

Site-to-Site-VPN mit Amazon Web Services

Ziel

In diesem Artikel erfahren Sie, wie Sie ein Site-to-Site-VPN zwischen Cisco Routern der RV-Serie und Amazon Web Services einrichten.

Anwendbare Geräte | Softwareversion

RV160| [1.0.00.17](#)

RV260|[1,0,00,17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

Einführung

Ein Site-to-Site-VPN ermöglicht die Verbindung mit zwei oder mehr Netzwerken, was Unternehmen und allgemeinen Benutzern die Möglichkeit gibt, eine Verbindung zu verschiedenen Netzwerken herzustellen. Amazon Web Services (AWS) bietet eine Vielzahl von Cloud Computing-Plattformen, darunter Site-to-Site-VPNS, mit denen Sie auf Ihre AWS-Plattformen zugreifen können. Dieser Leitfaden unterstützt Sie bei der Konfiguration des Site-to-Site-VPN auf dem Router RV16X, RV26X und RV34X für die Amazon Web Services.

Die beiden Teile sind wie folgt:

[Einrichten von Site-to-Site-VPN auf Amazon Web Services](#)

[Einrichten eines Site-to-Site-VPN auf einem RV16X/RV26X, RV34X Router](#)

Einrichten eines Site-to-Site-VPN auf Amazon Web Services

Schritt 1

Erstellen Sie einen neuen VPC, und definieren Sie einen **IPv4-CIDR-Block**, in dem wir später das LAN definieren, das als unser *AWS-LAN* verwendet wird. Wählen Sie *Erstellen aus*.

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

Schritt 2

Stellen Sie beim Erstellen des Subnetzes sicher, dass Sie das zuvor erstellte **VPC** ausgewählt haben. Definieren Sie ein Subnetz innerhalb des vorhandenen /16-Netzwerks, das zuvor erstellt wurde. In diesem Beispiel wird 172.16.10.0/24 verwendet.

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

VPC CIDRs	Status	Status Reason
172.16.0.0/16	associated	

2 IPv4 CIDR block* 172.16.10.0/24 ⓘ

* Required

Create

Schritt 3

Erstellen Sie ein **Kunden-Gateway**, und definieren Sie die **IP-Adresse** als *öffentliche IP-Adresse* Ihres Cisco RV-Routers.

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

Schritt 4

Erstellen eines **Virtual Private Gateway** - Erstellen eines *Name-Tags* zur späteren Identifizierung.

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](#) [Create Virtual Private Gateway](#)

Schritt 5

Verbinden Sie das **Virtual Private Gateway** mit dem zuvor erstellten **VPC**.

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id

1 VPC ⓘ

Filter by attributes

<input type="text" value="vpc-1234567890"/>	Cisco_Lab
---	-----------

* Required

[Cancel](#) [Yes, Attach](#)

Schritt 6

Erstellen Sie eine neue **VPN-Verbindung**, und wählen Sie den **Ziel-Gateway-Typ** *Virtual Private Gateway* aus. Verknüpfen Sie die **VPN-Verbindung** mit dem zuvor erstellten **Virtual Private Gateway**.

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
<input type="text" value="vpn-gw-1234567890"/>	AWS_WAN	<input type="text" value="vpc-1234567890"/>

Schritt 7

Wählen Sie **Vorhandenes Kunden-Gateway** aus. Wählen Sie das zuvor erstellte **Customer Gateway** aus.

1 Customer Gateway Existing
 New

2 Customer Gateway ID ⓘ

Routing Options

Filter by attributes

Customer Gateway ID	Name tag	IP Address	Certificate ARN
<input type="text" value="cgw-1234567890"/>	ToCiscoLab	<input type="text" value="10.0.0.0/16"/>	<input type="text" value="arn:aws:iam::1234567890:certificate/1234567890"/>

Schritt 8

Bei **Routing-Optionen** müssen Sie Statisch auswählen. Geben Sie alle **IP-Präfixe** einschließlich CIDR-Notation für alle Remote-Netzwerke ein, die das VPN passieren sollen. [Dies sind die Netzwerke, die auf Ihrem Cisco Router vorhanden sind.]

The screenshot shows the 'Routing Options' section of the AWS VPN console. A green box highlights the 'Static' radio button under 'Routing Options'. Below it, a table lists 'Static IP Prefixes'. A second green box highlights the 'IP Prefixes' column, which contains the entry '10.0.10.0/24'. An 'Add Another Rule' button is visible below the table.

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

Schritt 9

Die **Tunneloptionen** in diesem Leitfaden werden nicht behandelt. Wählen Sie *VPN-Verbindung erstellen aus*.

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

The screenshot shows the 'Tunnel Options' section. It contains four input fields for 'Inside IP CIDR' and 'Pre-Shared Key' for Tunnel 1 and Tunnel 2, all with the value 'Generated by Amazon'. Below these are 'Advanced Options' for each tunnel, with 'Use Default Options' selected for both.

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

* Required

Cancel [Create VPN Connection](#)

Schritt 10

Erstellen Sie eine **Routentabelle**, und ordnen Sie das zuvor erstellte **VPC** zu. Drücken Sie **Erstellen**.

[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.

The screenshot shows the 'Create route table' form. A green box highlights the 'Name tag' field with the value 'CiscoLab'. Another green box highlights the 'VPC*' dropdown menu, which is currently empty. A search dropdown is open below the VPC field, showing a search bar and a list of VPCs: 'vpc-0e3159af82f3ecfa4 Cisco_Lab' and 'vpc-791fec1f'. The 'Create' button is highlighted with a green border.

* Required

Cancel [Create](#)

Schritt 11

Wählen Sie die zuvor erstellte **Routentabelle** aus. Wählen Sie auf der Registerkarte **Subnetzuordnungen** die Option **Subnetzuordnungen bearbeiten aus**.

1

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main
<input checked="" type="checkbox"/>	aws-elasticmapreduce-...-vpc	subnet-1a1b1c1d	-	-	Yes
<input type="checkbox"/>	aws-elasticmapreduce-...-vpc	subnet-1e1f1g1h	-	-	Yes

Route Table: aws-elasticmapreduce-...-vpc

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

2 Edit subnet associations

Schritt 12

Wählen Sie auf der Seite **Subnetzuordnungen bearbeiten** das zuvor erstellte Subnetz aus. Wählen Sie die zuvor erstellte **Routentabelle** aus. Wählen Sie anschließend **Speichern aus**.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table: aws-elasticmapreduce-...-vpc

Associated subnets: subnet-1a1b1c1d

1

Schritt 13

Wählen Sie auf der Registerkarte **Route Propagation** die Option **Route-Propagation bearbeiten aus**.

[Create route table](#) Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge association
<input checked="" type="checkbox"/>	rt-1234567890	rt-1234567890	-	-
<input type="checkbox"/>	rt-9876543210	rt-9876543210	-	-

1

Route Table: rt-1234567890

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)

2 [Edit route propagation](#)

Virtual Private Gateway	Propagate
vpc-1234567890 AWS_WAN	No

Schritt 14

Wählen Sie das zuvor erstellte **Virtual Private Gateway** aus.

[Route Tables](#) > Edit route propagation

Edit route propagation

Route table: rt-1234567890

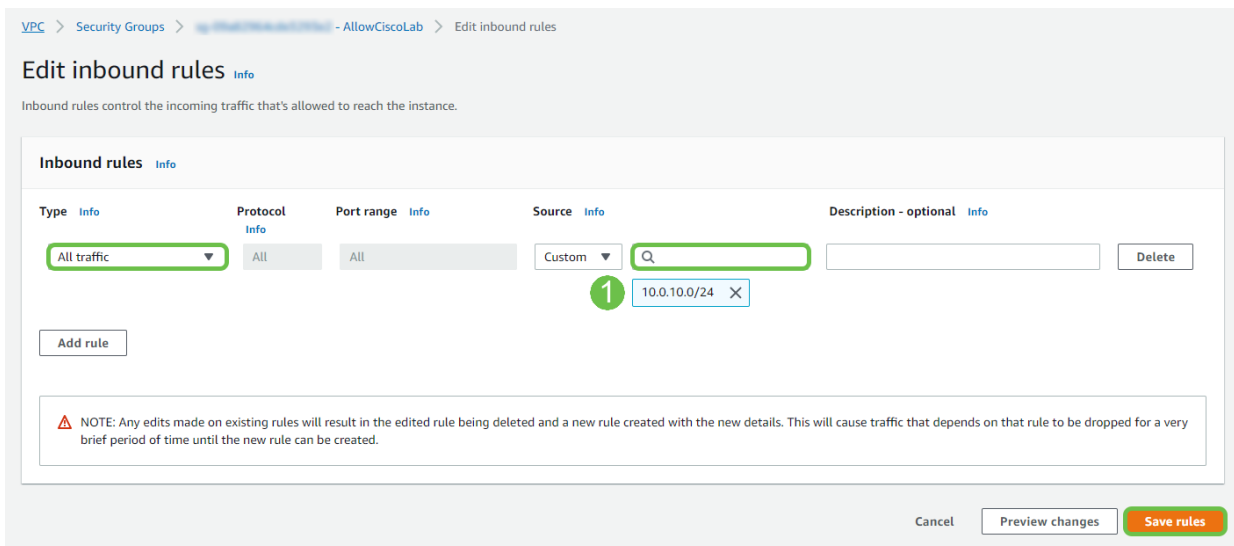
Route propagation	Virtual Private Gateway	Propagate
1	vpc-1234567890 AWS_WAN	<input checked="" type="checkbox"/>

* Required [Cancel](#) [Save](#)

Schritt 15

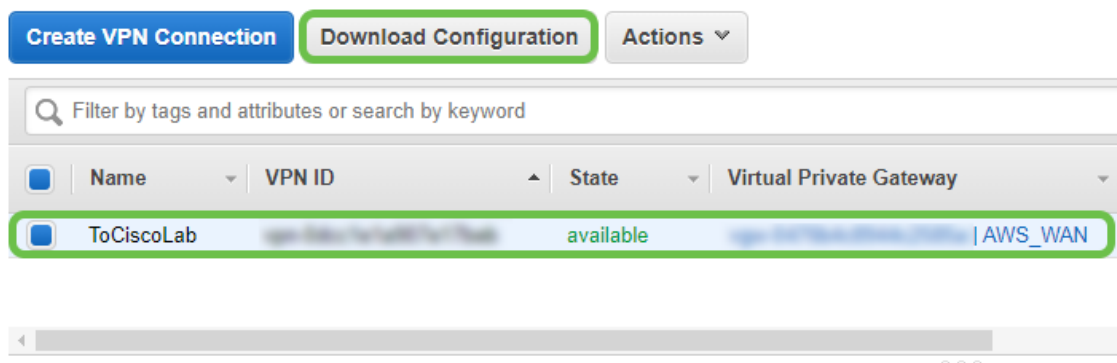
Stellen Sie **bei VPC > Security Groups** sicher, dass eine Richtlinie erstellt wurde, die den gewünschten Datenverkehr zulässt.

Hinweis: In diesem Beispiel wird eine Quelle von 10.0.10.0/24 verwendet, die dem Subnetz entspricht, das in unserem Beispiel für einen RV-Router verwendet wird.



Schritt 16

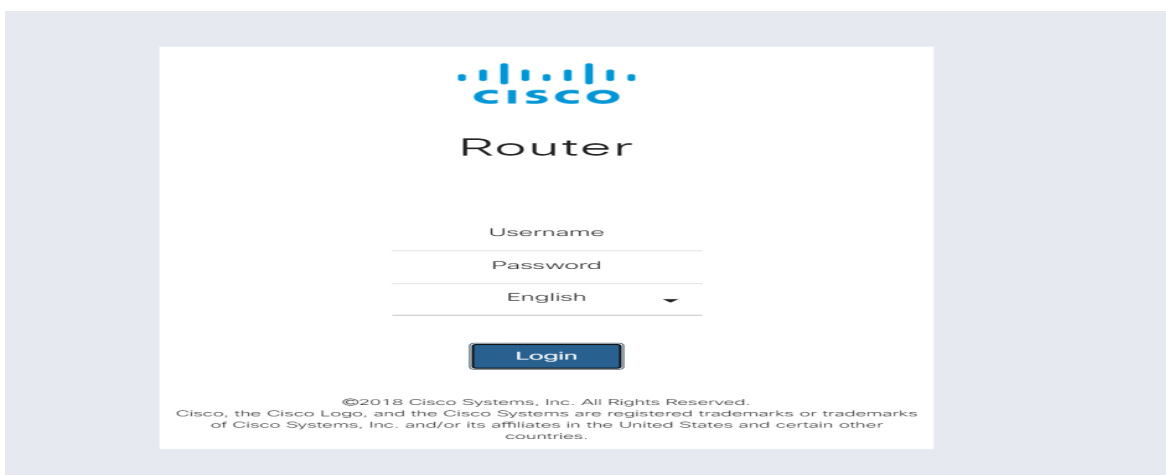
Wählen Sie die zuvor erstellte VPN-Verbindung aus, und wählen Sie *Download Configuration (Konfiguration herunterladen)*.



Standortübergreifende Einrichtung auf einem RV16X/RV26X, RV34X Router

Schritt 1

Melden Sie sich mit gültigen Anmeldeinformationen beim Router an.



Schritt 2

Navigieren Sie zu **VPN > IPSec-Profile**. Dadurch gelangen Sie zur Ipsec-Profilseite, und drücken Sie das Add-Symbol (+).

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

Schritt 3

Wir erstellen jetzt unser IPSEC-Profil. Stellen Sie beim Erstellen des **IPsec-Profiles** auf Ihrem Small Business-Router sicher, dass **DH Group 2** für Phase 1 ausgewählt ist.

Hinweis: AWS unterstützt niedrigere Verschlüsselungs- und Authentifizierungsstufen - in diesem Beispiel werden AES-256 und SHA2-256 verwendet.

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)

Schritt 4

Stellen Sie sicher, dass die Optionen in Phase 2 mit denen in Phase 1 übereinstimmen. Für AWS muss die DH-Gruppe 2 verwendet werden.

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

Schritt 5

Drücken Sie Apply (Übernehmen), und Sie werden zur IPSEC-Seite navigiert. Drücken Sie erneut Apply (Übernehmen).

IPSec Profiles Apply Cancel

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

Schritt 6

Navigieren Sie zu VPN < Client to site, und drücken Sie auf der Seite Client to Site das Pluszeichen (+).

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	

Schritt 7

Achten Sie beim Erstellen der IPsec-Site-to-Site-Verbindung darauf, das in den vorherigen Schritten erstellte **IPsec-Profil** auszuwählen. Verwenden Sie den **Remote Endpoint**-Typ der *statischen IP* und geben Sie die Adresse ein, die in der exportierten AWS-Konfiguration angegeben ist. Geben Sie den **Pre-Shared Key** ein, der in der exportierten Konfiguration von AWS bereitgestellt wird.

Schritt 8

Geben Sie die **lokale ID** für Ihren Small Business-Router ein. Dieser Eintrag sollte mit dem **Kunden-Gateway** übereinstimmen, das in AWS erstellt wurde. Geben Sie die **IP-Adresse** und die **Subnetzmaske** für Ihren Small Business-Router ein. Dieser Eintrag sollte mit dem **statischen IP-Präfix übereinstimmen, das der VPN-Verbindung** in AWS hinzugefügt wurde. Geben Sie die **IP-Adresse** und die **Subnetzmaske** für Ihren Small Business-Router ein. Dieser Eintrag sollte mit dem **statischen IP-Präfix übereinstimmen, das der VPN-Verbindung** in AWS hinzugefügt wurde.

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:

Schritt 9

Geben Sie den **Remote Identifier** für Ihre AWS-Verbindung ein. Dieser wird unter Tunneldetails der AWS **Site-to-Site-VPN-Verbindung** aufgeführt. Geben Sie die **IP-Adresse** und **Subnetzmaske** für Ihre AWS-Verbindung ein, die während der AWS-Konfiguration definiert wurde. Drücken Sie dann **Apply**.

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:

Schritt 10

Sobald Sie die Seite "IP Site to Site" aufgerufen haben, drücken Sie **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	

Schlussfolgerung

Sie haben nun erfolgreich ein Site-to-Site-VPN zwischen Ihrem Router der RV-Serie und Ihrem AWS erstellt. Bei Diskussionen in der Community über Site-to-Site-VPN können Sie auf der Seite [Cisco Small Business Support Community](#) nach Site-to-Site-VPN suchen.