

보안 방화벽에 대한 Azure vWAN Site-to-Site VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[다이어그램](#)

[Azure와 FTD 간의 단일 DIA 링크 vWAN 연결\(Azure 로드 밸런싱/이중화\)](#)

[구성](#)

[1단계: Azure vWAN/허브 구성](#)

[1단계: vWAN 생성](#)

[2단계: vWAN 허브 생성](#)

[2단계: Azure vWAN VPN 사이트 구성](#)

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

[2단계: Azure vWAN Site VPN 매개변수 구성](#)

[3단계: Azure vWAN 사이트 터널 구성 다운로드](#)

[3단계: FTD 컨피그레이션](#)

[1단계: Azure VPN 구성 분석](#)

[2단계: 루프백 구성](#)

[3단계: 1단계/2단계 정책 개체 구성](#)

[4단계: Azure에 대한 보안 연결 구성](#)

[5단계: Azure에 대한 초기 연결 확인](#)

[6단계: Azure Instance1 끝점에 대한 두 번째 터널 구성](#)

[7단계: ECMP 구성](#)

[8단계: 인스턴스 프라이빗 IP에 대한 고정 경로 구성](#)

[9단계: BGP 구성](#)

[10단계: BGP 다중 경로 구성](#)

[다음을 확인합니다.](#)

[기타 고려 사항](#)

[AS-Path 앞에 추가](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure Firewall에 대한 Microsoft Azure vWAN(Virtual WAN) Site-to-Site VPN 연결의 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

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

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

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

Microsoft vWAN(Azure Virtual WAN)은 여러 Azure 네트워킹, 보안 및 라우팅 기능을 단일 허브 구성 문 뒤에서 결합합니다. 각 vWAN 허브는 Secure Firewall과 같은 원격 디바이스가 게이트웨이 인프라를 구축 및 유지 관리할 필요 없이 Azure에 연결하기 위해 사용하는 Microsoft 관리 Site-to-Site VPN 게이트웨이를 호스팅할 수 있습니다.

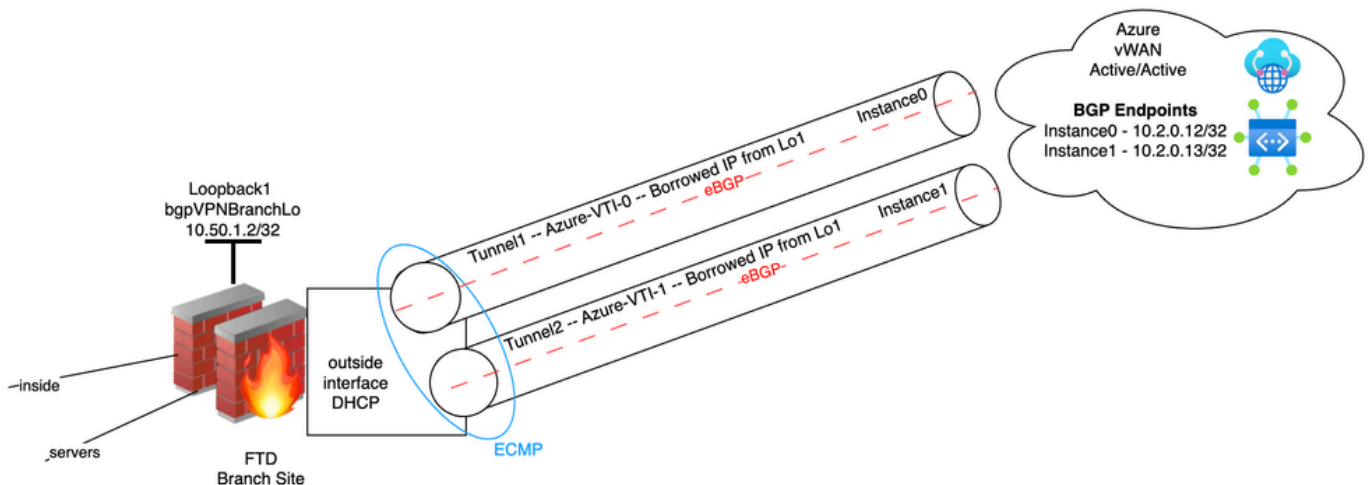
기존 2개 엔드포인트 IPsec VPN과 달리 Azure vWAN Site-to-Site VPN 게이트웨이는 각각 자체 공용 IP 주소 및 BGP(Border Gateway Protocol) 피어링 주소가 있는 활성-활성 인스턴스 쌍 (Instance0 및 Instance1)으로 구축됩니다. 이중화 및 추가 처리량을 위해 두 인스턴스를 모두 활용하기 위해 브랜치 FTD는 각 인스턴스에 하나의 IP 보안(IPsec) 터널을 설정하고, 인스턴스가 사용 가능해지거나 사용 불가능하게 될 때 고정 라우팅이 아닌 BGP를 사용하여 동적으로 경로를 학습하고 회수합니다. FTD의 ECMP(Equal-Cost Multi-Path) 라우팅 및 BGP 다중 경로는 두 터널을 패시브 스탠바이 상태로 간주하지 않고 동시에 액티브 상태로 유지합니다.

이 문서에서는 다음과 같은 세 단계로 설계를 구성합니다. azure vWAN 허브 및 VPN 사이트 개체가 먼저 생성되고, 결과 연결 매개 변수가 다운로드되며, 이러한 동일한 매개 변수를 사용하여 FMC를 통해 FTD에서 일치하는 VTI(Virtual Tunnel Interface), IKEv2(Internet Key Exchange Version 2)/IPsec 정책, 고정 경로, ECMP 및 BGP 피어링을 구성합니다.

다이어그램

다이어그램은 이 문서에서 설명한 구성의 토폴로지를 보여줍니다. 단일 DIA(Direct Internet Access) 변형 원본은 FTD에 있는 하나의 외부 인터페이스에서 두 Azure 터널을 모두 가져옵니다.

Azure와 FTD 간의 단일 DIA 링크 vWAN 연결(Azure 로드 밸런싱/이중화)



구성

순서대로 세 단계를 완료합니다. 1단계와 2단계에서 생성된 Azure 측 개체는 피어 IP 주소, BGP AS(Autonomous System) 번호 및 3단계에서 FTD에 적용하는 사전 공유 키를 생성합니다.

1단계: Azure vWAN/허브 구성

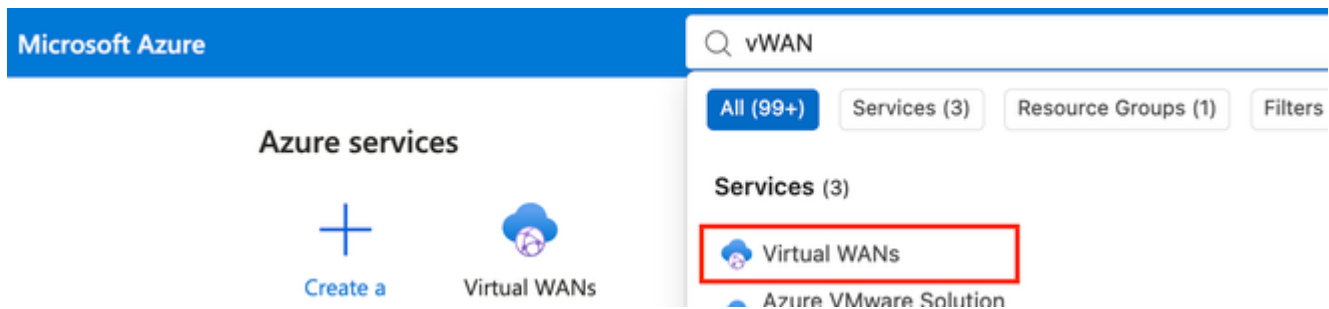


참고: 이 문서의 컨피그레이션 단계는 상위 레벨이며 FTD를 Azure vWAN에 연결하는 데 필요한 단계를 제공합니다. 컨피그레이션의 중요성에 대해 알아보려면 Microsoft의 Azure

vWAN 설명서를 참조하십시오. Azure [Virtual WAN이란?](#) 추가 문서를 참조하십시오.

1단계: vWAN 생성

a) vWAN을 검색하려면 Azure 검색 상자에서 Virtual WANs(가상 WAN)를 클릭합니다.



b) + Create(생성)를 클릭합니다.



c) 새 vWAN 인스턴스의 이름을 입력하고 Review + create를 클릭한 다음 마법사 내의 Review + Create(검토 + 생성) 페이지에서 Create(생성)를 클릭합니다.

Create WAN ...

Basics Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#) 

Project details

Subscription *

Resource group *

[Create new](#)

Virtual WAN details

Region *

Name *

Type ⓘ

Review + create

Previous

Next : Review + create >



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

d) 리소스로 이동을 클릭합니다.



VirtualWanDeployment | Overview

Deployment



Delete



Cancel



Redeploy



Download



Refresh

Overview

Inputs

Outputs

Template



Your deployment is complete



Deployment name : VirtualWanDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

2단계: vWAN 허브 생성

a) Connectivity(연결) > Hubs(허브)로 이동하고 + New Hub(새 허브)를 클릭합니다.



CX-vWAN | Hubs



Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub	Hub status	Region
No results		

b) 추가 구성에 대한 자세한 내용은 Azure 설명서를 참조하십시오. 할당된 허브 개인 주소 공간이 내부 주소 공간과 겹치지 않는지 확인하십시오. Name(이름), Virtual Hub(가상 허브), Hub(허브) 라우팅 환경 설정을 구성합니다. Next(다음)를 클릭합니다. 사이트 대 사이트 >.

Home > CX-vWAN | Hubs

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). [Learn more](#)

Project details

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

Subscription

Resource group

Virtual Hub Details

Region *

Name * ✓

Hub private address space * ⓘ ✓

Virtual hub capacity * ⓘ

Hub routing preference * ⓘ

Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next : Site to site >](#)

c) 제공된 필드에 대한 자세한 내용은 Microsoft Azure vWAN 허브 설명서를 참조하십시오. Site to Site(VPN 게이트웨이)를 생성하려면 Yes(예)를 토글합니다. RFC(Request For Comments) 6996 Defining Private Use AS Reservation에서 IETF(Internet Engineering Task Force)에 의해 할당된 기본 BGP AS(Autonomous System) 번호는 65515입니다.



참고: FMC에서 향후 컨피그레이션 단계를 위해 BGP AS를 기록합니다.

Create virtual hub ...

Basics Site to site Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

☒ Yes☐ No

Copied

AS Number

65515

Gateway scale units

Routing preference

☒ Microsoft network ☐ Internet

Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

Next : Point to site >

검토 + 생성을 클릭하거나 다음 을 클릭합니다. 선택적 설정을 구성하려면 사이트 >를 가리킵니다.

d) 요약이 확인되면 Create(생성)를 클릭합니다.



참고: Azure에서 허브를 만드는 데 30분이 소요됩니다.

Create virtual hub ...

✓ Validation passed

Basics Site to site Point to site ExpressRoute Tags Review + create

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

Basics

Region
Name CX-vWAN-Hub
Hub private address space 10.2.0.0/16
Virtual hub capacity
Hub routing preference

Site to site

Site to site (VPN gateway) Enabled
AS Number 65515
Gateway scale units

Point to site

Point to site (VPN gateway)

ExpressRoute

ExpressRoute gateway

Tags

i Creating a hub with a gateway will take 30 minutes.

Create

Previous

Next

[Download a template for automation](#)

e) 구축이 완료되면 원래 vWAN 리소스 이름을 검색합니다. 검색 범위를 더 좁히려면 리소스를 클릭합니다.

VirtualHubDeployment | Overview ...

Deployment

Search x << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

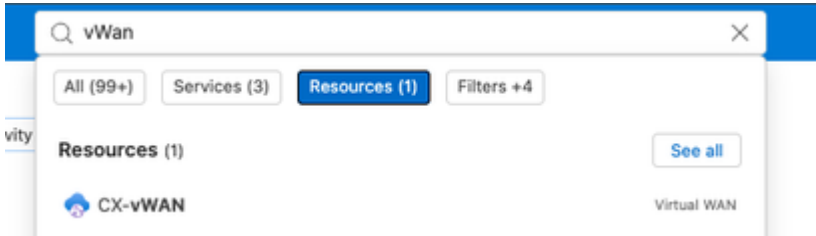
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

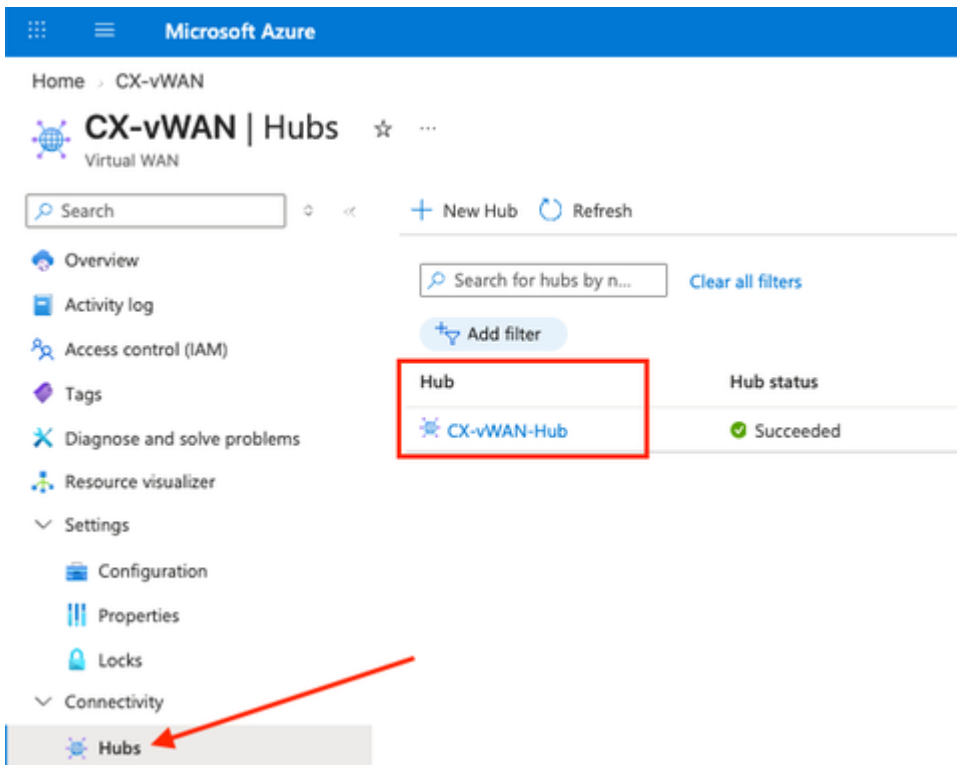
[Go to resource](#)



2단계: Azure vWAN VPN 사이트 구성

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

a) Connectivity(연결) > Hubs(허브)를 통해 생성된 허브에 입력하고 이전 단계에서 생성한 허브를 클릭합니다.



b) 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		

c) 필수 필드에 값을 입력합니다. 완료되면 다음을 클릭합니다. 링크 > 앞으로 이동합니다.

Create VPN site ...

Basics Links Review + create

Project details

Subscription	
Resource group *	

Instance details

Region *	
Name *	VPN-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.

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

Previous

Next : Links >

d) 필수 링크 정보를 입력합니다. Link BGP Address(링크 BGP 주소) 및 Link ASN 필드는 Azure와 Site-to-Site 터널을 통해 형성된 지사 사이트에 있는 내부 터널 BGP Layer 3 대상 주소 및 BGP AS 번호를 반영합니다. 링크 BGP 주소는 이전에 구성된 허브 전용 주소 공간 서브넷 외부에 있는 겹치지 않는 서브넷 주소(/32)입니다. Azure는 BGP 네이버로 연결하기 위해 /32 경로로 설치합니다. 링크 IP 주소/FQDN은 IPsec/IKEv2 연결을 프로비저닝하는 데 필요한 브랜치 사이트로 이동하는 트래픽의 외부 헤더 레이어 3 대상 IP 주소입니다.



참고: 터널 주소에 169.254.21.0~169.254.22.255 범위의 주소를 사용하는 경우 특정 요구 사항에 대해 [Azure VPN 게이트웨이에 대한 BGP를 구성하는 방법](#)을 검토해야 합니다.

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	
single-dia-link ✓	1000 ✓	provider ✓	✓	10.50.1.2 ✓	65500 ✓	...

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

Previous

Next : Review + create >

e) 설정이 올바른지 확인한 후 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

Name VPN-Site

Device vendor Cisco

Private address space

Links

Link name	single-dia-link
Link provider name	provider
Link speed	1000
Link IP address / FQDN	
Link ASN	65500
Link BGP address	169.254.10.2

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

Create

Previous

Next

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

Home



VpnSiteDeployment | Overview

Deployment

Search



Delete



Cancel



Redeploy



Download



Refresh



Overview



Inputs



Outputs



Template



Your deployment is complete



Deployment name : VpnSiteDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

vWan

All (99+)

Services (3)

Resources (1)

Filters +4

Resources (1)

See all



CX-vWAN

Virtual WAN

2단계: Azure vWAN Site VPN 매개변수 구성

a) Connectivity(연결) > Hubs(허브)를 통해 생성된 허브에 입력하고 이전 단계에서 생성한 허브를 클릭합니다.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

b) Connectivity(연결) > VPN(Site to Site)(VPN(사이트 대 사이트))으로 다시 이동하고 X를 클릭하여 허브 연결을 지웁니다. 연결이 끊긴 사이트를 볼 수 있는 연결된 필터링.

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

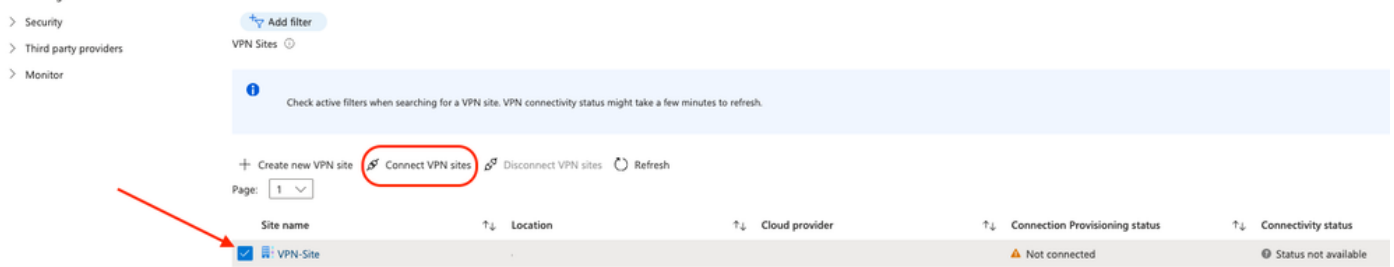
Search this page Clear all filters

Hub association : **Connected** X Add filter

VPN Sites ⓘ

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

c) 이전에 구성된 VPN 사이트 옆의 확인란을 선택한 다음 Connect VPN sites(VPN 사이트 연결)를 클릭합니다. 그러면 사이트가 선택된 후 활성화됩니다.



d) 연결 사이트 측면 드로어 패널이 나타납니다. PSK(Pre-shared key)를 입력하고 원하는 1단계 IKEv2 및 2단계 IPsec 설정을 구성합니다. IPsec 드롭다운 목록에서 Custom(사용자 지정)을 선택하면 값이 자동으로 채워집니다. 이 값은 FTD에서 일치해야 하므로 기록해 둡니다. 또한 PFS(Perfect Forward Secrecy)를 원하는지 선택해야 합니다. 경로 기반 터널이므로 설정을 적절하게 구성합니다. 완료되면 연결을 클릭하여 컨피그레이션을 저장합니다.



참고: 자세한 내용은 [내용은 Default vs. Custom IPsec Policies Azure vWAN](#)을 참조하십시오.

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 *

DHGroup24

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



VPN-Site

eastus

Connect

e) 게이트웨이가 업데이트 중임을 알리는 정보가 예상 완료 시간과 함께 표시됩니다.

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

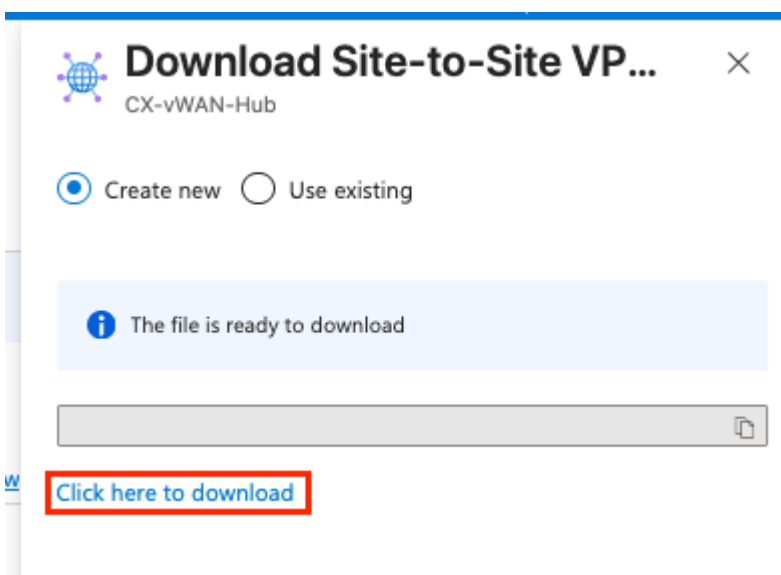
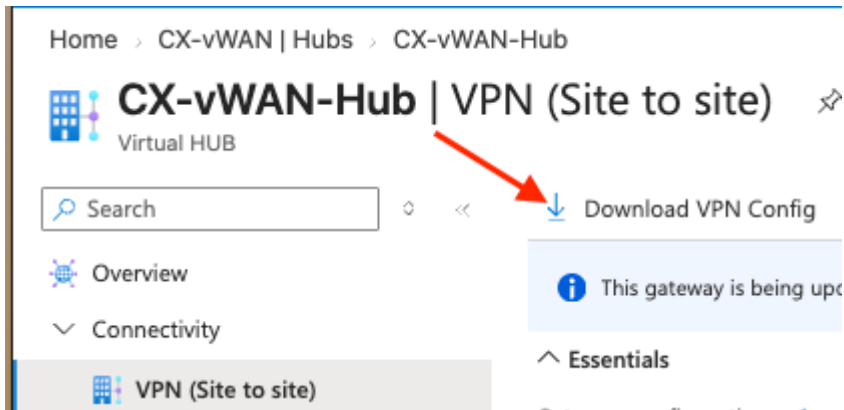
Connectivity



This gateway is being updated. It may take upto 30 minutes for the update

3단계: Azure vWAN 사이트 터널 구성 다운로드

a) 게이트웨이가 업데이트되는 동안 VPN 컨피그레이션을 다운로드할 수 있습니다.



VPN 사이트가 생성되고 연결 매개변수(피어 주소, BGP AS 번호 및 PSK)가 다운로드되면 3단계에서 FTD에서 일치하는 요소를 구성하는 데 동일한 값이 사용됩니다.

3단계: FTD 컨피그레이션

1단계: Azure VPN 구성 분석

a) Azure에서 다운로드한 VPN 구성 파일을 엽니다. 표시되는 압축된 출력과 유사하며 유용한 정보를 제공합니다.



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

```
[
  {
    "configurationVersion": {
      "LastUpdatedTime": "

    },
    "Version": "

    ",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "Region": "

      "
    },
    "gatewayConfiguration": {
      "IpAddresses": {
        "Instance0": "57.x.x.x",
        "Instance1": "52.x.x.x"
      },
      "BgpSetting": {
        "Asn": 65515,
        "BgpPeeringAddresses": {
          "Instance0": "10.2.0.12",
          "Instance1": "10.2.0.13"
        }
      }
    },
    "connectionConfiguration": {
      "IsBgpEnabled": true,
      "PSK": "

    },
    "IPsecParameters": {
      "IpsecEncryption": "GCMAES256",
      "IpsecIntegrity": "GCMAES256",
      "IkeEncryption": "GCMAES256",
      "IkeIntegrity": "SHA384",
      "PfsGroup": "None",
      "DhGroup": "DHGroup14",
      "SADataSizeInKilobytes": 0,
      "SALifeTimeInSeconds": 27000
    }
  }
]

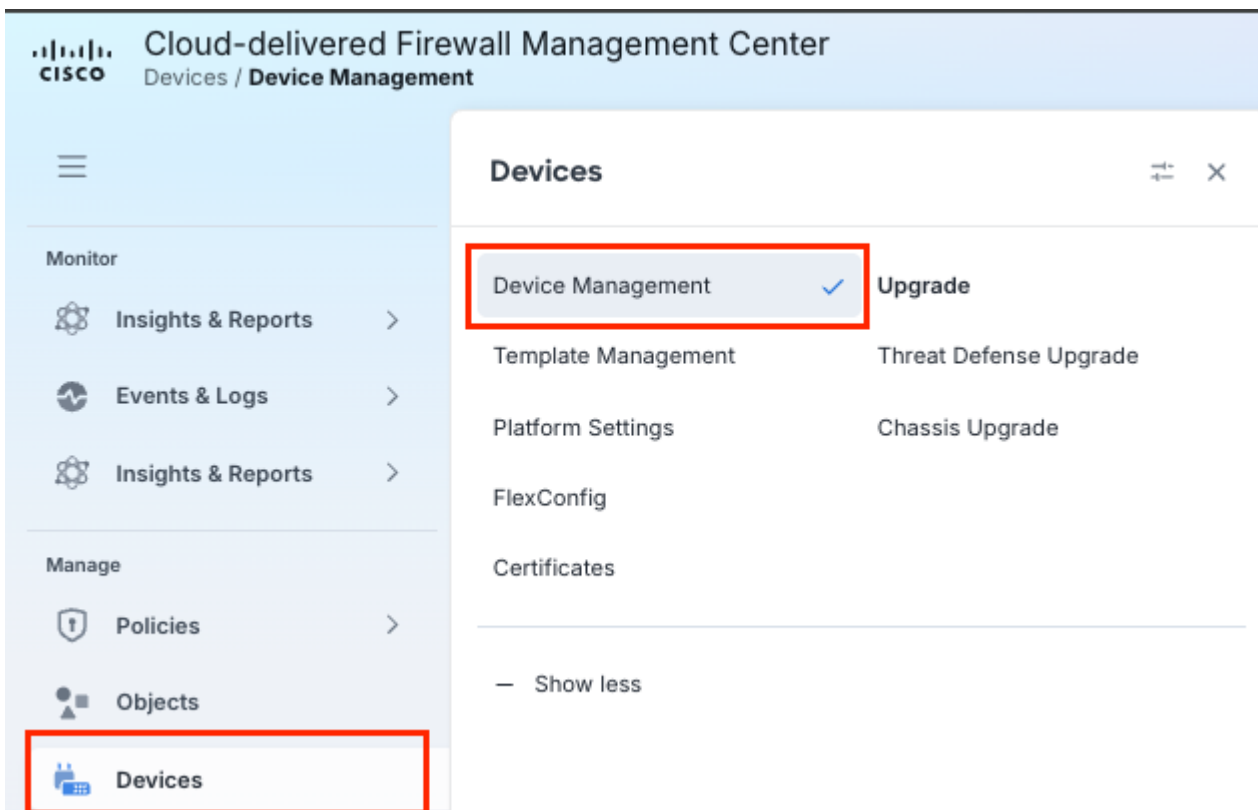
```

}
]

2단계: 루프백 구성

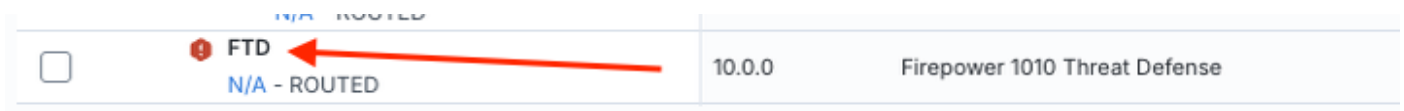
나중에 구성되는 각 VTI에는 안정적인 터널 소스가 필요하므로 루프백 인터페이스가 먼저 구성되고 두 VTI 간에 공유됩니다.

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

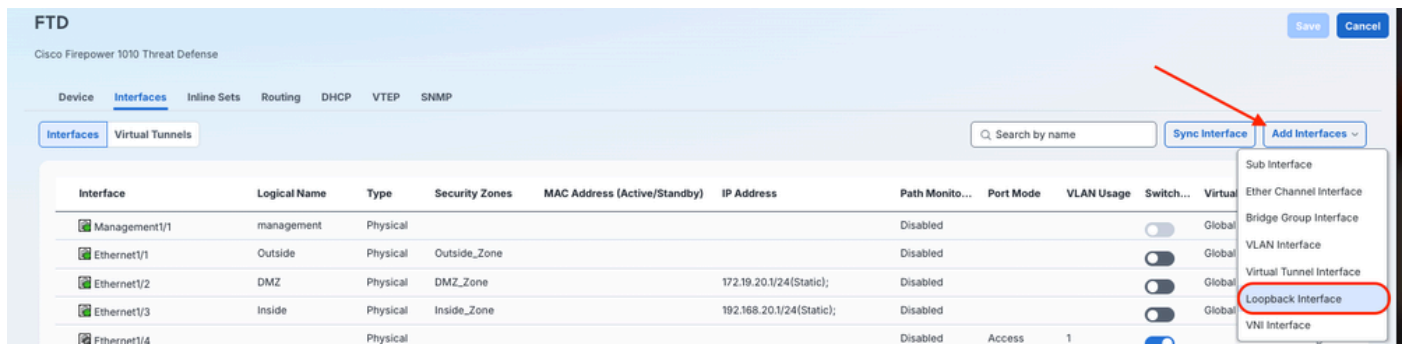


참고: 이 실습에서는 클라우드 기반 cdFMC(Firewall Management Center)를 사용합니다. 그러나 온프레미스 FMC의 단계는 동일합니다.

b) 브랜치/사이트 VPN 디바이스로 구성할 FTD를 선택합니다.



c) Add Interfaces(인터페이스 추가) 드롭다운 메뉴를 클릭하고 Loopback Interface(루프백 인터페이스)를 클릭합니다.



d) 루프백 인터페이스에 이름, 루프백 ID 및 설명을 지정합니다. IPv4를 클릭합니다.

The screenshot shows the 'Add Loopback Interface' configuration page. The 'General' tab is selected, and the 'IPv4' sub-tab is highlighted with a red circle. The 'Name' field contains 'bgpVPNBranchLo'. The 'Enabled' checkbox is checked. The 'Loopback ID' field contains '1', with a red arrow pointing to it from the text below. The 'Description' field contains 'Branch Loopback for BGP neighboring and VPN termination from Azure'. At the bottom, there are 'Cancel' and 'OK' buttons.

e) IP 유형이 Use Static IP(고정 IP 사용)로 정의되었는지 확인하고, Link BGP Address(링크 BGP 주소)를 2단계, 1d에서 구성된 대로 입력합니다. 다운로드한 VPN 구성 JSON에서 이전에 정의한 값을 참조할 수 있습니다 `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



참고: RFC 1918 주소 공간 내에서 /32 마스크로 주소를 정의합니다.

Add Loopback Interface

General **IPv4** IPv6

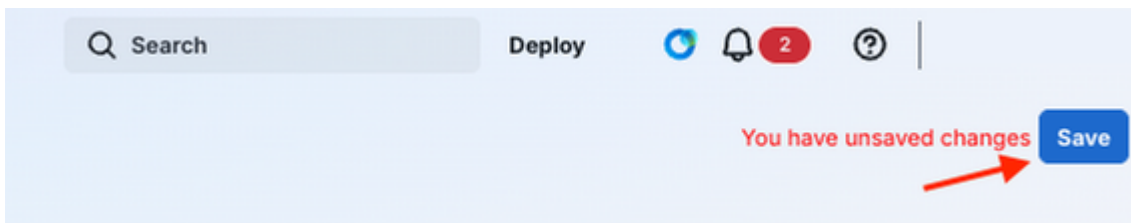
IP Type:
Use Static IP

IP Address:
10.50.1.2/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

f) Save(저장)를 클릭합니다.



3단계: 1단계/2단계 정책 개체 구성

a) FTD VPN 토폴로지에 적용할 FMC의 일치하는 IKEv2/IPsec 컨피그레이션을 구성하려면 Manage(관리) > Objects(개체)로 이동하고, 왼쪽 메뉴에서 아래로 스크롤하여 VPN으로 이동한 다음 하위 메뉴를 확장합니다. 메뉴에서 IKEv2 Policy(IKEv2 정책)를 선택하고 Add IKEv2 Policy(IKEv2 정책 추가)를 클릭하여 IKEv2 Phase 1 Policy(IKEv2 1단계 정책)를 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

IKEv2 Policy

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 >

b) 새 IKEv2 정책의 이름을 입력하고 Priority(우선순위) 및/또는 Lifetime(수명)을 선택합니다. 정책이 무결성, 암호화, PRF 및 DH(Diffie-Hellman) 그룹과 관련하여 터널의 양쪽 끝에서 일치하는지 확인합니다. Azure 구성과 일치시킬 정렬된 알고리즘/그룹 요소를 선택하고 [추가]를 클릭합니다.



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

New IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

Selected Algorithms

SHA256 

Cancel **Save**

c) 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

1
2
5
14
15
16
19
20
...

Add

Selected Groups

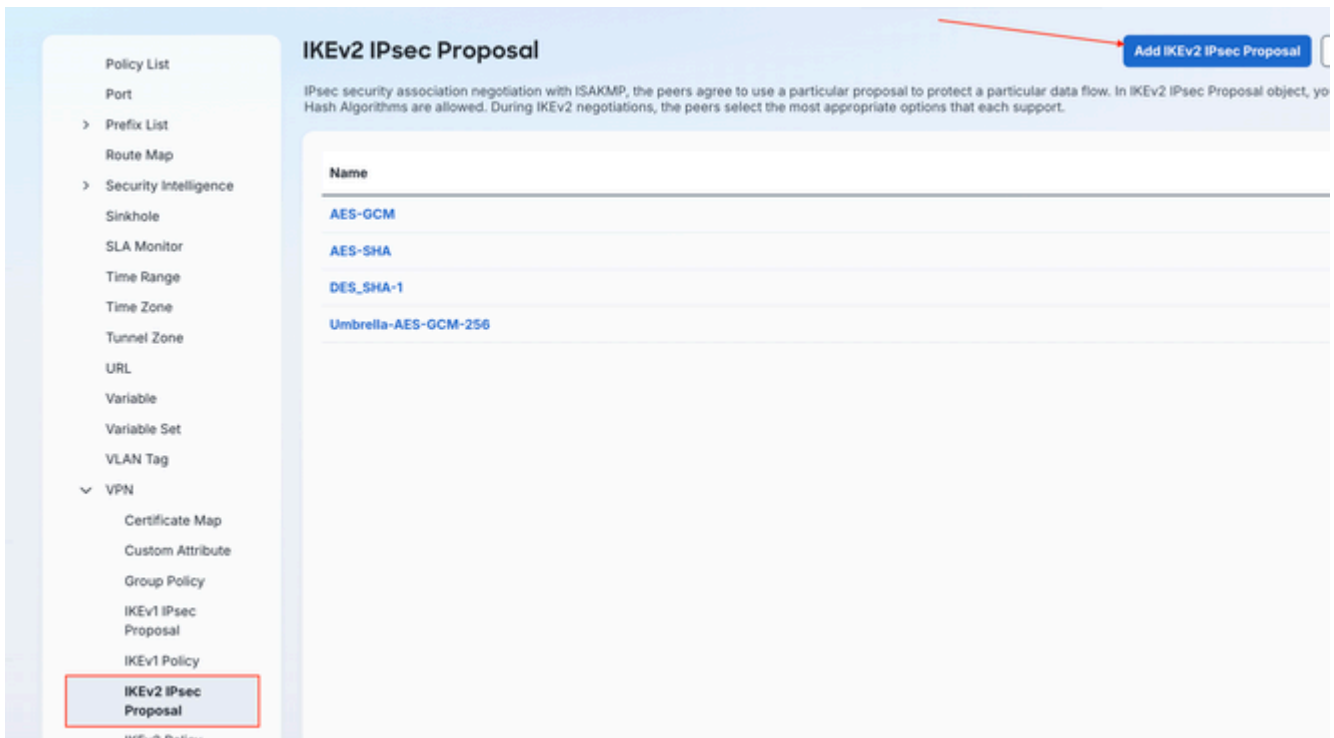
14



Cancel

Save

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



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



참고: 다운로드한 컨피그레이션 파일에서 다음 값을 참조할 수 있습니다

```
. vpnSiteConnections[0].connectionConfiguration.IPsecParameters
```

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256

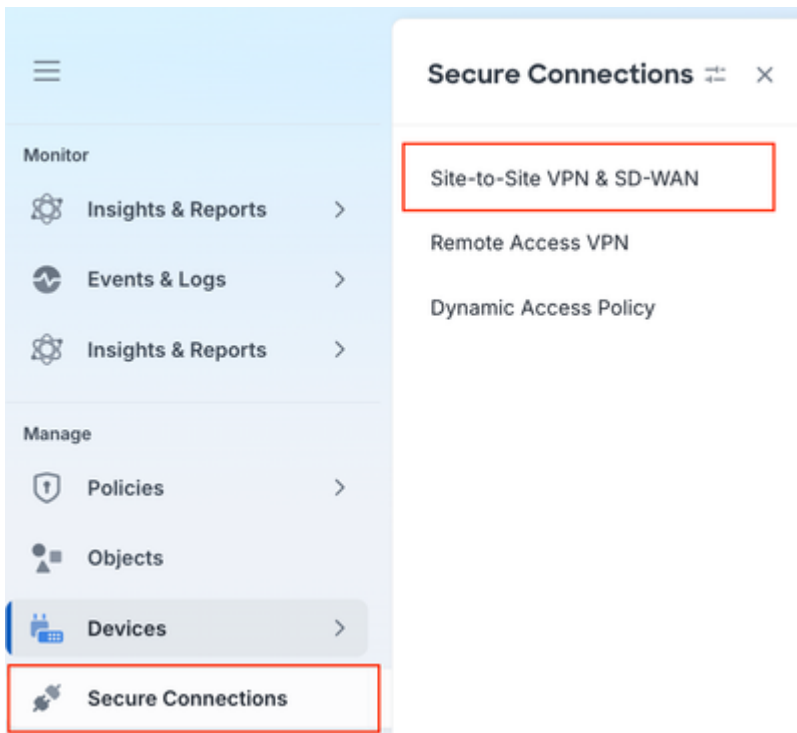


Cancel

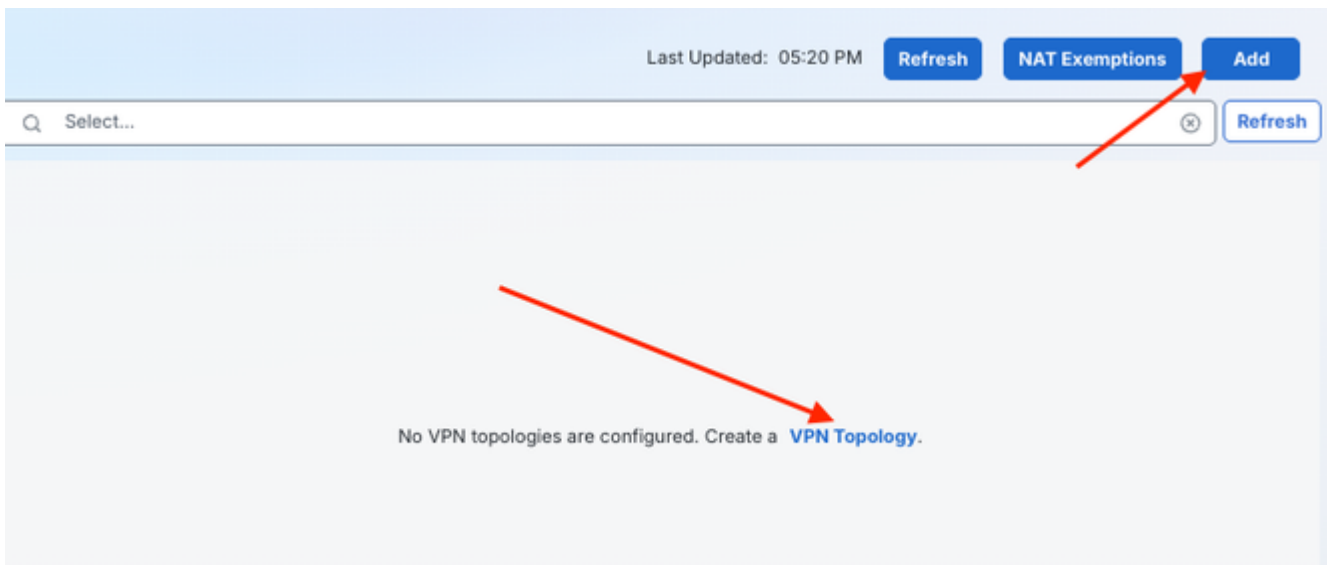
Save

4단계: Azure에 대한 보안 연결 구성

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



b) 중간에 있는 초기 VPN Topology(VPN 토폴로지) 구성 하이퍼링크를 클릭하거나 Add(추가)를 클릭합니다.



c) Azure Instance0에 대한 첫 번째 터널의 토폴로지 이름을 입력하고, Route-Based VPN 라디오 버튼을 클릭하고, Peer to Peer VPN 토폴로지 유형을 클릭합니다. 완료되면 Create(생성)를 클릭합니다.

Create VPN Topology

Topology name *

Azure-VTI-Instance0

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

d) 노드 A에서 Device(디바이스) 드롭다운 목록을 클릭하고 컨피그레이션을 구축할 매니지드 FTD/FTD HA-Pair의 이름을 선택합니다. 노드 B는 Azure vWAN 인스턴스에서 종료되는 토폴로지의 연결 원격 끝이므로 Device 드롭다운 목록에서 Extranet을 선택합니다. 다음으로, 노드 A의 경우 VTI(Virtual Tunnel Interface) 드롭다운 목록 옆에 있는+ 아이콘을 클릭합니다.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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

Node A

Device:*

FTD

Virtual Tunnel Interface:*

+

☐ Tunnel Source IP is Private [Edit VTI](#)

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

Cancel Save

e) 첫 번째 VTI에 Name(이름)을 지정하고 Enabled(활성화됨)인지 확인합니다. VTI에 새 보안 영역 또는 기존 보안 영역을 할당하고, 터널 소스를 할당하며, 인접한 드롭다운 목록에서 IP 주소를 선택합니다.

Add Virtual Tunnel Interface

Tunnel Type

☒ Static ☐ Dynamic

Name:*

Azure-VTI-0

☒ Enabled

Description:

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:*

Ethernet1/1 (Outside) Dynamic

f) 그런 다음 Borrow IP (IP unnumbered)(IP 번호 없음 차입) 라디오 버튼이 선택되었는지 확인한 다음 오른쪽 드롭다운 목록에서 동일한 루프백을 선택합니다. 완료되면 OK(확인)를 클릭합니다.

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:*
 (0 - 10413)

Tunnel Source:*

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 ⓘ
☒ Borrow IP (IP unnumbered) Loopback1 (bgpVPNBranchLo) ▾ +

Cancel OK



g) VTI가 구성되고 적용된 후에는 터널 소스 IP 주소(상위 인터페이스 주소가 DHCP에서 채워지면 자동으로 채워짐)를 수동으로 채우고, 노드 B 디바이스 이름 및 인스턴스 엔드포인트 IP 주소가 구성되었는지 확인합니다. 완료되면 IKE 탭을 클릭합니다.



참고: 다운로드한 컨피그레이션 파일에서 Instance0 Endpoint IP Address 값을 참조할 수 있습니다. `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

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](#)

h) 아래로 스크롤하여 IKEv2 Settings(IKEv2 설정)로 이동하고 Authentication Type(인증 유형)이 Pre-shared Manual Key(사전 공유 수동 키)로 설정되어 있는지 확인한 다음 이전 단계에서 Azure에 구성된 PSK를 입력합니다. 사용 가능한 IKEv2 정책을 수정하려면 연필 아이콘을 클릭하여 IKEv2 1단계 정책을 구성합니다.



참고: 참고: 다운로드한 컨피그레이션 파일에서 사전 공유 키를 참조할 수 있습니다.

`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) 3단계에서 처음 구성된 IKEv2 1단계 정책을 추가합니다.

IKEv2 Policy



Available IKEv2 Policy  +

 Search

AES-GCM-NULL-SHA
AES-GCM-NULL-SHA-LAT...
AES-SHA-SHA
AES-SHA-SHA-LATEST
Azure_IKEv2
DES-SHA-SHA
DES-SHA-SHA-LATEST

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

j) IPsec 탭을 선택합니다.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Azure_IKEv2



Authentication Type:

Pre-shared Manual Key



Key:*

.....

Confirm Key:*

.....

☐

Enforce hex-based pre-shared key only

k) 연필 아이콘을 클릭하여 Transform Sets(변형 집합) 아래에서 IKEv2 IPsec 제안서를 편집합니다.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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  IKEv2 IPsec Proposals* 

tunnel_aes256_sha

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

l) 휴지통 아이콘을 클릭하여 기본 AES-GCM 변형 집합을 제거하고 3단계 후반에 만든 사용자 지정 Azure_IPsec 변형 집합/IKEv2 IPsec 제안을 추가합니다. OK(확인)를 클릭합니다.

IKEv2 IPsec Proposal



Available Transform Sets  +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec 

Cancel

OK

m) 아래로 스크롤하여 Azure 매개 변수와 일치하는 수명 기간 동안 27000을 입력합니다. 해당되는 경우 PFS 그룹을 활성화합니다. 저장을 클릭합니다.



참고: 다운로드한 컨피그레이션 파일의 수명 값은

`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

☐ 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

Lifetime Duration*: 27000 Seconds (Range 120-2147483647)

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

> ESPv3 Settings

Cancel Save

n) 변경 사항을 구축합니다.

Search Deploy

Search Device Advanced Deploy Deploy All

FTD

In Progress... (83%)
Applying updated policy configurat

o) 구축이 완료되면 Manage(관리) > Secure Connections(보안 연결) > Site-to-Site VPN & SD-WAN(터널 상태 배포)에서 확인하십시오. 연결에 성공하면 녹색(위쪽)이 반영됩니다.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✓

첫 번째 터널이 구축된 경우, 이중화를 위해 두 번째 터널을 구성하기 전에 IKE/IPsec 및 BGP 레이어 모두에서 성공적으로 설정되었는지 확인합니다.

5단계: Azure에 대한 초기 연결 확인

a) FTD에 SSH를 입력하고 `system support diagnostic-cli,en` 입력한 후 Enter를 누릅니다. 읽기 전용 FTD CLI에 비밀번호가 없습니다.

```
<#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>
```

```
en
```

```
Password:
```

```
ftd#
```

b) 1단계/2단계 터널 상태를 확인합니다.

```
<#root>
```

```
ftd#
```

```
show crypto isakmp sa | i Status:
```

```
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show crypto ipsec sa | i State|spi
```

```
current outbound spi: 5E83023A
```

```
current inbound spi : 62BC7C9E
```

```
spi: 0x62BC7C9E (0x00010B45)
```

```
SA State: active
```

```
spi: 0x5E83023A (0x0002029B)
```

```
SA State: active
```

```
ftd#
```

c) 캡처를 수행하여 터널의 Azure에서 수신된 BGP TCP(Transmission Control Protocol) 패킷 및 Instance-0 Azure 터널의 공용 IP에서 외부 캡처의 NAT-T(Network Address Translation - Traversal) UDP(User Datagram Protocol) 포트 4500/UDP 포트 500 트래픽을 확인합니다.

```
<#root>
```

ftd#

capture out-instance-0 trace interface Outside match ip host

any

ftd#

capture tun-vti-0 interface Azure-VTI-0 trace match ip host

any

ftd#

show cap tun-vti-0

3 packets captured

1: 03:23:43.510074 10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240

2: 03:23:44.511204 10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240

3: 03:23:46.512211 10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240

ftd#

Instance0에 대한 연결이 확인된 경우 두 Azure 게이트웨이 인스턴스에 모두 연결할 수 있도록

Instance1에 대해 동일한 VTI 및 VPN 토폴로지 구성을 반복합니다.

6단계: Azure Instance1 끝점에 대한 두 번째 터널 구성

a) 동일한 루프백에서 두 번째 VTI(Azure-VTI-1) 차입을 생성합니다(3단계 b-f).

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:*
 (0 - 10413)

Tunnel Source:*

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
☒ Borrow IP (IP unnumbered)

VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b) 두 번째 인스턴스 VPN 토폴로지 구성(4단계 g-n)



참고: 다운로드한 컨피그레이션 파일에서 Instance1 엔드포인트 IP 주소 값을 참조할 수 있습니다. `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

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

Node B

Device:*

Device Name*:

Endpoint IP Address*:

+ Add Backup VTI (optional)

Additional

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

c) 컨피그레이션 변경을 구축하고 터널 상태를 확인합니다.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	
> Azure-VTI-Instance1	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	

d) Azure에서 체크 인하면 Instance0 및 Instance1이 모두 Connected를 반환합니다.

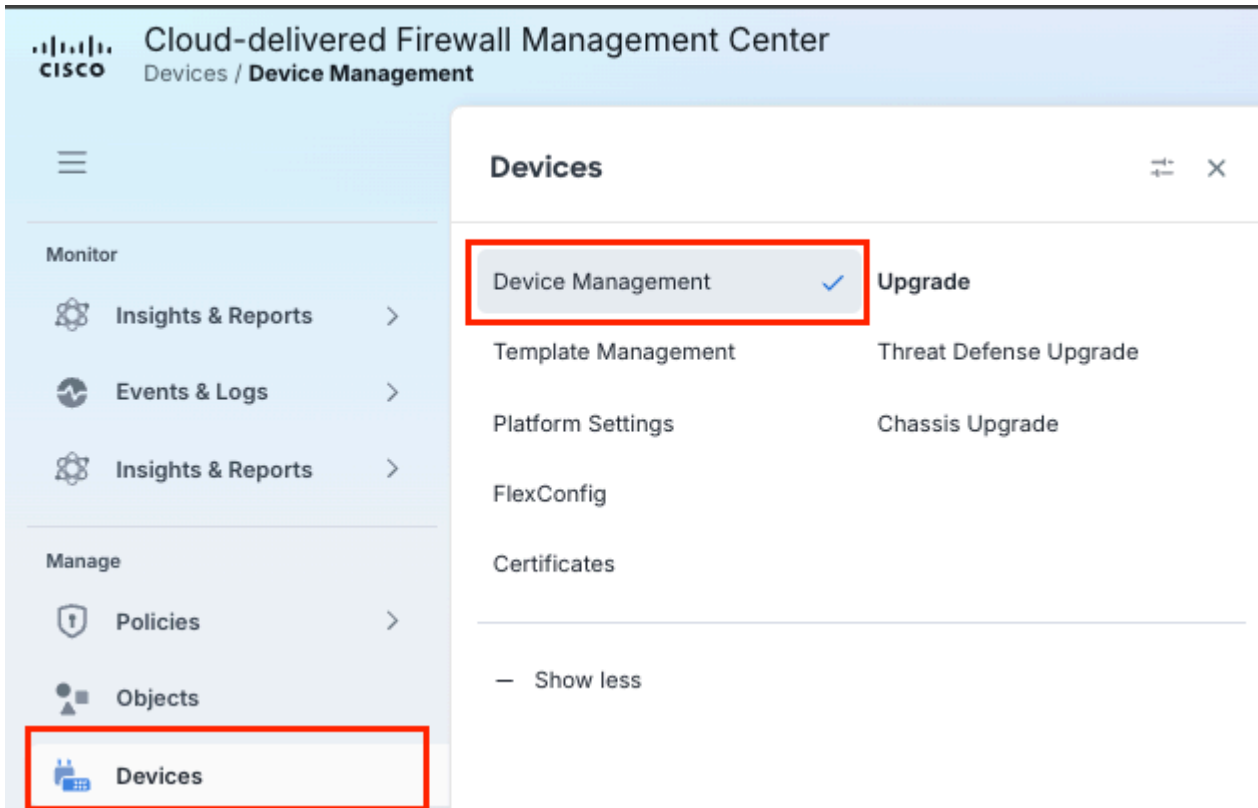
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

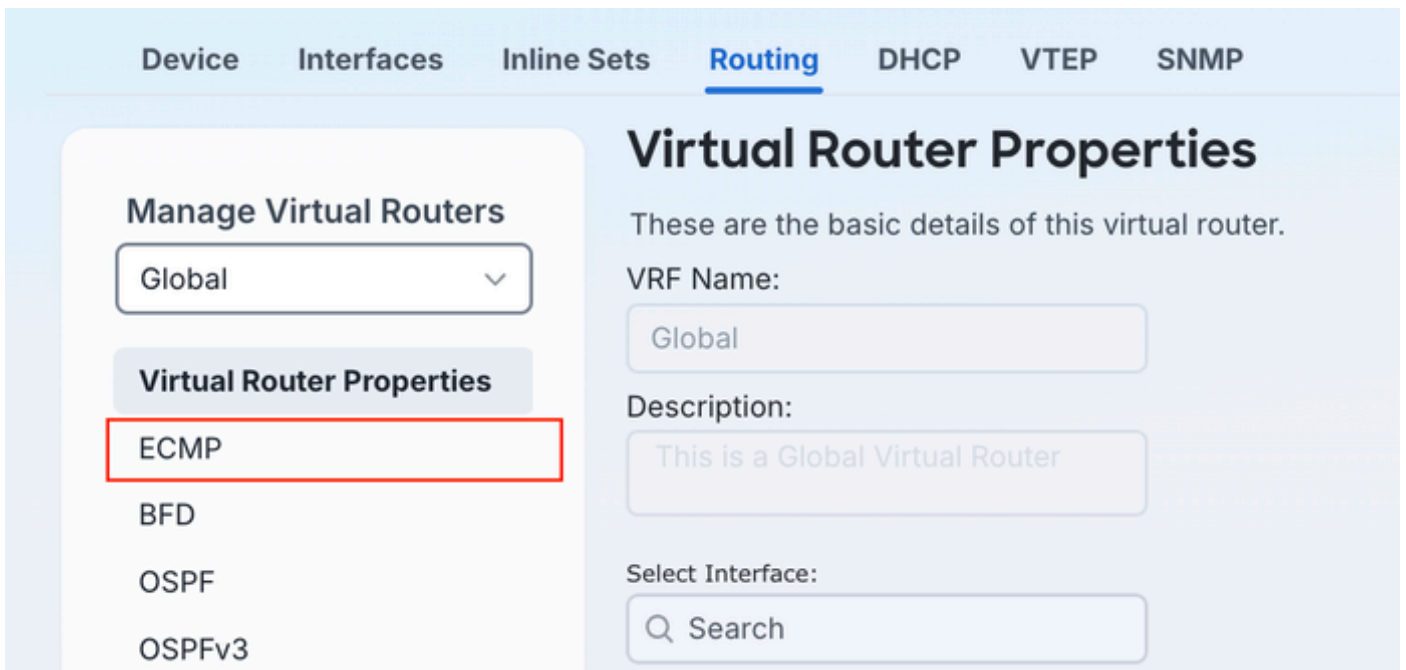
두 터널이 모두 활성 상태인 경우, FTD는 트래픽이 두 번째 터널을 패시브 스탠바이 상태로 처리하지 않고 두 경로를 동시에 사용할 수 있도록 ECMP 라우팅을 필요로 합니다.

7단계: ECMP 구성

a) Manage(관리) > Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 Azure에 대한 VPN으로 구성된 FTD를 선택합니다.



b) Routing(라우팅) 탭을 클릭하고 ECMP를 선택합니다.



c) Add(추가)를 클릭하여 새 ECMP 영역을 생성합니다.

Equal-Cost Multipath Routing (ECMP)

Add

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

d) Available Interfaces(사용 가능한 인터페이스) 패널에서 두 VTI를 모두 클릭하여 VTI를 강조 표시하고 Add(추가)를 클릭하여 명명된 ECMP 영역에 VTI를 적용합니다.

Add ECMP

Name

Available Interfaces

Outside
DMZ
Inside

Add

Selected Interfaces

Azure-VTI-0
Azure-VTI-1

Cancel OK

e) 설정이 올바른지 확인한 후 Save(저장)를 클릭합니다.

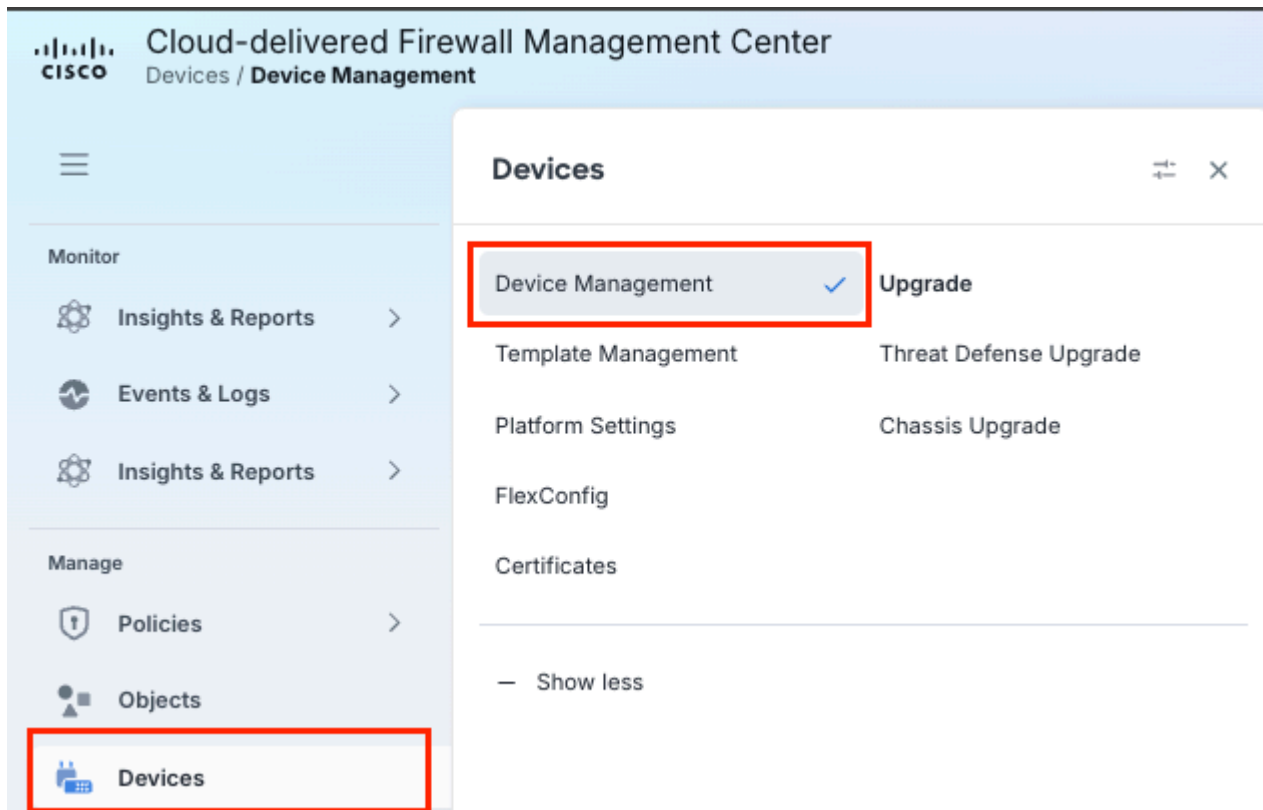
You have unsaved changes

Save

8단계: 인스턴스 프라이빗 IP에 대한 고정 경로 구성

BGP는 인접 디바이스에 성공적으로 연결하기 위한 경로를 필요로 하며, 엔드포인트가 직접 연결되지 않으므로 기본적으로 경로는 채워지지 않습니다. ECMP를 사용하면 동일한 대상에 대해 동일한 메트릭(관리 거리)을 가진 고정 경로를 구성할 수 있으므로 두 경로가 모두 RIB(Routing Information Base)에 설치되고 동시에 사용됩니다.

a) Manage(관리) > Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 해당 FTD 디바이스를 선택합니다.



b) Routing(라우팅) > Static Route(고정 경로)로 이동합니다.

c) + Add Route를 클릭합니다.

d) Instance0 VTI에 대한 첫 번째 경로를 생성하여 두 인스턴스 IP 주소에 대한 경로를 추가하고, 사용 가능한 네트워크 옆에 있는 +를 클릭하여 해당 대상 네트워크 개체를 추가합니다. 그런 다음 목록에서 네트워크 개체를 클릭하고 [추가] 단추를 클릭하여 정적 경로의 대상으로 추가합니다. Instance0 IP를 선택하고 이를 게이트웨이로 설정했는지 확인합니다. 완료되면 확인을 클릭합니다.



참고: 이러한 고정 경로 대상 네트워크 값은 다운로드한 컨피그레이션 파일 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` 및 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` 아래에 있습니다.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*: Azure-VTI-0

(Interface starting with this icon signifies it is available for route leak)

Available Network: Azure-Instance0-BGP_Peer, Azure-Instance1-BGP_Peer

Selected Network: Azure-Instance0-BGP_Peer (10.2.0.12)

Ensure that egress virtualrouter has route to that destination

Gateway: Azure-Instance0-BGP_Peer

Metric: 1 (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e) c-d 단계를 반복하여 Instance1 VTI를 통해 두 번째 고정 경로를 추가합니다. 변경 사항을 저장하려면 Save를 클릭합니다.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Azure-Instance1-BGP_Peer	Azure-VTI-1	Global	Azure-Instance1-BGP_Peer (10.2.0.13)	false	1	
Azure-Instance0-BGP_Peer	Azure-VTI-0	Global	Azure-Instance0-BGP_Peer (10.2.0.12)	false	1	
IPv6 Routes						

고정 경로는 BGP 피어링 주소에만 도달합니다. Azure와 FTD가 서로 더 큰 네트워크로/서로 동적으로 경로를 교환하도록 BGP 자체는 계속 사용하도록 설정되고 피어링되어야 합니다.

9단계: BGP 구성

a) Routing(라우팅) > General Settings(일반 설정) > BGP(BGP) 아래의 FTD에서 BGP Process 65500(BGP 프로세스 설정)를 활성화합니다. Enable BGP(BGP 활성화) 확인란을 선택하고 2단계 1에서 앞서 구성한 AS 번호를 입력합니다. Routing(라우팅) > BGP > IPv4 옆으로 이동합니다.

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

SNMP

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*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id
Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

b) 인접한 Enable IPv4(IPv4 활성화) 확인란을 선택하여 프로세스/AS 65500에 대해 IPv4 BGP 라우팅을 활성화하고 Neighbor(인접 디바이스)를 클릭하여 BGP 인접 디바이스를 구성합니다.

FTD
Cisco Firepower 1010 Threat Defense

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

Enable IPv4: ☒ AS Number 65500

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3

General **Neighbor** Add Aggregate Address Filtering Networks Redis

Setting
Learned Route Map

c) + Add(추가)를 클릭합니다.

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

+ Add

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
No records to display				

d) Instance0 BGP 피어링 정보를 입력하고 vWAN 허브에서 확인된 BGP AS를 참조하여 Neighbor Remote AS로 입력한 다음 원하는 경우 설명을 추가합니다. Advanced(고급)를 클릭합니다.



중요: FTD에서 두 VTI 인터페이스의 루프백 상위 항목을 참조하도록 BGP 업데이트 소스를 변경해야 합니다.

Add Neighbor

IP Address*
10.2.0.12

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
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e) FTD의 BGP Neighbor 컨피그레이션의 Advanced(고급) 메뉴에서 TTL 홉의 수를 eBGP 기본값 1

hop에서 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.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Azure Instance1 BGP Peer에 대해 동일한 단계를 반복합니다.

Add Neighbor ?

IP Address*
10.2.0.13

Remote AS*
65515
(1-4294967295 or 1.0-65535.65535)

BFD Fallover
none

Update Source:
bgpVPNBranchLo

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description
Instance1 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

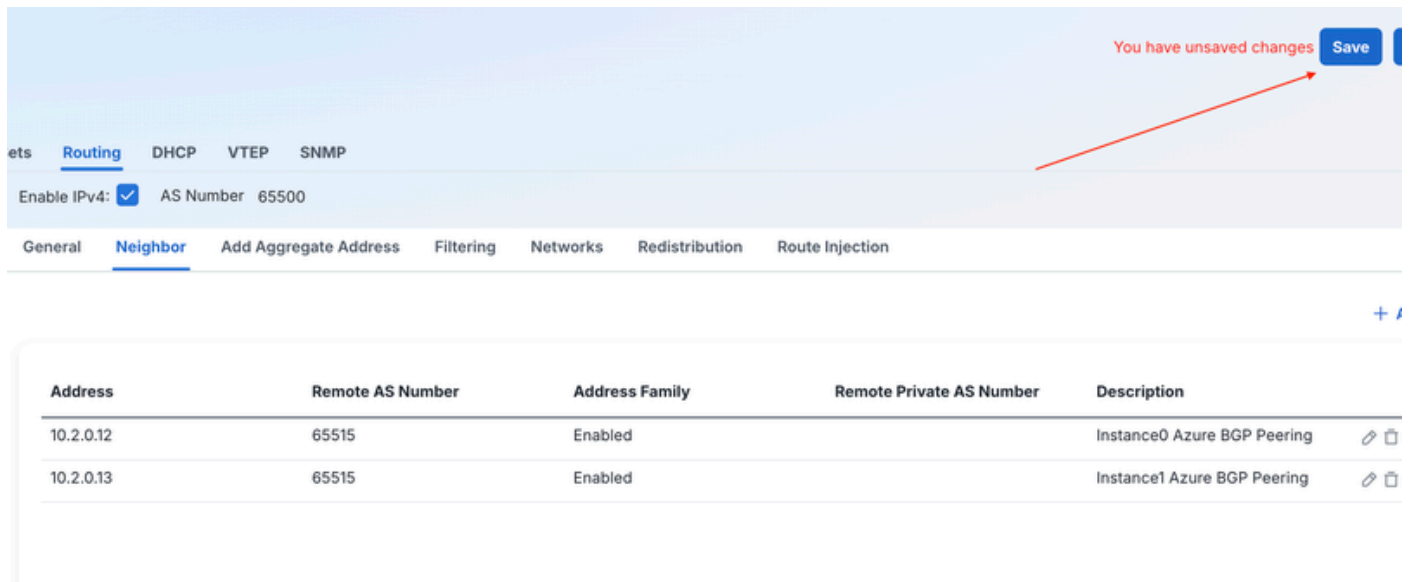
☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50
(1-255)

g) 완료 후 변경 사항을 저장해야 합니다.



기본적으로 ECMP에서 두 고정 경로를 모두 사용할 수 있게 만들지만 BGP는 라우팅 테이블에 최상의 단일 경로만 설치합니다. BGP 다중 경로는 학습된 두 경로가 동시에 설치 및 사용되도록 별도로 활성화해야 합니다.

10단계: BGP 다중 경로 구성

a) 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.

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

Enable IPv4: ☒ AS Number 65500

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 Rout

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

b) Number of Paths(경로 수) 필드 기본값을 1에서 2로 변경합니다.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) 변경 사항을 저장하고 구축했는지 확인합니다.

다음을 확인합니다.

배포가 완료되면 BGP가 두 Azure 인스턴스 모두와 인접성을 형성하는지 확인합니다. 이후 경로가 두 터널을 통해 학습되고, 트래픽이 3단계, 5단계에서 설정한 것과 동일한 진단 CLI 액세스를 사용하여 두 VTI를 모두 사용하는지 확인합니다.

FTD CLI에서 `system support diagnostic-cli`로 이동합니다.

a) 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#

show bgp summary

BGP router identifier 10.50.1.2, local AS number 65500

BGP table version is 5, main routing table version 5

2 network entries using 400 bytes of memory

4 path entries using 320 bytes of memory

2 multipath network entries and 4 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 952 total bytes of memory

BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.2.0.12	4	65515	5	3	5	0	0	00:01:02	2
10.2.0.13	4	65515	3	4	5	0	0	00:00:55	2

ftd#

b) Azure에서 받은 경로가 다중 경로 경로로 표시되는지 확인합니다.

<#root>

ftd#

show bgp

BGP table version is 7, local router ID is 10.50.1.2

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	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i
*m 172.27.0.0	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i

ftd#

c) VTI 패킷 수를 확인합니다.

<#root>

ftd#

show interface Tunnel1 | i packets

118 packets input, 31385 bytes
134 packets output, 8780 bytes
0 packets dropped

ftd#

show interface Tunnel2 | i packets

127 packets input, 33629 bytes
230 packets output, 15119 bytes
0 packets dropped

ftd#

d) BGP 인접 디바이스에 대한 고정 경로를 확인합니다.

<#root>

ftd#

show running-config route

route Azure-VTI-0 10.2.0.12 255.255.255.255 10.2.0.12 1
route Azure-VTI-1 10.2.0.13 255.255.255.255 10.2.0.13 1
ftd#

e) ECMP 영역을 확인합니다.

<#root>

ftd#

show zone

Zone: Azure-VTI-ECMP-Zone ecmp
Security-level: 0
Zone member(s): 2
Azure-VTI-1 Tunnel2
Azure-VTI-0 Tunnel1

ftd#

f) BGP 컨피그레이션을 확인합니다.

<#root>

ftd#

show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.2.0.12 remote-as 65515
    neighbor 10.2.0.12 description Instance0 Azure BGP Peering
    neighbor 10.2.0.12 ebgp-multihop 50
    neighbor 10.2.0.12 transport path-mtu-discovery disable
    neighbor 10.2.0.12 update-source bgpVPNBranchLo
    neighbor 10.2.0.12 activate
    neighbor 10.2.0.13 remote-as 65515
    neighbor 10.2.0.13 description Instance1 Azure BGP Peering
    neighbor 10.2.0.13 ebgp-multihop 50
    neighbor 10.2.0.13 transport path-mtu-discovery disable
    neighbor 10.2.0.13 update-source bgpVPNBranchLo
    neighbor 10.2.0.13 activate
  no auto-summary
  no synchronization
  exit-address-family
ftd#
```

g) 라우팅 테이블을 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 10.0.0.1 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
B      172.27.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
```

기타 고려 사항

이 문서의 기본 컨피그레이션에서는 브랜치 FTD에서 단일 외부 인터페이스 및 단일 ISP를 가정합니다. 이러한 고려 사항은 해당 설계를 확장합니다.

AS-Path 앞에 추가

ECMP 및 BGP 다중 경로를 통해 로드를 균등하게 공유하는 대신 Azure 또는 FTD가 기본 터널로 선호하는 터널에 영향을 주려면 보조 터널로 취급될 BGP 인접 디바이스에서 로컬 AS 번호 앞에 하나 이상의 추가 시간을 추가합니다. AS 경로가 더 긴 인접 디바이스는 ECMP 영역에서 해당 인접 디바이스를 완전히 제거할 필요 없이 표준 BGP 최적 경로 선택 과정에서 우선순위가 저하됩니다.

문제 해결

- 1단계/2단계 터널이 작동하지 않음: 사전 공유 키와 IKEv2/IPsec 정책 매개 변수(암호화, 무결성, PRF, DH 그룹 및 수명)가 FMC IKEv2 정책/IPsec 제안과 다운로드한 Azure VPN 구성 파일의 값 간에 정확히 일치하는지 확인합니다. 3단계, 5단계 `show crypto isakmp sa`에 나와 있는 것처럼 및 `show crypto ipsec sa`을 사용합니다.
- 터널이 작동하지만 BGP 인접 디바이스가 형성되지 `update-source` 않습니다. BGP가 VTI 자체가 아닌 루프백 인터페이스로 설정되었는지, 그리고 FTD에 직접 연결되지 않은 `ebgp-multihop` Azure BGP 피어링 주소에 도달할 수 있을 만큼 높은 값으로 구성되었는지 확인합니다.
- BGP 양식이지만 트래픽을 전달하는 터널은 하나뿐입니다. 3단계, 10단계에서 설명한 대로 두 VTI가 동일한 ECMP 영역의 멤버이고, 두 Azure 인스턴스 BGP 주소에 대한 고정 경로가 동일한 관리 거리로 설치되고, BGP 다중 경로가 두 경로에 대해 구성되었는지 확인합니다.
- 반환 트래픽이 없거나 Azure로 비대칭 라우팅: Azure vWAN은 두 터널을 통해 허브 주소 공간을 광고하므로 라우팅 컨피그레이션의 다른 곳에서 ECMP가 비활성화되지 않았는지 확인하고 트래픽을 단일 경로에 고정할 수 있는 경로 맵 또는 정책 기반 라우팅을 확인합니다.
- BGP가 작동 중이고 경로가 설치되었지만 트래픽이 차단된 것 같습니다. 트래픽이 인그레스 및 이그레스(egress)에 도달할 수 있도록 VTI에 할당된 보안 영역으로 액세스 제어 규칙이 구성되어 있는지 확인합니다.

관련 정보

- [Azure Virtual WAN이란?](#)
- [Azure VPN Gateway에 대한 BGP를 구성하는 방법](#)
- [Azure vWAN에서 기본 정책과 사용자 지정 IPsec 정책 비교](#)
- [Azure VPN 게이트웨이의 BGP 문제 해결](#)
- [액티브-액티브 모드 VPN 게이트웨이 정보](#)
- [자습서: Azure 가상 WAN을 사용하여 Site-to-Site 연결 만들기](#)

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.