

# 보안 방화벽에서 루프백 인터페이스로 eBGP 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[루프백 인터페이스를 사용하는 eBGP 컨피그레이션](#)

[시나리오](#)

[네트워크 다이어그램](#)

[루프백 컨피그레이션](#)

[고정 경로 컨피그레이션](#)

[BGP 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개

이 문서에서는 Cisco Secure Firewall에서 루프백 인터페이스를 사용하여 eBGP를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- BGP 프로토콜

BGP에 대한 루프백 인터페이스 지원은 Secure Firewall Management Center 및 Cisco Secure Firepower Threat Defense에 필요한 최소 버전인 버전 7.4.0에 도입되었습니다.

### 사용되는 구성 요소


- Secure Firewall Management Center for VMware 버전 7.4.1
- 2 Cisco Secure Firepower Threat Defense for VMware 버전 7.4.1

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

BGP(Border Gateway Protocol)는 확장성, 유연성 및 네트워크 안정성을 제공하는 EGP(Exterior Gateway Protocol) 표준화된 경로 벡터 라우팅 프로토콜입니다. 동일한 AS(Autonomous System)를 사용하는 두 피어 간의 BGP 세션을 iBGP(Internal BGP)라고 합니다. 서로 다른 AS(Autonomous Systems)를 사용하는 두 피어 간의 BGP 세션을 eBGP(External BGP)라고 합니다

일반적으로 피어 관계는 피어와 가장 가까운 인터페이스의 IP 주소로 설정되지만, BGP 피어 간에 여러 경로가 있는 경우 BGP 세션을 종료하지 않으므로 루프백 인터페이스를 사용하여 BGP 세션을 설정하는 것이 유용합니다.

 참고: 이 프로세스에서는 eBGP 피어에 대한 Loopback 사용을 설명하지만 iBGP 피어에 대한 Loopback은 참조로 사용될 수 있도록 동일한 프로세스입니다.

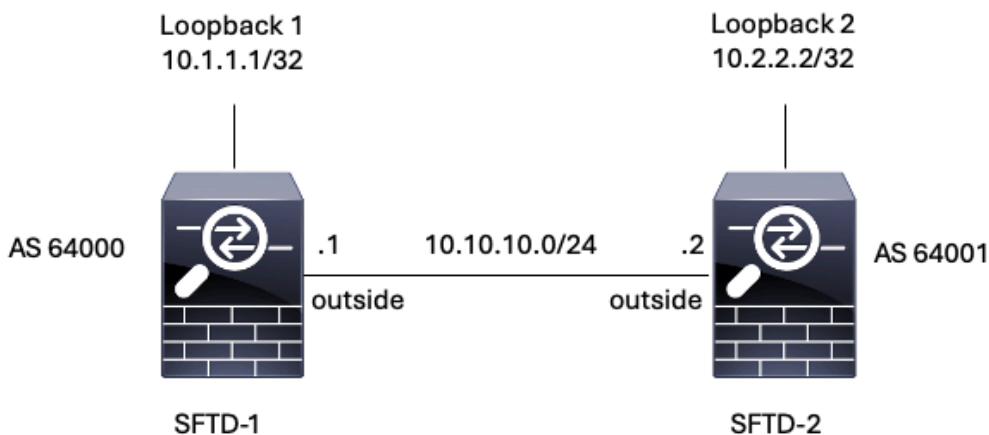
## 루프백 인터페이스를 사용하는 eBGP 컨피그레이션

### 시나리오

이 구성에서 방화벽 SFTD-1에는 IP 주소 10.1.1.1/32이 있는 루프백 인터페이스가 있고 AS 64000, 방화벽 SFTD-2에는 IP 주소 10.2.2.2/32 및 AS 주소가 있는 루프백 인터페이스가 64001. 두 방화벽 모두 외부 인터페이스를 사용하여 다른 방화벽의 루프백 인터페이스에 연결합니다(이 시나리오에서는 외부 인터페이스가 두 방화벽에서 모두 미리 구성됨).

### 네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



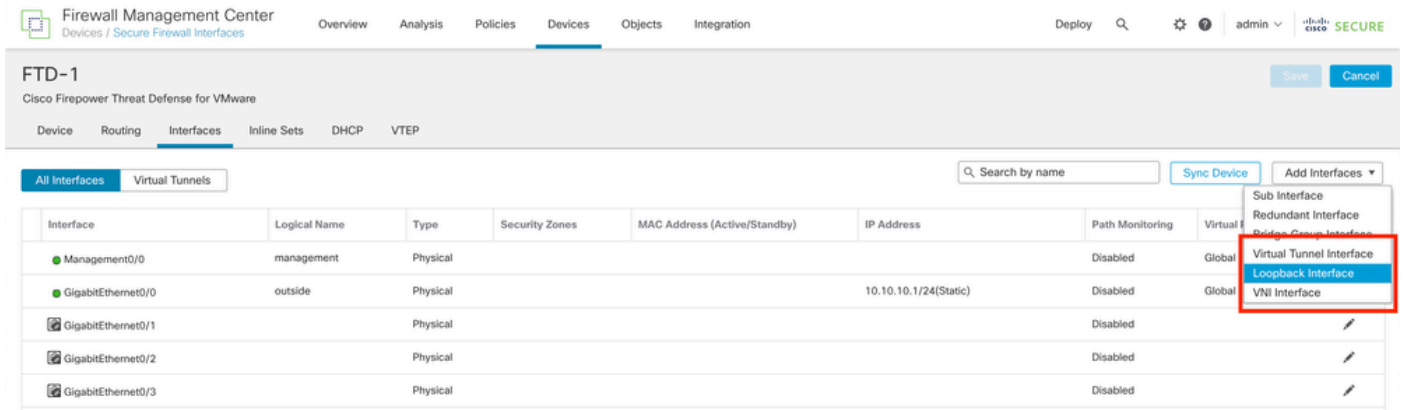
이미지 1. 에세나리오 도표

## 루프백 컨피그레이션

1단계. Devices > Device Management를 클릭하고 루프백을 구성할 디바이스를 선택합니다.

2단계. Interfaces(인터페이스) > All Interfaces(모든 인터페이스)를 클릭합니다.

3단계. Add Interface > Loopback Interface를 클릭합니다.



이미지 2. 인터페이스 루프백 추가

4단계. General(일반) 섹션에서 루프백의 이름을 구성하고 Enabled(활성화됨) 확인란을 선택하고 루프백 ID를 구성합니다.

# Add Loopback Interface



General

IPv4

IPv6

Name:

Loopback1

Enabled

Loopback ID:\*

1

(1-1024)

Description

Cancel

OK

이미지 3. 기본 루프백 인터페이스 컨피그레이션

5단계. IPv4 섹션의 IP Type 섹션에서 Use Static IP 옵션을 선택하고, 루프백 IP를 구성한 다음 OK를 클릭하여 변경 사항을 저장합니다.

# Edit Loopback Interface



General

**IPv4**

IPv6

IP Type:

Use Static IP

IP Address:

10.1.1.1/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

이미지 4. 루프백 IP 주소 컨피그레이션

6단계. 저장을 클릭합니다.

The screenshot shows the Firewall Management Center interface for a device named FTD-1. The 'Interfaces' tab is selected, and a table lists the configured interfaces. The 'Loopback1' interface is highlighted, showing its configuration: Logical Name: Loopback1, Type: Loopback, IP Address: 10.1.1.1/32(Static). A red box highlights the 'Save' button in the top right corner, indicating that the configuration has been saved.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↶
GigabitEthernet0/0	outside	Physical			10.10.10.1/24(Static)	Disabled	Global	✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
Loopback1	Loopback1	Loopback			10.1.1.1/32(Static)	Disabled	Global	✎ 🗑

이미지 5. 루프백 인터페이스 컨피그레이션 저장

7단계. 두 번째 방화벽으로 프로세스를 반복합니다.

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 Cisco SECURE

FTD-2  
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical			10.10.10.2/24(Static)	Disabled	Global
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
Loopback1	Loopback2	Loopback			10.2.2.2/32(Static)	Disabled	Global

이미지 6. 피어의 루프백 인터페이스 컨피그레이션

## 고정 경로 컨피그레이션

피어링에 사용되는 원격 피어 주소(루프백)가 원하는 인터페이스를 통해 연결할 수 있도록 고정 경로를 구성해야 합니다.

1단계. Devices > Device Management를 클릭한 다음 고정 경로를 구성할 디바이스를 선택합니다.

2단계. Routing(라우팅) > Manage Virtual Routers(가상 라우터 관리) > Static Route(고정 경로)를 클릭한 다음 Add Route(경로 추가)를 클릭합니다.

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 Cisco SECURE

FTD-1  
Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets 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

+ Add Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

이미지 7. 새 고정 경로 추가

3단계. 유형에 대한 IPv4 옵션을 선택합니다. Interface 옵션에서 원격 피어의 루프백에 연결하는 데 사용되는 물리적 인터페이스를 선택한 다음, Gateway 섹션에서 루프백에 연결할 다음 홉을 지정합니다.

## Edit Static Route Configuration



Type:  IPv4  IPv6

Interface\*

outside

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

Available Network  

Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2



Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:





Cancel

OK

이미지 8. 고정 경로 컨피그레이션

4단계. Available Network 섹션 옆에 있는 아이콘(+)을 클릭합니다.

## Edit Static Route Configuration



Type:  IPv4  IPv6

Interface\*

outside

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

Available Network 



Selected Network

Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2



Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

Cancel

OK

이미지 9. 새 네트워크 개체 추가

5단계. 참조용 이름과 원격 피어의 Looback IP를 구성하고 저장합니다.



## New Network Object



Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

Cancel

Save

이미지 10. 고정 경로에서 네트워크 대상 구성

6단계. 검색 막대에서 만든 새 객체를 검색하여 선택한 다음 Add(추가)를 클릭하고 OK(확인)를 클릭합니다.

## Edit Static Route Configuration






Type:  IPv4  IPv6

Interface\*

outside

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

Available Network 	+	Selected Network
<input type="text" value="Loopback-FTD2"/> 	<input type="button" value="Add"/>	Loopback-FTD2 
Loopback-FTD2		

Ensure that egress virtualrouter has route to that destination

Gateway

10.10.10.2  +

Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

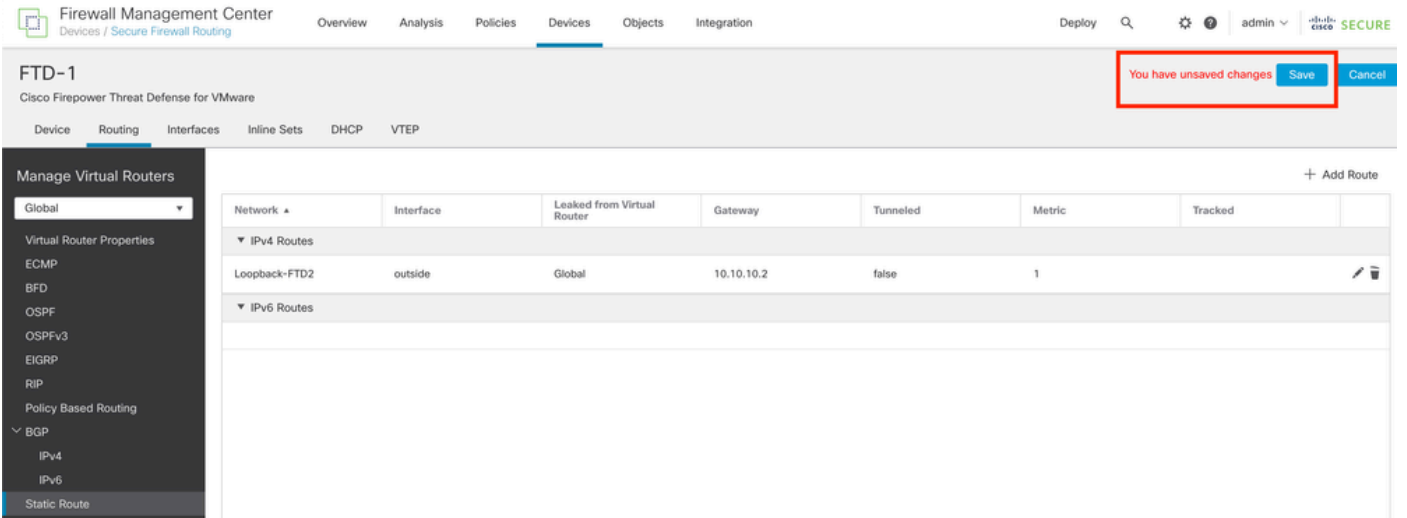
+

Cancel

OK

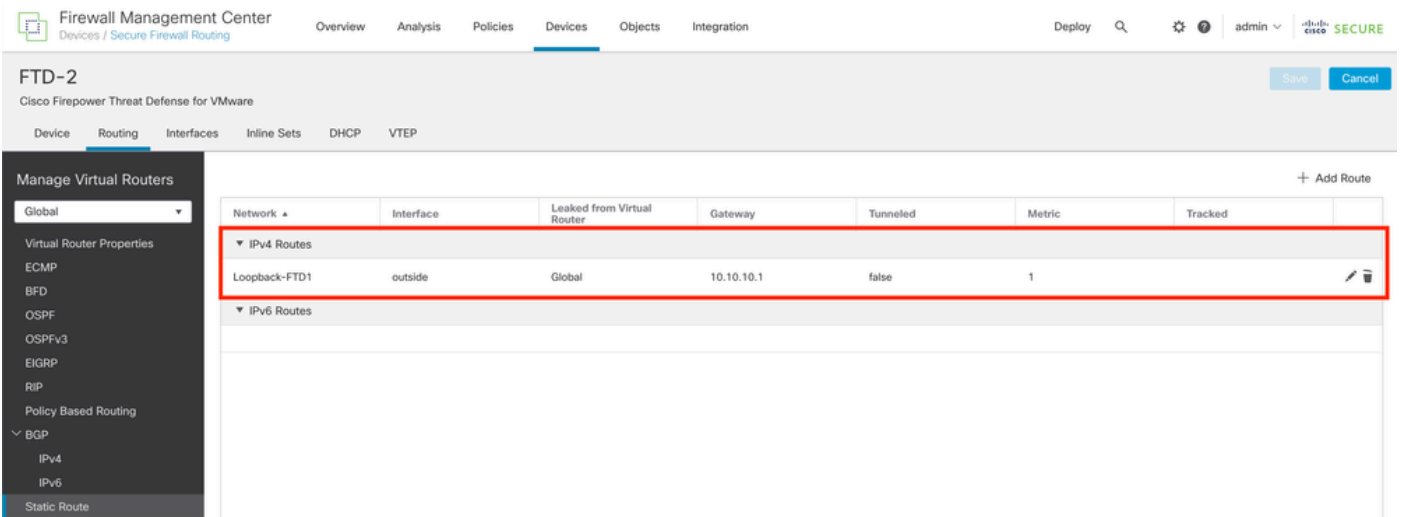
이미지 11. 고정 경로에서 다음 홉 구성

7단계. 저장을 클릭합니다.



이미지 12. 고정 경로 인터페이스 컨피그레이션 저장

8단계. 두 번째 방화벽으로 프로세스를 반복합니다.



이미지 13. 피어에서 고정 경로 구성

## BGP 컨피그레이션

1단계. Devices > Device Management를 클릭하고 BGP를 활성화할 디바이스를 선택합니다.

2단계. Routing(라우팅) > Manage Virtual Routers(가상 라우터 관리) > General Settings(일반 설정)를 클릭한 다음 BGP를 클릭합니다.

3단계. Enable BGP(BGP 활성화) 상자를 선택한 다음 AS Number(AS 번호) 섹션에 방화벽의 로컬 AS를 구성합니다.

### FTD-1

Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets 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\*  
64000

(1-4294967295 or 1.0-65535.65535)

Override BGP general settings router-id address:

Router Id  
Automatic

IP Address\*

#### General

Scanning Interval	60
Number of AS numbers in AS_PATH attribute of received routes	None
Log Neighbor Changes	Yes
Use TCP path MTU discovery	Yes
Reset session upon failover	Yes
Enforce the first AS is peer's AS for EBGp routes	Yes
Use dot notation for AS number	No
Aggregate Timer	30

#### Best Path Selection

Default local preference	100
--------------------------	-----

#### Neighbor Timers

Keepalive Interval	
Hold time	
Min hold time	

#### Next Hop

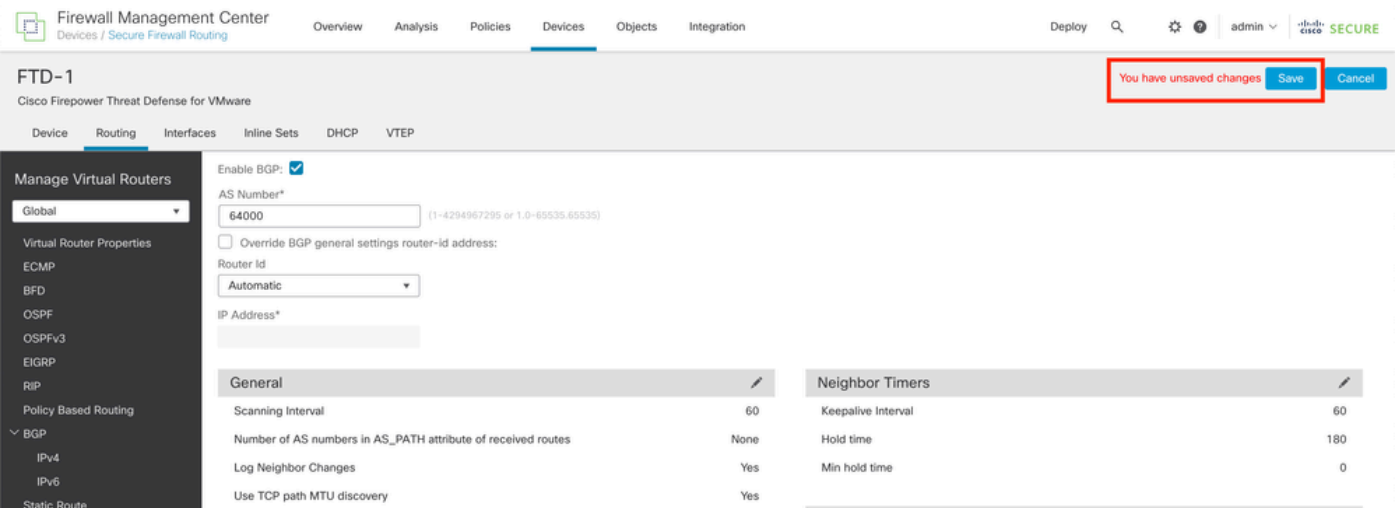
Address tracking	
Delay interval	

#### Graceful Restart (use in f

Graceful Restart	
Restart time	

이미지 14. BGP 전역 활성화

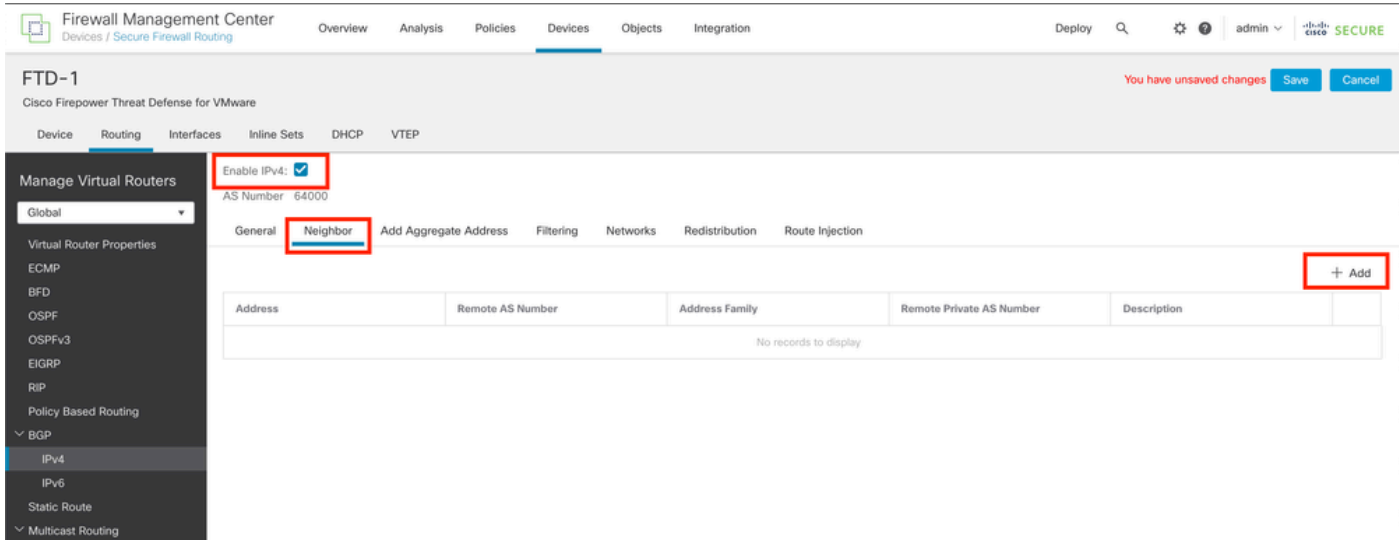
4단계. Save(저장) 버튼을 클릭하여 변경 사항을 저장합니다.



이미지 15. BGP Enable Change 저장

5단계. Manage Virtual Routers 섹션에서 BGP 옵션으로 이동한 다음 IPv4를 클릭합니다.

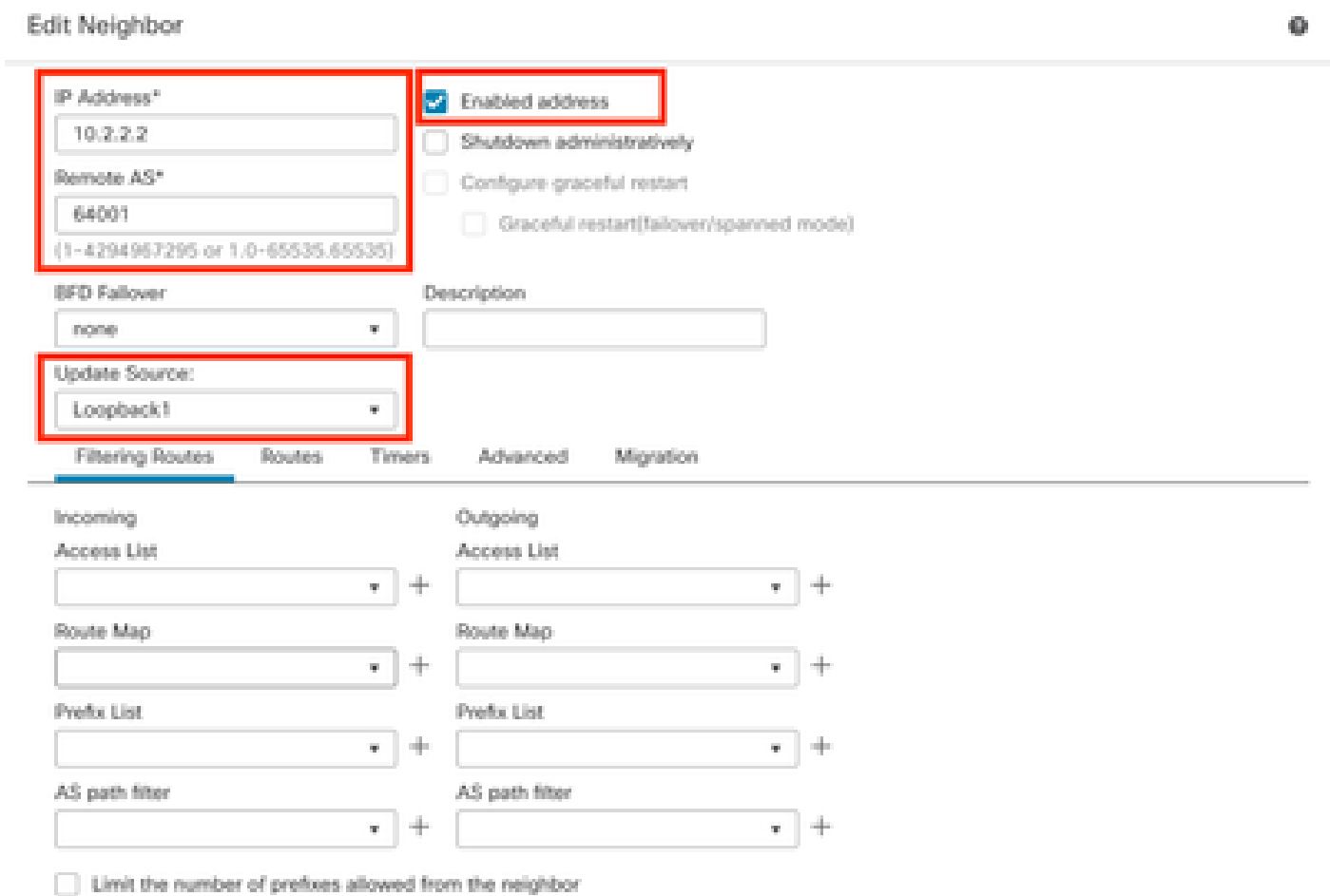
6단계. Enable IPv4(IPv4 활성화) 상자를 선택하고 Neighbor(인접 디바이스)를 클릭한 다음 + Add(추가)를 클릭합니다.



이미지 16. 새 BGP 피어 추가

7단계. IP Address(IP 주소) 섹션에서 원격 피어의 IP 주소를 구성한 다음, Remote AS(원격 AS) 섹션에서 원격 피어의 AS를 구성하고 Enable address(주소 활성화) 상자를 선택합니다.

8단계. Update Source(소스 업데이트) 섹션에서 로컬 인터페이스 루프백을 선택합니다.



이미지 17. 기본 BGP 피어 매개변수

 참고: Update Source 옵션은 neighbor update-source 명령을 활성화하며, 이는 모든 운영 인

터페이스(루프백 포함)를 허용하는 데 사용됩니다. TCP 연결을 설정하기 위해 이 명령을 지정할 수 있습니다.

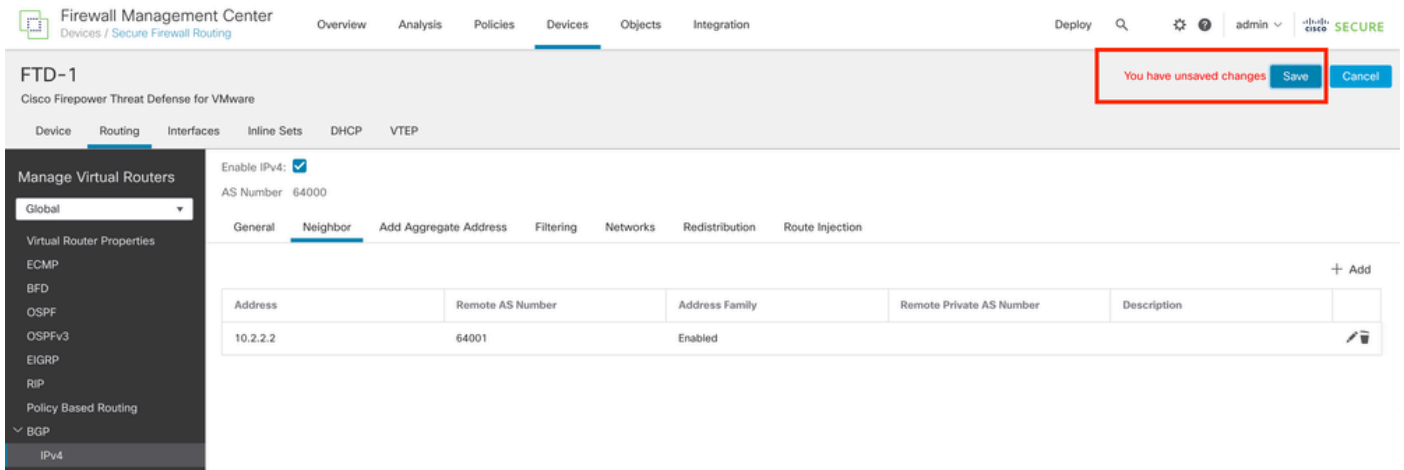
9단계. Advanced(고급)를 클릭한 다음 TTL Hops(TTL 홉) 옵션에서 숫자 2를 구성하고 OK(확인)를 클릭합니다.

The screenshot shows the 'Edit Neighbor' configuration window. The 'Advanced' tab is selected and highlighted with a red box. The 'TTL Hops' field is set to '2' and also highlighted with a red box. The 'OK' button at the bottom right is also highlighted with a red box.

이미지 18. TTL 홉 번호 구성

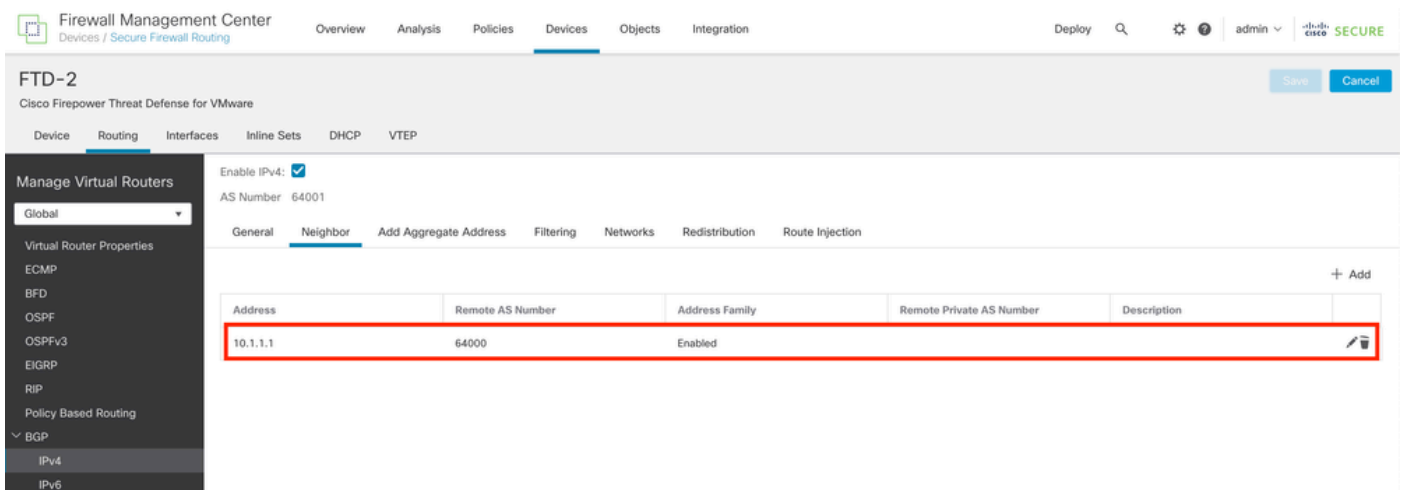
참고: TTL Hops 옵션은 패킷이 직접 연결되지 않았거나 직접 연결된 인터페이스가 아닌 외부 BGP 피어에 도달할 수 있도록 TTL 값을 변경하는 데 사용되는 `ebgp-multihop` 명령을 활성화합니다.

10단계. Save(저장)를 클릭하고 변경 사항을 구축합니다.



이미지 19. BGP 컨피그레이션 저장

11단계. 두 번째 방화벽으로 프로세스를 반복합니다.



이미지 20. 피어에서 BGP 구성

다음을 확인합니다.

1단계. 루프백 및 고정 경로 컨피그레이션을 확인한 다음, ping 테스트를 통해 BGP 피어 간의 연결을 확인합니다.

show running-config interface interface\_name

running-config 경로 표시

show destination\_ip

SFTD-1	SFTD-2
show running-config interface Loopback1 인터페이스 루프백1	show running-config interface Loopback1 인터페이스 루프백1

nameif 루프백1 ip 주소 10.1.1.1 255.255.255.255 running-config 경로 표시 외부 경로 10.2.2.2 255.255.255 10.10.10.2 1 ping 10.2.2.2 5, 100바이트 ICMP Echo를 10.2.2.2로 보내는 경우 시간 초과는 2초입니다. !!!! 성공률은 100%(5/5), 왕복 최소/평균/최대 = 1/1/1ms	nameif Looback2 ip 주소 10.2.2.2 255.255.255.255 running-config 경로 표시 외부 경로 10.1.1.1 255.255.255 10.10.1 1 ping 10.1.1.1 10.1.1.1에 5, 100바이트 ICMP 에코 보내기, 시간 제한은 2초입니다. !!!! 성공률은 100%(5/5), 왕복 최소/평균/최대 = 1/1/1ms
---	---

2단계. BGP 컨피그레이션을 확인한 다음 BGP 피어링이 설정되었는지 확인합니다.

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2
show running-config router bgp 라우터 bgp 64000 bgp 로그 인접 디바이스 변경 bgp router-id vrf auto-assign 주소군 ipv4 유니캐스트 neighbor 10.2.2.2 remote-as 64001 neighbor 10.2.2.2 ebgp-multihop 2 네이버 10.2.2.2 전송 경로 mtu 검색 비활성화 네이버 10.2.2.2 update-source 루프백1 네이버 10.2.2.2 활성화 자동 요약 없음	show running-config router bgp 라우터 bgp 64001 bgp 로그 인접 디바이스 변경 bgp router-id vrf auto-assign 주소군 ipv4 유니캐스트 neighbor 10.1.1.1 remote-as 64000 neighbor 10.1.1 ebgp-multihop 2 인접 디바이스 10.1.1.1 전송 경로 mtu-discovery disable 인접 디바이스 10.1.1.1 update-source Looback2 네이버 10.1.1.1 활성화



<p>동기화 안 함</p> <p>출구 주소군</p> <p>!</p> <p>show bgp neighbors   i BGP</p> <p>BGP 인접 디바이스 10.2.2.2, vrf single_vf, 원격 AS 64001, 외부 링크</p> <p>BGP 버전 4, 원격 라우터 ID 10.2.2.2</p> <p>BGP 상태 = Established, 최대 1d15h</p> <p>BGP 테이블 버전 7, 인접 디바이스 버전 7/0</p> <p>외부 BGP 인접 디바이스는 최대 2홉 거리에 있을 수 있습니다.</p> <p>show bgp summary</p> <p>BGP 라우터 식별자 10.1.1.1, 로컬 AS 번호 64000</p> <p>BGP 테이블 버전은 7, 기본 라우팅 테이블 버전은 7입니다.</p> <p>네이버 V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd</p> <p>10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0</p>	<p>자동 요약 없음</p> <p>동기화 안 함</p> <p>출구 주소군</p> <p>!</p> <p>show bgp neighbors   i BGP</p> <p>BGP 인접 디바이스 10.1.1.1, vrf single_vf, 원격 AS 64000, 외부 링크</p> <p>BGP 버전 4, 원격 라우터 ID 10.1.1.1</p> <p>BGP 상태 = Established, 최대 1d16h</p> <p>BGP 테이블 버전 1, 인접 디바이스 버전 1/0</p> <p>외부 BGP 인접 디바이스는 최대 2홉 거리에 있을 수 있습니다.</p> <p>show bgp summary</p> <p>BGP 라우터 식별자 10.2.2.2, 로컬 AS 번호 64001</p> <p>BGP 테이블 버전이 1, 기본 라우팅 테이블 버전 1임</p> <p>네이버 V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd</p> <p>10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0</p>
--	--

## 문제 해결

프로세스 중에 문제가 발생하는 경우 다음 문서를 검토하십시오.

· [BGP\(Border Gateway Protocol\)](#)

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.