** e associare la **VPC** creata in precedenza. Premere **Crea**.

[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

## Passaggio 11

Selezionate la **tabella di stesura** creata in precedenza. Nella scheda **Associazioni subnet** scegliere **Modifica associazioni subnet**.

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

## Passaggio 12

Nella pagina **Modifica associazioni subnet** selezionare la subnet creata in precedenza. Selezionate la **tabella di stesura** creata in precedenza. Quindi selezionare **Salva**.

[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	<b>Subnet ID</b>   AWS_LAN	172.16.10.0/24	-	<b>Route Table ID</b>

\* Required

Cancel **Save**

## Passaggio 13

Dalla scheda **Propagazione route**, scegliere **Modifica propagazione route**.

The screenshot shows the AWS IAM console interface. At the top, there is a 'Create route table' button and an 'Actions' dropdown. Below is a search bar with the text 'Filter by tags and attributes or search by keyword'. A table lists route tables with columns: Name, Route Table ID, Explicit subnet association, and Edge association. A green circle with the number '1' highlights the first row. Below the table, there are tabs for 'Summary', 'Routes', 'Subnet Associations', 'Edge Associations', and 'Route Propagation'. The 'Route Propagation' tab is selected and highlighted with a green circle. Under this tab, there is a table with columns 'Virtual Private Gateway' and 'Propagate'. A green circle with the number '2' highlights the 'Edit route propagation' button. Below this, a table shows a 'Virtual Private Gateway' with the value 'AWS\_WAN' and a 'Propagate' checkbox that is currently unchecked.

## Passaggio 14

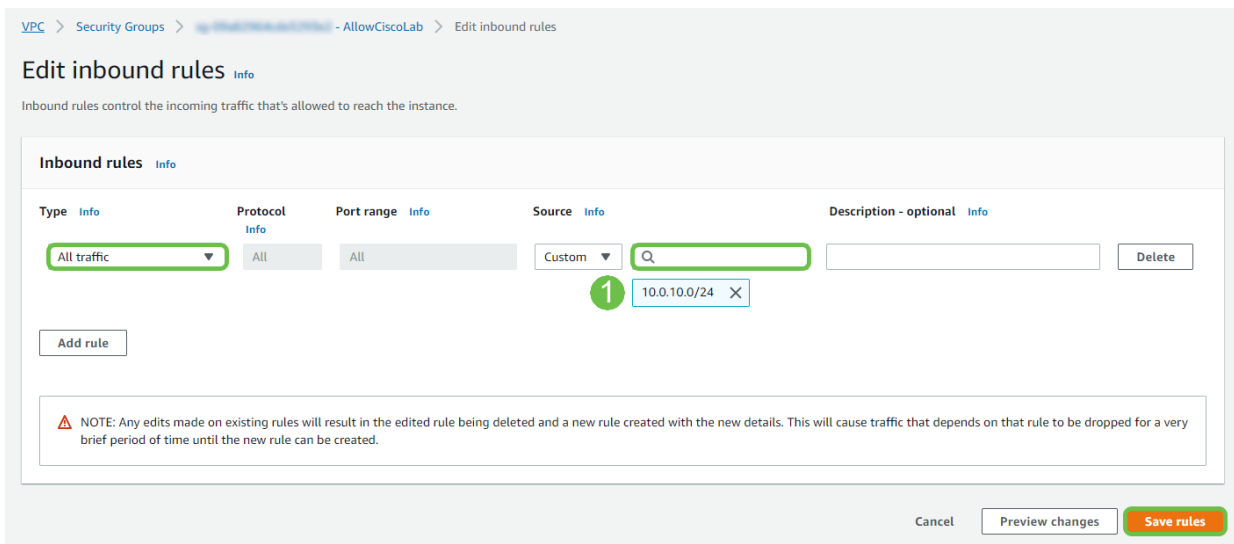
Selezionare il **gateway privato virtuale** creato in precedenza.

The screenshot shows the 'Edit route propagation' page in the AWS IAM console. The breadcrumb is 'Route Tables > Edit route propagation'. The page title is 'Edit route propagation'. Below, there is a 'Route table' section with a dropdown menu. Underneath, there is a 'Route propagation' section with a table. The table has two columns: 'Virtual Private Gateway' and 'Propagate'. A green circle with the number '1' highlights the 'Virtual Private Gateway' dropdown menu, which is currently set to 'AWS\_WAN'. The 'Propagate' checkbox is checked. At the bottom left, there is a '\* Required' label. At the bottom right, there are 'Cancel' and 'Save' buttons.

## Passaggio 15

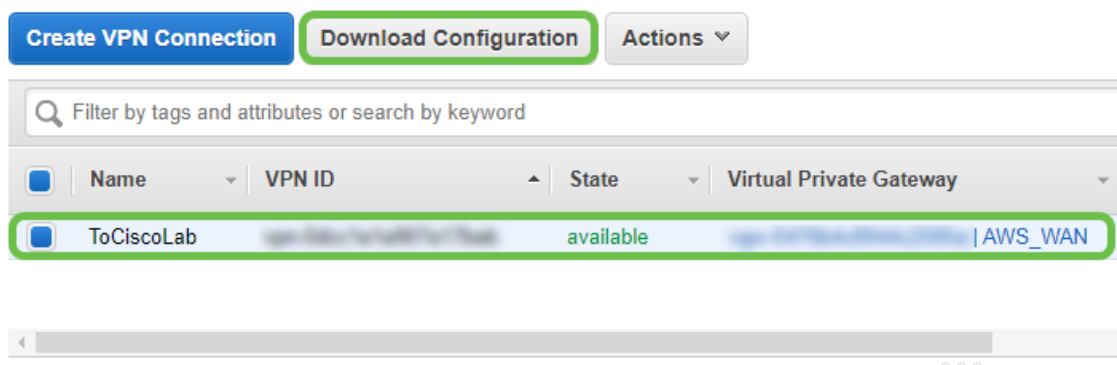
Da **VPC > Gruppi di sicurezza**, verificare di disporre di una policy creata per consentire il traffico desiderato.

**Nota:** Nell'esempio, viene usata l'origine 10.0.10.0/24, che corrisponde alla subnet in uso sul router RV di esempio.



## Passaggio 16

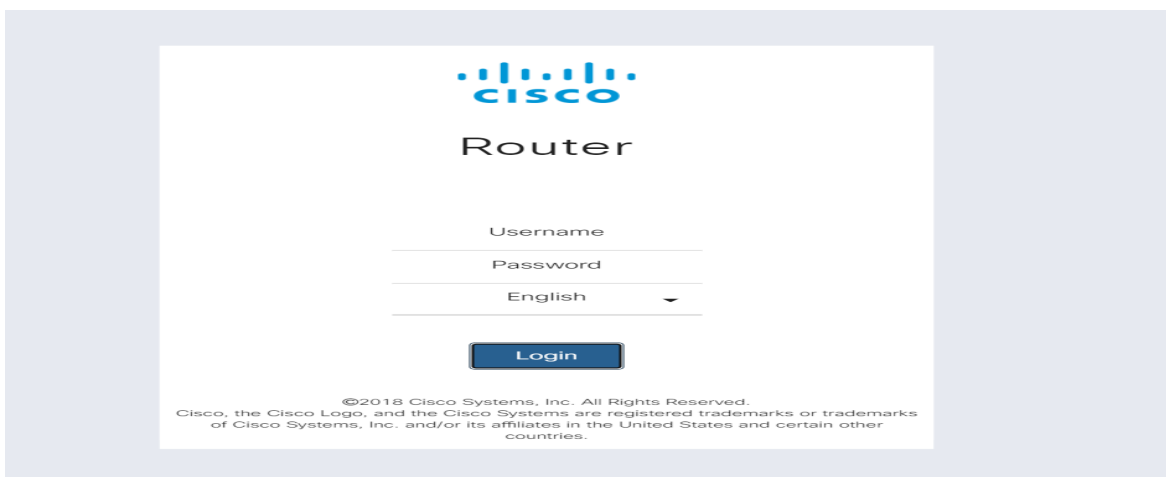
Selezionare la connessione VPN creata in precedenza e scegliere *Scarica configurazione*.



## Configurazione di una connessione da sito a sito su un router RV16X/RV26X e RV34X

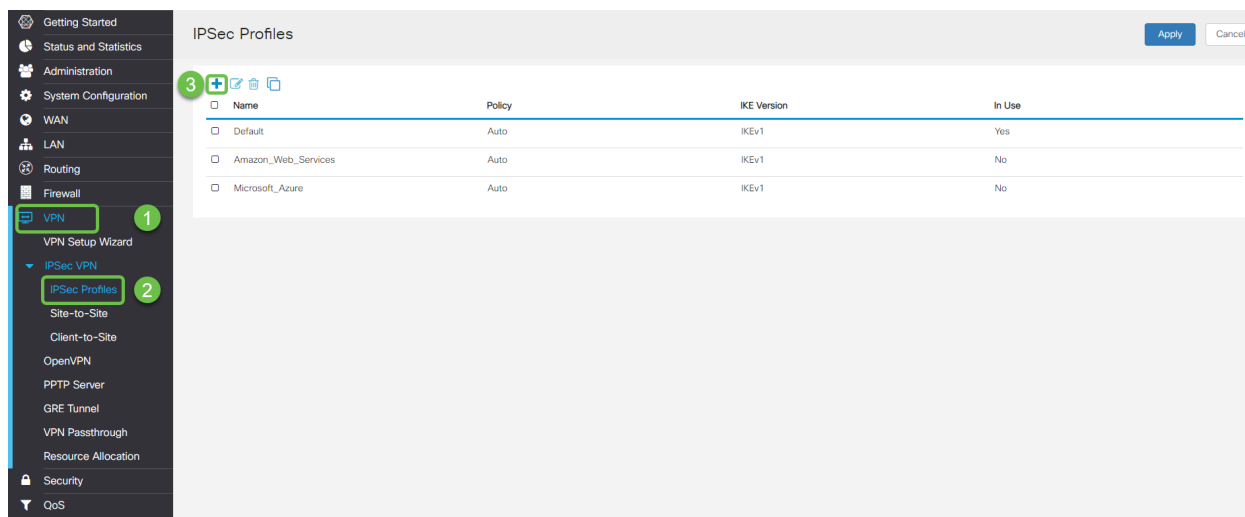
### Passaggio 1

Accedere al router utilizzando credenziali valide.



### Passaggio 2

Selezionare **VPN > Profili Ipsec**. Verrà visualizzata la pagina del profilo IPsec. Premere l'icona di aggiunta (+).



### Passaggio 3

Verrà ora creato il profilo IPSEC. Quando si crea il **profilo IPsec** sul router per piccole imprese, verificare che **DH Group 2** sia selezionato per la fase 1.

**Nota:** AWS supporta livelli di crittografia e autenticazione inferiori: nell'esempio vengono utilizzati AES-256 e SHA2-256.

### 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)

### Passaggio 4

Assicurarsi che le opzioni della Fase 2 corrispondano a quelle della Fase 1. Per AWS DH Group 2 utilizzare.



## 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

### Passaggio 5

Premere Apply (Applica) per passare alla pagina IPSEC, accertarsi di premere nuovamente Apply (Applica).

IPSec Profiles Apply Cancel

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

### Passaggio 6

Passare a VPN < Client su sito e nella pagina da client a sito premere l'icona più (+).

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	

### Passaggio 7

Quando si crea la connessione da sito a sito IPsec, assicurarsi di selezionare il **profilo IPsec** creato nei passaggi precedenti. Usare il tipo di **endpoint remoto IP statico** e immettere l'indirizzo fornito nella configurazione AWS esportata. Immettere la **chiave già condivisa** fornita nella configurazione esportata da AWS.

## Passaggio 8

Immettere l'**identificatore locale** del router per piccole imprese. Questa voce deve corrispondere al **gateway cliente** creato in AWS. Immettere l'**indirizzo IP** e la **subnet mask** per il router per piccole imprese. Questa voce deve corrispondere al **prefisso IP statico** aggiunto alla **connessione VPN** in AWS. Immettere l'**indirizzo IP** e la **subnet mask** per il router per piccole imprese. Questa voce deve corrispondere al **prefisso IP statico** aggiunto alla **connessione VPN** in 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:

## Passaggio 9

Immettere l'**identificatore remoto** per la connessione AWS. Questo valore verrà elencato in Dettagli tunnel della **connessione VPN da sito a sito** AWS. Immettere l'**indirizzo IP** e la **subnet mask** della connessione AWS, definiti durante la configurazione di AWS. Quindi premere **Apply (Applica)**.

## 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:

## Passaggio 10

Nella pagina Ip Site to Site (Da sito IP a sito), premere **Apply** (Applica).

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	

## Conclusioni

La creazione di una VPN da sito a sito tra il router della serie RV e il server AWS è stata completata. Per le discussioni della community sulla VPN da sito a sito, andare alla pagina [della community di supporto di Cisco Small Business](#) ed eseguire una ricerca di VPN da sito a sito.