

보안 방화벽에서 Azure Dual ISP vWAN 연결 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[다이어그램](#)

[듀얼 DIA\(Direct Internet Access\) 링크\(Azure + FTD 로드 밸런싱/이중화\)](#)

[구성](#)

[1단계: Azure vWAN VPN 사이트 구성](#)

[1단계: Azure vWAN VPN 사이트 만들기\(원격 FTD 장치\)](#)

[2단계: Azure APIPA 게이트웨이 매개 변수 구성](#)

[3단계: Azure vWAN Site VPN 매개변수 구성](#)

[4단계: VPN 사이트 링크 인스턴스에서 사용자 지정 BGP APIPA 활성화 및 활성화](#)

[5단계: VPN 사이트 구성 파일 다운로드](#)

[2단계: Azure vWAN에 대한 듀얼 ISP 연결을 위한 FTD 구성](#)

[1단계: 다운로드한 VPN 컨피그레이션 분석](#)

[2단계: 링크 BGP 업데이트 소스 루프백 인터페이스 구성](#)

[3단계: 1단계/2단계 정책 개체 구성](#)

[4단계: VTI\(Virtual Tunnel Interface\) 구성](#)

[5단계: IPsec VPN 토폴로지 프로비저닝](#)

[6단계: VPN 토폴로지 검증](#)

[7단계: ECMP 구성](#)

[8단계: BGP 구성](#)

[9단계: eBGP 다중 경로 구성](#)

[확인/문제 해결](#)

소개

이 문서에서는 듀얼 WAN 링크를 사용하여 Microsoft Azure vWAN(Virtual WAN) Site-to-Site VPN Connectivity to Secure Firewall을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Microsoft vWAN(Azure Virtual WAN)
- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Secure Firewall Threat Defense)

이러한 구성 요소가 Azure 환경에서 초기에 구성되었는지 확인합니다.

- Microsoft Azure vWAN 인스턴스
- Microsoft Azure vWAN 허브

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure FTD 버전 10.0
- Cisco Secure FMC 버전 10.0
- Microsoft Azure vWAN

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

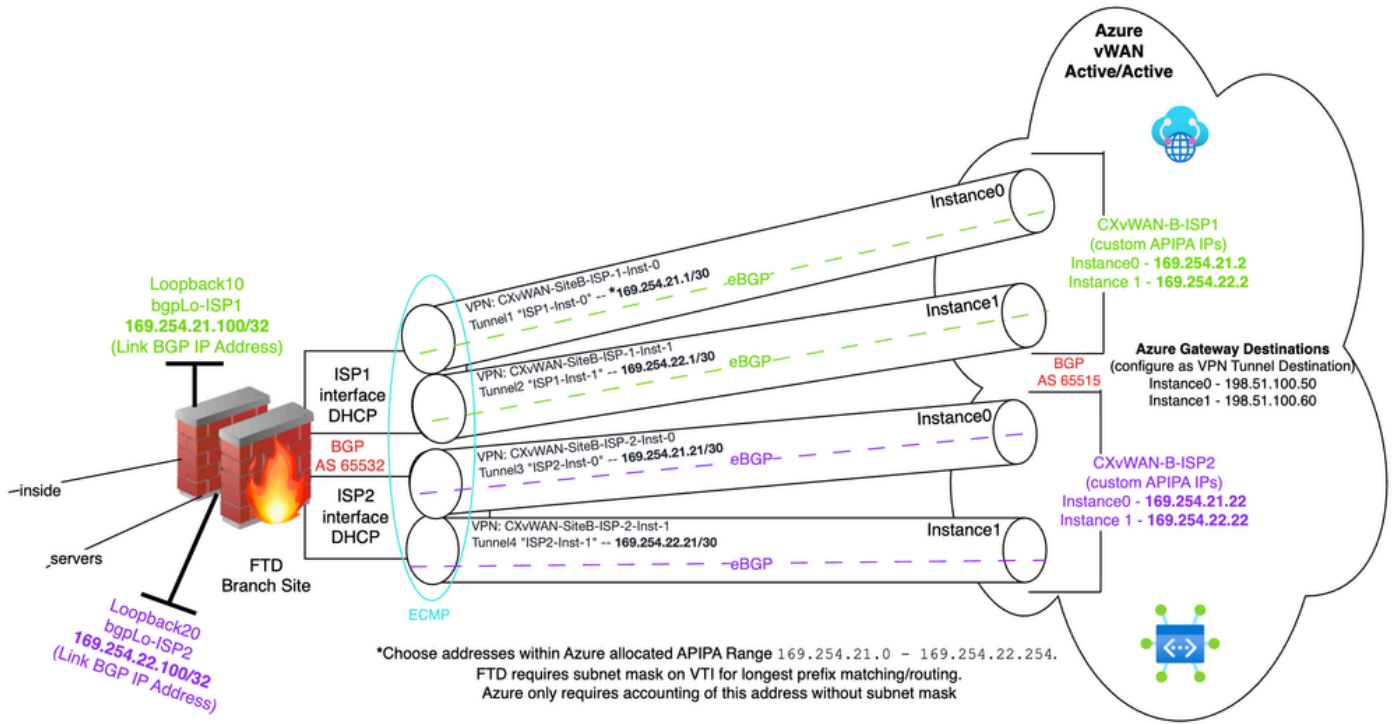
브랜치 FTD에 2개의 ISP(Internet Service Provider) 대면 외부 인터페이스가 있는 경우 각 인터페이스는 Azure vWAN에 중복적으로 능동적으로 연결할 수 있으므로 각 ISP 링크가 사용됩니다. Azure vWAN은 사이트 링크당 IPsec 터널 2개(Azure 허브 Instance0에 1개, Instance1에 1개)를 생성하여 각 ISP 인터페이스가 2개의 터널을 종료합니다. 두 ISP 링크 모두에서 이로 인해 FTD에서 4개의 IPsec 터널이 종료됩니다.

Azure 인스턴스는 로드 밸런싱 및 이중화를 위해 액티브/액티브 모드에서 작동하므로 FTD는 네 개의 모든 IPsec 터널에 ECMP(Equal-Cost Multi-Pathing) 구성을 통해 이를 반영합니다. 사용자 지정 APIPA(Automatic Private IP Addressing) 주소를 사용하여 4개의 터널 각각에 대해 고유한 ASN(Private Autonomous System Number)을 가진 eBGP(External Border Gateway Protocol) 인접 디바이스가 설정됩니다. 이를 통해 BGP 다중 경로 기능을 활성화하여 인스턴스의 각 Azure 허브 사이트 링크 쌍에 대한 다중 중복 경로를 제공합니다.

다이어그램

다이어그램은 이 문서에서 설명한 구성의 토폴로지를 보여줍니다. 듀얼 DIA(Direct Internet Access) 링크 변형 원본은 FTD의 두 외부 인터페이스에서 생성되는 두 Azure 터널입니다.

듀얼 DIA(Direct Internet Access) 링크(Azure + FTD 로드 밸런싱/이중화)



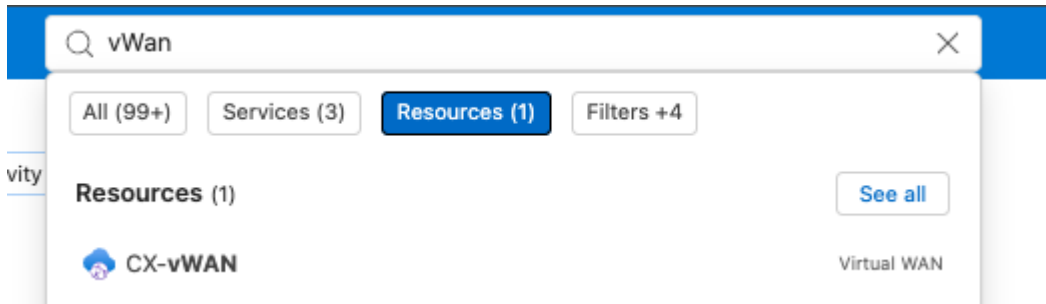
이중 직접 인터넷 액세스 연결 토폴로지

구성

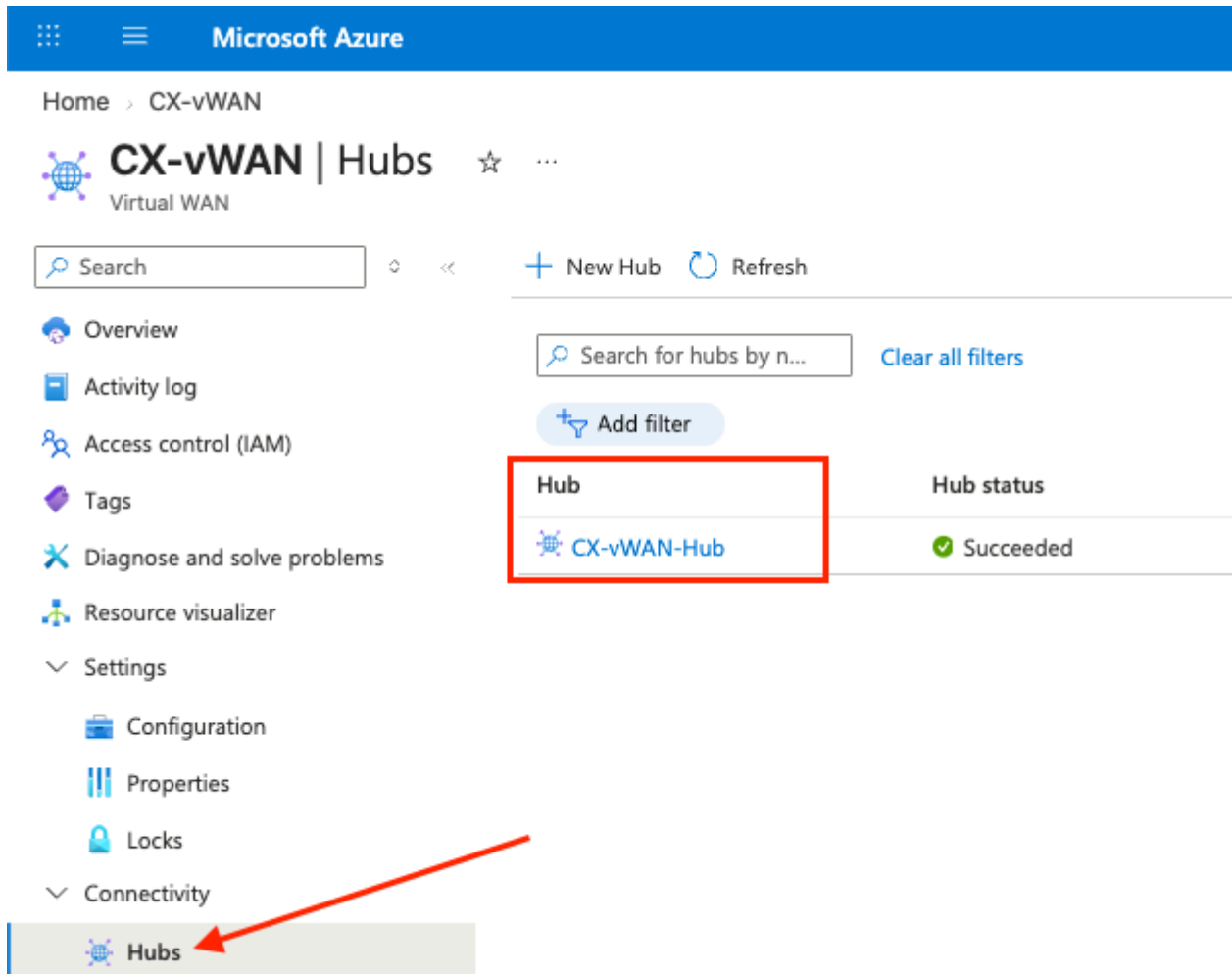
1단계: Azure vWAN VPN 사이트 구성

1단계: Azure vWAN VPN 사이트 만들기(원격 FTD 장치)

1) Azure 검색 필드에서 vWAN을 검색하려면 Virtual WANs를 클릭하여 기존 Azure vWAN 허브에 입력합니다. 그런 다음 Connectivity(연결) > Hubs(허브)로 이동하고 기존 Azure vWAN 허브를 클릭합니다.



가상 WAN에 대한 검색 쿼리



기존 가상 WAN 허브 선택

2) Connectivity(연결) > VPN(Site to Site)(VPN(사이트 대 사이트))을 클릭하고 + Create new VPN site(새 VPN 사이트 생성)를 클릭합니다.

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

Site name	Location	Cloud
No results		

새 가상 WAN 사이트 생성



참고: 이미지의 여러 필드에 있는 값을 다루는 공백은 이 문서를 게시하기 위한 의도적인 것입니다.

3) 필수 필드에 값을 입력 합니다. 완료되면 다음을 클릭합니다. 링크 > 앞으로 이동합니다.

Create VPN site ...

Basics Links Review + create

Project details

Subscription

Resource group *

Instance details

Region *

Name *

Dual-ISP-Site

Device vendor *

Cisco

Private address space

At least one address space is required if BGP isn't configured. To configure BGP, please go to Links tab.

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Links >

일반 VPN 사이트 구성 설정

4) 필수 링크 정보를 입력합니다. Link BGP Address(링크 BGP 주소) 및 Link ASN은 사이트 대 사이트 터널을 통해 인접 관계가 형성되는 브랜치 측의 내부 터널 BGP Layer 3 대상 주소 및 BGP AS 번호입니다. 링크 BGP 주소는 구성된 허브 전용 주소 공간 서브넷 외부에 있는 겹치지 않는 서브넷 주소(/32)입니다. Azure는 BGP 인접 디바이스로 연결하기 위해 /32 경로로 설치합니다. FTD의 이후 섹션에서 2개의 루프백 인터페이스가 생성되어 각 듀얼 사이트 링크의 링크 BGP 주소를 나타냅니다. 링크 IP 주소/FQDN(정규화된 도메인 이름)은 IPsec(IP 보안)/IKEv2(인터넷 키 교환 버전 2) 연결을 프로비전하는 데 필요한 지점 사이트로 이동하는 트래픽의 외부 헤더 레이어 3 대상 IP 주소입니다. 다음을 클릭하여 완료하면 다음 단계로 진행하십시오. 검토 + 생성 >.



참고: 터널 주소에 169.254.21.0~169.254.22.255 범위의 주소를 사용하는 경우 특정 Azure 설명서를 검토해야 합니다. [BGP APIPA 주소를 선택합니다.](#)

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

Link name	Link speed	Link provider name	Link IP address / FQDN	Link BGP address	Link ASN	
ISP-1-Link	1000	ISP1		169.254.21.100	65532	...
ISP-2-Link	1000	ISP2		169.254.22.100	65532	...

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Review + create >

사이트 링크 매개변수 구성

5) 원하는 대로 정보가 확인되면 Create(생성)를 클릭합니다.

Create VPN site ...

 Validation passed

- basics
- links
- Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	

Links

Link name	ISP-1-Link
Link provider name	ISP1
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.21.100

Link name	ISP-2-Link
Link provider name	ISP2
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.22.100

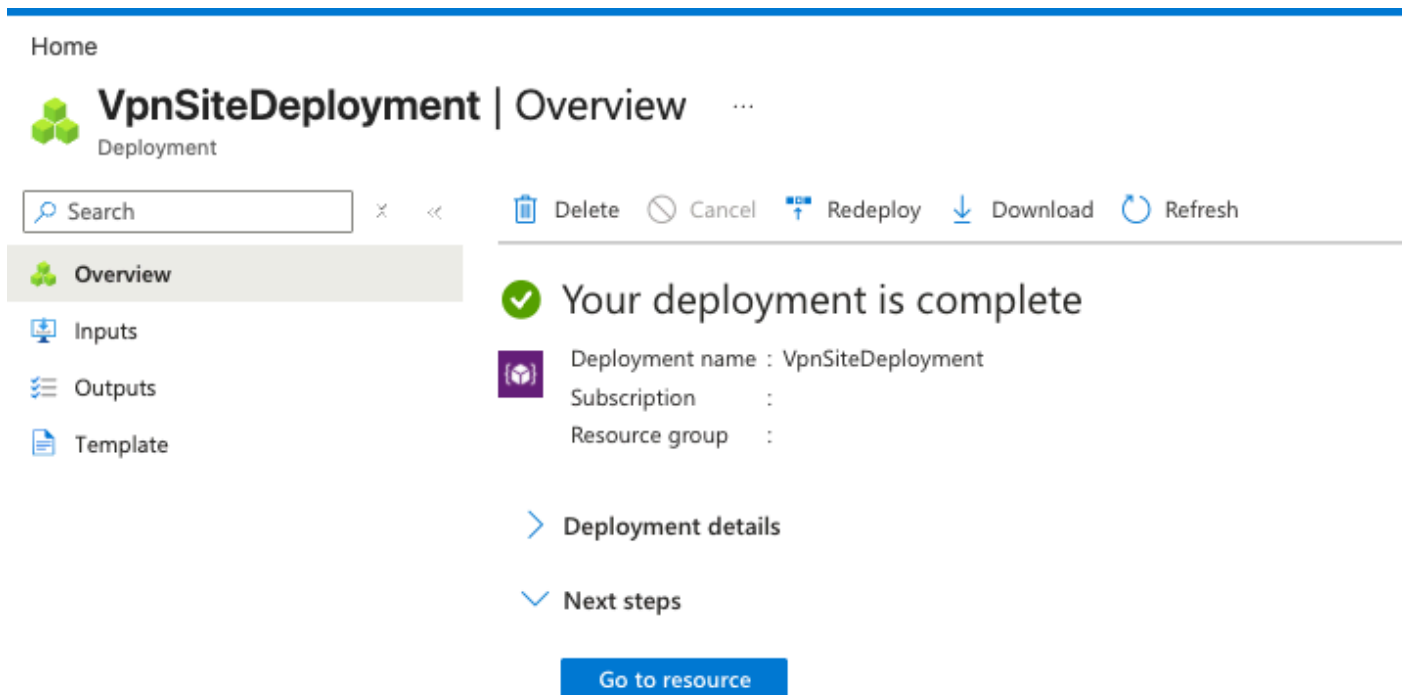
 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Create

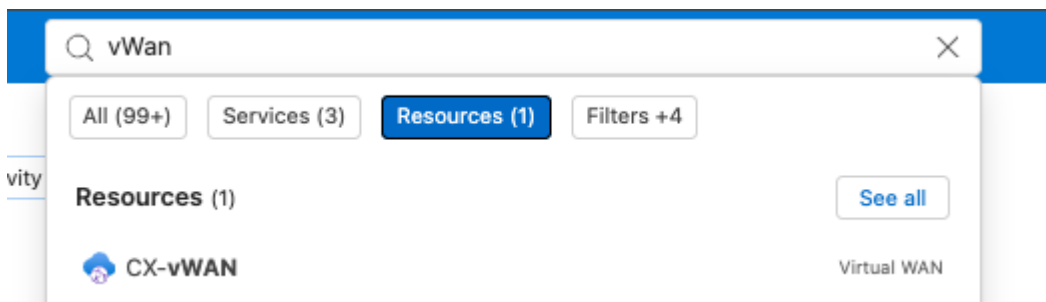
Previous

Next

6) VPN 사이트 구축이 완료되면 vWAN 허브 컨피그레이션으로 다시 이동합니다.



가상 WAN 사이트 구축 진행률



가상 WAN에 대한 검색 쿼리

2단계: Azure APIPA 게이트웨이 매개 변수 구성

Azure에서는 169.254.0.0/16 IPv4 주소 공간 내에서 APIPA(Automatic Private IP Addressing) 주소에 대한 추가 구성이 필요합니다.

1) Connectivity(연결) > Hubs(허브)를 통해 기존 허브를 입력합니다.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs

Virtual WAN Hub Connectivity(가상 WAN 허브 연결)로 이동

2) Connectivity(연결) > VPN(Site to Site)(VPN(사이트 대 사이트))으로 다시 이동하고 Gateway Configuration(게이트웨이 컨피그레이션) 하이퍼링크를 클릭합니다.

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ①

액세스 게이트웨이 구성 하이퍼링크

3) 측면 패널이 VPN Gateway를 편집하는 것으로 나타납니다. VPN Gateway Instance0 및 VPN Gateway Instance1에서 IPsec 터널을 통해 BGP 네이버에 대해 각 인스턴스의 네이버 IP로 작동하는 고유한 사용자 지정 BGP IP 주소 2개를 입력합니다. 이 토폴로지 내에서 APIPA 주소 지정을 사용하도록 선택한 경우 이 작업이 필요합니다. Peer Address(피어 주소)라는 필드에 FTD에서 Azure 인스턴스에 연결하는 데 사용할 BGP 인접 IP를 입력합니다. APIPA 주소 지정이 사용 중인 경우 Azure는 FTD와의 BGP 설정을 시도하지 않습니다. 따라서 FTD는 Azure와의 각 터널을 통해 eBGP 인접 디바이스 설정을 시도합니다.

총 링크 2개 x 암시적 터널 2개, ISP 링크당 Instance0 및 Instance1에 대한 터널 1개 Azure와 2개의 FTD ISP 인터페이스 간에 BGP 인접 관계가 있는 IPsec 터널 4개가 모두 포함됩니다.

이러한 주소는 고유해야 하며, 이 데모에서는 각 터널에 할당된 /30 서브넷의 두 번째 및 최종 호스트 주소를 FTD에서 사용하도록 구성합니다. 구성이 완료되면 Edit를 클릭합니다.



참고: 터널 주소에 169.254.21.0~169.254.22.255 범위의 주소를 사용하는 경우 특정 Azure 설명서를 검토해야 합니다. [BGP APIPA 주소 선택](#)

Edit VPN Gateway



A Site to site (VPN gateway) enables you to connect VPN sites to a hub.

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ

☒ Microsoft network ☐ Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



Updating a hub can take 30 minutes or more. [Learn more.](#)

Edit

Cancel

VPN 게이트웨이 사용자 지정 BGP IP 주소 편집



참고: Azure에서 언급했듯이, 업데이트에 최대 30분 이상이 소요될 수 있습니다.

3단계: Azure vWAN Site VPN 매개변수 구성

1) Connectivity(연결) > VPN(Site to Site) 페이지에서 Azure vWAN Hub 컨피그레이션 내의 X를 클릭하여 허브 연결을 지웁니다. 연결 해제된 VPN 사이트를 보기 위해 연결된 필터링.

The screenshot shows the Azure portal interface for a CX-vWAN-Hub. The left-hand navigation pane has 'Connectivity' and 'VPN (Site to site)' selected. The main area displays the 'VPN Sites' tab. At the top of this tab, there is a search bar and a filter bar. The filter bar shows 'Hub association : Connected' with an 'X' icon to its right. A red arrow points to this 'X' icon, indicating that clicking it will remove the filter. Below the filter bar, there is a message box that says: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

허브 연결 필터 지우기

2) 최근 프로비저닝된 VPN 사이트 옆의 확인란을 선택하고 Connect VPN Site(VPN 사이트 연결)를 클릭합니다.



CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

[Download VPN Config](#)[Packet Capture](#)[Delete gateway](#)[Reset gateway](#)

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Routing Intent and Routing Policies

BGP Peers

Route Tables

Effective Routes

Security

Azure Firewall and Firewall Manager

Third party providers

Essentials

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

VPN Sites

Metrics

[Restore previous filters](#)[Add filter](#)

VPN Sites ⓘ



Check active filters when searching for a VPN site. VPN connectivity status might take a few mi

[+ Create new VPN site](#)[Connect VPN sites](#)[Disconnect VPN sites](#)[Refresh](#)

Page:

Site name

Location

☒ Dual-ISP-Site

VPN 연결 사이트 작업

3) 원하는 PSK(Pre-Shared key)를 구성하고, Custom(사용자 지정) 토글 옵션을 클릭하여 원하는 IPsec 매개변수를 구성합니다. 이러한 IPsec 매개변수는 이후 단계에서 FMC/FTD 컨피그레이션과 일치해야 합니다. 저장하려면 연결을 클릭합니다.



참고: FTD/FMC 버전 6.7에서 DH(Diffie-Hellman) 그룹 24 지원이 제거되었습니다.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

i When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

These sites will be connected to the [CX-vWAN-Hub] hub.

Site name	↑↓	Region	↑↓
 Dual-ISP-Site		eastus	

Connect

사전 공유 키 및 IPsec 매개변수 구성

4) VPN 사이트 프로비저닝이 성공적으로 완료되었는지 확인합니다.

Notifications



[More events in the activity log →](#)

[Dismiss all](#)



Successfully created VPN connection



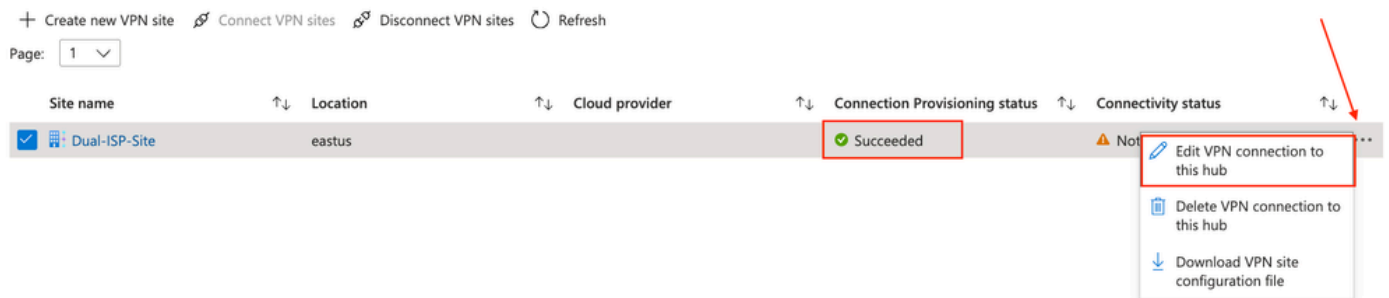
Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

VPN 사이트 프로비저닝 상태 확인

4단계: VPN 사이트 링크 인스턴스에서 사용자 지정 BGP APIPA 활성화 및 활성화

1) VPN(Site to site) 페이지를 새로 고치고 Connection Provision status(연결 프로비저닝 상태) 열이 성공적으로 표시되는지 확인합니다. 그러면 생략 부호를 클릭하여 이 허브에 대한 VPN 연결 편집 드롭다운 메뉴 항목을 클릭할 수 있습니다.



연결 성공 확인 및 VPN 연결 수정

2) ISP1(Link Connection 1)을 구성하고 해당 PSK(Pre-Shared Key)를 다시 입력한 다음 Custom BGP IP Address(맞춤형 BGP IP 주소) 옆의 Enable(활성화) 토글을 클릭하고 FTD에 의해 생성된 BGP IP 헤더의 내부 터널 대상 IP 주소 필드 값이 될 /30 서브넷의 나머지 호스트 주소를 매핑합니다.

기본적으로 Azure Instance0에 대한 ISP1 VTI Tunnel1에는 주소 할당이 169.254.21.1/30이고, FTD에서 종료되는 두 번째 ISP1 VTI Tunnel2에는 Instance1에 대해 할당된 IP가 169.254.22.1/30입니다.

다음을 클릭합니다. ISP 2 링크 매개변수로 진행하려면 Link Connection 2>를 클릭합니다.



참고: PSK를 다시 입력하고 Azure의 드롭다운 메뉴에서 정렬된 PFS 그룹 옵션을 다시 클릭해야 할 수 있습니다.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable

Disable

Connection status: NotConnected

Pre-shared key (PSK)

.....

Connection Mode

Default

Initiator Only

Responder Only

Border gateway protocol

Disable

Enable

Custom BGP IP Addresses

Disable

Enable

Custom BGP IP Address

Instance 0

169.254.21.2

Instance 1

169.254.22.2

Use Azure Private IP Address

Yes

No

Protocol

IKEv2

IKEv1

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector

Enable

Disable

IPsec

Default

Custom

SA Lifetime in seconds

27000

IKE Phase 1

Encryption

GCMAES256

Integrity/PRF

SHA384

DH Group

DHGroup14

IKE Phase 2(ipsec)

IPsec Encryption

GCMAES256

IPsec Integrity

GCMAES256

PFS Group

NONE

DPD timeout in seconds

45

Review + create

Previous

Next : Link connection 2 >

3) 이전 단계를 반복하고 Link Connection 2(ISP2 link)에서 적용 가능한 매개변수를 적용합니다. 완료되면 생성을 누릅니다.

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection **Enable** Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

Connection Mode ⓘ **Default** Initiator Only Responder Only

Border gateway protocol ⓘ Disable **Enable**

Custom BGP IP Addresses ⓘ Disable **Enable**

Custom BGP IP Address

Instance 0 ⓘ 169.254.21.22 ▾

Instance 1 ⓘ 169.254.22.22 ▾

Use Azure Private IP Address ⓘ Yes **No**

Protocol IKEv2 **IKEv1**

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ Enable **Disable**

IPsec ⓘ Default **Custom**

SA Lifetime in seconds * ⓘ 27000

IKE Phase 1 ⓘ Encryption * Integrity/PRF * DH Group *
GCMAES256 ▾ SHA384 ▾ DHGroup14 ▾

IKE Phase 2(ipsec) ⓘ IPsec Encryption * IPsec Integrity * PFS Group *
GCMAES256 ▾ GCMAES256 ▾ NONE ▾

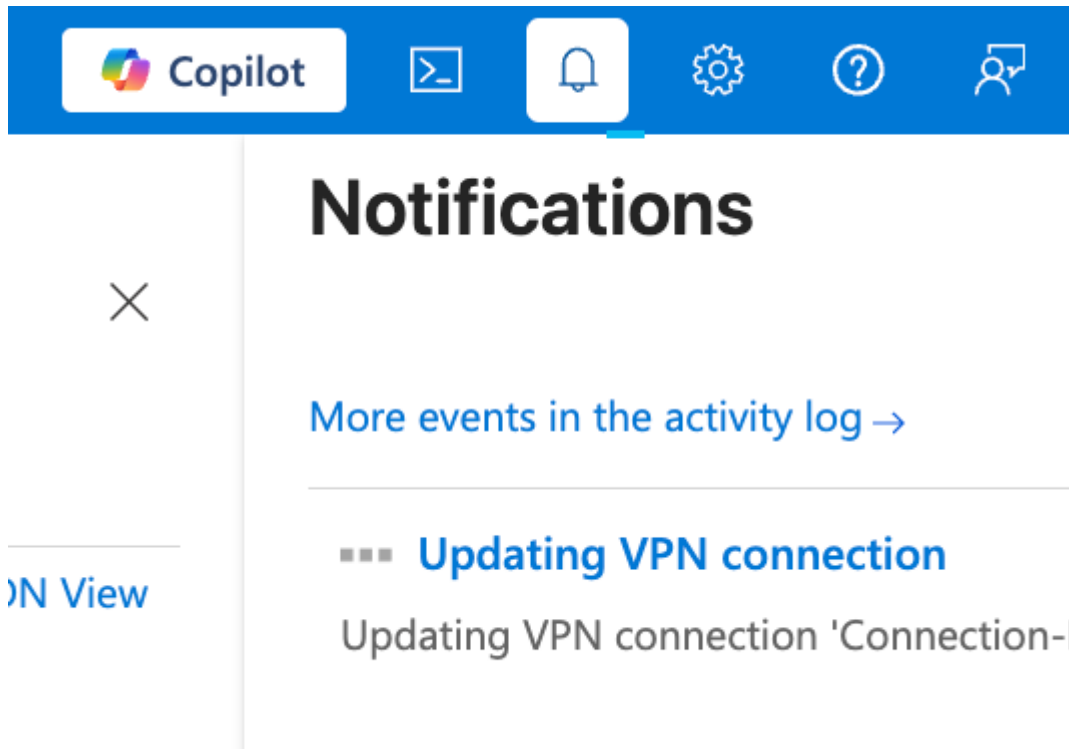
DPD timeout in seconds * ⓘ 45

Create

Previous

Next

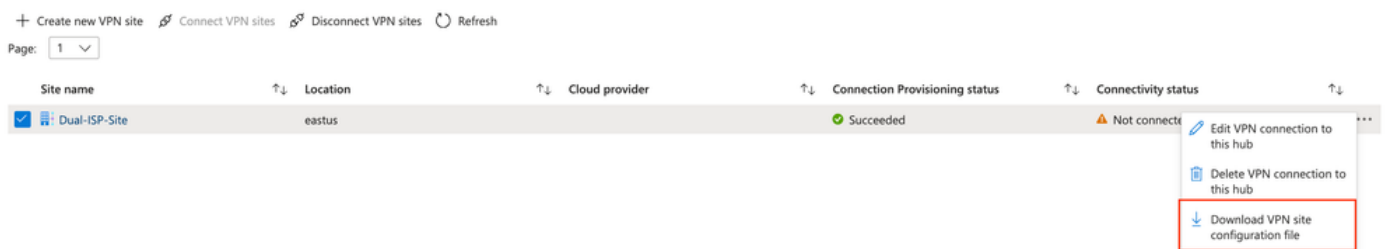
4) Azure UI의 알림은 업데이트 작업이 시작되는 것을 표시합니다.



Azure 업데이트 작업 시작 알림

5단계: VPN 사이트 구성 파일 다운로드

1) Azure의 동일한 VPN(Site to Site) 페이지에서 구성된 VPN 사이트의 맨 오른쪽에 있는 줄임표 아이콘을 선택하고 Download VPN site configuration file(VPN 사이트 구성 파일 다운로드) 옵션을 선택합니다.



VPN 사이트 구성 파일 다운로드 옵션

2) 하이퍼링크를 다운로드하려면 여기를 클릭하십시오.



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



VPN 사이트 구성 파일 다운로드

2단계: Azure vWAN에 대한 듀얼 ISP 연결을 위한 FTD 구성

1단계: 다운로드한 VPN 컨피그레이션 분석

1) 다운로드한 구성 파일을 열고 유사한 JSON(JavaScript Object Notation) 출력이 나타납니다. 출력에는 파일에 작성된 두 개체 중 하나가 표시됩니다. 이 정보는 FTD 컨피그레이션에 유용한 컨텍스트를 제공합니다.



참고: 포커스를 높이기 위해 여러 개의 관련 없는 객체와 키/값 쌍을 간결하게 정리합니다.



참고: 다운로드한 파일의 ISP-Link-1 JSON 개체 순서가 반전되었습니다. 코드 출력의 생략 부호는 해당 구성이 있는 ISP-2-Link 개체를 나타냅니다.

```
...
{
  "configurationVersion": {
    "LastUpdatedTime": "2026-09-25T20:20:26.7658453Z",
    "Version": "15221e61-4e2c-42f5-b9e4-96d674f5a9a3"
  },
  "vpnSiteConfiguration": {
    "Name": "Dual-ISP-Site",
    "IPAddress": "FTD_ISP1_WAN_IP",
    "BgpSetting": {
      "Asn": 65532,
      "BgpPeeringAddress": "169.254.21.100",
```

```

        "PeerWeight": 32768
    },
    "LinkName": "ISP-1-Link"
},
"vpnSiteConnections": [
{
    "gatewayConfiguration": {
        "IpAddresses": {
            "Instance0": "Inst0IP",
            "Instance1": "Inst1IP"
        },
        "BgpSetting": {
            "Asn": 65515,
            "CustomBgpPeeringAddresses": {
                "Instance0": [
                    "169.254.21.22",
                    "169.254.21.2"
                ],
                "Instance1": [
                    "169.254.22.22",
                    "169.254.22.2"
                ]
            }
        },
    },
    "connectionConfiguration": {
        "IsBgpEnabled": true,
        "PSK": "PSK",
        "IPsecParameters": {
            "IpsecEncryption": "GCMAES256",
            "IpsecIntegrity": "GCMAES256",
            "IkeEncryption": "GCMAES256",
            "IkeIntegrity": "SHA384",
            "PfsGroup": "None",
            "DhGroup": "DHGroup14",
            "SALifeTimeInSeconds": 27000
        }
    }
}
]
}
]

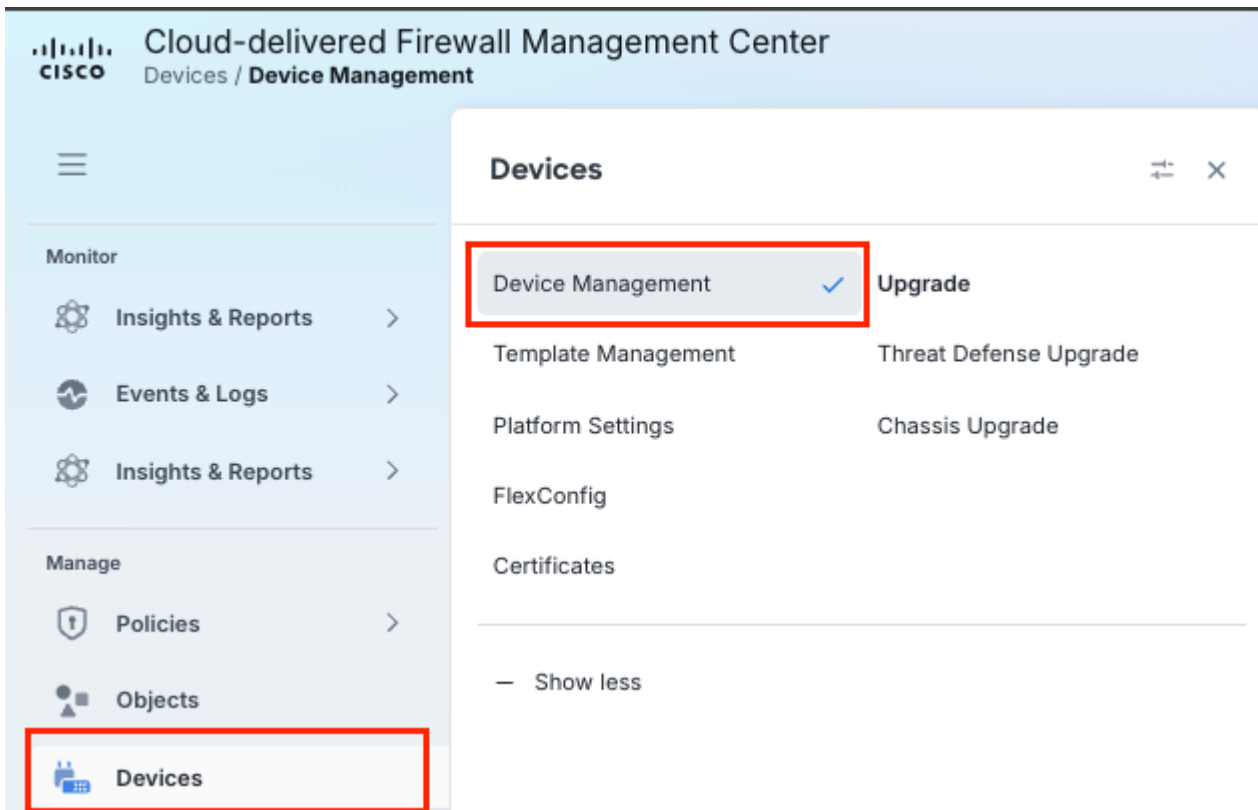
```

단계를 완료할 때 이 출력을 참조로 유지합니다.

2단계: 링크 BGP 업데이트 소스 루프백 인터페이스 구성

FTD의 이후 단계에서 구성된 FTD BGP 프로세스 아래의 BGP 네이버 컨피그레이션 항목에는 Azure Site Link 컨피그레이션의 해당 링크 BGP IP 주소를 나타내는 안정적인 소스가 필요합니다.

1) Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다.



firepower Management Center에서 Device Management(디바이스 관리)로 이동합니다.



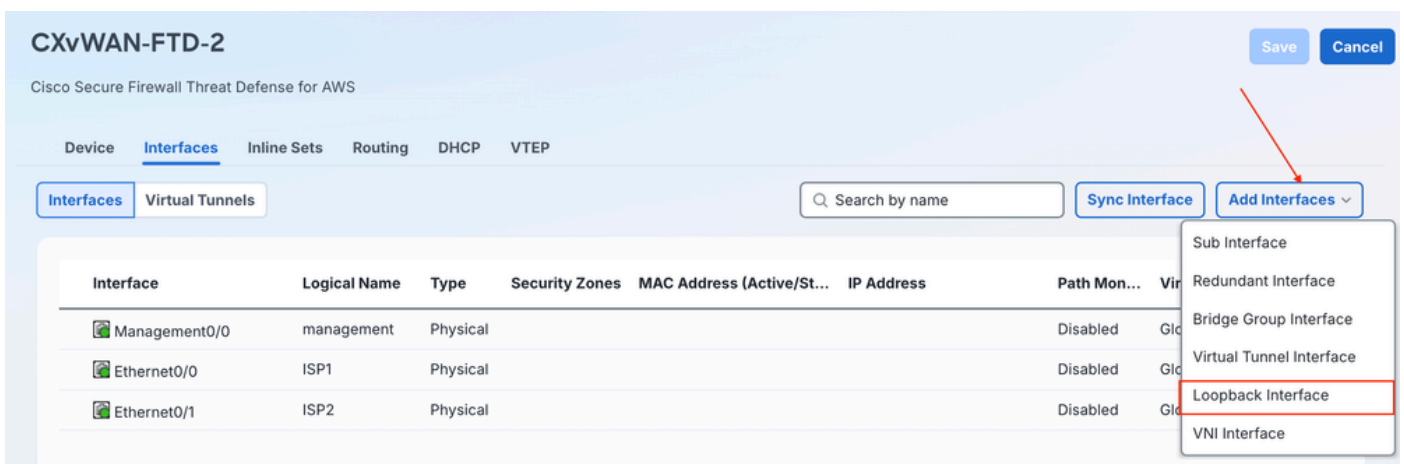
참고: 이 실습에서는 클라우드 기반 cdFMC(Firewall Management Center)를 사용합니다. 그러나 온프레미스 FMC의 단계는 동일합니다.

2) 듀얼 ISP 연결을 통해 브랜치/사이트 VPN 디바이스로 구성하는 FTD를 클릭합니다.

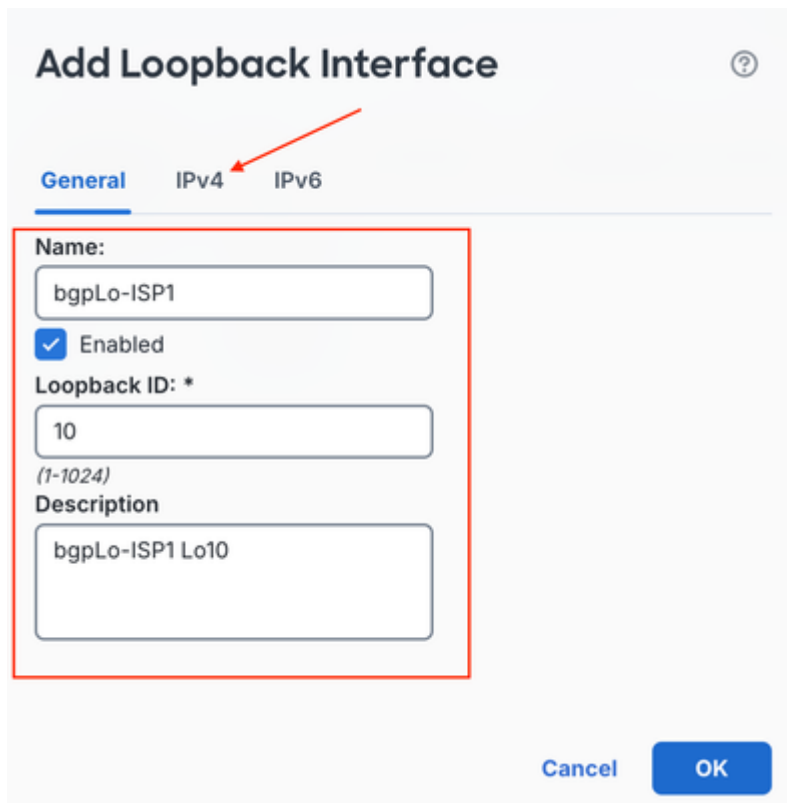
N/A - ROUTED			
	 CXvWAN-FTD-2		10.0.0
N/A - ROUTED			

컨피그레이션 구축을 위한 FTD 선택

3) Add Interfaces 드롭다운 메뉴를 클릭하고 Loopback Interface를 클릭합니다.



4) 루프백 인터페이스의 이름을 입력하고, 사용 확인란을 선택하고 루프백 ID를 입력합니다. 필요한 경우 설명을 입력합니다. 완료되면 IPv4 탭을 클릭합니다.



Add Loopback Interface ⓘ

General **IPv4** IPv6

Name:
bgpLo-ISP1

☒ Enabled

Loopback ID: *
10
(1-1024)

Description
bgpLo-ISP1 Lo10

Cancel **OK**

루프백 인터페이스 정보 및 IPv4 주소 구성

5) Azure의 ISP1 사이트 링크에 대해 이전 단계에서 구성한 링크 BGP IP 주소가 될 루프백 IP 주소를 입력합니다. 이 IP는 ISP1을 통해 FTD와 Azure 인스턴스 간에 구성된 네이버에서 BGP 업데이트 원본으로 사용됩니다.



참고: ISP1의 vpnSiteConfiguration.BgpSetting.BgpPeeringAddress 아래에서 다운로드된 VPN 구성 JSON에 이전에 정의된 값을 참조할 수 있습니다

Add Loopback Interface ?

General **IPv4** IPv6

IP Type:
Use Static IP

IP Address:
169.254.21.100/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

루프백 IPv4 주소를 입력하고 OK(확인)를 누릅니다

6) ISP2 BGP 루프백 컨피그레이션에 대해 이 시퀀스에서 하위 단계 c-e를 반복합니다.

Loopback10	bgpLo-ISP1	Loopb...	169.254.21.100/32(Static);	Disabled	Global		
Loopback20	bgpLo-ISP2	Loopb...	169.254.22.100/32(Static);	Disabled	Global		

첫 번째 및 두 번째 루프백 인터페이스 생성

7) 컨피그레이션을 저장합니다.

You have unsaved changes

Save Cancel

변경 내용 저장

3단계: 1단계/2단계 정책 개체 구성

1) FMC에서 FTD VPN 토폴로지로 일치하는 IKEv2/IPsec 컨피그레이션을 구성하려면 Manage(관리) > Objects(개체)로 이동하고, 탐색 메뉴에서 VPN으로 스크롤한 다음, 하위 메뉴를 확장합니다. 메뉴에서 IKEv2 Policy(IKEv2 정책)를 선택하고 Add IKEv2 Policy(IKEv2 정책 추가)를 클릭하여 IKEv2 Phase 1 정책을 구성합니다.

Policy List

Port

> Prefix List

Route Map

> Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

URL

Variable

Variable Set

VLAN Tag

VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

Secure Client Customization

Secure Client File

IKEv2 Policy

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

Add IKEv2 Policy

Filter

Name	
AES-GCM-NUL- SHA	Q ☐ ⚙
AES-GCM-NUL- SHA-LATEST	Q ☐ ⚙
AES- SHA -SHA	Q ☐ ⚙
AES- SHA - SHA-LATEST	Q ☐ ⚙
DES- SHA -SHA	Q ☐ ⚙
DES- SHA - SHA-LATEST	Q ☐ ⚙
Umbrella-AES-GCM-256	Q ☐ ⚙

Displaying 1 - 7 of 7 rows | < < Page 1 of 1 >

새 IKEv2 정책 개체 만들기

2) 새 IKEv2 정책의 이름을 입력하고 Priority(우선순위) 및/또는 Lifetime(수명)을 선택합니다. 무결성, 암호화, PRF(Pseudo Random Function) 및 DH 그룹에 대한 터널 양쪽 끝에서 정책이 일치하는지 확인합니다. Azure 구성과 일치시킬 알고리즘/그룹 요소를 선택하고 [추가]를 클릭합니다.



참고: vpnSiteConnections[0].connectionConfiguration.IPsecParameters에서 다운로드한 구성 파일 내에서 이러한 정확한 값을 참조할 수 있습니다

New IKEv2 Policy

Name:*

Azure_IKEv2

Description:

Priority:*

(1-65535)

Lifetime:

seconds (120-2147483647)

3600

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

MD5

SHA

SHA512

SHA256

SHA384

NULL

Selected Algorithms

SHA256

Cancel

Save

IKEv2 정책 생성

3) 컨피그레이션이 완료되면 Save(저장)를 클릭합니다.

Edit IKEv2 Policy

Name: *
Azure_IKEv2

Description:

Priority: * (1-65535)
5

Lifetime: seconds (120-2147483647)
3600

Available Groups

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

Selected Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20

Add

Cancel Save

IKEv2 정책 저장

4) IKEv2 IPsec Proposal(IKEv2 IPsec 제안) 하위 메뉴에서 Phase 2/IPsec 매개변수를 구성하고 Add IKEv2 IPsec Proposal(IKEv2 IPsec 제안 추가)을 클릭합니다.

IKEv2 IPsec Proposal

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can configure the Phase 2 algorithms. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Name

- AES-GCM
- AES-SHA
- DES_SHA-1
- Umbrella-AES-GCM-256

Add IKEv2 IPsec Proposal

Policy List

- Port
- Prefix List
- Route Map
- Security Intelligence
- Sinkhole
- SLA Monitor
- Time Range
- Time Zone
- Tunnel Zone
- URL
- Variable
- Variable Set
- VLAN Tag
- VPN
 - Certificate Map
 - Custom Attribute
 - Group Policy
 - IKEv1 IPsec Proposal
 - IKEv1 Policy
 - IKEv2 IPsec Proposal**

IKEv2 IPsec 제안 생성

5) IKEv2 IPsec 제안서의 이름을 지정하고 동일한 설정이 일치하는지 확인합니다. 완료되면 저장을 클릭합니다.

Edit IKEv2 IPsec Proposal

Name:*

Azure_IPsec

Description:

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

AES-GCM-256

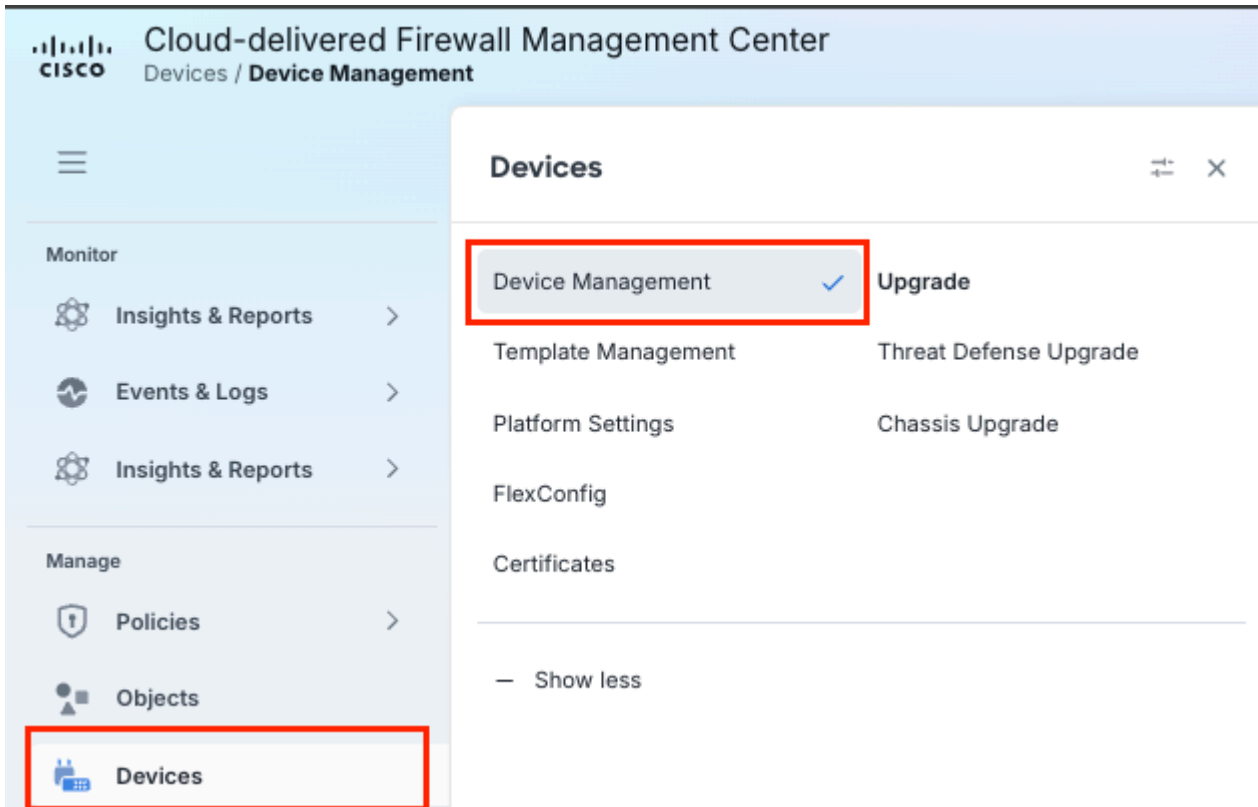
Cancel

Save

IKEv2 IPsec 제안의 이름을 지정하고 Save(저장)를 클릭합니다.

4단계: VTI(Virtual Tunnel Interface) 구성

1) Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다.



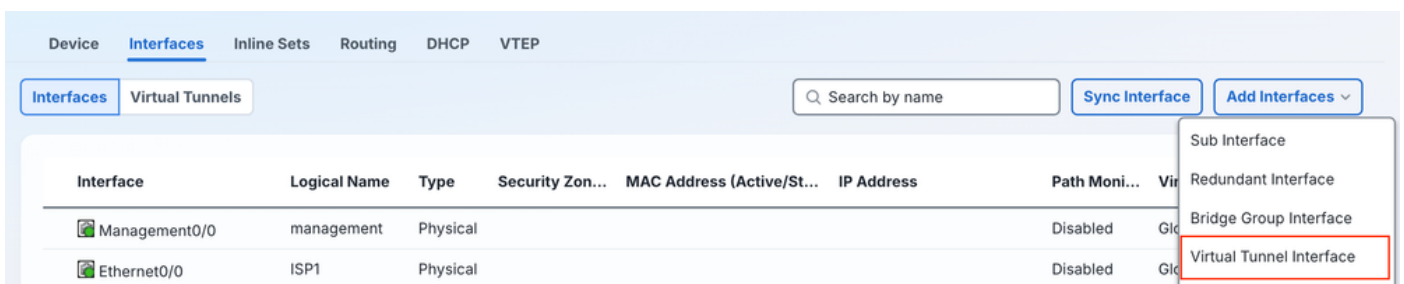
firepower Management Center에서 Device Management(디바이스 관리)로 이동합니다.

2) 듀얼 ISP 연결을 통해 브랜치/사이트 VPN 디바이스로 구성하는 FTD를 클릭합니다.

	✓	CXvWAN-FTD-2 N/A - ROUTED	10.0.0
--	---	-------------------------------------	--------

컨피그레이션 구축을 위한 FTD 선택

3) Add Interfaces(인터페이스 추가) 드롭다운 메뉴를 클릭하고 Virtual Tunnel Interface (VTI)를 선택합니다.



가상 터널 인터페이스 생성

4) 터널 정보를 입력합니다. Enabled(활성화됨) 확인란을 선택하고 Name(이름)을 입력하고(설명), 원하는 경우 선택적인 Security Zone(보안 영역)이 선택되었는지 확인합니다. 올바른 상위 ISP 연결 인터페이스를 정렬하여 VTI를 구성하고, VTI의 내부 터널 IPsec 연결에 적절한 IP 주소를 구성합니다. 완료되면 OK(확인)를 누릅니다.



팁: 참조 다이어그램은 FTD를 사용한 Azure 듀얼 WAN 연결에 대한 잠재적인 VPN 구성에 대한 추가 컨텍스트를 보여줍니다.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

For "CXvWAN-SiteB-ISP-1-Inst-0" VPN topology

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



Cancel

OK

5) 상위 ISP1 및 ISP2 인터페이스 전반에 걸쳐 3개의 추가 VTI를 구성합니다.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
Ethernet0/0	ISP1	Physical				Disabled	Global
Tunnel1	ISP1-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.1/30(Static);	Disabled	Global
Tunnel2	ISP1-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.1/30(Static);	Disabled	Global
Ethernet0/1	ISP2	Physical				Disabled	Global
Tunnel3	ISP2-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.21/30(Static);	Disabled	Global
Tunnel4	ISP2-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.21/30(Static);	Disabled	Global
Loopback10	bgpLo-ISP1	Loopback			169.254.21.100/32(Static);	Disabled	Global
Loopback20	bgpLo-ISP2	Loopback			169.254.22.100/32(Static);	Disabled	Global

추가 가상 터널 인터페이스 구성

f) Save를 클릭하여 변경 사항을 저장합니다.

You have unsaved changes

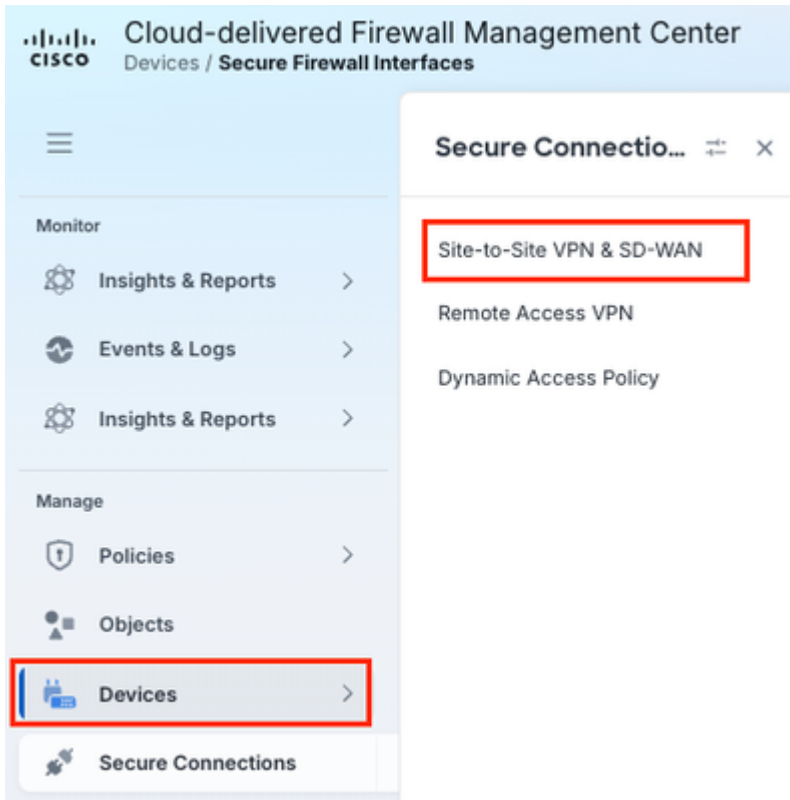
Save

Cancel

변경 내용 저장

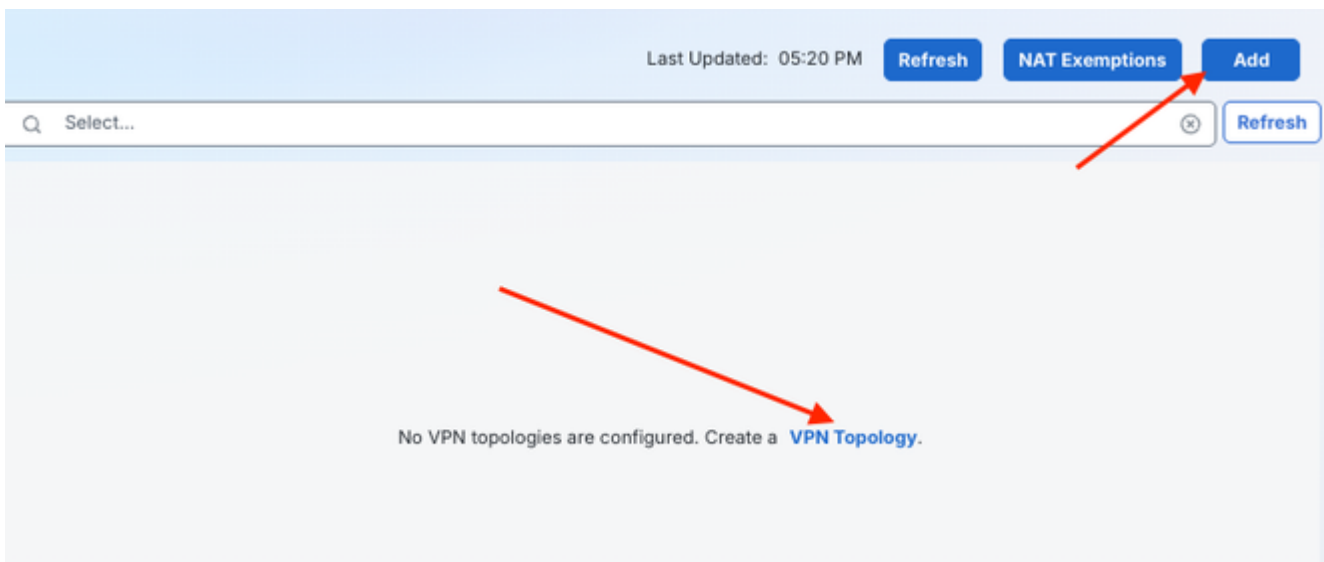
5단계: IPsec VPN 토폴로지 프로비저닝

1) Manage(관리) > Secure Connections(보안 연결) > Site-to-Site VPN & SD-WAN으로 이동합니다



사이트 대 사이트 VPN 및 SD-WAN 연결 관리

2) 초기 출력 중간에 있는 초기 VPN Topology configuration(초기 VPN 토폴로지 컨피그레이션) 하이퍼링크를 클릭하거나 Add(추가) 버튼을 클릭합니다.



새 VPN 토폴로지 구성 추가

3) Azure Instance0에 대한 ISP1 링크를 통해 첫 번째 터널의 토폴로지 이름을 입력합니다. Route-Based VPN 라디오 버튼을 클릭하고 Peer to Peer VPN 토폴로지 유형을 클릭합니다. 완료되면 Create(생성)를 클릭합니다.

Create VPN Topology ?

Topology name *
 CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

SD-WAN Topology
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ Hub and Spoke

[Prerequisites](#)

Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ Peer to Peer

Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

SASE Topology

SASE topology cannot be selected because Secure Access and Umbrella are not configured.

[Prerequisites](#)

[Refresh](#)

[Cancel](#) [Create](#)

경로 기반 VPN 토폴로지 유형 구성

4) 먼저 Node A 디바이스를 선택하고 Device 드롭다운 목록에서 Azure에서 VPN 터널을 종료하는 FTD를 나타냅니다. 마법사에서 디바이스에서 사용 가능한 VTI를 가져온 후 드롭다운 메뉴에서 구성하고 있는 상위 인터페이스 및 인스턴스에 적합한 VTI를 선택합니다. [노드 B 장치] 메뉴에서 VPN 토폴로지 구성의 엑스트라넷 노드가 될 Azure를 선택합니다. 노드 B에 대해 친숙한 이름을 구성하고 알맞은 엔드포인트 IP 주소를 입력하도록 합니다. 완료되면 IKE 탭을 클릭하여 1단계 터널 컨피그레이션을 구현합니다.



참고: `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` 및 `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`에서 다운로드한 컨피그레이션 파일의 인스턴스 엔드포인트 IP 주소 값을 참조할 수 있습니다

Edit VPN Topology

Topology Name:*

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source IP is Dynamic (DHCP) [Edit VTI](#)

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

[Cancel](#) [Save](#)

노드 A 및 노드 B 토폴로지 엔드포인트 정의

5) 탐색 메뉴에서 IKEv2 Settings(IKEv2 설정)로 스크롤하고 연필 아이콘을 클릭하여 최근 구성된 IKEv2 Policy(IKEv2 정책)로 정책을 편집합니다. 다음으로, Authentication Type 드롭다운 메뉴에서 Pre-shared Manual Key 옵션을 선택하고 Azure에서 이전에 구성한 PSK를 입력합니다. 완료되면 IPsec 탭을 클릭하여 2단계 IPsec 터널 매개변수를 구성합니다.



참고: `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`에서 다운로드한 구성 파일의 사전 공유 키를 참조할 수 있습니다

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Azure_IKEv2

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

IKEv2 설정 및 인증 키 편집

6) IKEv2 IPsec Proposal Transform Set(IKEv2 IPsec 제안 변형 집합) 옆의 연필 아이콘을 클릭하고 이전에 구성한 IPsec 정책 매개변수를 선택합니다. Azure vWAN VPN 설정과 일치하도록 수명 기간 값을 변경하세요. 구성된 정보가 확인되면 저장을 클릭합니다.



참고:

vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds에서 다운로드한 컨피그레이션 파일의 수명 값을 참조할 수 있습니다

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals

tunnel_aes256_sha

IKEv2 IPsec Proposals*

Azure_IPsec



Enable Security Association (SA) Strength Enforcement



Enable Perfect Forward Secrecy

Modulus Group:



Lifetime Duration*:

27000

Seconds (Range 120-2147483647)

Lifetime Size:

Unlimited

Kbytes (Range 10-2147483647)

Cancel

Save

IPsec 제안 수명 기간 구성

7) ISP1 Instance1, ISP2 Instance0 및 ISP2 Instance1을 통해 다른 Azure 터널을 만들려면 5단계 내에서 이전 하위 단계를 반복합니다.

> CXvWAN-SiteB-ISP-1-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓	✎	✕
> CXvWAN-SiteB-ISP-1-Inst-1	Route Based (VTI)	Point-to-Point	Deployment Pending	✓	✎	✕
> CXvWAN-SiteB-ISP-2-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓	✎	✕
> CXvWAN-SiteB-ISP-2-Inst-1	Route Based (VTI)	Point-to-Point	0- Tunnels	✓	✎	✕

추가 사이트 대 사이트 VPN 토폴로지 생성

6단계: VPN 토폴로지 검증

system support diagnostic-cli에 입력하고, en을 입력한 후 enter 키를 누릅니다(읽기 전용 CLI).

1) IKE Phase 1 Tunnel(IKE 1단계 터널) 연결을 확인합니다.

```
`show crypto isakmp sa | i UP|READY`
```

2) IPsec Phase 2 연결을 확인합니다.

```
show crypto ipsec sa | i int|current_peer|pkts
```



참고: IPsec SA(Security Associations) 출력과 pkts decaps 및 pkts decrypt 카운터가 증가하고 있지만 pkts encaps 및 pkts encrypt가 증가하지 않은 경우 이 시나리오에서 이러한 현상이 발생할 수 있습니다. Azure에서 허브 전용 IP 공간 주소를 통해 BGP 네이버를 구성하려고 시도하고 있으며, 인접 종단이 APIPA BGP 주소 지정을 사용하는 경우 Azure에서 협상을 시작하지 않습니다. 사용자 지정 APIPA가 사용될 때 BGP 협상을 시작하는 것은 Azure에 연결하는 장치의 책임입니다.

3) 레이어 2 연결을 확인합니다.

```
show arp
```

4) IP Routing(IP 라우팅)을 선택합니다.

```
show route
```

5) ISP1 및 ISP2 인터페이스에서 캡처를 수행합니다.

```
capture isp1 interface ISP1 match udp any any eq 500
capture isp1 interface ISP1 match udp any any eq 4500
capture isp1 interface ISP1 match esp any any
...
show cap
show cap isp1
show cap isp2
```

6) Azure Verification(Azure 확인) - vWAN 허브 > 연결로 이동합니다.> VPN Sites(VPN 사이트) > 구성된 사이트를 선택합니다.

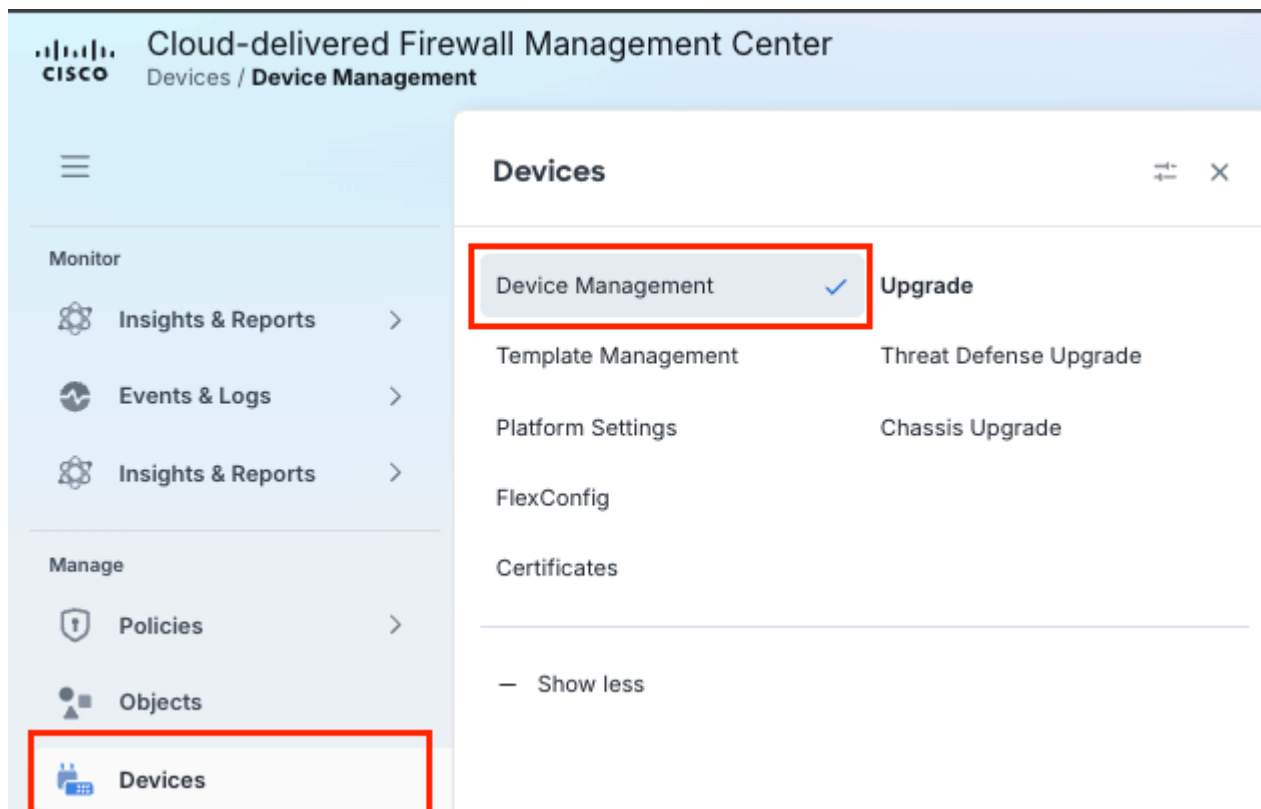
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ ISP-1-Link	ISP1	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub
☐ ISP-2-Link	ISP2	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Azure 링크 연결 확인

7단계: ECMP 구성

1) Manage(관리) > Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 FTD를 클릭합니다.



firepower Management Center에서 Device Management(디바이스 관리)로 이동합니다.

☐	CXvWAN-FTD-2 N/A - ROUTED	10.0.0
--------------------------	-------------------------------------	--------

컨피그레이션 구축을 위한 FTD 선택

2) Routing(라우팅) 탭을 클릭하고 ECMP를 선택합니다.

Device Interfaces Inline Sets **Routing** DHCP VTEP SNMP

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

동일 비용 다중 경로 구성 설정

3) Add(추가)를 클릭합니다.

Equal-Cost Multipath Routing (ECMP)

Add

There are no ECMP zone records [Add](#)

동일 비용 다중 경로 구성 설정 추가

4) ECMP 영역의 이름을 지정하고 사용 가능한 VTI 인터페이스를 클릭한 다음 Add(추가) 버튼을 클릭하여 Selected Interfaces(선택한 인터페이스) 옆에 적용하고 OK(확인)를 클릭합니다

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

동일 비용 다중 경로 영역에 대한 인터페이스 선택

5) 변경 사항을 저장합니다.

You have unsaved changes

Save

Cancel

변경 내용 저장

8단계: BGP 구성

1) Routing(라우팅) > General Settings(일반 설정) > BGP에서 FTD의 BGP 프로세스를 활성화합니다. Enable BGP(BGP 활성화) 확인란을 선택하고 1단계 1d에서 앞서 구성한 AS 번호를 입력합니다. Routing(라우팅) > BGP > IPv4 옆으로 이동합니다.

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

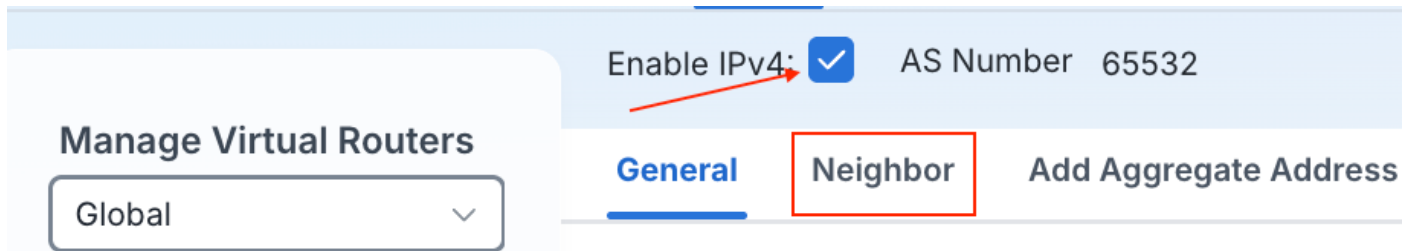
Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

2) BGP 프로세스에 대해 IPv4 사용 확인란을 선택하고 Neighbor를 클릭하여 Azure에서 BGP 인접 디바이스를 구성합니다.



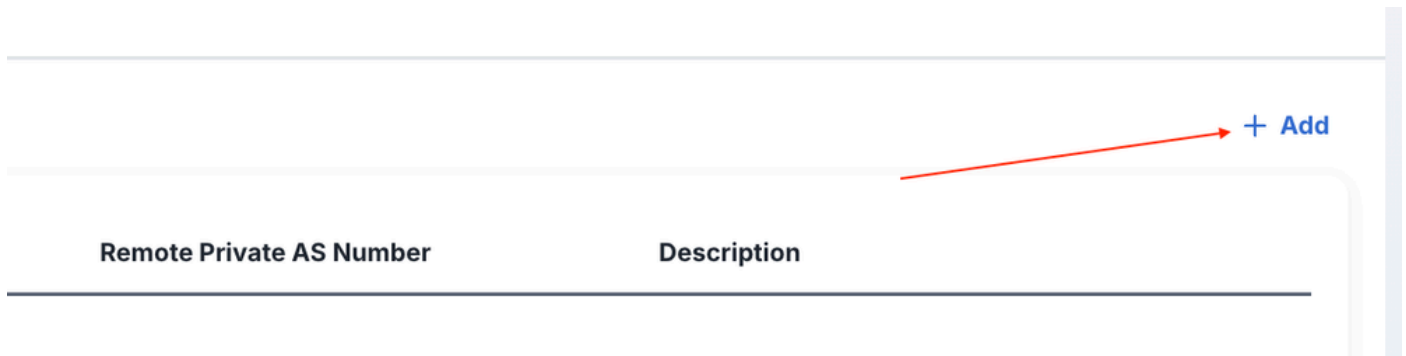
Manage Virtual Routers

Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

3) + Add(추가)를 클릭합니다.



Remote Private AS Number	Description
--------------------------	-------------

+ Add

4) ISP1 Instance0 BGP 피어링 정보를 입력하고, vWAN 허브에서 기록된 BGP AS를 참조하여 Neighbor Remote AS로 입력한 다음, 원하는 경우 Description(설명)을 추가합니다. Advanced(고급)를 클릭합니다.



참고: Azure에 구성된 ISP1 링크에 매핑된 FTD의 VTI 인터페이스에 대한 루프백을 참조하려면 BGP 업데이트 원본을 선택해야 합니다.

Add Neighbor



IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Border Gateway Protocol 피어링 정보 구성

5) FTD의 BGP Neighbor 컨피그레이션의 Advanced(고급) 메뉴에서 TTL(Time To Live) 홉 수를 eBGP 기본값의 1 홉에서 변수 번호로 변경할 수 있습니다. Azure BGP 끝점은 터널을 통해 Azure 인프라에 직접 연결되지 않으며, 기본 eBGP TTL 1보다 더 많은 홉이 끝점에 있는 경향이 있습니다. OK(확인)를 클릭합니다.

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

고급 보더 게이트웨이 프로토콜 네이버 설정

6) 하위 단계 3-5를 반복하여 ISP1 Instance1에 대해 Tunnel2를 구성합니다.

7) 하위 단계 3~5를 두 번 반복하여 ISP2 Instance0/Instance1 BGP 피어링 정보를 구성합니다.



참고: Azure에 구성된 ISP2 링크에 매핑된 FTD에서 VTI 인터페이스에 대한 루프백을 참조하는 정렬된 BGP 업데이트 원본을 선택해야 합니다.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

ISP2 인스턴스 1 BGP 네이버 컨피그레이션

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

ISP 2 인스턴스 2 BGP 인접 디바이스 컨피그레이션

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.21.2	65515	Enabled		
169.254.22.2	65515	Enabled		
169.254.21.22	65515	Enabled		
169.254.22.22	65515	Enabled		

완료되면 저장을 클릭합니다.

You have unsaved changes

Save

변경 내용 저장

기본적으로 ECMP가 Azure에 대한 모든 VTI에 걸쳐 구성되더라도 BGP는 라우팅 테이블에 최상의 단일 경로만 설치합니다. BGP 다중 경로는 학습된 두 경로가 동시에 설치 및 사용되도록 별도로 활성화해야 합니다.

9단계: eBGP 다중 경로 구성

1) Routing(라우팅) > BGP > IPv4로 이동하고 General(일반) 탭을 클릭한 다음 Forward Packets Over Multiple Paths(여러 경로를 통해 패킷 전달) 옆에 있는 연필 아이콘을 클릭합니다.

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP**
- IPv4
- IPv6
- Static Route
- Multicast Routing
 - IGMP
 - PIM
 - Multicast Routes
 - Multicast Boundary Filter

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP (Use filtering to limit the number of prefixes that are redistributed)	No

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

Forward Packets Over Multiple Paths(여러 경로를 통해 패킷 전달) 설정

2) Number of Paths(경로 수) 필드 기본값을 1에서 4로 변경합니다. OK(확인)를 클릭합니다.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Change Forward Packets Over Multiple Paths(여러 경로를 통해 패킷 전달 변경) 설정

3) 변경 사항을 저장하고 구축했는지 확인합니다.

확인/문제 해결

구축이 완료되면 FTD BGP 프로세스에서 각 터널의 두 Azure 인스턴스와 네이버 인접성을 설정하고 경로를 학습하고 인터페이스가 작동하며 프로토콜 연결이 연결 테이블에 반환되는지 확인합니다.

2단계system support diagnostic-cli7단계에서 수행한 대로 FTD CLI에서 이동합니다.

1) 구축되면 BGP 인접 디바이스가 가동되고 접두사가 수신됩니다.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show bgp summary
```

```
BGP router identifier 169.254.22.100, local AS number 65532  
BGP table version is 29, main routing table version 29
```

```

2 network entries using 400 bytes of memory
8 path entries using 640 bytes of memory
2 multipath network entries and 8 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1272 total bytes of memory
BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

```

```

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.21.2 4 65515 20 17 29 0 0 00:13:14 2
169.254.22.2 4 65515 20 20 29 0 0 00:13:22 2
169.254.21.22 4 65515 19 21 29 0 0 00:13:19 2
169.254.22.22 4 65515 20 19 29 0 0 00:13:17 2
ftd#

```

2) Azure에서 받은 경로가 다중 경로 경로로 표시되는지 확인합니다.

```
<#root>
```

```
ftd#
```

```
show bgp
```

```

BGP table version is 29, local router ID is 169.254.22.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i
*m 172.27.0.0	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i

3) 라우팅 테이블 채우기를 확인합니다.

```
<#root>
```

```
ftd#
```

```
show route bgp
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

```

ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 172.31.3.33 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
B      172.27.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
```

4) BGP 세션에 대한 연결 테이블을 확인합니다.

<#root>

ftd#

show conn all | include TCP|179

```
TCP ISP2-Inst-0 169.254.21.22:179 bgpLo-ISP2 169.254.22.100:1603, idle 0:00:10, bytes 1517, flags UIO
TCP ISP2-Inst-1 169.254.22.22:179 bgpLo-ISP2 169.254.22.100:41883, idle 0:00:01, bytes 1486, flags UIO
TCP ISP1-Inst-1 169.254.22.2:179 bgpLo-ISP1 169.254.21.100:3804, idle 0:00:53, bytes 1467, flags UIO
TCP ISP1-Inst-0 169.254.21.2:179 bgpLo-ISP1 169.254.21.100:61287, idle 0:00:04, bytes 1331, flags UIO
TCP bgpLo-ISP1 169.254.22.2:179 NP Identity Ifc 169.254.21.100:3804, idle 0:00:53, bytes 751, flags U
TCP bgpLo-ISP2 169.254.21.22:179 NP Identity Ifc 169.254.22.100:1603, idle 0:00:10, bytes 844, flags
TCP bgpLo-ISP2 169.254.22.22:179 NP Identity Ifc 169.254.22.100:41883, idle 0:00:01, bytes 751, flags
TCP bgpLo-ISP1 169.254.21.2:179 NP Identity Ifc 169.254.21.100:61287, idle 0:00:04, bytes 639, flags
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.