보안 방화벽에서 BGP AS 재정의 구성

목차

소개

이 문서에서는 Cisco Secure Firewall Threat Defense에서 BGP AS(Autonomous System) 재정의를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- BGP(Border Gateway Protocol)
- 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.

- 버전 7.7.0을 실행하는 Cisco Secure Firewall Management Center

- 버전 7.7.0을 실행하는 Cisco Secure Firewall Threat Defense

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

지리적으로 분산된 위치를 가진 대기업의 경우 여러 사이트가 동일한 AS(Autonomous System) 번호를 사용할 때 엔드 투 엔드 연결을 달성하는 것이 어려울 수 있습니다. 현재 BGP 동작은 AS 경로에 자체 AS 번호가 포함된 경우 수신된 라우팅 업데이트를 삭제하여 네트워크에서 루프를 방지하는 것입니다.

7.6 릴리스에서는 특별히 SD-WAN 관련 활용 사례에 대한 as-override 지원을 도입했습니다. 그러나 7.7 릴리스부터는 핵심 라우팅 요구 사항으로 인해 모든 구축에서 eBGP에 대한 as-override 지원을 사용할 수 있습니다. 이렇게 하면 동일한 AS 번호를 가진 동일한 사이트를 가질 수 있습니다.

애플리케이션 및 관리자:

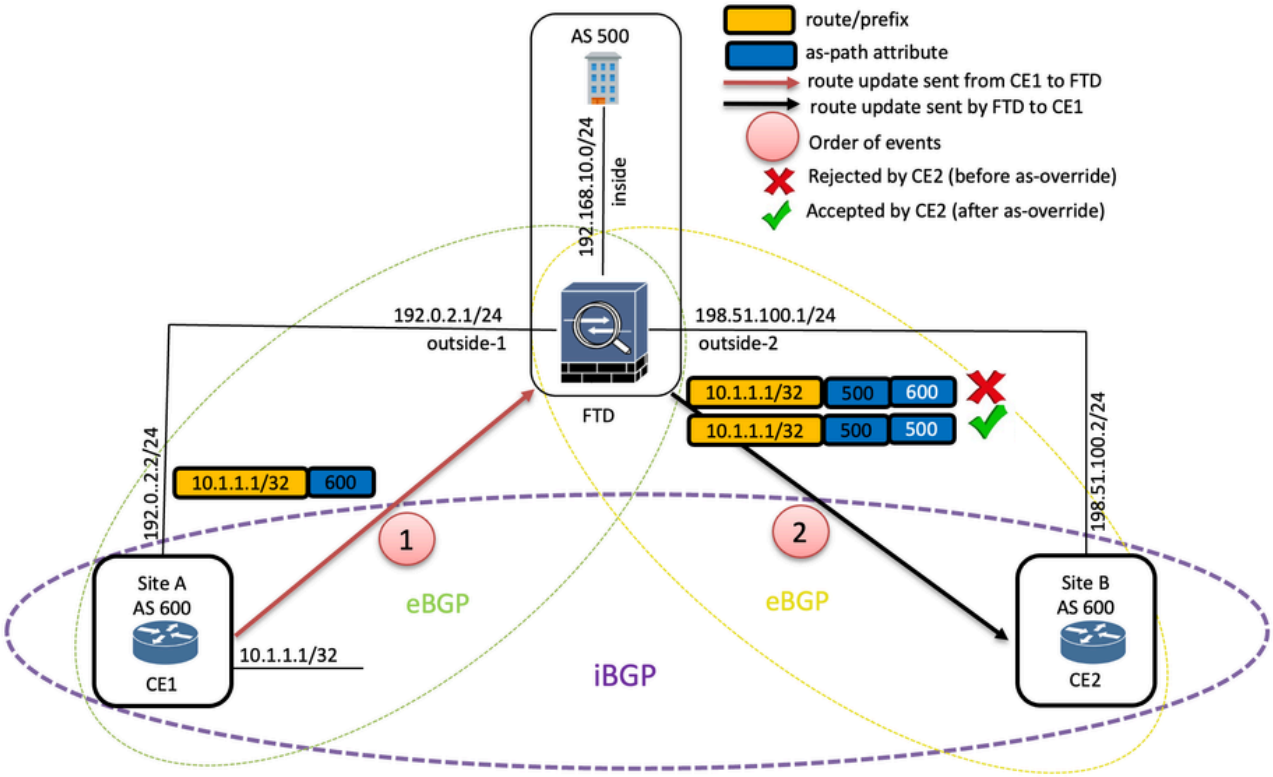
FTD	모든 FTD 플랫폼
7.7.0의 FMC FMC REST API	예 예
FTD 지원 버전	7.7.0만 해당
Snort 지원	Snort 3
FDM on 7.7.0	지원되지 않음

BGP AS 재정의 패킷 처리 흐름

- BGP는 UPDATE 메시지를 통해 피어/네이버에 경로 업데이트를 전송합니다.
- 잘 알려진 필수 특성은 모든 BGP 피어에서 인식되고 모든 피어에 전달되며 모든 UPDATE 메시지에 표시됩니다.
- UPDATE 메시지의 AS-path 특성에는 이 업데이트가 통과한 모든 자율 시스템의 순서가 지정된 목록이 포함되어 있습니다.
- as-override CLI가 활성화된 경우 인접 디바이스 AS 번호가 발생할 때마다 as-path의 로컬 AS 번호로 교체됩니다.

구성

네트워크 다이어그램



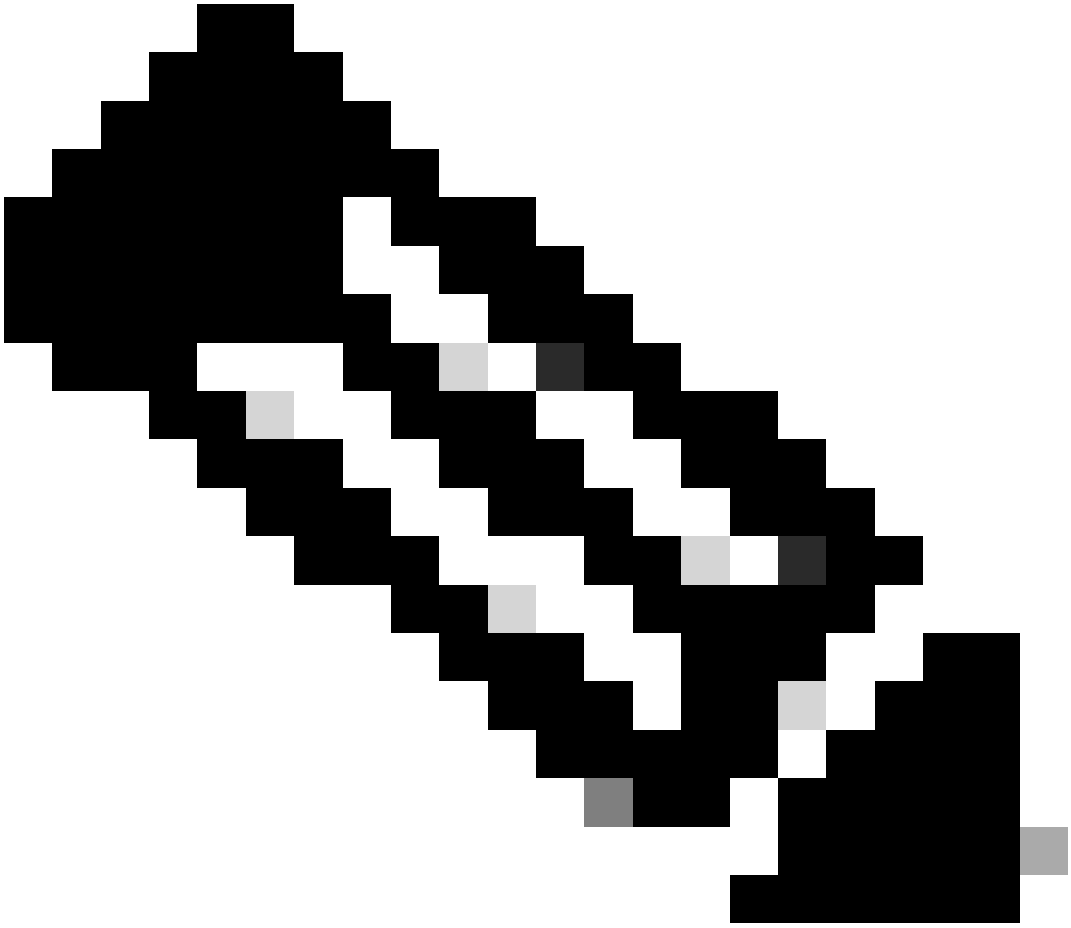
토폴로지

경로 업데이트 흐름

- 사이트 A와 사이트 B는 동일한 AS 번호의 디바이스/피어를 포함하는 동일한 사이트 두 개입니다.
- 이 경우 10.1.1.1/32은 FTD를 통해 사이트 A의 CE1에서 사이트 B의 CE2로 광고되는 접두사/경로 업데이트입니다.
- as-override를 활성화하기 전에 FTD는 경로 업데이트를 현재 상태 그대로 사이트 B의 CE2에 전달합니다. 그러나 CE2가 수신되면 as-path(600)에서 자체 AS 번호가 표시되므로 경로 업데이트를 취소합니다.
- as-override를 활성화한 후 FTD는 as-path의 CE1 AS 번호를 자체/로컬 AS 번호(500)로 대체하여 경로 업데이트를 CE2로 전달합니다. 이제 CE2에서 경로 업데이트를 수락합니다.

기능 개요

- AS 재정의를 활성화하기 위한 FMC의 새 확인란.
- 새 CLI 명령 neighbor <neighbor-ip-address> as-overrides가 이 기능의 일부로 BGP에 도입되었습니다.



참고: BGP AS Override 기능은 FMC(Secure Firewall Management Center)를 통해서만 컨피그레이션에 사용할 수 있습니다.

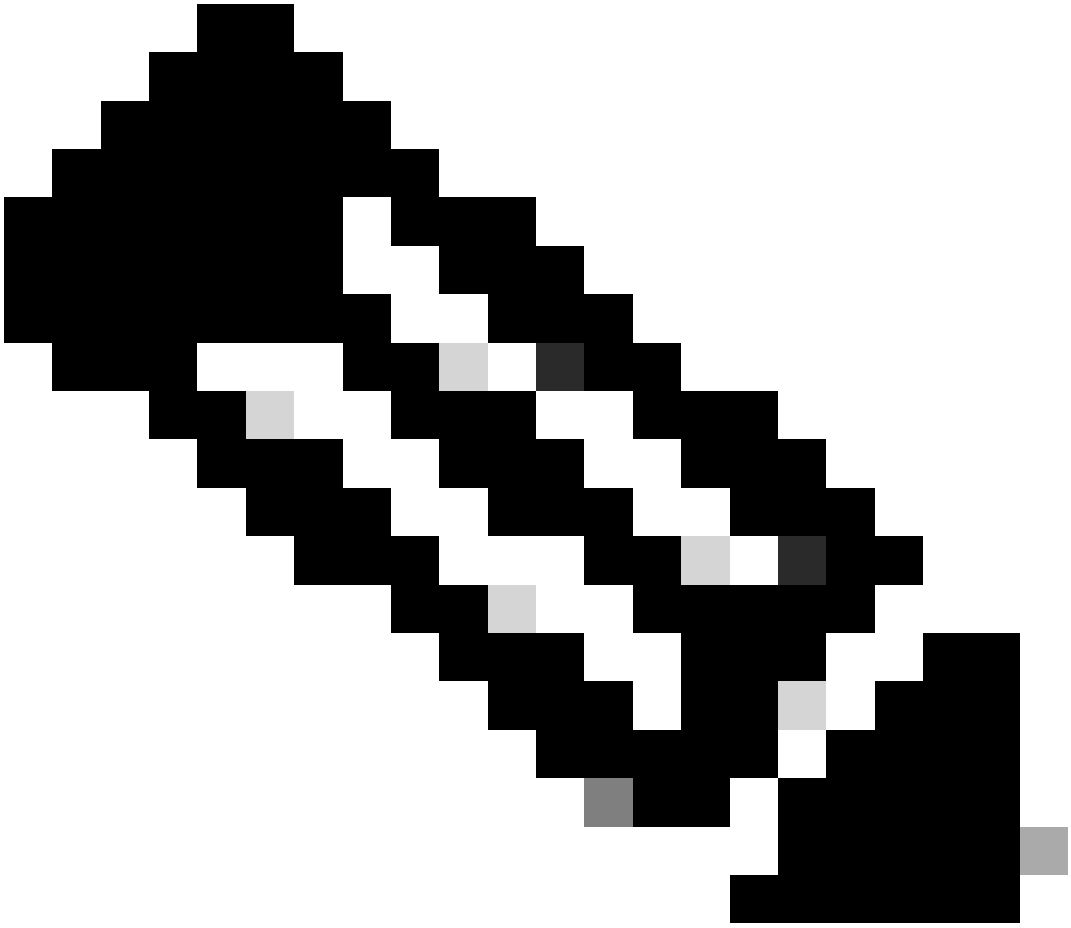
FMC의 컨피그레이션 단계

1단계: Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 위협 방어 디바이스를 수정합니다.

2단계: 라우팅을 선택합니다.

3단계: (가상 라우터 인식 디바이스의 경우) General Settings(일반 설정)에서 BGP를 클릭합니다.

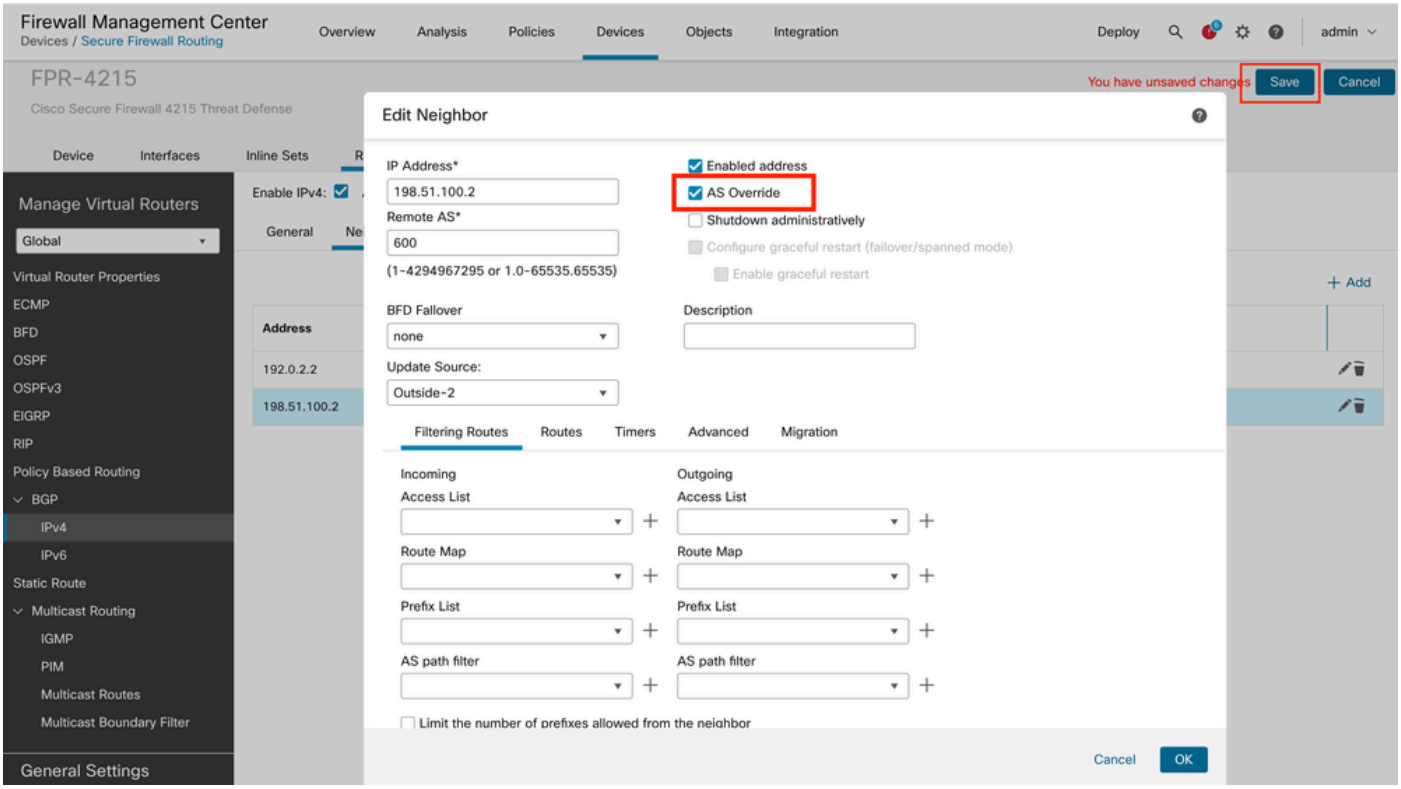
4단계: BGP 라우팅 프로세스를 활성화하려면 Enable BGP 확인란을 선택합니다.



참고: BGP 라우팅을 구성하려면 Cisco Secure Firewall Management Center Device Configuration Guide, 7.7을 참조하십시오

BGP IPv4 인접 디바이스

- 198.51.100.2 네이버에 대해 AS 재정의를 활성화합니다.
- 저장 및 배포를 클릭합니다.



AS 재정의 사용

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FTD 종료:

<#root>

FTD# show running-config router bgp all

router bgp 500

 bgp log-neighbor-changes
 address-family ipv4 unicast

(Same applicable for IPv6 as well)

   neighbor 192.0.2.2 remote-as 600
   neighbor 192.0.2.2 update-source Outside-1
   neighbor 192.0.2.2 activate
   neighbor 198.51.100.2 remote-as 600
   neighbor 198.51.100.2 update-source Outside-2
   neighbor 198.51.100.2 activate

   neighbor 198.51.100.2 as-override

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

FTD# show bgp ipv4 unicast neighbors 198.51.100.2

```
BGP neighbor is 198.51.100.2,  vrf single_vf,  remote AS 600, external link
 BGP version 4, remote router ID 198.51.100.2
 BGP state = Established, up for 01:13:02
 Last read 00:00:07, last write 00:00:54, hold time is 180, keepalive interval is 60 seconds
 Neighbor sessions:
  1 active, is not multisession capable (disabled)
 Neighbor capabilities:
   Route refresh: advertised and received(new)
   Four-octets ASN Capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Multisession Capability:
Message statistics:
 InQ depth is 0
 OutQ depth is 0

.


.
For address family: IPv4 Unicast
 Session: 198.51.100.2
 BGP table version 4, neighbor version 4/0
 Output queue size : 0
 Index 5
 5 update-group member
```

Overrides the neighbor AS with my AS before sending updates

```
.
.


Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

FTD# show bgp ipv4 unicast neighbors 198.51.100.2 advertised-routes

```
BGP table version is 4, local router ID is 198.51.100.1
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
*> 10.1.1.1/32     192.0.2.2           0               0  600 i
Total number of prefixes 1
```

수신자 종료:

<#root>

```
As-path for 10.1.1.1/32 prefix/route has been modified from 600 to 500 by FTD (where as-override is enab

Cisco_C1127#show bgp ipv4 unicast


BGP table version is 10, local router ID is 198.51.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   10.1.1.1/32      198.51.100.1                           0

500 500

 i


Cisco_C1127#show bgp ipv4 unicast 10.1.1.1


BGP routing table entry for 10.1.1.1/32, version 10
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1

  500 500


    198.51.100.1 from 198.51.100.1 (198.51.100.1)
    Origin IGP, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0x0
    Updated on Apr 6 2025 17:02:24 UTC
```

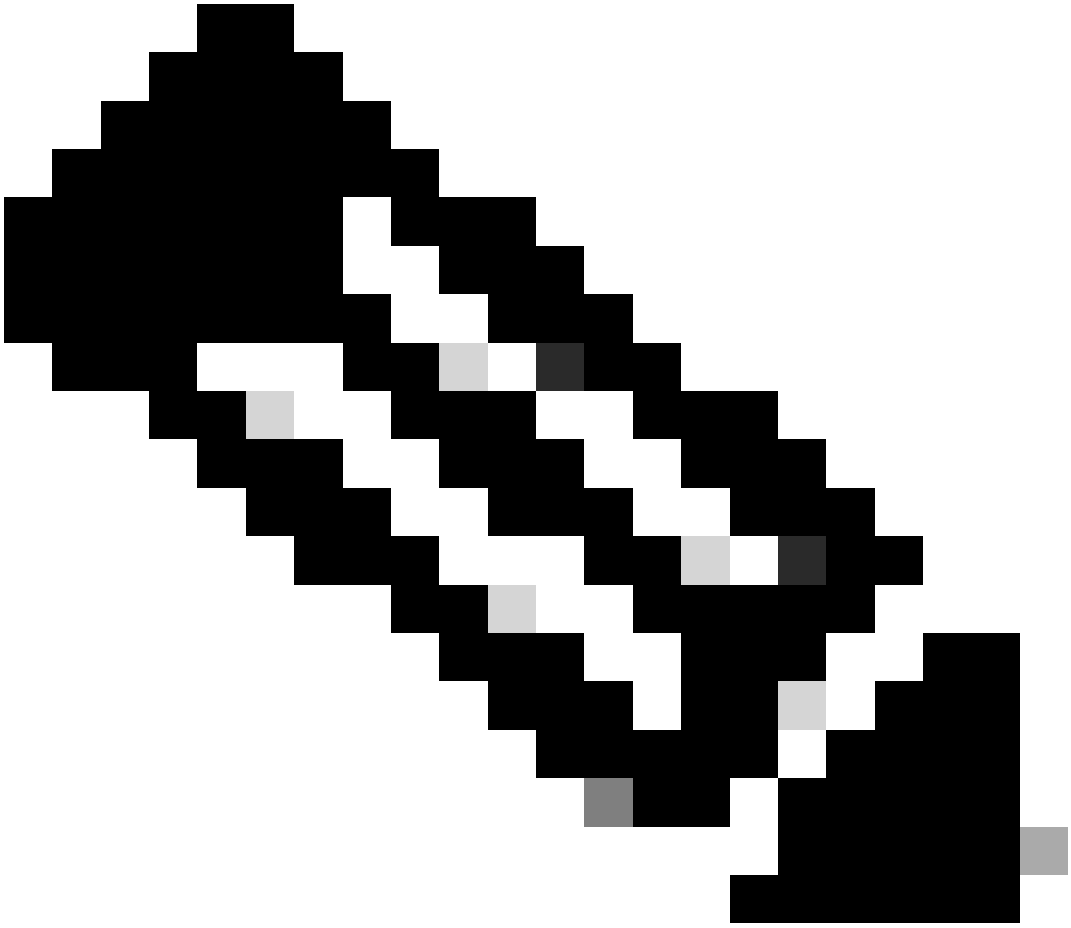
문제 해결

명령

- show run router bgp 모두 FTD에서 AS-override CLI가 활성화되어 있어야 합니다.
- show bgp <ipv4/ipv6> ftd의 유니캐스트 인접 디바이스는 as-override가 활성화되었음을 나타내는 이 텍스트를 지정해야 합니다. -> 업데이트를 전송하기 전에 인접 디바이스 AS를 my AS로 재정의합니다.
- 수신자 측의 show bgp <ipv4/ipv6> 유니캐스트에 변경된 경로 정보가 있어야 합니다.

디버그

```
debug ip bgp updates
debug ip bgp ipv6 unicast updates
debug ip bgp all updates
```



참고: as-override를 활성화하기 전후의 디버그는 변경되지 않습니다.

시스템 파일

이 로그 파일에는 FMC에서 as-override 기능의 구축과 관련된 정보가 포함되어 있습니다.

/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log

<#root>

```
router bgp 500
address-family ipv4 unicast

neighbor 198.51.100.2 as-override


exit-address-family
```

관련 정보

Cisco 기술 지원 및 다운로드

Cisco Secure Firewall Management Center Device Configuration Guide, 7.7

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.