긴급 온디바이스 컨피그레이션에 Recovery-config 모드 사용

목차

소개

이 문서에서는 FTD 7.7 Use Recovery-config Mode for Emergency on-device Configuration에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Firepower 위협 방어)
- Cisco FMC(Firepower 관리 센터)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 7.7.0 이상
- FMC 7.7.0 이상

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

이 기능은 버전 7.7.0에서 도입되었으며 관리 연결이 중단될 때 대역 외 컨피그레이션을 변경하는 데 사용할 수 있습니다.

이러한 컨피그레이션 변경은 디바이스 CLI에서 직접 수행하여 다음을 수행합니다.

- 관리자 액세스에 데이터 인터페이스를 사용하는 경우 관리 연결을 복원합니다.
- 연결이 복원될 때까지 기다릴 수 없는 선택 정책 변경을 수행합니다.

관리 연결이 복원되면

1. 대역 외 컨피그레이션 알림에 표시된 컨피그레이션 차이를 승인해야 합니다.
2. 로컬 변경 사항은 항상 FMC 구축에서 덮어쓰기되므로 구축하기 전에 FMC에서 동일한 변경 사항을 수행합니다.

recovery-config 모드의 진단 CLI에서 다음 기능 영역을 구성할 수 있습니다.

- 인터페이스
- 고정 경로
- 동적 라우팅: BGP 및 OSPF
- 사전 필터
- 사이트 대 사이트 VPN

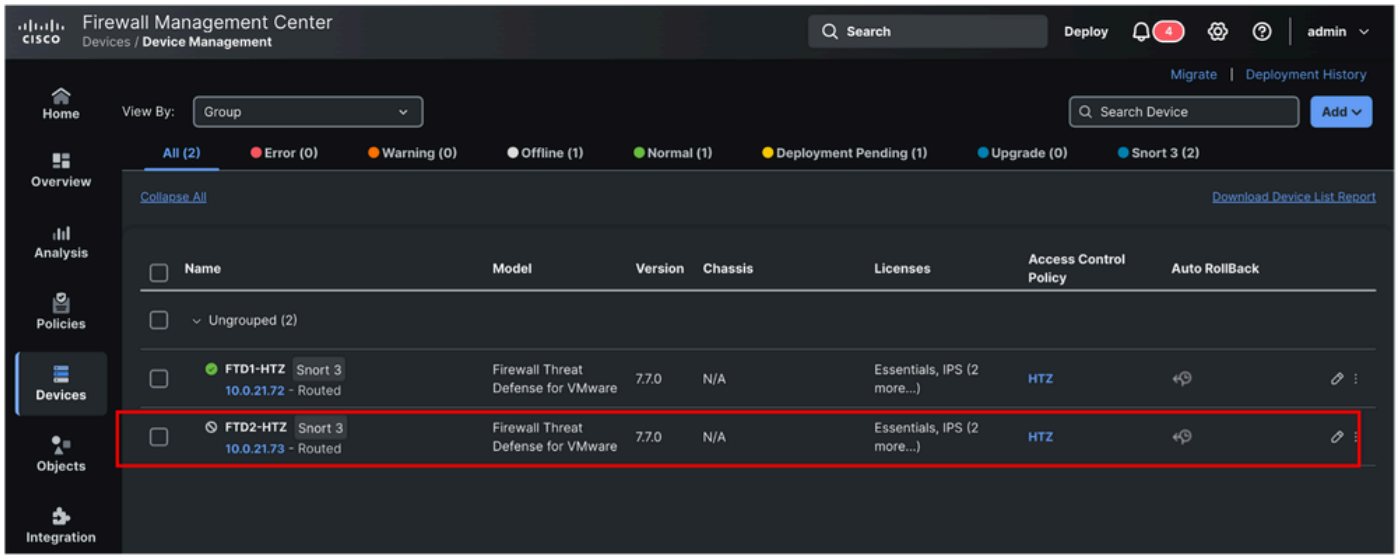
컨피그레이션 예시

실습 배경

이 시나리오에서 FMC에 등록된 FTD 디바이스(데이터 인터페이스를 관리 인터페이스로 사용)가 관리 연결을 상실했으며, 이 문제를 해결하기 위해 recovery-config 기능을 사용하여 FTD에 고정 경로가 추가됩니다.

FMC에는 2개의 위협 방어 디바이스가 등록되어 있지만(10.0.21.72 및 10.0.21.73) 다음 이미지(cli 및 GUI)에 표시된 대로 그중 하나만 연결할 수 있습니다.

```
root@FMC-HTZ:/Volume/home/admin# netstat -tan | grep -i 8305
tcp        0      0 10.0.21.71:8305         0.0.0.0:*               LISTEN
tcp        0      0 10.0.21.71:35069        10.0.21.72:8305         ESTABLISHED
tcp        0      0 10.0.21.71:8305         10.0.21.72:37995        ESTABLISHED
root@FMC-HTZ:/Volume/home/admin#
```



FTD는 FMC에 대한 등록 프로세스에 데이터 인터페이스를 사용하고 있습니다.

```
----------------------[ IPv4 ]----------------------
Configuration                 : Manual
Address                       : 7.7.7.11
Netmask                       : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration                 : Disabled

===============[ Proxy Information ]===============
State                         : Disabled
Authentication                : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers                   : [redacted]

Interfaces                    : GigabitEthernet0/2

===============[ GigabitEthernet0/2 ]===============
State                         : Enabled
Link                          : Up
Name                          : outside
MTU                           : 1500
MAC Address                   : 00:50:56:B3:BE:87
----------------------[ IPv4 ]----------------------
Configuration                 : Manual
Address                       : 10.0.21.73
Netmask                       : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration                 : Disabled
```

또한 FTD는 sftunnel을 통해 FMC에 연결하지 않습니다.

```
root@FTD2-HTZ:/home/admin# netstat -tan | grep -i 8305
tcp        0      0 169.254.1.2:8305        0.0.0.0:*               LISTEN
tcp        0      0 7.7.7.11:8305           0.0.0.0:*               LISTEN
tcp6       0      0 fd00:0:0:1::2:8305      :::*                    LISTEN
root@FTD2-HTZ:/home/admin# _
```

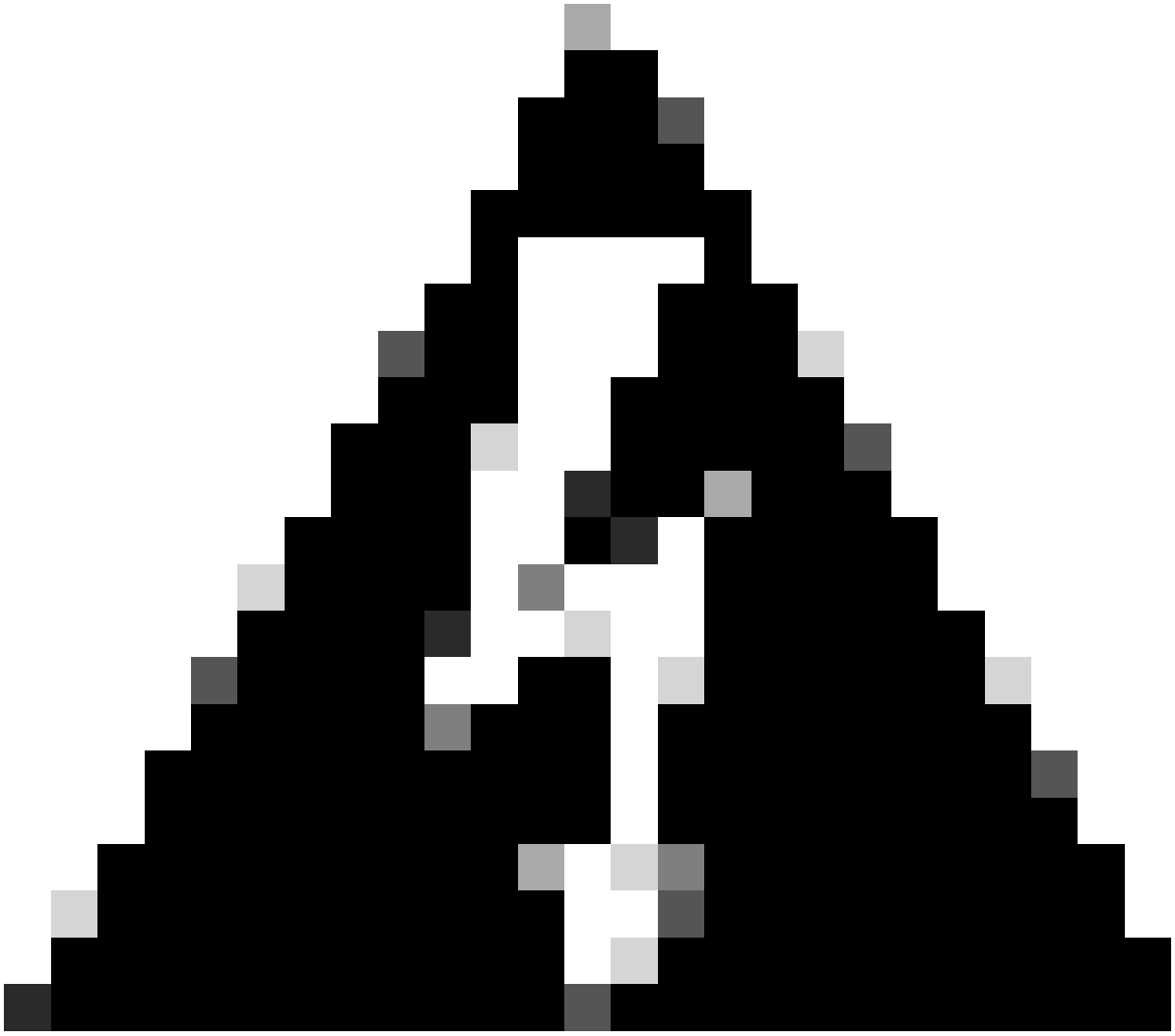
컨피그레이션 단계

1. recovery-config 기능을 사용하려면 FTD CLI에 로그인하고 lina 모드(시스템 지원 진단-cli)로 이동해야 합니다.

2. configure recovery-config 명령을 실행합니다.

3. 물음표(?)를 입력하면 지원되는 모든 명령이 다음 목록에 나와 있습니다.

```
firepower(recovery-config)# ?

  access-list           Configure an access control element
  as-path               BGP autonomous system path filter
  bfd                   BFD configuration commands
  bfd-template          BFD template configuration
  cluster               Cluster configuration
  community-list        Add a community list entry
  crypto                Configure IPSec, ISAKMP, Certification authority, key
  end                   Exit from configure mode
  exit                  Exit from config mode
  extcommunity-list     Add a extended community list entry
  group-policy          Configure or remove a group policy
  interface             Select an interface to configure
  ip                    Configure IP address pools
  ipsec                 Configure transform-set, IPSec SA lifetime and PMTU
                        Aging reset timer
  ipv6                  Configure IPv6 address pools
  ipv6                  Global IPv6 configuration commands
  isakmp                Configure ISAKMP options
  jumbo-frame           Configure jumbo-frame support
  management-interface  Management interface
  mtu                   Specify MTU(Maximum Transmission Unit) for an interface
  no                    Negate a command or set its defaults
  policy-list           Define IP Policy list
  prefix-list           Build a prefix list
  route                 Configure a static route for an interface
  route-map             Create route-map or enter route-map configuration mode
  router                Enable a routing process
  sla                   IP Service Level Agreement
  sysopt                Set system functional options
  tunnel-group          Create and manage the database of connection specific
                        records for IPSec connections
  vpdn                  Configure VPDN feature
  vrf                   Configure a VRF
  zone                  Create or show a Zone
```



경고: 복구 또는 긴급 사용에 필요한 명령을 알아야 합니다. 어떤 명령을 사용해야 할지 잘 모르는 경우 Cisco TAC에 문의하여 지침을 받는 것이 좋습니다.

---

4. configure recovery-config 명령을 실행하면 경고가 표시되고 확인 및 진행하라는 메시지가 표시됩니다.

```
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the ma
nagement center is
unreachable, and use it only under exceptional circumstances, such as loss of co
nnectivity or
to restore manager access. Do not change management center's auto-generated conf
igurations.

 After your management center is reachable, manually make the same configuration
 changes in the
management center. The management center cannot implement them automatically. Wh
en you deploy
from the management center, out-of-band configuration changes will be overwritte
n. Also, node join
will be blocked till config CLI session is active, so make sure to exit from the
 config CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: _
```

5. 확인했으면 사용 가능한 config 명령을 사용할 수 있습니다. 이 시나리오에서는 고정 경로가 외부 인터페이스에 추가됩니다. 컨피그레이션이 완료되면 exit 명령을 실행하여 복구 모드를 종료합니다 .

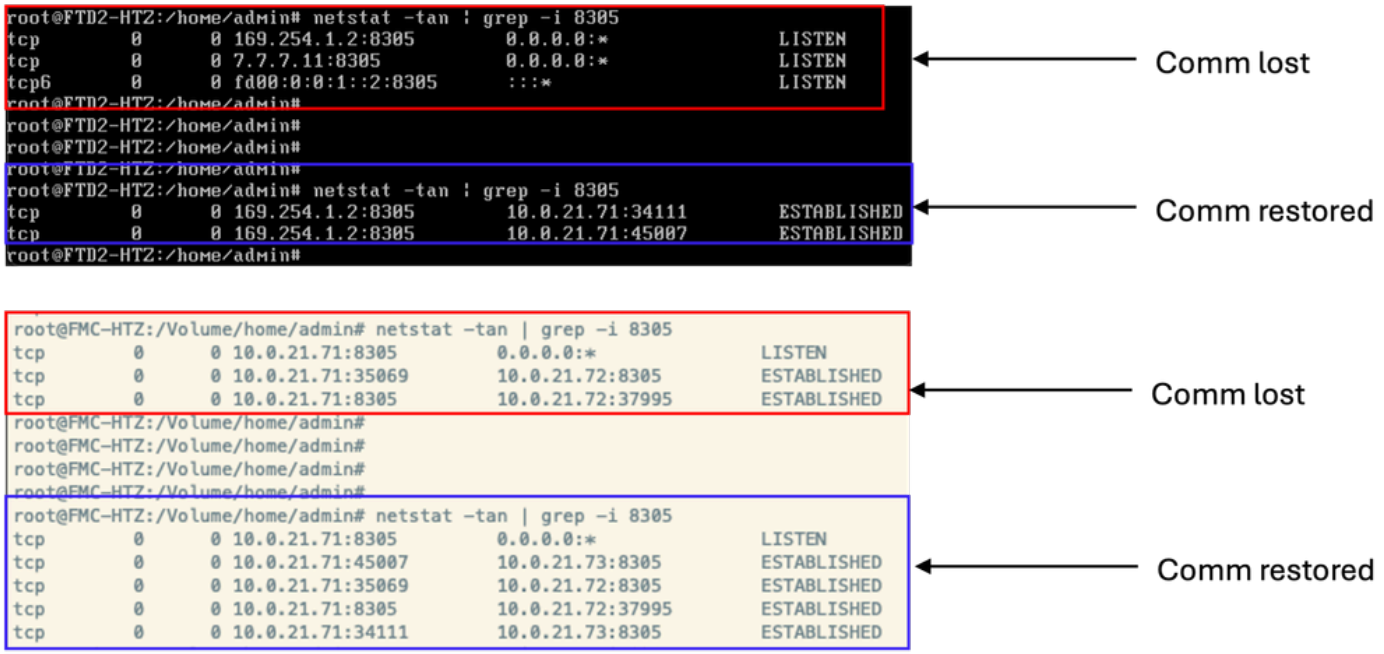
이제 변경 사항을 저장하라는 메시지가 표시되며, 디바이스를 재부팅할 경우 변경 사항이 유지되지 않음을 알리는 알림이 표시됩니다.

```
firepower(recovery-config)# route outside 0.0.0.0 0.0.0.0 10.0.21.13
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o:
No

firepower#
firepower# _
```

6. 컨피그레이션이 적용되었는지 확인할 수 있습니다. 이 경우에는 경로를 표시합니다.

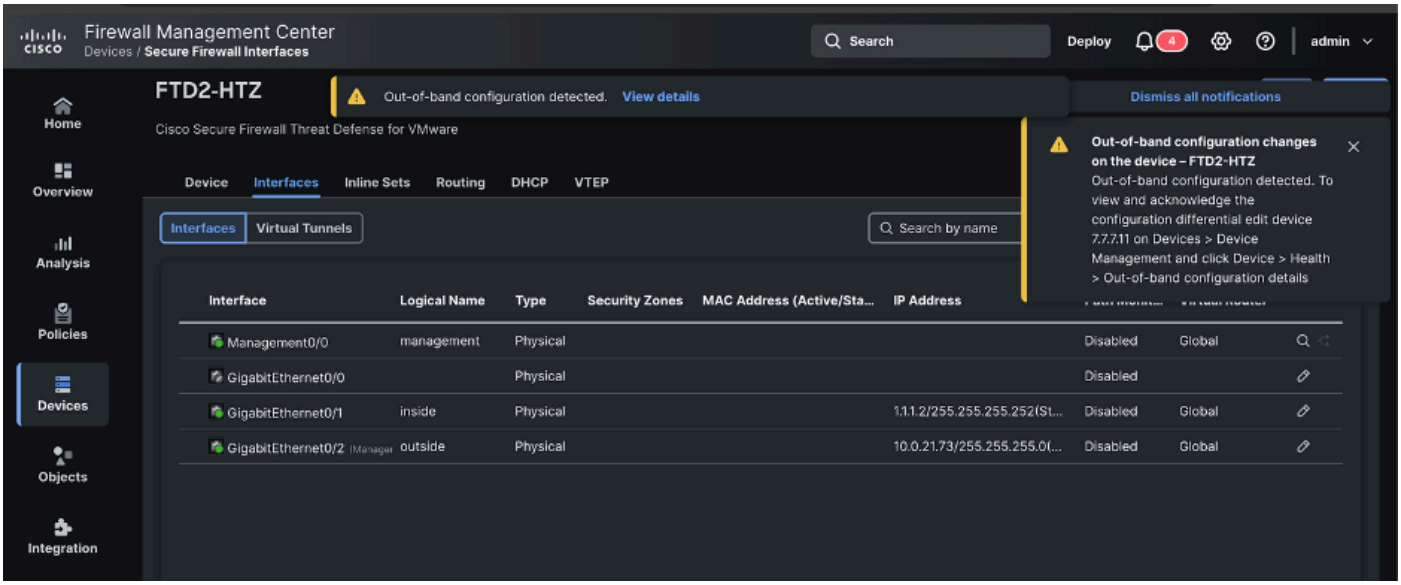
```
firepower# show route

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 10.0.21.13 to network 0.0.0.0

S*        0.0.0.0 0.0.0.0 [1/0] via 10.0.21.13, outside
C         1.1.1.0 255.255.255.252 is directly connected, inside
L         1.1.1.2 255.255.255.255 is directly connected, inside
```

7. 몇 분 후에 이 변경 사항으로 FMC와의 통신이 복원됩니다. 다음 그림에서는 먼저 FTD에서, 다음에는 FMC CLI에서 설정된 연결을 보여 줍니다.

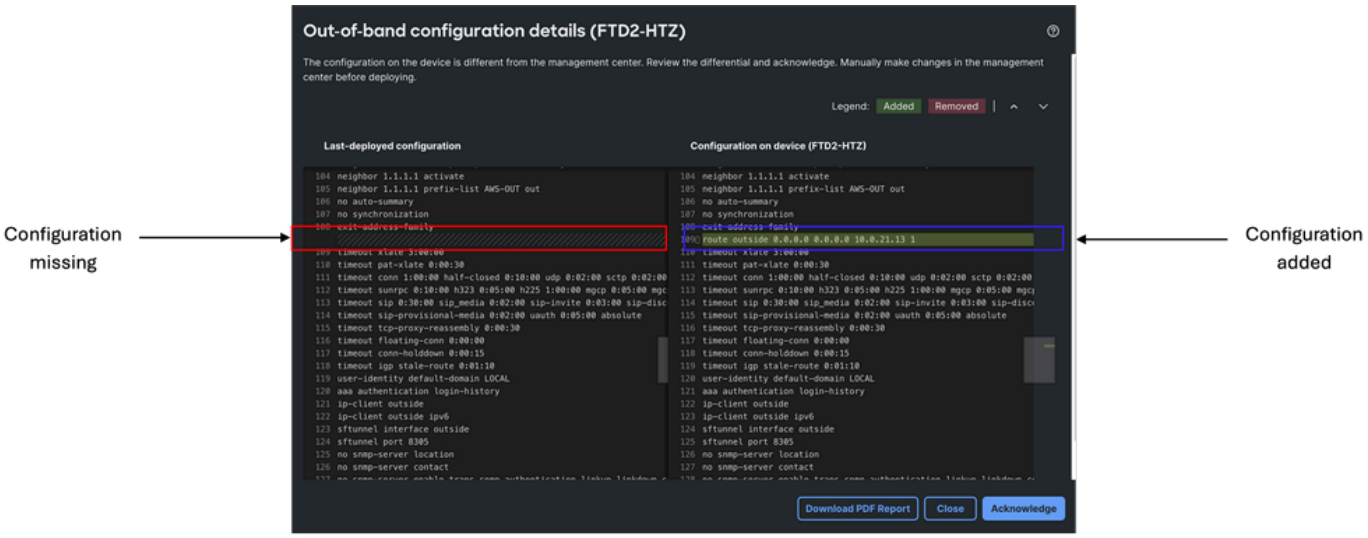


8. 컨피그레이션이 복원된 후 FMC GUI에서 Device(디바이스) > Device Management(디바이스 관리)로 이동하고 디바이스(이 경우 FTD2-HTZ)를 클릭할 수 있습니다.

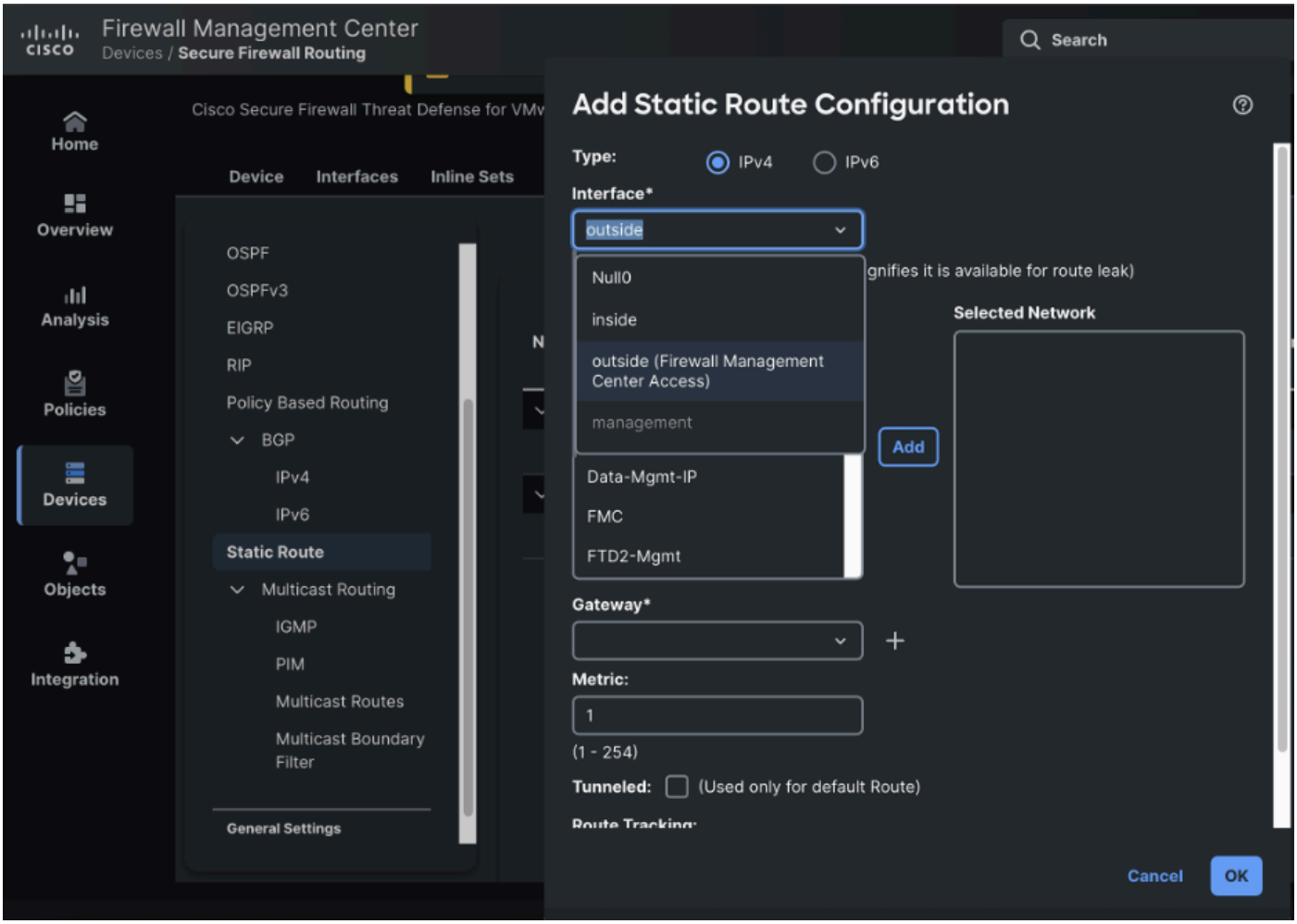
이 화면에서는 OOB(Out of Band) 컨피그레이션 탐지 알림이 표시됩니다. 구성의 차이점을 보려면 View details(세부 정보 보기)를 클릭합니다.

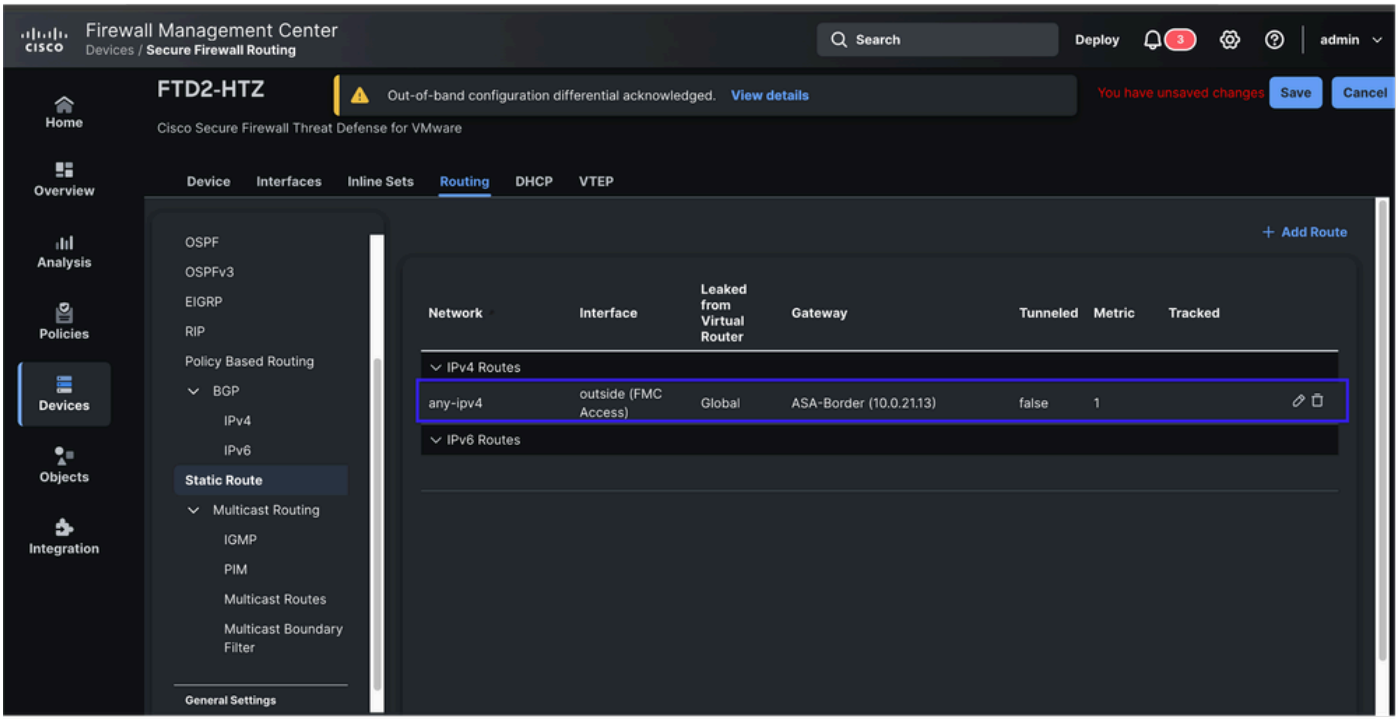


9. OOB(Out of Band) 구성 세부 정보를 검토하고 차이점을 확인합니다.



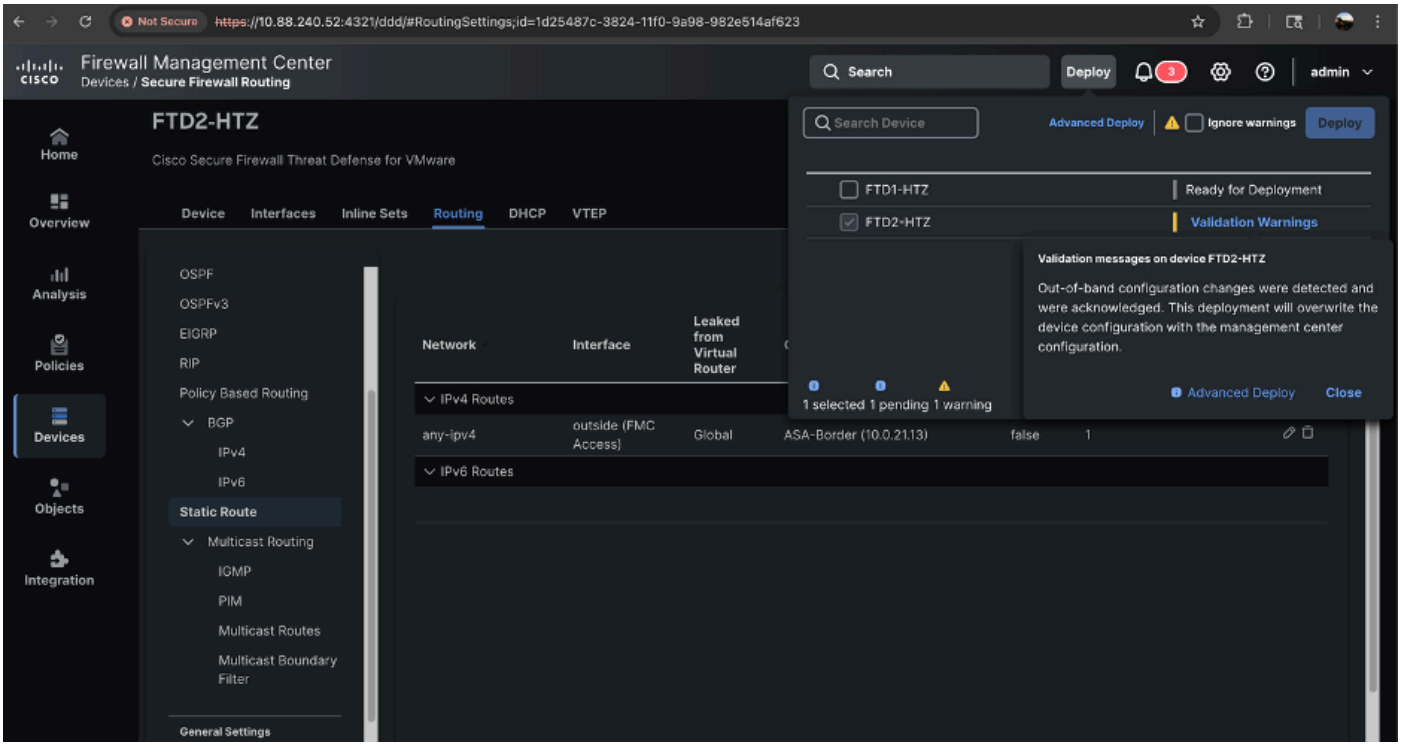
10. 컨피그레이션 차이를 확인한 후 복구 모드에서 수행한 것과 동일한 변경 사항을 구성하되, 이제 FMC GUI를 통해 구성합니다. 이 시나리오에서는 고정 경로가 추가됩니다.

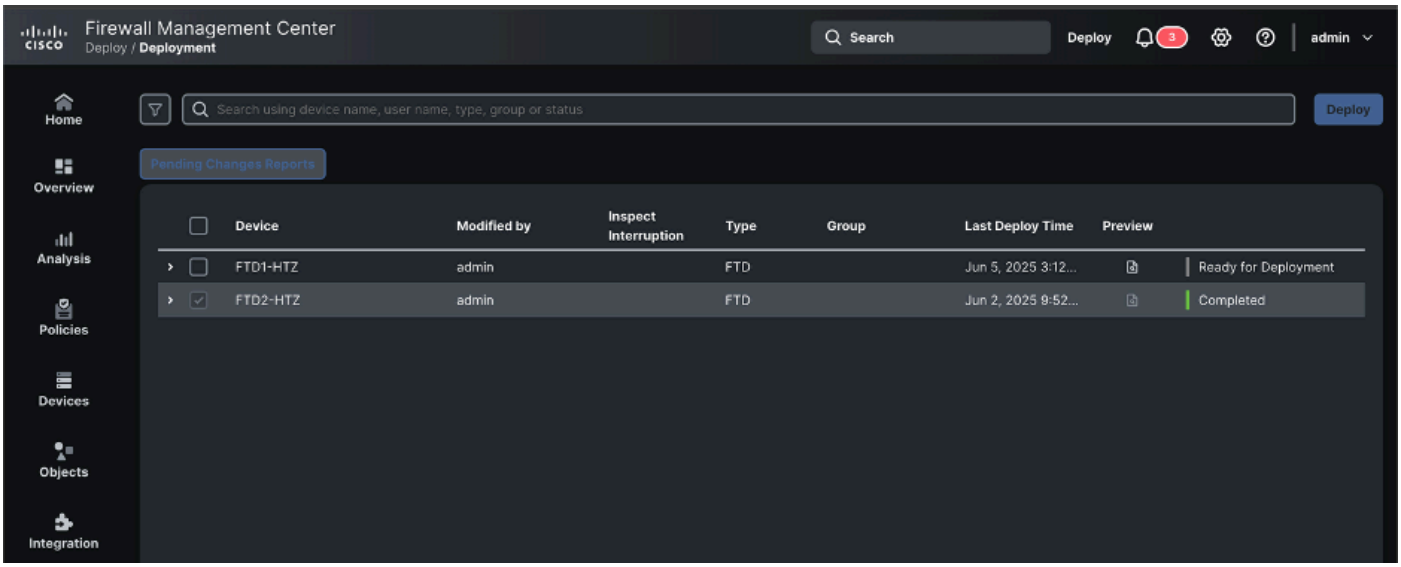




11. 컨피그레이션 변경 사항이 저장되면 변경 사항 구축을 진행합니다. Out-of-band 컨피그레이션 변경 사항이 탐지 및 확인되었으며 변경 사항이 현재 구축에 의해 재정의되었음을 알리는 또 다른 알림이 표시됩니다.

구축에 성공하면 컨피그레이션이 다시 동기화됩니다.





참조

- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/release-notes/threat-defense/770/threat-defense-release-notes-77.html
- https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for

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.