



## Cisco Secure Management Center와 AWS VPC 사이의 경로 기반 사이트 간 VPN 구성

### Cisco Secure Management Center와 AWS VPC 사이의 경로 기반 사이트 간 VPN 구성 2

소개 2

가이드의 적합성 확인 2

시나리오 2

시스템 요구 사항 2

이점 3

사전 요구 사항 3

Management Center와 AWS 사이의 사이트 간 VPN 구성 요소 3

Management Center와 AWS VPC 사이에 경로 기반 VPN을 구성하기 위한 엔드 투 엔드 절차 4

AWS에서 탄력적 IP 주소 구성 6

AWS에서 가상 프라이빗 클라우드 생성 6

AWS에서 고객 게이트웨이 생성 9

AWS에서 가상 프라이빗 게이트웨이 생성 11

AWS에서 VPN 연결 생성 12

Management Center에서 경로 기반 VPN 구성 15

Management Center에서 라우팅 정책 구성 20

VTI 터널 상태 및 구성 확인 23

# Cisco Secure Management Center와 AWS VPC 사이의 경로 기반 사이트 간 VPN 구성

## 소개

Secure Firewall Management Center(Management Center)에는 매니지드 Threat Defense 디바이스에서 사이트 간 VPN의 구성을 간소화하도록 설계된 직관적인 VPN 마법사가 있습니다.

또한 이러한 마법사를 사용하면 Threat Defense 디바이스와 엑스트라넷 디바이스 간의 경로 기반 사이트 간 VPN을 쉽게 설정할 수 있습니다. 관리 센터의 직접 관리 대상이 아닌 엑스트라넷 디바이스는 퍼블릭 클라우드 인프라 내에 있는 게이트웨이로 구성될 수 있습니다. 경로 기반 VPN은 VPN 터널의 기반을 형성하는 라우팅 가능한 논리적 인터페이스인 VTI(Virtual Tunnel Interface)를 사용합니다.

## 가이드의 적합성 확인

이 가이드는 Management Center를 사용하여 본사에 위치한 Threat Defense 디바이스와 AWS VPC(가상 프라이빗 클라우드) 간에 사이트 간 VPN을 설정하는 네트워크 관리자를 대상으로 합니다.

## 시나리오

한 중간 규모 기업이 여러 브랜치 오피스를 운영하고 있으며, 각 브랜치 오피스마다 AWS에서 호스팅되는 인스턴스 집합이 있습니다. 이 조직은 강력한 네트워크 인프라를 설정하여 모든 위치에서 안전하고 원활한 커뮤니케이션을 지원해야 합니다. 이 솔루션에는 각 브랜치의 AWS VPC를 조직의 중앙 본사에 있는 Threat Defense 디바이스에 연결하는 사이트 간 VPN을 구성하는 작업이 포함됩니다. 기본적으로 AWS VPC 인스턴스는 외부 네트워크와 격리되어 있으므로 이 연결성은 매우 중요합니다. 이 VPN의 구현은 브랜치를 기업 네트워크에 통합할 수 있도록 하여 중앙 집중식 액세스 및 데이터 보안을 보장합니다.

## 시스템 요구 사항

다음 테이블에는 이 기능을 위한 플랫폼이 나와 있습니다.

제품	버전	이 문서에 사용된 버전
Cisco Secure Firewall Threat Defense(구 Firepower Threat Defense/FTD)	6.7 이상	7.4.1
Cisco Secure Firewall Management Center(구 Firepower Management Center/FMC)	6.7 이상	7.4.1

제품	버전	이 문서에 사용된 버전
AWS 계정	-	-

## 이점

제안된 솔루션은 다음과 같은 상당한 이점을 제공합니다.

- 간소화된 설정: VTI는 VPN 구성에 간소화된 접근 방식을 제공하여 기존 암호화 맵 및 액세스 목록의 복잡성을 제거합니다.
- 적응형 라우팅: VTI는 BGP, EIGRP, OSPF 등의 동적 라우팅 프로토콜을 수용하여, 네트워크 조건의 변화에 대응하여 VPN 엔드포인트 간에 경로를 자동으로 업데이트합니다.
- ISP 복원력: VTI는 보조 백업 터널을 생성하여 연결성 신뢰성을 높입니다.
- 로드 밸런싱: VTI에서는 ECMP 라우팅을 통해 VPN 트래픽을 균일하게 분산할 수 있습니다.

## 사전 요구 사항

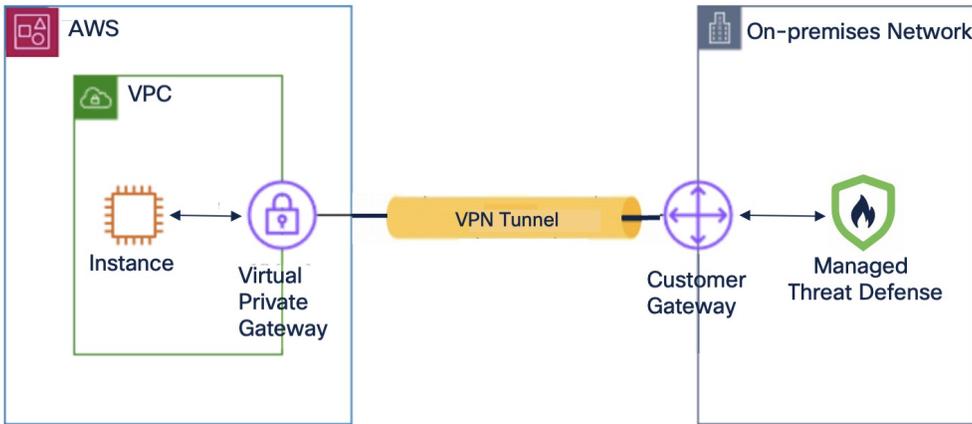
- 라이선스: Management Center Essentials(구 Base) 라이선스는 내보내기 제어 기능을 허용해야 합니다. Management Center에서 이 기능을 확인하려면 **System(시스템) > License(라이선스) > Smart License(스마트 라이선스)**를 선택합니다.
- Threat Defense 디바이스에 인터넷 라우팅이 가능한 퍼블릭 IP 주소를 구성합니다.
- Threat Defense 디바이스의 인터페이스에 적절한 논리 이름과 IP 주소를 할당합니다.
- AWS 어카운트를 소유합니다.

## Management Center와 AWS 사이의 사이트 간 VPN 구성 요소

Management Center와 AWS 사이의 사이트 간 VPN은 다음과 같이 구성됩니다.

- 가상 프라이빗 게이트웨이
- 고객 게이트웨이 디바이스(매니지드 위협 방어)
- 고객 게이트웨이

그림 1: AWS VPC와 온프레미스 네트워크 사이의 사이트 간 VPN



### 가상 프라이빗 게이트웨이

가상 프라이빗 게이트웨이는 사이트 간 VPN 연결의 AWS 측에 있는 VPN 집선 장치입니다. 가상 프라이빗 게이트웨이를 생성하고 VPC(가상 프라이빗 클라우드)에 연결합니다.

### 고객 게이트웨이

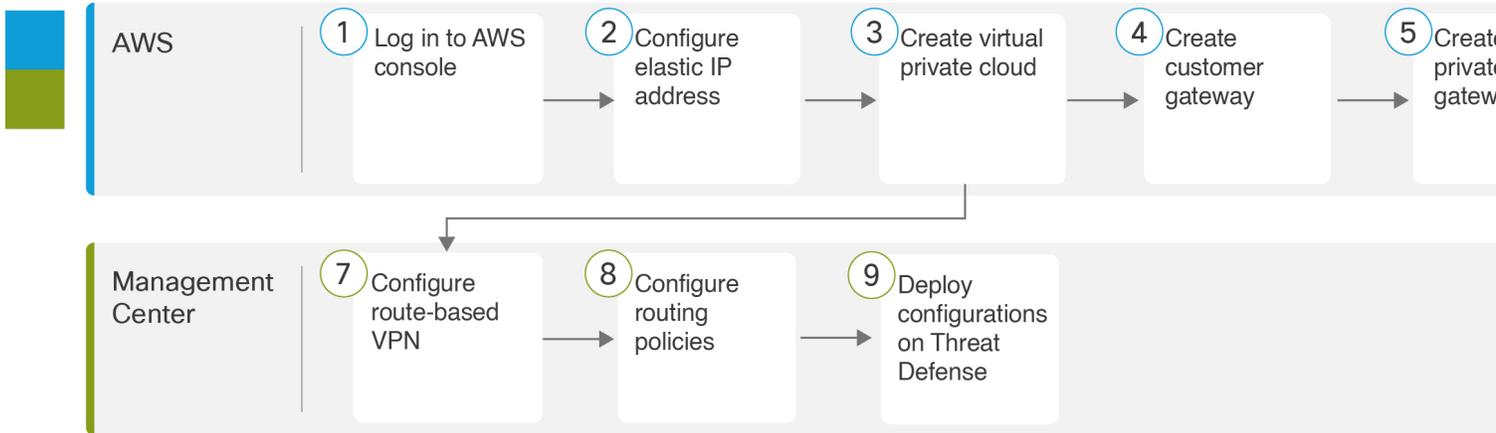
고객 게이트웨이는 온프레미스 네트워크의 고객 게이트웨이 디바이스를 나타내는 AWS에서 생성하는 리소스입니다. 고객 게이트웨이를 생성할 때는 디바이스에 대한 정보를 AWS에 제공합니다.

### 고객 게이트웨이 디바이스(매니지드 위협 방어)

고객 게이트웨이 디바이스는 중앙 본사의 온프레미스 네트워크에 있는 Threat Defense 디바이스입니다. AWS 사이트 간 VPN 연결과 함께 작동하도록 디바이스를 구성합니다.

## Management Center와 AWS VPC 사이에 경로 기반 VPN을 구성하기 위한 엔드 투 엔드 절차

다음 순서도는 Management Center와 AWS VPC 간에 경로 기반 VPN을 구성하는 워크플로우를 보여줍니다.



- 1 AWS에서 탄력적 IP 주소 구성, 6 페이지
- 2 Management Center에서 라우팅 정책 구성, 20 페이지
- 3 AWS에서 가상 프라이빗 클라우드 생성, 6 페이지
- 4 AWS에서 고객 게이트웨이 생성, 9 페이지
- 5 AWS에서 가상 프라이빗 게이트웨이 생성, 11 페이지
- 6 AWS에서 VPN 연결 생성, 12 페이지
- 7 Management Center에서 경로 기반 VPN 구성, 15 페이지

단계	설명
①	AWS 콘솔에 로그인합니다.
②	탄력적 IP 주소를 구성합니다. <a href="#">AWS에서 탄력적 IP 주소 구성, 6 페이지</a> 을 참조하십시오.
③	가상 프라이빗 클라우드를 생성합니다. <a href="#">AWS에서 가상 프라이빗 클라우드 생성, 6 페이지</a> 을 참조하십시오.
④	고객 게이트웨이를 생성합니다. <a href="#">AWS에서 고객 게이트웨이 생성, 9 페이지</a> 을 참조하십시오.
⑤	가상 프라이빗 게이트웨이를 생성합니다. <a href="#">AWS에서 가상 프라이빗 게이트웨이 생성, 11 페이지</a> 을 참조하십시오.
⑥	AWS에서 VPN 연결을 생성합니다. <a href="#">AWS에서 VPN 연결 생성, 12 페이지</a> 을 참조하십시오.
⑦	경로 기반 VPN을 구성합니다. <a href="#">Management Center에서 경로 기반 VPN 구성, 15 페이지</a> 을 참조하십시오.
⑧	라우팅 정책을 구성합니다. <a href="#">Management Center에서 라우팅 정책 구성, 20 페이지</a> 을 참조하십시오.
⑨	구성을 위협 방어 디바이스에 구축합니다.

## AWS에서 탄력적 IP 주소 구성

탄력적 IP 주소는 AWS 어카운트에 할당되는 고정 공용 IPv4 주소입니다.

프로시저

---

단계 1 **Services**(서비스) > **Networking and Content Delivery**(네트워킹 및 콘텐츠 전달) > **VPC**를 선택합니다.

단계 2 왼쪽 창에서 **Elastic IPs**(탄력적 IP)를 클릭합니다.

단계 3 **Allocate Elastic IP address**(탄력적 IP 주소 할당)를 클릭합니다.

단계 4 **Allocate Elastic IP address**(탄력적 IP 주소 할당) 대화 상자에서 다음 매개변수를 구성합니다.

- a) **Network Border Group**(네트워크 경계 그룹)에는 기본값을 사용합니다.
  - b) **Amazon's pool of IPv4 addresses**(Amazon의 IPv4 주소 풀) 라디오 버튼을 클릭합니다.
  - c) **Allocate**(할당)을 클릭합니다.
- 

## AWS에서 가상 프라이빗 클라우드 생성

VPC는 AWS 어카운트 전용 가상 네트워크이며, AWS Cloud의 다른 가상 네트워크와 논리적으로 격리되어 있습니다. VPC를 생성할 때 AWS는 IP 주소, 서브넷, 라우트 테이블, 네트워크 게이트웨이 및 보안 설정을 구성합니다.

프로시저

---

단계 1 **Services**(서비스) > **Networking and Content Delivery**(네트워킹 및 콘텐츠 전달) > **VPC**를 선택합니다.

단계 2 왼쪽 창에서 **VPC Dashboard**(VPC 대시보드)를 클릭합니다.

단계 3 **Create VPC**(VPC 생성)를 클릭합니다.

단계 4 **Create VPC**(VPC 생성) 대화 상자에서 다음 매개변수를 구성합니다.

aws Services Search

VPC > Your VPCs > Create VPC

## Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such

### VPC settings

**Resources to create [Info](#)**  
Create only the VPC resource or the VPC and other networking resources.

VPC only  VPC and more

**Name tag auto-generation [Info](#)**  
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate  
project-doc-demo

**IPv4 CIDR block [Info](#)**  
Determine the starting IP and the size of your VPC using CIDR notation.

65,536 IPs

**IPv6 CIDR block [Info](#)**

No IPv6 CIDR block  
 Amazon-provided IPv6 CIDR block

**Tenancy [Info](#)**

Default

**Number of Availability Zones (AZs) [Info](#)**  
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

▶ Customize AZs

**Number of public subnets** [Info](#)  
 The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0  2

**Number of private subnets** [Info](#)  
 The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0  2  4

▶ **Customize subnets CIDR blocks**

---

**NAT gateways (\$)** [Info](#)  
 Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None  In 1 AZ  1 per AZ

**VPC endpoints** [Info](#)  
 Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at anytime.

None  S3 Gateway

---

**DNS options** [Info](#)

Enable DNS hostnames  
 Enable DNS resolution

▶ **Additional tags**

- a) **VPC and more**(VPC 및 기타) 라디오 버튼을 클릭합니다.
- b) **Name tag**(이름 태그) 필드에 VPC를 식별하는 이름을 입력합니다.
- c) **IPv4 CIDR block**(IPv4 CIDR 차단) 필드에 IP 주소를 입력합니다.  
 CIDR 블록 크기는 /16 ~ /28이어야 합니다.
- d) **Tenancy**(테넌시) 드롭다운 목록에서 **Default**(기본값)를 선택합니다.  
 이 옵션은 VPC에서 실행하는 인스턴스가 다른 AWS 어카운트와 공유되는 하드웨어 또는 사용 전용 하드웨어에서 실행되는지 정의합니다.
- e) 두 개 이상의 가용성 영역에서 서브넷을 프로비저닝하려면 **Number of Availability Zones (AZs)**(가용성 영역(AZ)의 수)로 **2**를 선택합니다.
- f) 서브넷을 구성할 **Number of public subnets**(퍼블릭 서브넷 수) 및 **Number of private subnets**(프라이빗 서브넷 수)의 값을 선택합니다.
- g) **Customize subnets CIDR Blocks**(서브넷 CIDR 블록 사용자 지정)을 확장하여 서브넷의 IP 주소 범위를 선택합니다. AWS에서 직접 선택하도록 할 수도 있습니다.
- h) (선택 사항) **NAT gateways**(NAT 게이트웨이)에 대해 프라이빗 서브넷의 리소스가 IPv4를 통해 퍼블릭 인터넷에 액세스해야 하는 경우, NAT 게이트웨이를 생성할 AZ 수를 선택합니다.
- i) **VPC endpoints**(VPC 엔드포인트)에 대해 **None**(없음) 또는 **S3 Gateway**(S3 게이트웨이)를 선택합니다.

- j) (선택 사항) **DNS options(DNS 옵션)**에서 두 옵션 모두 기본적으로 활성화됩니다.
- k) **Create VPC(VPC 생성)**를 클릭합니다.

## AWS에서 서브넷을 경로 테이블과 연결

VPC의 각 서브넷을 VPC의 라우팅 테이블과 연결해야 합니다.

시작하기 전에

AWS에서 VPC를 생성합니다.

프로시저

단계 1 왼쪽 창에서 **Route tables(라우팅 테이블)**를 클릭합니다.

단계 2 VPC에 할당된 라우팅 테이블을 선택합니다.

단계 3 **Subnet associations(서브넷 연결)** 탭을 클릭합니다.

단계 4 **Edit subnet associations(서브넷 연결 편집)**을 클릭합니다.



단계 5 프라이빗 및 퍼블릭 서브넷 체크 박스를 선택합니다.

단계 6 **Save Associations(연결 저장)**를 클릭합니다.

## AWS에서 고객 게이트웨이 생성

디바이스에 대한 정보를 AWS에 제공할 고객 게이트웨이를 생성합니다.

프로시저

단계 1 왼쪽 창에서 **VPN(Virtual Private Network)**을 확장합니다.

단계 2 고객 게이트웨이를 클릭합니다.

단계 3 **Create customer gateway**(고객 게이트웨이 생성)를 클릭합니다.

단계 4 **Create Customer Gateway**(고객 게이트웨이 생성) 대화 상자에서 다음 매개변수를 구성합니다.

The screenshot shows the AWS console interface for creating a customer gateway. The breadcrumb navigation is 'VPC > Customer gateways > Create customer gateway'. The main heading is 'Create customer gateway' with an 'Info' link. Below the heading is a brief description: 'A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.' The form is divided into two main sections: 'Details' and 'Tags'.  
In the 'Details' section, there are five fields:  
1. 'Name tag - optional': A text input field containing 'FTD-doc-demo'. Below it, a note says 'Value must be 256 characters or less in length.'  
2. 'BGP ASN': A text input field containing '65000'. Below it, a note says 'Value must be in 1 - 2147483647 range.'  
3. 'IP address': An empty text input field. Below it, a note says 'Specify the IP address for your customer gateway device's external interface.'  
4. 'Certificate ARN': A dropdown menu with the text 'Select certificate ARN'. Below it, a note says 'The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).'  
5. 'Device - optional': A text input field with the placeholder text 'Enter device name'.  
In the 'Tags' section, there is a description of tags and a list of existing tags. The list shows a key 'Name' and a value 'FTD-doc-demo'. There is a 'Remove' button next to the tag. Below the list is an 'Add new tag' button and a note: 'You can add 49 more tags.' At the bottom of the form, there are 'Cancel' and 'Create customer gateway' buttons.

- a) **Name tag**(이름 태그) 필드에 고객 게이트웨이를 식별하는 이름을 입력합니다.
- b) **BGP ASN** 필드에 위협 방어 디바이스의 BGP ASN(자율 시스템 번호)을 입력합니다.  
범위는 1~2,147,483,647입니다. 이 예에서 ASN은 65000입니다. 이 ASN은 Management Center에서 BGP 라우팅을 구성할 때 필요합니다.
- c) **IP address**(IP 주소) 필드에 Threat Defense 디바이스 외부 인터페이스의 IP 주소를 입력합니다.  
IP 주소는 고정이어야 합니다. 고객 게이트웨이 디바이스가 NAT 디바이스 뒤에 있는 경우 NAT 디바이스의 IP 주소를 사용합니다.
- d) (선택 사항) **Certificate ARN**(인증서 ARN) 필드에 위협 방어 디바이스에 대한 AWS Certificate Manager(ACM) 프라이빗 인증서의 Amazon 리소스 이름(ARN)을 제공하여 인증서 기반 인증을 활성화합니다.
- e) (선택 사항) **Device**(디바이스) 필드에 Threat Defense 디바이스의 이름을 입력합니다.
- f) **Create customer gateway**(고객 게이트웨이 생성)를 클릭합니다.

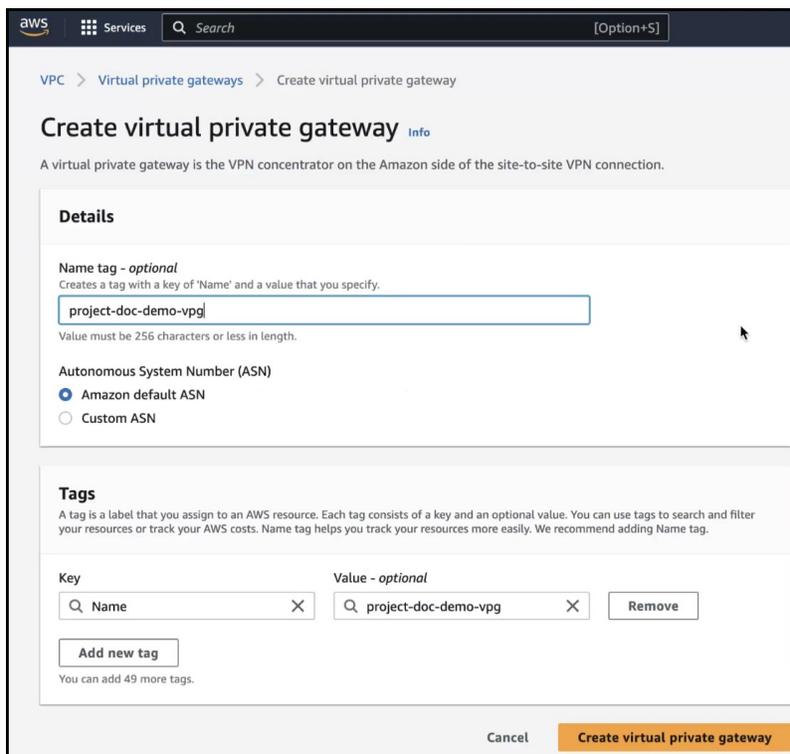
# AWS에서 가상 프라이빗 게이트웨이 생성

프로시저

단계 1 왼쪽 창에서 **Virtual private network (VPN)**(VPN(Virtual 프라이빗 네트워크))을 확장합니다.

단계 2 **Create Virtual Private Gateway**(가상 프라이빗 게이트웨이 생성)를 클릭합니다.

단계 3 **Create Virtual Private Gateway**(가상 프라이빗 게이트웨이 생성) 대화 상자에서 다음 매개변수를 구성합니다.



- a) **Name tag**(이름 태그) 필드에 가상 프라이빗 라우터의 이름을 입력합니다.
- b) **Amazon default ASN**(Amazon 기본 ASN) 또는 **Custom ASN**(맞춤형 ASN) 라디오 버튼을 클릭합니다.  
Amazon ASN은 64512입니다.
- c) **Tags**(태그)의 경우, 기본적으로 이름이 태그로 지정됩니다.
- d) **Create Virtual Private Gateway**(가상 프라이빗 게이트웨이 생성)를 클릭합니다.

## 가상 프라이빗 클라우드에 가상 프라이빗 게이트웨이 연결

가상 프라이빗 게이트웨이를 생성한 후에는 VPC에 연결해야 합니다.

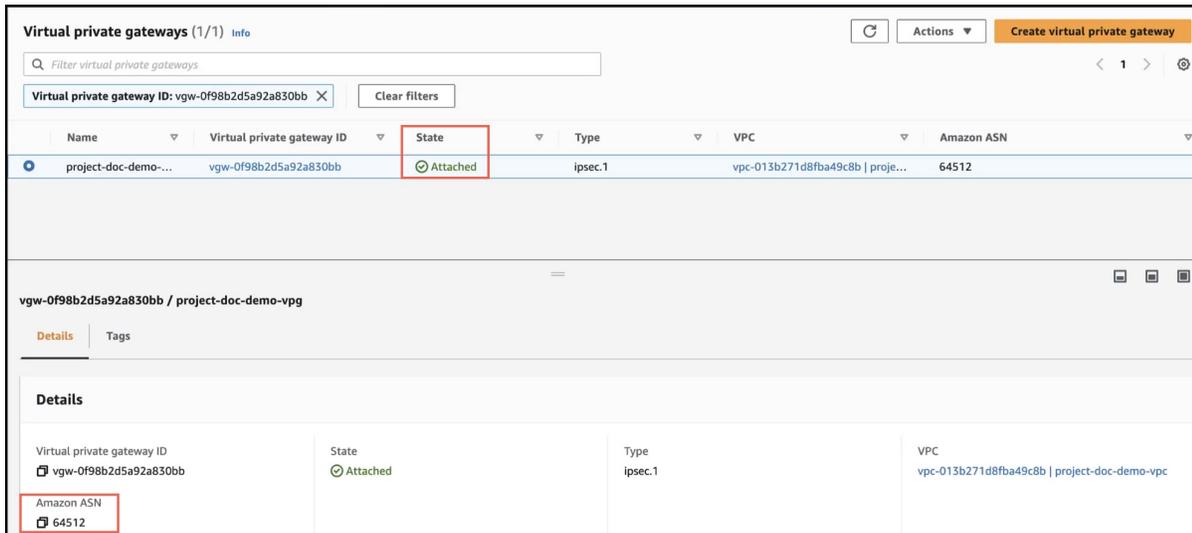
단계 1 생성한 가상 프라이빗 게이트웨이를 선택 합니다.

단계 2 **Action**(작업) 드롭다운 목록에서 **Attach to VPC**(VPC에 연결)를 선택합니다.

단계 3 **Attach to VPC**(VPC에 연결) 대화 상자에서 **Available VPCs**(사용 가능한 VPC) 드롭다운 목록에서 VPC를 선택합니다.

단계 4 **Attach to VPC**(VPC에 연결)를 클릭합니다.

단계 5 가상 프라이빗 게이트웨이의 **State**(상태)가 **Attached**(연결됨)상태인지 확인합니다.



## AWS에서 VPN 연결 생성

시작하기 전에

VPC, 고객 게이트웨이 및 가상 프라이빗 게이트웨이가 있는지 확인합니다.

단계 1 왼쪽 창에서 **Virtual private network (VPN)**(VPN(Virtual 프라이빗 네트워크))을 확장합니다.

단계 2 **Site-to-Site VPN connections**(사이트 간 VPN 연결)을 클릭합니다.

단계 3 **Create VPN Connection**(VPN 연결 생성)을 클릭합니다.

단계 4 **Create VPN connection**(VPN 연결 생성) 대화 상자에서 다음 VPN 매개변수를 구성합니다.

VPC > VPN connections > Create VPN connection

## Create VPN connection [Info](#)

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

project-doc-demo-vpn

Value must be 256 characters or less in length.

**Target gateway type [Info](#)**

Virtual private gateway  
 Transit gateway  
 Not associated

**Virtual private gateway**

vgw-0f98b2d5a92a830bb / project-doc-demo-vpg

**Customer gateway [Info](#)**

Existing  
 New

**Customer gateway ID**

cgw-0c016b07c5cbd7cfa / FTD-doc-demo

**Routing options [Info](#)**

Dynamic (requires BGP)  
 Static

**Local IPv4 network CIDR - optional**  
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

0.0.0.0/0

**Remote IPv4 network CIDR - optional**  
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

0.0.0.0/0

- Name tag**(이름 태그) 필드에 VPN 연결의 이름을 입력합니다.
- Target gateway type**(대상 게이트웨이 유형)에 대해 **Virtual private gateway**(가상 프라이빗 게이트웨이) 라디오 버튼을 클릭합니다.
- Virtual Private Gateway**(가상 프라이빗 게이트웨이) 드롭다운 목록에서 가상 프라이빗 게이트웨이를 선택합니다.
- Customer gateway**(고객 게이트웨이)에 대해 **Existing**(기존) 라디오 버튼을 클릭하고 **Customer gateway ID** 드롭다운 목록에서 고객 게이트웨이를 선택합니다.
- Routing options**(라우팅 옵션)에서 **Dynamic (requires BGP)**(동적(BGP 필요)) 라디오 버튼을 클릭합니다.
- (선택 사항) **Local IPv4 네트워크 CIDR**(로컬 IPv4 네트워크 CIDR)에 Threat Defense 디바이스의 보호되는 네트워크 IP 주소를 입력하거나 기본값인 0.0.0.0/0을 사용합니다.
- (선택 사항) **Remote IPv4 network CIDR**(원격 IPv4 네트워크 CIDR)에 AWS 측 네트워크의 IP 주소를 입력하거나 기본값인 0.0.0.0/0을 사용합니다.
- Tunnel 1 options**(터널 1 옵션)을 확장하여 VPN 터널 매개변수를 구성합니다.

1. AWS는 터널 1의 내부 IPv4 CIDR을 위해 IPv4 주소를 생성합니다.
2. 가상 프라이빗 게이트웨이와 고객 게이트웨이 간의 인증을 위해 **Pre-shared key for tunnel 1**(터널 1의 사전 공유 키) 필드에 PSK(사전 공유 키)를 입력합니다. PSK를 지정하지 않으면 AWS는 PSK를 생성합니다.  
Management Center에서 VPN을 설정하려면 이 PSK가 필요합니다.
3. **Advanced options for tunnel 1**(터널 1의 고급 옵션)에서 **Use default options**(기본 옵션 사용) 라디오 버튼을 클릭합니다.

i) (선택 사항) **Tunnel 2 options**(터널 2 옵션)을 확장하여 백업 VPN 터널 매개변수를 구성합니다.

참고  
두 터널에 동일한 PSK를 사용하는지 확인합니다.

단계 5 **Create VPN Connection**(VPN 연결 생성)을 클릭합니다.

VPN 연결이 생성되면 **State**(상태)가 **Pending**(보류 중)에서 **Available**(사용 가능)로 변경됩니다.

a) 세부 정보를 확인하기 위해 생성한 VPN 연결을 선택합니다.

b) **Tunnel details**(터널 세부 정보) 탭을 클릭합니다.

**VPN connections (1/1) Info**

Filter VPN connections

VPN ID: vpn-0aad3c4d3d0f1b872 X Clear filters

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway
project-doc-demo-...	vpn-0aad3c4d3d0f1b872	Available	vgw-0f98b2d5a92a830bb	-	cgw-0c016b07c5cbd

vpn-0aad3c4d3d0f1b872 / project-doc-demo-vpn

Details **Tunnel details** Tags

**Tunnel state**

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details
Tunnel 1	209.165.201.28	198.51.100.8/30	-	Down	June 1, 2023, 10:52:06 (UTC+05:30)	IPSEC IS DO
Tunnel 2	203.0.113.238	192.0.2.128/30	-	Down	June 1, 2023, 10:52:55 (UTC+05:30)	IPSEC IS DO

위의 예에서 다음 세부 정보에 유의하십시오.

터널	외부(엑스트라넷) IP 주소	AWS VTI IP 주소	Threat Defense 디바이스 VTI IP 주소
터널 1	209.165.201.28	198.51.100.9/30	198.51.100.10/30
터널 2	203.0.113.238	192.0.2.129/30	192.0.2.130/30

Management Center에서 경로 기반 VPN을 구성할 때 위의 세부 정보가 필요합니다.

## Management Center에서 경로 기반 VPN 구성

시작하기 전에

AWS에서 VPN 터널의 내부 및 외부 IP 주소를 적어 둡니다.

프로시저

**단계 1** **Devices**(디바이스) > **Site To Site**(사이트 대 사이트)를 선택합니다.

단계 2 + **Site To Site VPN**(사이트 간 VPN)을 클릭합니다.

단계 3 **Topology Name**(토폴로지 이름) 필드에 VPN 토폴로지의 이름을 입력합니다.

단계 4 **Route Based (VTI)**(경로 기반(VTI)) 라디오 버튼을 클릭합니다.

단계 5 **Point-to-Point**(포인트 간) 탭을 클릭합니다.

단계 6 **IKEv2** 체크 박스를 선택합니다.

단계 7 **Endpoint**(엔드포인트) 탭을 클릭합니다.

단계 8 **Node A**(노드 A)의 경우 다음과 같은 매개변수를 구성합니다.

a) **Device**(디바이스) 드롭다운 목록에서 위협 방어 디바이스를 선택합니다.

b) **Virtual Tunnel Interface**(가상 터널 인터페이스) 드롭다운 목록에서 위협 방어 디바이스의 SVTI(정적 가상 터널 인터페이스)를 선택하거나 +를 클릭하여 SVTI를 생성합니다.

SVTI 만들기에 대한 자세한 내용은 [Management Center](#)에서 위협 방어 디바이스에 대한 정적 VTI 생성, 19 페이지의 내용을 참조하십시오.

c) (선택 사항) + **Add Backup VTI**(백업 VTI 추가)를 클릭하여 백업 VTI를 구성하고 필요한 매개변수를 구성합니다.

**Tunnel Source**(터널 소스)는 두 VTI 터널에서 모두 동일합니다. 이 예에서 백업 VTI IP 주소는 192.0.2.130/30입니다. [AWS에서 VPN 연결 생성, 12 페이지](#)의 IP 주소 테이블을 참조하십시오.

단계 9 **Node B**(노드 B)의 경우 다음과 같은 매개변수를 구성합니다.

a) **Device**(디바이스) 드롭다운 목록에서 **Extranet**(엑스트라넷)을 선택합니다.

b) **Device Name**(디바이스 이름)에 엑스트라넷 디바이스 이름을 입력합니다.

c) **Endpoint IP Address**(엔드포인트 IP 주소) 필드에 AWS VPN의 IP 주소를 입력합니다.

이 예에서 IP 주소는 209.165.201.28 및 203.0.113.238입니다.

Create New VPN Topology ?

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

<p style="text-align: center;">Node A</p> <p>Device:*  <input type="text" value="branch1-ftd.xyz.com"/></p> <p>Virtual Tunnel Interface:*  <input type="text" value="outside-isp1_static_vti_2 (IP: )"/> +</p> <p><i>Tunnel Source: outside-isp1 (IP: 209.165.202.130) Edit VTI</i></p> <p><input type="checkbox"/> Tunnel Source IP is Private</p> <p><input type="checkbox"/> Send Local Identity to Peers</p> <hr style="border-top: 1px dashed #ccc;"/> <p>Backup VTI: <span style="float: right;">Remove</span></p> <p>Virtual Tunnel Interface:*  <input type="text" value="outside-isp1_static_vti_3 (IP: )"/> +</p> <p><i>Tunnel Source: outside-isp1 (IP: 209.165.202.130) Edit VTI</i></p>	<p style="text-align: center;">Node B</p> <p>Device:*  <input style="border: 2px solid red;" type="text" value="Extranet"/></p> <p>Device Name*:  <input type="text" value="AWS-Doc-Demo"/></p> <p>Endpoint IP Address*:  <input style="border: 2px solid red;" type="text" value="209.165.201.28, 203.0.113.238"/></p>
--	---

단계 10 IKE 탭을 클릭하여 다음 매개변수를 구성합니다.

- a) **IKEv2 Settings**(IKEv2 설정)의 경우 **Policies**(정책) 옆에 있는 편집 아이콘을 클릭하고 드롭다운 목록에서 **AES-SHA-SHA-LATEST**를 선택합니다. 이 프로토콜은 AWS VPN의 기본 IKE 프로토콜입니다.
- b) **Authentication Type**(인증 유형) 드롭다운 목록에서 **Pre-shared Manual Key**(사전 공유 수동 키)를 선택합니다.
- c) **Key**(키) 및 **Confirm Key**(키 확인) 필드에 키를 입력합니다.

이 예시에서는 AWS VPN에서 구성한 PSK를 사용합니다.

단계 11 **IPsec** 및 **Advanced**(고급) 구성의 경우 기본값을 사용합니다.

단계 12 **Save**(저장)를 클릭합니다.

**Site-to-Site VPN Summary**(사이트 간 VPN 요약) 페이지(**Devices**(디바이스) > **Site-to-site VPN**(사이트 간 VPN))에서 토폴로지를 확인할 수 있습니다. 모든 디바이스에 구성을 구축한 후 이 페이지에서 모든 터널의 상태를 확인할 수 있습니다.

## Management Center에서 위협 방어 디바이스에 대한 정적 VTI 생성

시작하기 전에

Management Center에서 경로 기반 VPN 구성, 15 페이지에 설명된 대로 라우트 기반 지점 간 VPN 토폴로지에 대한 기본 매개변수를 구성하고, Endpoints(엔드포인트) 탭을 클릭한 다음 Device(디바이스) 드롭다운 목록에서 Threat Defense 디바이스를 Node A(노드 A)로 선택합니다.

프로시저

**Add Virtual Tunnel Interface**(가상 터널 인터페이스 추가) 대화 상자에서 다음 매개변수를 구성합니다.

The screenshot shows the 'Add Virtual Tunnel Interface' configuration window. The 'General' tab is active. Under 'Tunnel Type', 'Static' is selected. The 'Name' field contains 'outside-isp1\_static\_vti\_2'. The 'Enabled' checkbox is checked. The 'Security Zone' dropdown is empty. The 'Priority' field is set to '0'. In the 'Virtual Tunnel Interface Details' section, the 'Tunnel ID' is '2' and the 'Tunnel Source' is 'GigabitEthernet0/1 (outside-isp1)' with IP '209.165.202.130'. In the 'IPsec Tunnel Details' section, 'IPsec Tunnel Mode' is 'IPv4'. The 'IP Address' field is highlighted with a red box, showing '198.51.100.10/30' selected under the 'Configure IP' option. The 'Borrow IP (IP unnumbered)' option is also visible. At the bottom, there are 'Cancel' and 'OK' buttons.

- Name(이름) 필드에 SVTI의 이름을 입력합니다.
- 활성화 확인란을 선택합니다.
- (선택 사항) Security Zone(보안 영역) 드롭다운 목록에서 정적 VTI의 보안 영역을 선택합니다.

- d) **Priority**(우선순위) 필드에 여러 VTI 간에 트래픽을 로드 밸런싱할 우선순위를 입력합니다.  
범위는 0~65535입니다. 가장 낮은 숫자가 가장 높은 우선 순위를 가집니다.
- e) **Tunnel ID**(터널 ID) 필드에 고유한 터널 ID를 입력합니다.  
범위는 0~10413입니다.
- f) **Tunnel Source**(터널 소스) 드롭다운 목록에서 터널 소스 인터페이스를 선택합니다.
- g) **IPSec Tunnel Mode**(IPSec 터널 모드)에서 **IPv4** 라디오 버튼을 클릭하여 IPsec 터널에 대한 트래픽 유형을 지정합니다.
- h) **Configure IP**(IP 구성) 필드에 SVTI의 IP 주소를 입력합니다.  
이 예에서 SVTI IP 주소는 198.51.100.10/30입니다. [AWS에서 VPN 연결 생성, 12 페이지](#)의 IP 주소 테이블을 참조하십시오.
- i) **OK**(확인)를 클릭합니다.

## Management Center에서 라우팅 정책 구성

### Management Center에서 언더레이 라우팅 정책 구성

AWS를 오고가는 트래픽을 활성화하려면 언더레이 라우팅 정책을 구성해야 합니다. 정적 경로 또는 동적 라우팅 프로토콜을 설정할 수 있습니다. 이 예시에서는 정적 경로를 사용합니다.

프로시저

- 
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.
  - 단계 2 편집할 인터페이스 옆에 있는 편집 아이콘을 클릭합니다.
  - 단계 3 라우팅 탭을 클릭합니다.
  - 단계 4 왼쪽 창에서 **Static Route**(정적 경로)를 클릭하여 정적 경로를 구성합니다.
  - 단계 5 **+Add Route**(경로 추가)를 클릭합니다.
  - 단계 6 **Add Static Route Configuration**(정적 경로 구성 추가) 대화 상자에서 다음 매개변수를 구성합니다.
    - a) **IPv4** 라디오 버튼을 클릭합니다.
    - b) **Interface**(인터페이스) 드롭다운 목록에서 **Threat Defense** 디바이스의 외부 인터페이스를 선택합니다.
    - c) **Available Network**(사용 가능한 네트워크)에서 **+**를 클릭하여 AWS 네트워크에 대한 네트워크 개체를 생성합니다.
    - d) **New Network Object**(새 네트워크 개체) 대화 상자에서 다음 매개변수를 구성합니다.

1. **Name**(이름) 필드에 AWS 네트워크의 이름을 입력합니다.
  2. **Host**(호스트) 라디오 버튼을 클릭하고 AWS 네트워크의 IP 주소를 입력합니다.  
이 예에서 AWS 네트워크의 IP 주소는 209.165.201.28입니다.
  3. **Save**(저장)를 클릭합니다.
- e) 6c단계부터 6d단계까지 반복하여 백업 AWS 네트워크의 네트워크 개체를 생성합니다.  
이 예에서 백업 AWS 네트워크의 IP 주소는 203.0.113.238입니다.
- f) **Available Network**(사용 가능한 네트워크) 목록에서 AWS 네트워크 및 백업 AWS 네트워크를 선택하고 **Add**(추가)를 클릭하여 **Selected Network**(선택한 네트워크) 목록으로 이동합니다.

- g) **Gateway**(게이트웨이) 필드에 Threat Defense 디바이스 게이트웨이의 IP 주소를 입력합니다.
- h) **OK**(확인)를 클릭합니다.

## Management Center에서 오버레이 라우팅 정책 구성

VPN 트래픽에 대한 오버레이 라우팅 정책을 구성해야 합니다. 이 예시에서는 BGP 라우팅 정책을 구성합니다.

프로시저

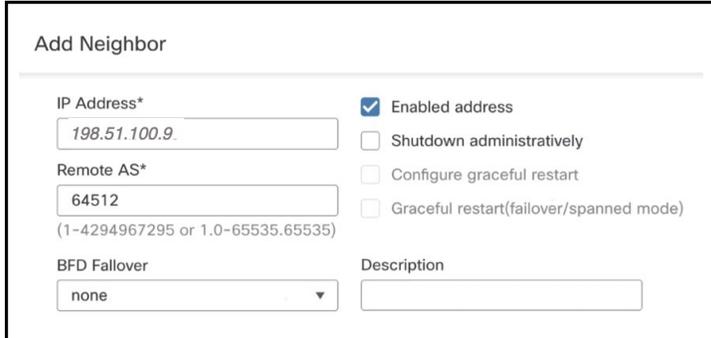
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.
- 단계 2 편집할 인터페이스 옆에 있는 편집 아이콘을 클릭합니다.
- 단계 3 라우팅 탭을 클릭합니다.
- 단계 4 왼쪽 창에서 **General Settings**(일반 설정) 아래의 **BGP**를 클릭합니다.
- 단계 5 **Enable BGP**(BGP 활성화) 체크 박스를 선택합니다.
- 단계 6 AWS 고객 게이트웨이에 대해 구성한 Threat Defense 디바이스의 AS 번호를 **AS Number**(AS 번호) 필드에 입력합니다.  
이 예에서는 65000입니다.
- 단계 7 **Save**(저장)를 클릭합니다.

단계 8 왼쪽 창에서 **BGP > IPv4**를 선택합니다.

단계 9 **Enable IPv4(IPv4 활성화)** 확인란을 선택합니다.

단계 10 **Neighbor(인접한 라우터)** 탭을 선택하고 **+Add(추가)**를 클릭합니다.

단계 11 **Add Neighbor(인접한 라우터 추가)** 대화 상자에서 다음 매개변수를 구성합니다.



a) **IP Address(IP 주소)** 필드에 AWS VPN 구성의 AWS VTI IP 주소(Tunnel1)를 입력합니다.

이 예에서 AWS IP 주소는 198.51.100.9입니다.

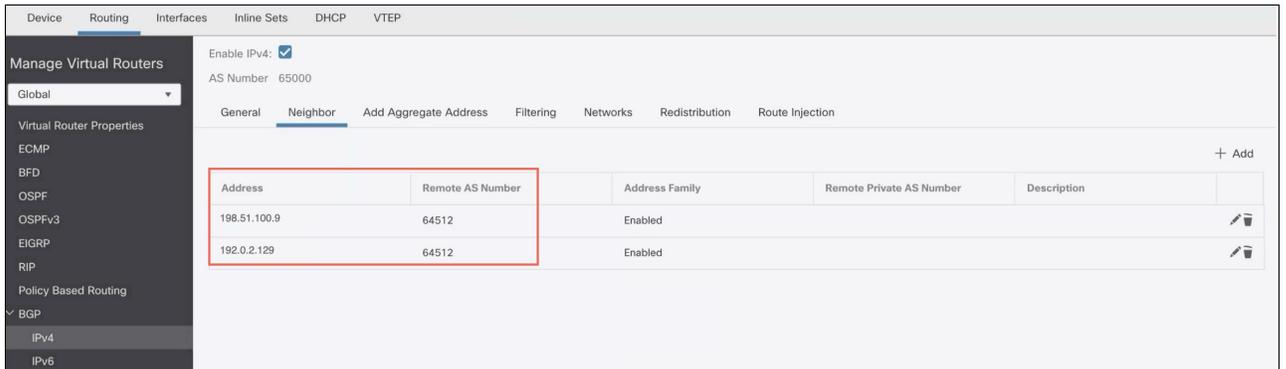
b) AWS VPN 구성의 AWS AS 번호를 **Remote AS(원격 AS)** 필드에 입력합니다.

이 예에서 AWS AS 번호는 64512입니다.

c) **OK(확인)**를 클릭합니다.

단계 12 11a~11c 단계를 반복하여 백업 AWS IP 주소(Tunnel2)를 인접한 라우터로 추가합니다.

이 예에서 IP 주소는 192.0.2.129이고 AWS AS 번호는 64512입니다.



Address	Remote AS Number	Address Family	Remote Private AS Number	Description
198.51.100.9	64512	Enabled		
192.0.2.129	64512	Enabled		

단계 13 **Save(저장)**를 클릭합니다.

## VTI 터널 상태 및 구성 확인

Threat Defense 디바이스에서 구성을 구축한 후 디바이스, Management Center 및 AWS에서 VTI 터널 구성 및 상태를 확인할 수 있습니다.

## AWS의 터널 상태 확인

AWS에서 VPN 터널을 확인하려면 다음을 수행합니다.

1. **Virtual private network (VPN)**(VPN(Virtual Private Network) > **Site-to-Site VPN connections**(사이트 간 VPN 연결)를 선택합니다.
2. VPN 옆의 라디오 버튼을 클릭합니다.
3. **Tunnel details**(터널 세부 정보) 탭을 클릭합니다. 터널의 **Status**(상태) 는 **Up**(작동)이어야 합니다.

The screenshot shows the AWS VPN connections console. At the top, there's a search bar and a filter for 'VPN ID: vpn-0aad3c4d3d0f1b872'. Below that is a table of VPN connections. The first connection is 'project-doc-demo-...' with VPN ID 'vpn-0aad3c4d3d0f1b872' and State 'Available'. Below the table, the 'Tunnel details' tab is selected, showing a table of tunnel states. Two tunnels are listed: Tunnel 1 and Tunnel 2, both with a status of 'Up'.

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway ID
project-doc-demo-...	vpn-0aad3c4d3d0f1b872	Available	vgw-0f98b2d5a92a830bb	-	cgw-0c016b07c5cbd7cfa	123.63...

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate
Tunnel 1	209.165.201.28	198.51.100.8/30	-	Up	June 1, 2023, 11:18:30 (UTC+05:30)	0 BGP ROUTES	-
Tunnel 2	203.0.113.238	192.0.2.128/30	-	Up	June 1, 2023, 11:31:09 (UTC+05:30)	0 BGP ROUTES	-

## Threat Defense 디바이스의 터널 및 라우팅 구성 확인

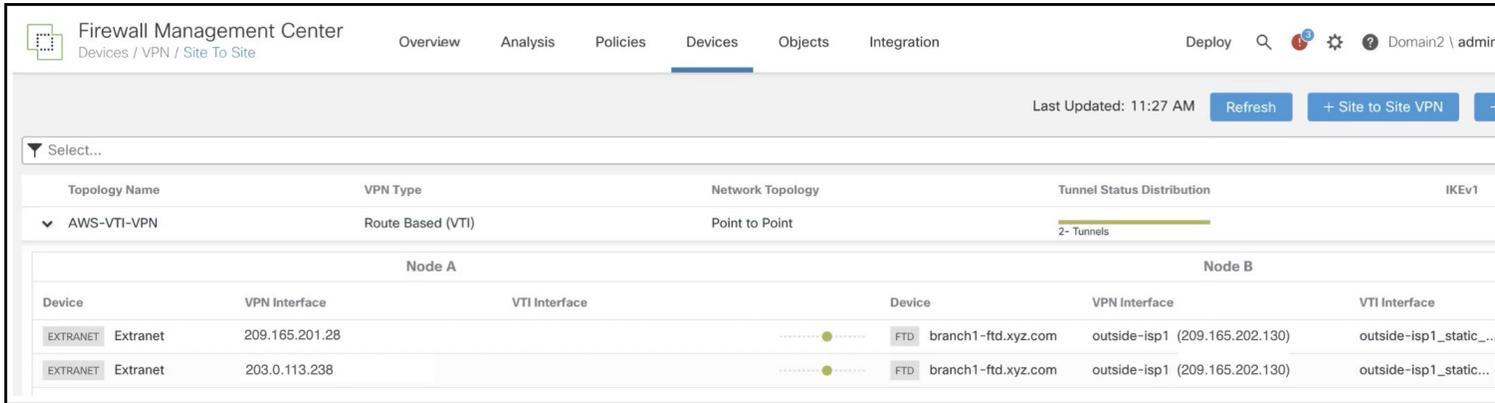
- Threat Defense 디바이스의 인터페이스 구성을 확인하려면 **show running-config interface** 명령을 사용합니다.

```
interface Tunnel2
 nameif outside-isp1 static_vti_2
 ip address 198.51.100.10 255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 209.165.201.28
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
!
interface Tunnel3
 nameif outside-isp1 static_vti_3
 ip address 192.0.2.130 255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 203.0.113.238
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
!
```

- Threat Defense 디바이스의 BGP 구성을 확인하려면 **show bgp** 명령을 사용합니다.

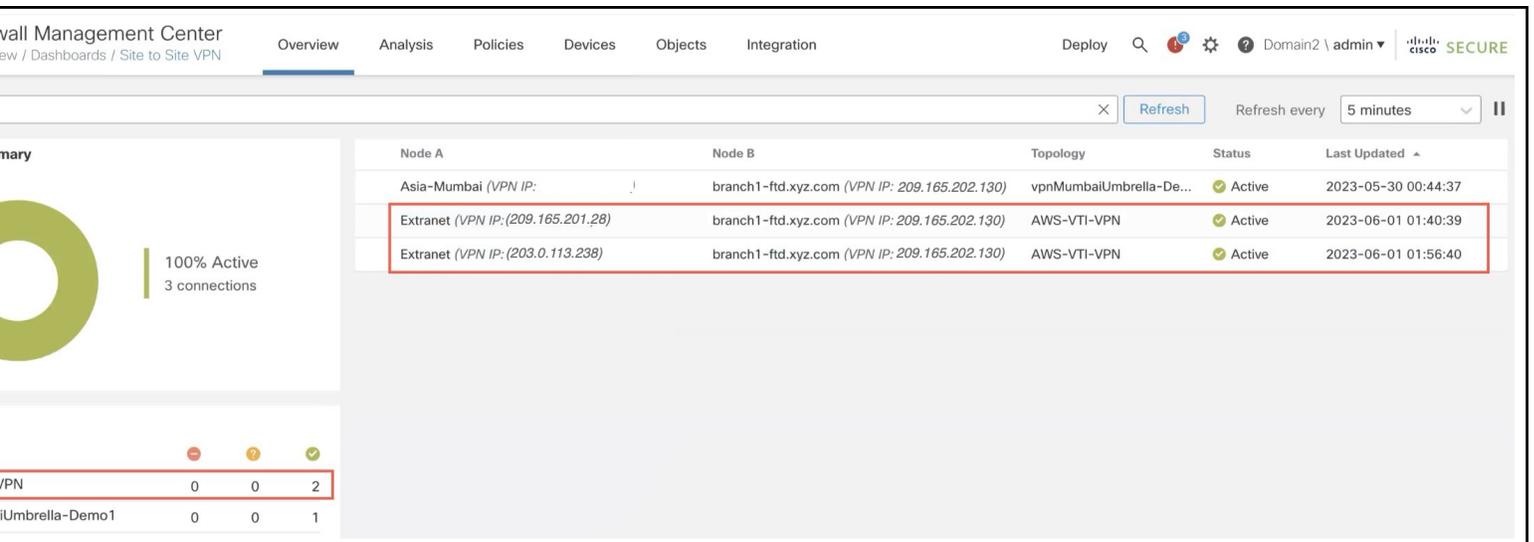
사이트 간 VPN 요약 페이지의 터널 상태 확인

VPN 터널의 상태를 확인하려면 **Device**(디바이스) → **VPN > Site To Site**(사이트 간)를 선택합니다.



사이트 간 VPN 대시보드의 터널 상태 확인

VPN 터널의 세부 정보를 보려면 **Overview**(개요) > **Dashboards**(대시보드) > **Site to Site VPN**(사이트 간 VPN)을 선택합니다.



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. 모든 권리 보유.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

**Asia Pacific Headquarters**  
CiscoSystems(USA)Pte.Ltd.  
Singapore

**Europe Headquarters**  
CiscoSystemsInternationalBV  
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.