

Secure Firewall Threat Defense에서 BGP 다중 경로 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[다이어그램](#)

[BGP 컨피그레이션](#)

[BGP 다중 경로 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[질문과 대답](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure Firewall Threat Defense에서 BGP(Border Gateway Protocol) 다중 경로를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Secure Firewall Threat Defense)의 BGP 컨피그레이션
- 일반 BGP
- Cisco FMC(Secure Firewall Management Center)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 버전 7.6
- Cisco FMC 버전 7.6

경고문: 이 문서에서 참조하는 네트워크 및 IP 주소는 개별 사용자, 그룹 또는 조직과 연결되어 있지 않습니다. 이 컨피그레이션은 랩 환경에서만 사용하도록 만들어졌습니다.

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

이 문서에서는 동일한 AS(예: 동일한 ISP)의 다른 라우터에서 동일한 대상에 대한 경로를 수신할 때 Firepower Threat Defense에서 BGP 다중 경로 로드 공유를 구성하는 방법에 대해 설명합니다.

BGP Multipath는 동일한 대상 접두사에 대한 여러 동일 비용 BGP 경로의 IP 라우팅 테이블에 설치를 허용합니다. 목적지 접두사로 가는 트래픽은 설치된 모든 경로에서 공유됩니다.

이러한 경로는 로드 공유를 위한 최상의 경로와 함께 라우팅 테이블에 추가됩니다. BGP 다중 경로는 최적의 경로를 선택하는 프로세스에 영향을 주지 않습니다. 예를 들어, FTD는 알고리즘을 기반으로 한 최상의 경로 하나를 선택하고 이 최상의 경로를 BGP 피어에 광고합니다.

다중 경로의 후보로 적합하려면 동일한 대상에 대한 경로가 다음 특성에서 최상의 경로와 일치해야 합니다.

- 무게
- 로컬 기본 설정
- AS-PATH 길이
- 오리진 코드
- MED(다중 출구 판별기)

다음 중 하나:

- 인접 AS 또는 하위 AS(BGP 다중 경로 추가 이전)
- AS-PATH(BGP 다중 경로 추가 이후)

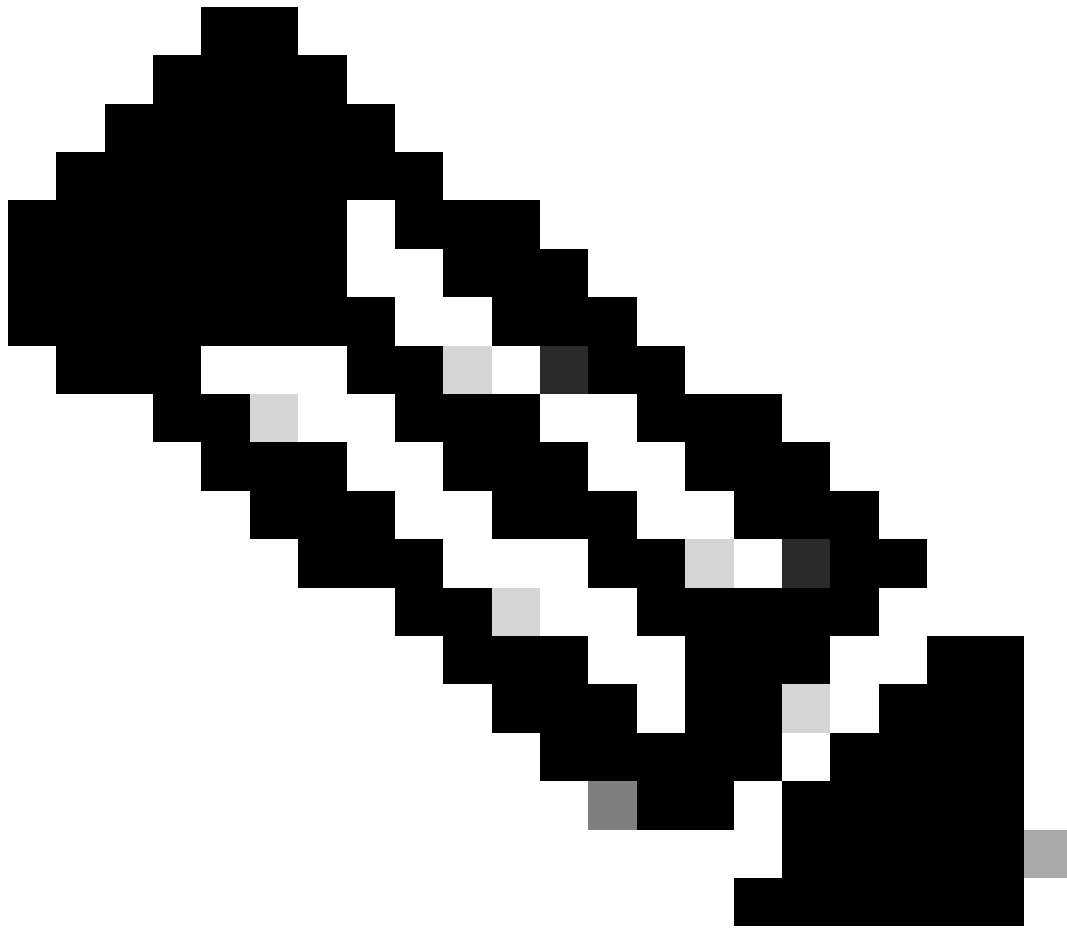
특정 BGP 다중 경로 기능은 다중 경로 후보에 추가적인 요구 사항을 부과합니다.

- 경로는 외부 또는 eBGP(Confederation-External Neighbor)에서 시작해야 합니다.
- BGP next hop에 대한 IGP 메트릭은 최적 경로의 IGP 메트릭과 일치해야 합니다.

iBGP(internal BGP) 다중 경로 후보의 경우 다음과 같은 추가 요구 사항이 적용됩니다.

- 경로는 내부 인접 라우터(iBGP)에서 확인되어야 합니다.
- BGP next hop에 대한 IGP 메트릭은 라우터가 unequal-cost iBGP 다중 경로에 대해 설정되지 않는 한 최상의 경로 IGP 메트릭과 일치해야 합니다.

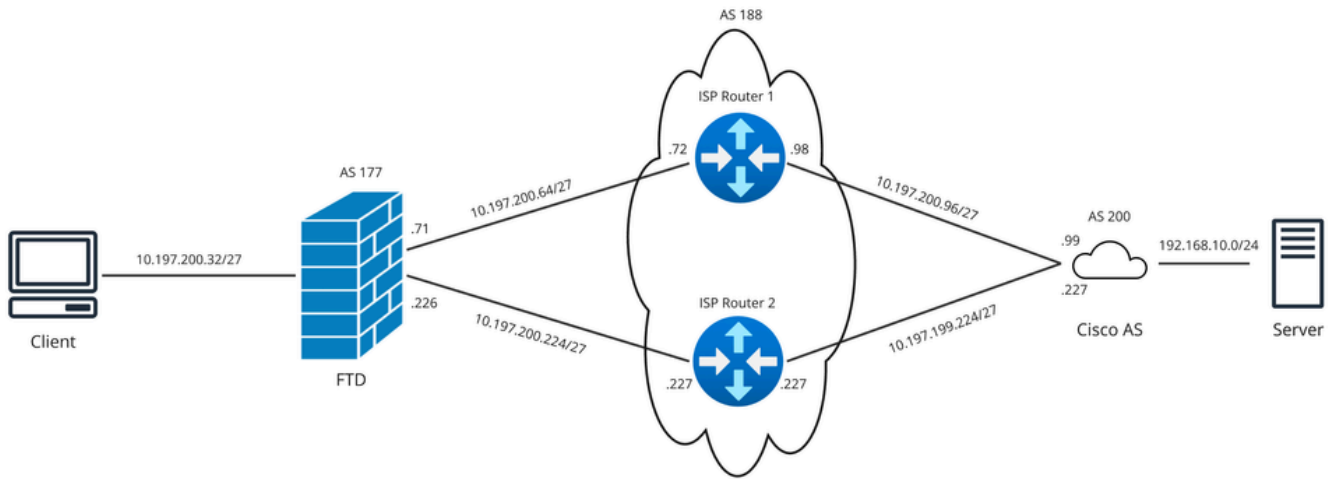
BGP는 다중 경로 후보에서 가장 최근에 수신한 경로를 n개까지 IP 라우팅 테이블에 삽입합니다. 여기서 n은 BGP 다중 경로를 구성할 때 지정한 대로 라우팅 테이블에 설치할 경로의 수입니다. n의 값 범위는 FTD의 경우 1~8입니다. 다중 경로가 비활성화된 경우 기본값은 1입니다.



참고: 동일한 next-hop-self는 내부 피어에 전달되기 전에 eBGP 다중 경로 중에서 선택된 최적의 경로에서 수행됩니다.

구성

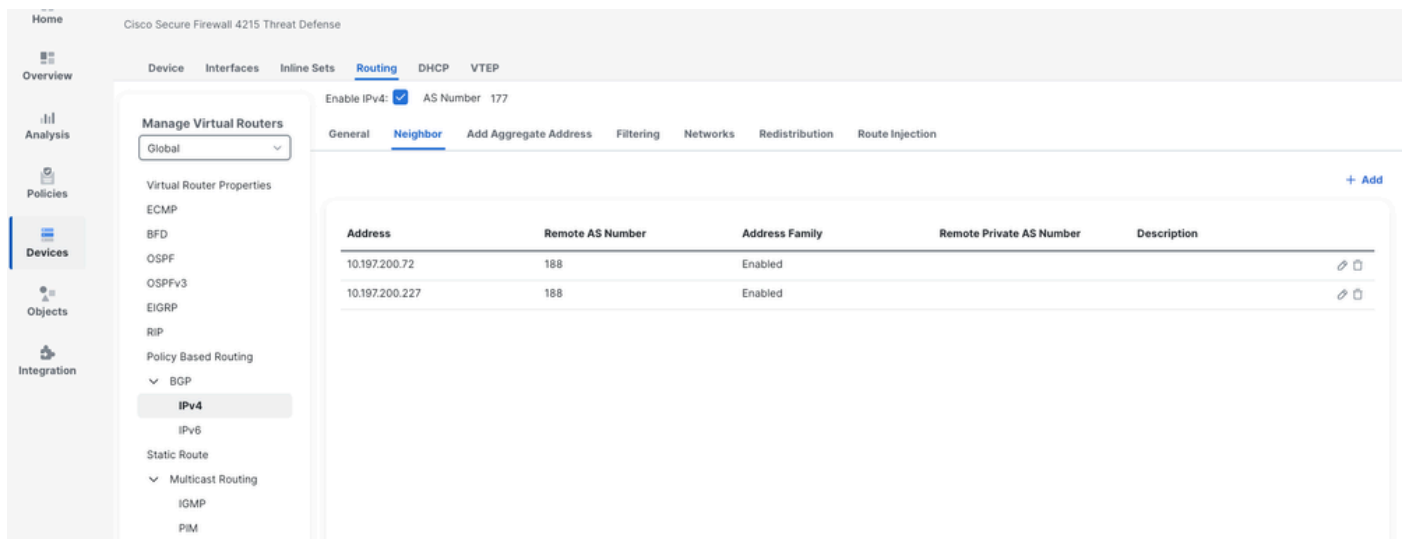
다이어그램



네트워크 다이어그램

BGP 컨피그레이션

BGP를 활성화한 후 Devices > Device management > Edit Device > Routing > BGP > IPv4로 이동하여 BGP를 구성합니다.



BGP 컨피그레이션

LINA의 BGP 컨피그레이션:

```
router bgp 177
  bgp log-neighbor-changes
  bgp router-id 1.1.x.x
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.197.200.72 remote-as 188
    neighbor 10.197.200.72 transport path-mtu-discovery disable
    neighbor 10.197.200.72 activate
    neighbor 10.197.200.227 remote-as 188
    neighbor 10.197.200.227 transport path-mtu-discovery disable
    neighbor 10.197.200.227 activate
  no auto-summary
```

```
no synchronization
exit-address-family
!
```

다음과 같은 두 BGP 인접 디바이스:

```
ftd1# show bgp summary
BGP router identifier 1.1.x.x, local AS number 177
BGP table version is 9, main routing table version 9
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 40 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 968 total bytes of memory
BGP activity 4/2 prefixes, 10/6 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.197.200.72	4	188	67	66	9	0	0	01:10:15	1
10.197.200.227	4	188	60	60	9	0	0	01:00:56	1

동일한 목적지 네트워크에 대해 각 네이버에서 하나씩 2개의 유효한 경로를 수신했습니다.

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 9
Paths: (2 available, best #2, table default)
  Advertised to update-groups: 3
  188 200
    10.197.200.227 from 10.197.200.227 (3.3.x.x)
      Origin incomplete, localpref 100, valid, external
  188 200
    10.197.200.72 from 10.197.200.72 (2.2.x.x)
      Origin incomplete, localpref 100, valid, external, best
```

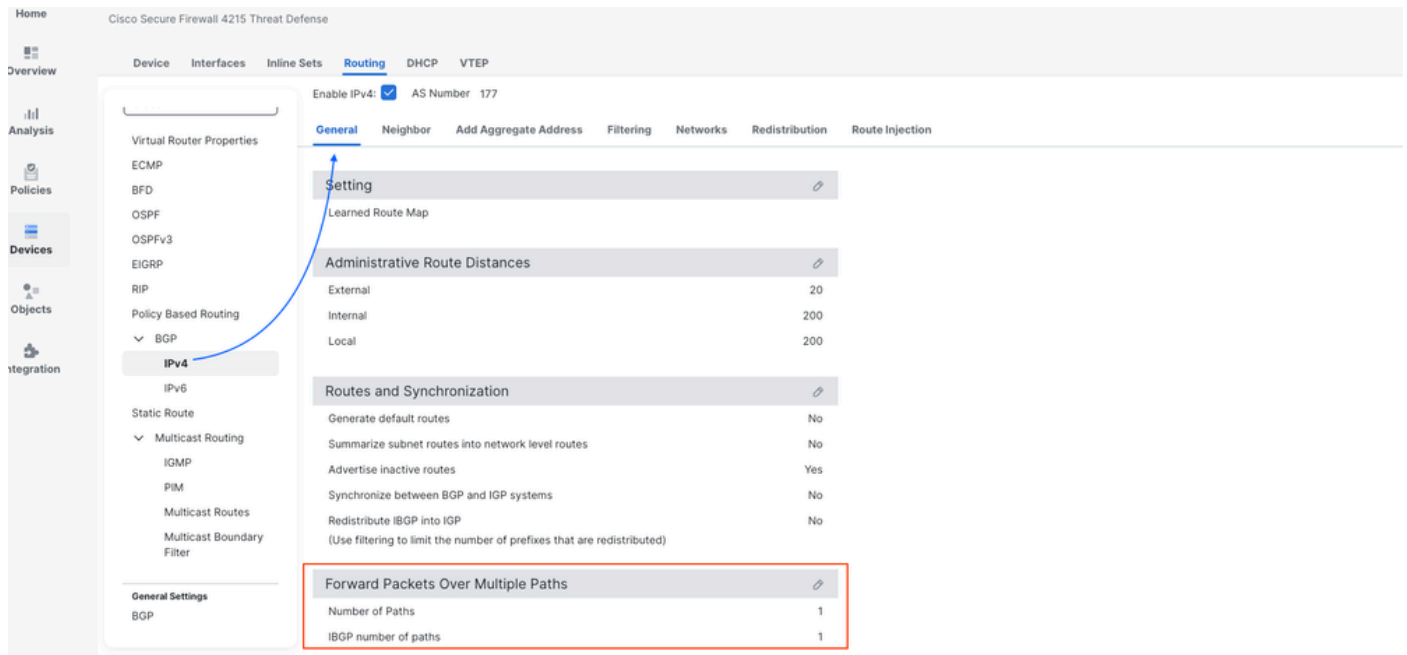
라우팅 테이블에서 선택 및 설치되는 최상의 경로는 네이버 10.197.200.72에서 수신하는 경로입니다.

```
ftd1# 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
Gateway of last resort is not set
```

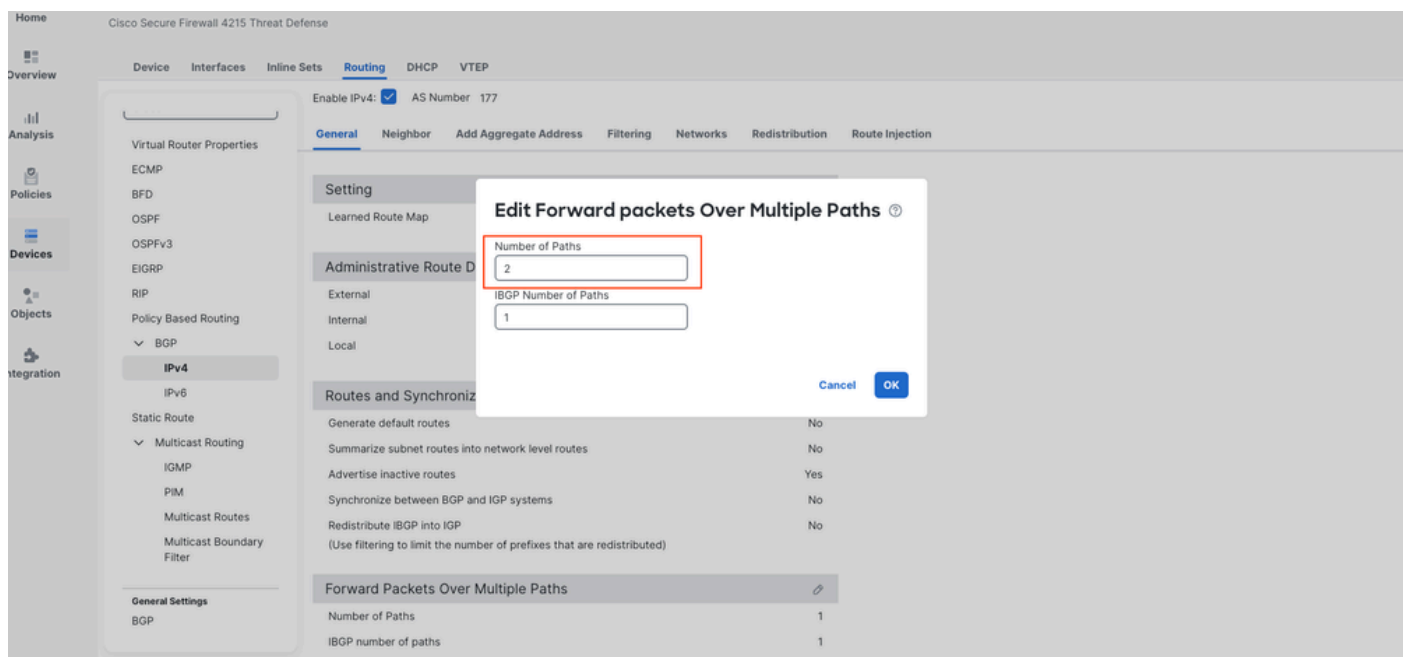
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.72, 00:01:55

BGP 다중 경로 컨피그레이션

Devices(디바이스) > Device management(디바이스 관리) > Edit Device(디바이스 수정) > Routing(라우팅) > BGP > IPv4 > Edit Forward Packets Over Multiple Paths(다중 경로를 통한 전달 패킷 수정)에서 BGP 다중 경로를 구성합니다.



FMC의 BGP 다중 경로



FMC의 BGP 다중 경로

변경 사항을 저장하고 구축합니다.

다음을 확인합니다.

다중 경로를 활성화한 후 LINA에서 BGP 컨피그레이션:

<#root>

```
ftd1# sh run router
router bgp 177
bgp log-neighbor-changes
bgp router-id 1.1.x.x
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 10.197.200.72 remote-as 188
neighbor 10.197.200.72 transport path-mtu-discovery disable
neighbor 10.197.200.72 activate
neighbor 10.197.200.227 remote-as 188
neighbor 10.197.200.227 transport path-mtu-discovery disable
neighbor 10.197.200.227 activate
```

maximum-paths 2

```
no auto-summary
no synchronization
exit-address-family
```

다중 경로를 나타내는 경로 중 하나 앞에 m이 있습니다

<#root>

```
ftd1# show bgp
```

```
BGP table version is 11, local router ID is 1.1.x.x
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 192.168.10.0 10.197.200.227 0 188 200 ?
```

```
*> 10.197.200.72 0 188 200 ?
```

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 11
Paths: (2 available, best #2, table default)
Multipath: eBGP
Advertised to update-groups: 3
188 200
10.197.200.227 from 10.197.200.227 (3.3.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

```
188 200
10.197.200.72 from 10.197.200.72 (2.2.x.x)
Origin incomplete, localpref 100, valid, external,
multipath
, best
```

BGP 다중 경로를 활성화한 후 라우팅 테이블에 설치된 동일한 대상에 대한 두 가지 경로가 있습니다.

<#root>

```
ftd1# 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
Gateway of last resort is not set
```

```
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.227, 00:01:17
```

```
[20/0] via 10.197.200.72, 00:01:17
```

문제 해결

1. BGP 컨피그레이션 확인:

show bgp 명령을 사용하여 BGP 테이블을 확인하고 여러 경로가 multipat로 표시되는지 확인합니다.

Number of Paths가 여러 경로를 허용하도록 구성되었는지 확인합니다.

2. 경로 속성 확인:

경로에 다중 경로에 필요한 동일한 BGP 특성이 있는지 확인합니다. 가중치, 로컬 환경 설정, AS 경로 길이 등과 같은 작업을 수행할 수 있습니다.

3. 부하 공유 확인:

show route 명령을 사용하여 경로가 로드 공유에 사용되고 있는지 확인합니다. 출력에는 동일한 대상에 대한 여러 경로가 표시되어야 합니다.

질문과 대답

1. bgp bestpath as-path multipath-relax 명령은 Flex config를 통한 FTD에서 로드 공유를 지원합니까?

아니요. FTD/ASA에서 이 기능이 지원되기 위한 향상된 기능이 이미 있습니다. Cisco 버그 ID [CSCvw16654](#)

관련 정보

[일반적인 BGP 문제 해결](#)

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.