

Amazon Web Services를 사용한 사이트 간 VPN

목표

이 문서의 목적은 Cisco RV Series 라우터와 Amazon Web Services 간에 사이트 대 사이트 VPN을 설정하는 방법을 안내하는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

RV160| [1.0.00.17](#)

RV260|[1.0.00.17](#)

RV340| [1.0.03.18](#)

RV345| [1.0.03.18](#)

소개

Site-to-Site VPN을 사용하면 두 개 이상의 네트워크에 연결할 수 있으므로 기업과 일반 사용자가 서로 다른 네트워크에 연결할 수 있습니다. Amazon Web Services(AWS)는 AWS 플랫폼에 액세스할 수 있는 사이트 간 VPNs를 비롯한 다양한 온디맨드 클라우드 컴퓨팅 플랫폼을 제공합니다. 이 가이드는 Amazon Web Services에 대한 RV16X, RV26X, RV34X 라우터의 사이트 대 사이트 VPN을 구성하는 데 도움이 됩니다.

두 부분은 다음과 같습니다.

[Amazon Web Services에서 사이트 대 사이트 VPN 설정](#)

[RV16X/RV26X, RV34X 라우터에서 사이트 대 사이트 VPN 설정](#)

Amazon Web Services에서 사이트 대 사이트 VPN 설정

1단계

새 VPC를 생성하고 IPv4 CIDR 블록을 정의하면 나중에 AWS LAN으로 사용되는 LAN을 정의합니다. 생성을 선택합니다.

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

2단계

서브넷을 생성할 때 이전에 생성한 VPC를 선택했는지 확인합니다. 이전에 생성한 기존 /16 네트워크 내에서 서브넷을 정의합니다. 이 예에서는 172.16.10.0/24이 사용됩니다.

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

3단계

고객 게이트웨이를 생성하여 IP 주소를 Cisco RV 라우터의 공용 IP 주소로 정의합니다.

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

4단계

가상 사설 게이트웨이 만들기 - 이름 태그를 만들어 나중에 식별할 수 있습니다.

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

5단계

이전에 생성한 VPC에 Virtual Private Gateway를 연결합니다.

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

단계 6

새 VPN 연결을 생성하고 Target Gateway Type Virtual Private Gateway를 선택합니다. VPN 연결을 이전에 생성한 Virtual Private Gateway와 연결합니다.

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

7단계

기존 고객 게이트웨이를 선택합니다. 이전에 생성한 고객 게이트웨이를 선택합니다.

1 Customer Gateway Existing
 New

2 Customer Gateway ID ⓘ

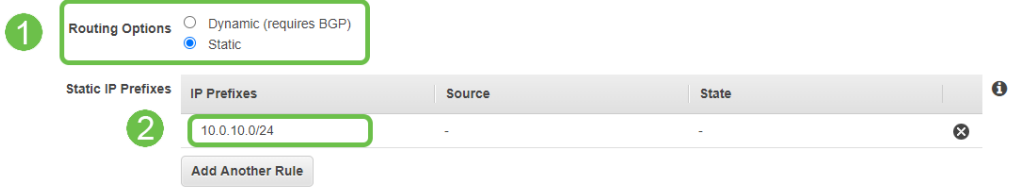
Routing Options

Filter by attributes

Customer Gateway ID	Name tag	IP Address	Certificate ARN
vpn-gw-0123456789012345	ToCiscoLab	vpn-gw-0123456789012345	vpn-gw-0123456789012345

8단계

라우팅 옵션의 경우 정적을 선택합니다.VPN을 통과할 것으로 예상되는 원격 네트워크에 대한 CIDR 표기법을 포함한 IP 접두사를 입력합니다. [이러한 네트워크는 Cisco 라우터에 있는 네트워크입니다.]



9단계

이 가이드에서 터널 옵션은 다루지 않습니다. *Create VPN Connection(VPN 연결 생성)*을 선택합니다.

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](#) [Create VPN Connection](#)

10단계

경로 테이블을 생성하고 이전에 생성한 VPC를 연결합니다.생성을 누릅니다.

[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

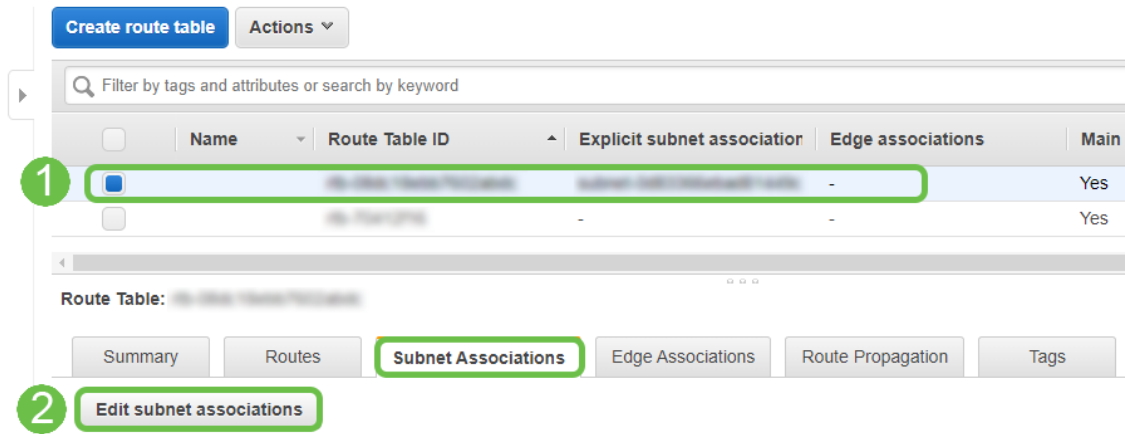
vpc-791fec1f

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

11단계

이전에 생성한 **Route Table**을 선택합니다.Subnet Associations(서브넷 연결) 탭에서 Edit subnet

associations(서브넷 연결 편집)를 선택합니다.

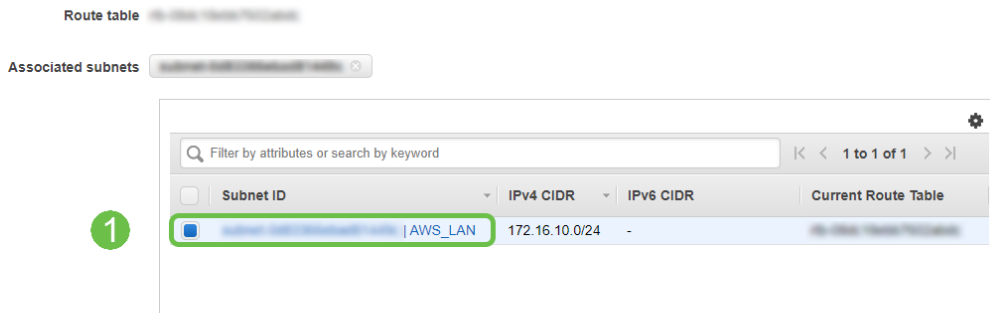


12단계

Edit subnet associations(서브넷 연결 수정) 페이지에서 이전에 생성한 서브넷을 선택합니다. 이전에 생성한 **Route Table**을 선택합니다. 그런 다음 **저장**을 선택합니다.

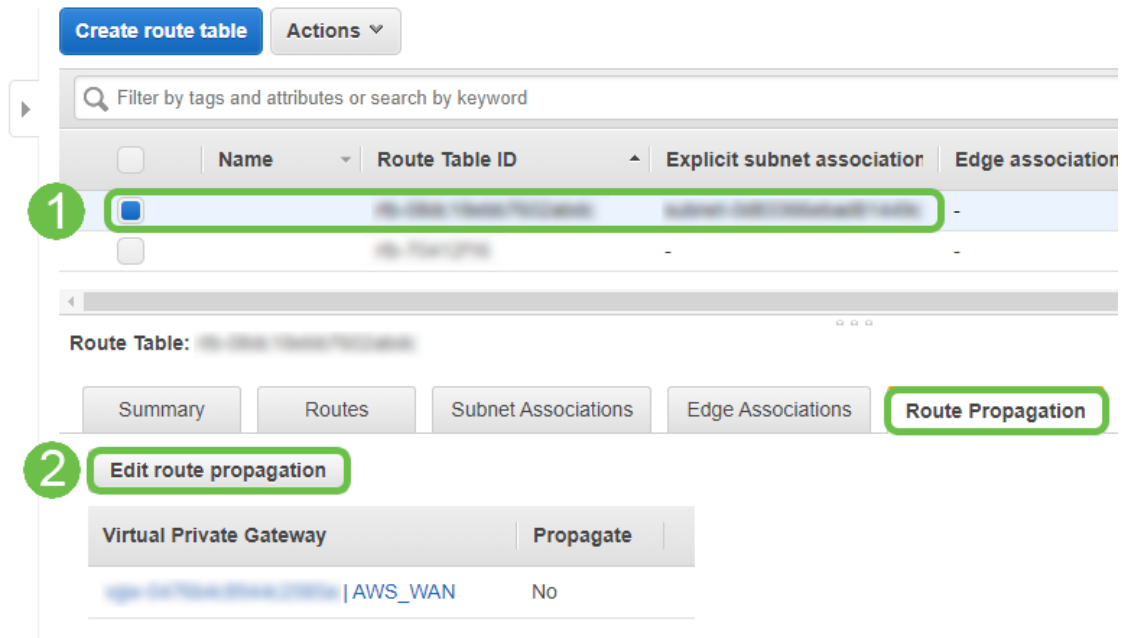
[Route Tables](#) > Edit subnet associations

Edit subnet associations



13단계

Route Propagation 탭에서 *Edit route propagation*을 선택합니다.



14단계

이전에 생성한 가상 프라이빗 게이트웨이를 선택합니다.

[Route Tables](#) > Edit route propagation

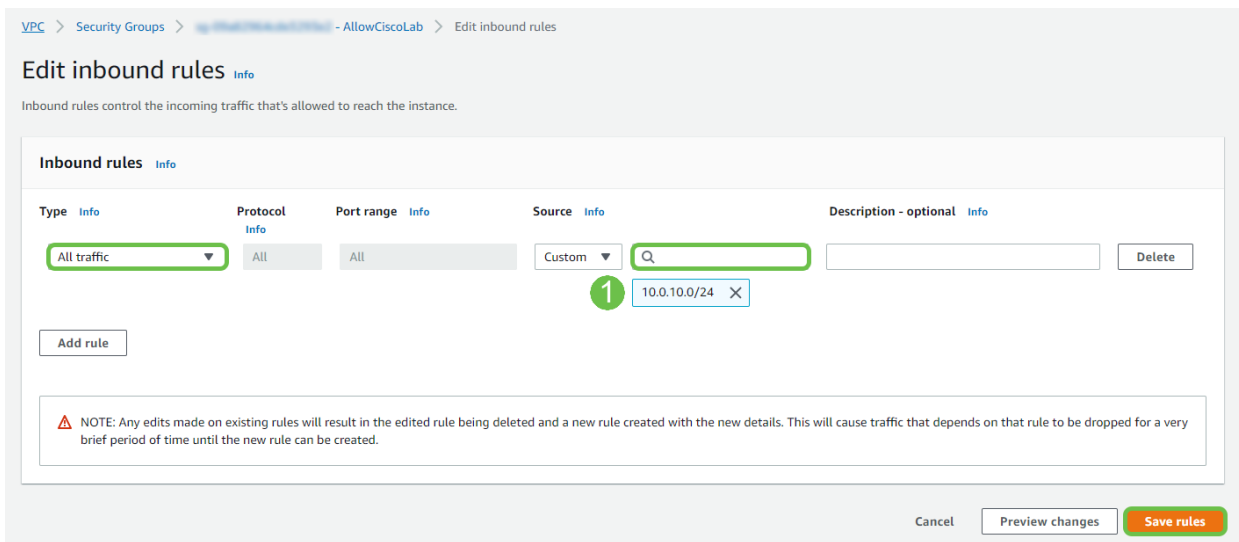
Edit route propagation



15단계

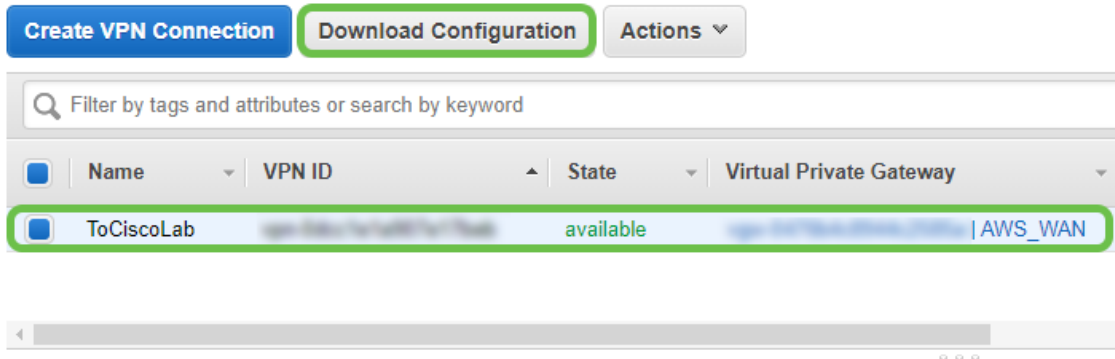
VPC > **Security Groups**에서 원하는 트래픽을 허용하도록 정책을 생성했는지 확인합니다.

참고: 이 예에서는 RV 라우터에서 사용 중인 서브넷에 해당하는 10.0.10.0/24 소스를 사용합니다.



16단계

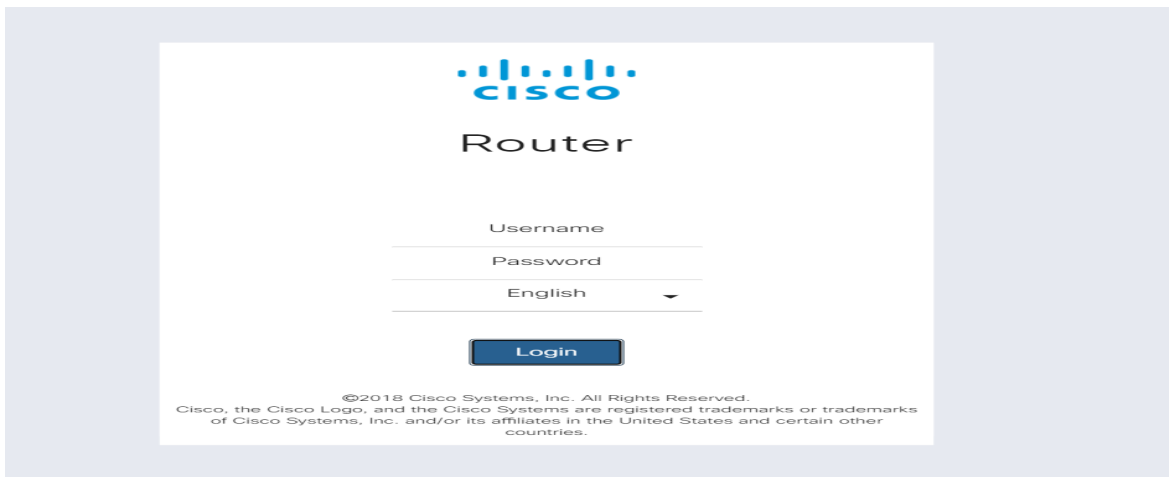
이전에 생성한 VPN Connection(VPN 연결)을 선택하고 Download Configuration(컨피그레이션 다운로드)을 선택합니다.



RV16X/RV26X, RV34X 라우터에서 사이트 대 사이트 설정

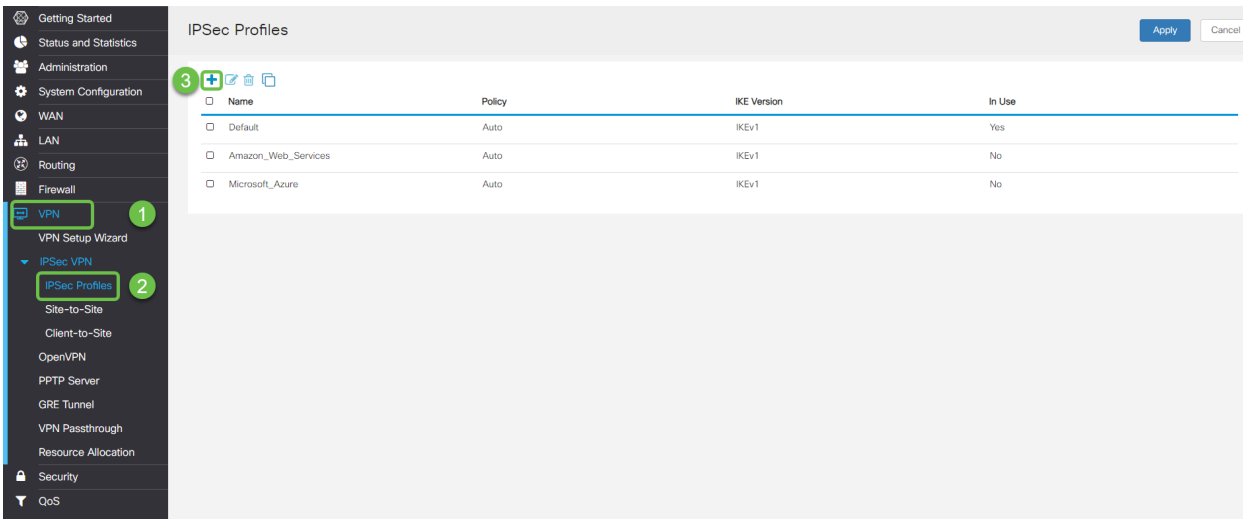
1단계

유효한 자격 증명을 사용하여 라우터에 로그인합니다.



2단계

VPN > Ipsec Profiles로 이동합니다.그러면 Ipsec 프로파일 페이지로 이동하고 추가 아이콘(+)을 누릅니다.



3단계

이제 IPSEC 프로필을 생성합니다. Small Business 라우터에서 IPsec 프로필을 생성할 때 DH 그룹 2가 1단계에 대해 선택되었는지 확인합니다.

참고: AWS는 더 낮은 수준의 암호화 및 인증을 지원합니다. 이 예에서는 AES-256 및 SHA2-256이 사용됩니다.

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)

4단계

단계 2 옵션이 1단계에서 만든 옵션과 일치하는지 확인합니다. AWS DH 그룹 2의 경우 이를 사용해야 합니다.

Phase II Options

Protocol Selection:

Encryption:

Authentication:

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

Perfect Forward Secrecy: Enable

DH Group:

5단계

Apply(적용)를 누르면 IPSEC 페이지로 이동합니다. Apply(적용)를 다시 누릅니다.

IPSec Profiles Apply Cancel

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

6단계

VPN < Client to site(VPN 클라이언트 대 사이트)로 이동하고 Client to Site(클라이언트 대 사이트) 페이지에서 더하기 아이콘(+)을 누릅니다.

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	

7단계

IPsec Site-to-Site Connection을 생성할 때 이전 단계에서 생성한 IPsec 프로필을 선택해야 합니다. 고정 IP의 원격 엔드포인트 유형을 사용하고 내보낸 AWS 컨피그레이션에 제공된 주소를 입력합니다. AWS에서 내보낸 컨피그레이션에 제공된 사전 공유 키를 입력합니다.

8단계

Small Business 라우터의 로컬 식별자를 입력합니다. 이 항목은 AWS에서 생성한 고객 게이트웨이와 일치해야 합니다. Small Business 라우터의 IP 주소 및 서브넷 마스크를 입력합니다. 이 항목은 AWS의 VPN 연결에 추가된 정적 IP 접두사와 일치해야 합니다. Small Business 라우터의 IP 주소 및 서브넷 마스크를 입력합니다. 이 항목은 AWS의 VPN 연결에 추가된 정적 IP 접두사와 일치해야 합니다.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

Remote Group Setup

Remote Identifier Type:

Remote Identifier:

Remote IP Type:

IP Address:

Subnet Mask:

Aggressive Mode:

9단계

AWS 연결의 원격 식별자를 입력합니다. 이 ID는 AWS Site-to-Site VPN Connection의 Tunnel Details(터널 세부사항)에 나열됩니다. AWS 컨피그레이션 중에 정의된 AWS 연결의 IP 주소 및 서브넷 마스크를 입력합니다. 그런 다음 Apply(적용)를 누릅니다.

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:

10단계

Ip Site to Site 페이지에서 Apply를 누릅니다.

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	

결론

이제 RV 시리즈 라우터와 AWS 간에 사이트 대 사이트 VPN을 성공적으로 생성했습니다. Site-to-Site VPN에 대한 커뮤니티 논의를 보려면 [Cisco Small Business Support Community](#) 페이지로 이동하여 Site-to-Site VPN을 검색합니다.