緊急オンデバイス設定のためのRecovery-configモードの使用

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景](#)

[設定例](#)

- [ラボの背景](#)
- [設定手順](#)

[参考資料](#)

はじめに

このドキュメントでは、FTD 7.7の「緊急オンデバイス設定のためのRecovery-configモードの使用」について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Threat Defense（FTD）
- Cisco Firepower Management Center（FMC）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTD 7.7.0+
- FMC 7.7.0以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

この機能はバージョン7.7.0で導入され、管理接続がダウンしているときにアウトオブバンドの設定変更を行うために使用できます。

これらの設定変更は、次の目的でデバイスのCLIで直接実行されます。

- マネージャ・アクセス用のデータ・インタフェースを使用している場合は、管理接続を復元します。
- 接続が復元されるまで待機できないポリシー変更を選択します。

管理接続が復元されたら、次の手順を実行します。

1. アウトオブバンド(OOB)設定アラートに示されている設定の違いを認識する必要があります。
2. ローカルの変更は常にFMCの導入によって上書きされるため、導入する前にFMCで同じ変更を実行します。

これらの機能領域は、recovery-configモードの診断CLIで設定できます。

- インターフェイス
- スタティック ルート
- ダイナミックルーティング：BGPとOSPF
- プレフィルタ
- サイト間 VPN

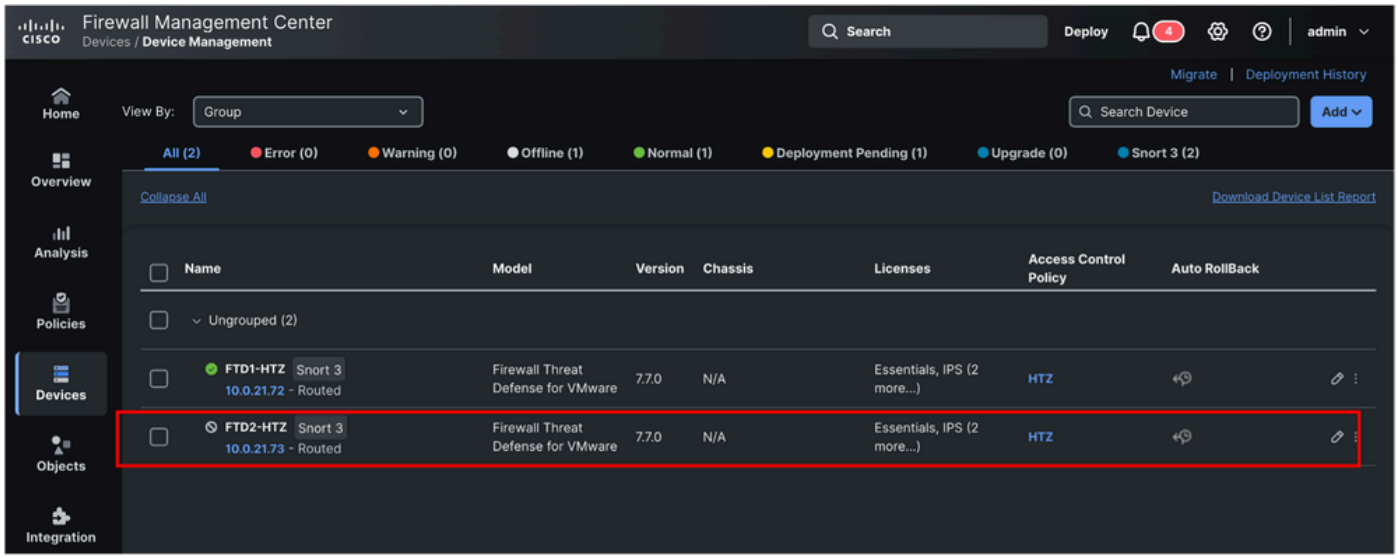
設定例

ラボの背景

このシナリオでは、FMC（データインターフェイスを管理インターフェイスとして使用）に登録されたFTDデバイスで管理接続が失われ、この問題を修正するために、recovery-config機能を使用してスタティックルートがFTDに追加されます。

FMCには2つの脅威対策デバイス（10.0.21.72および10.0.21.73）が登録されていますが、次の図（CLIおよびGUI）に示すように、これらのうち1つだけが到達可能です。

```
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#
```



FTDはFMCへの登録プロセスにデータインターフェイスを使用しています。

```
----------------------[ 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
```

また、FTDはsftunnel経由でFMCに接続できません。

```
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# _
```

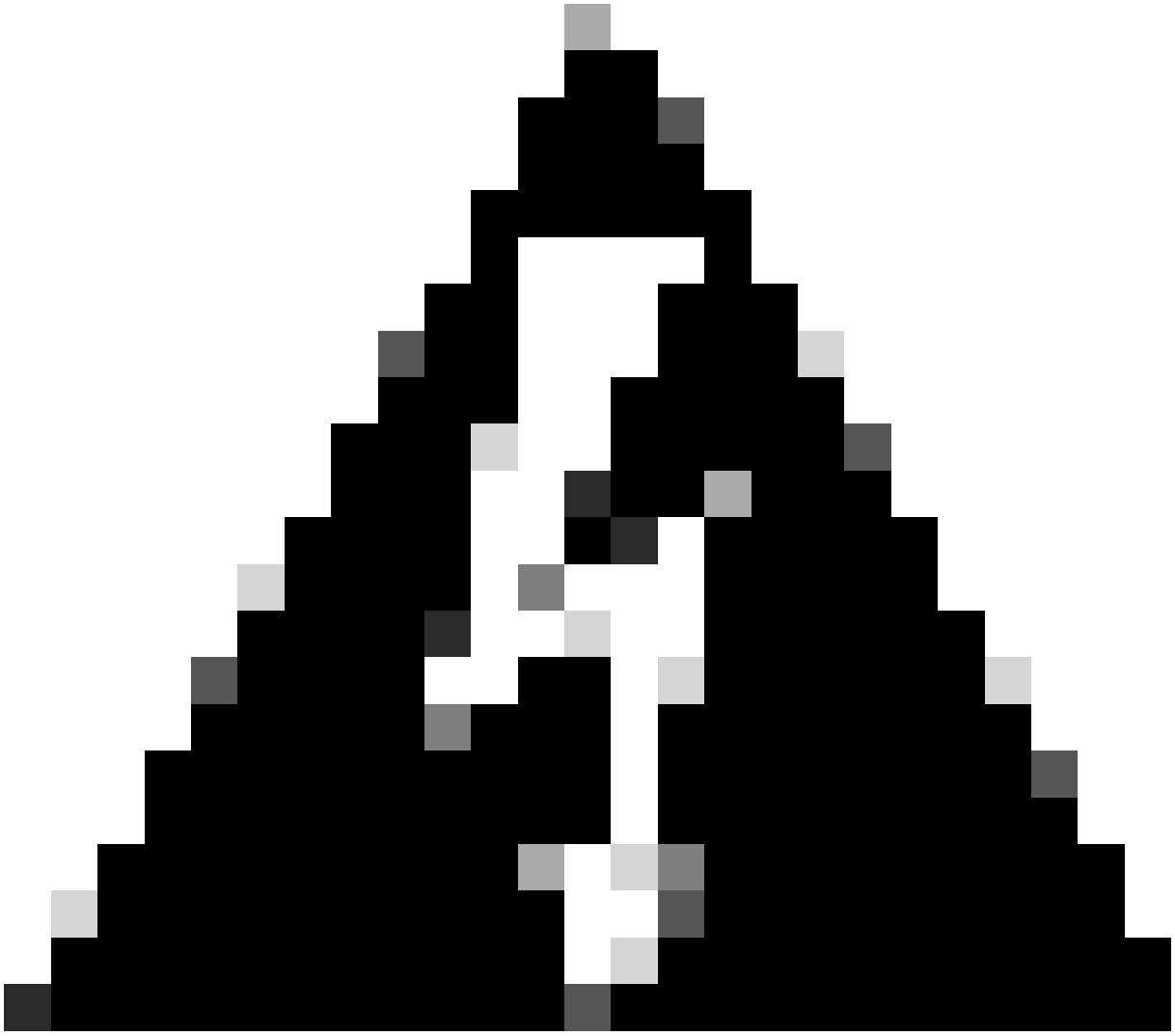
設定手順

1. recovery-config機能を使用できるようにするには、FTD CLIにログインし、回線モード(システムサポート診断CLI)に入る必要があります。

2. configure recovery-configコマンドを実行します。

3. 疑問符(?)を入力すると、サポートされているすべてのコマンドが次のリストに示すように表示されます。

```
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
```



警告：回復または緊急の使用に必要なコマンドを理解していることが必要です。どのコマンドを使用すべきかわからない場合は、Cisco TACに連絡して指示を受けることをお勧めします。

---

4. configure recovery-configコマンドを実行すると、アラートが表示され、確認と続行を求められます。

```
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. 確認したら、使用可能な設定コマンドを使用して開始できます。このシナリオでは、スタティックルートが外部インターフェイスに追加されます。設定が完了したら、exitコマンドを実行してリカバリモードを終了します。

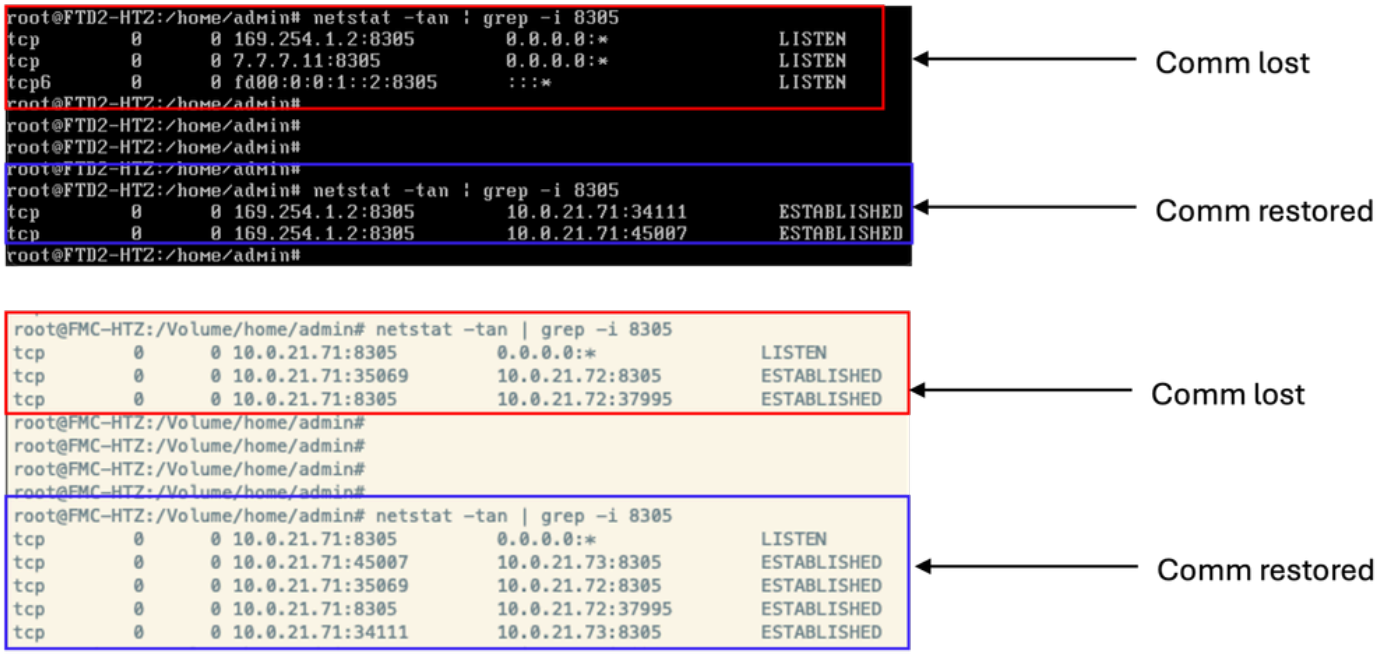
ここで変更を保存するように求められ、デバイスがリブートされた場合に変更が保持されないことを通知するアラートが表示されます。

```
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. 設定が適用されたことを確認できます。この場合、ルートが表示されます。

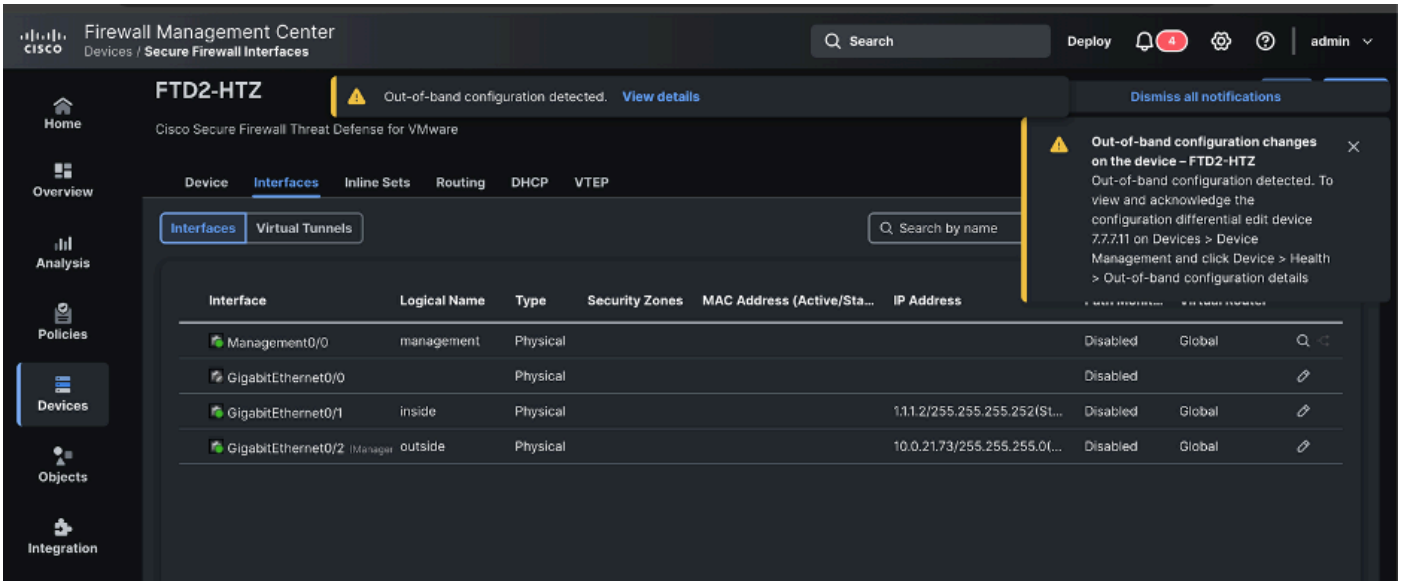
```
firepower# show route

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. 数分後、この変更によりFMCとの通信が復旧します。次の図は、最初にFTDで、次にFMC CLIで接続が確立されたことを示しています。

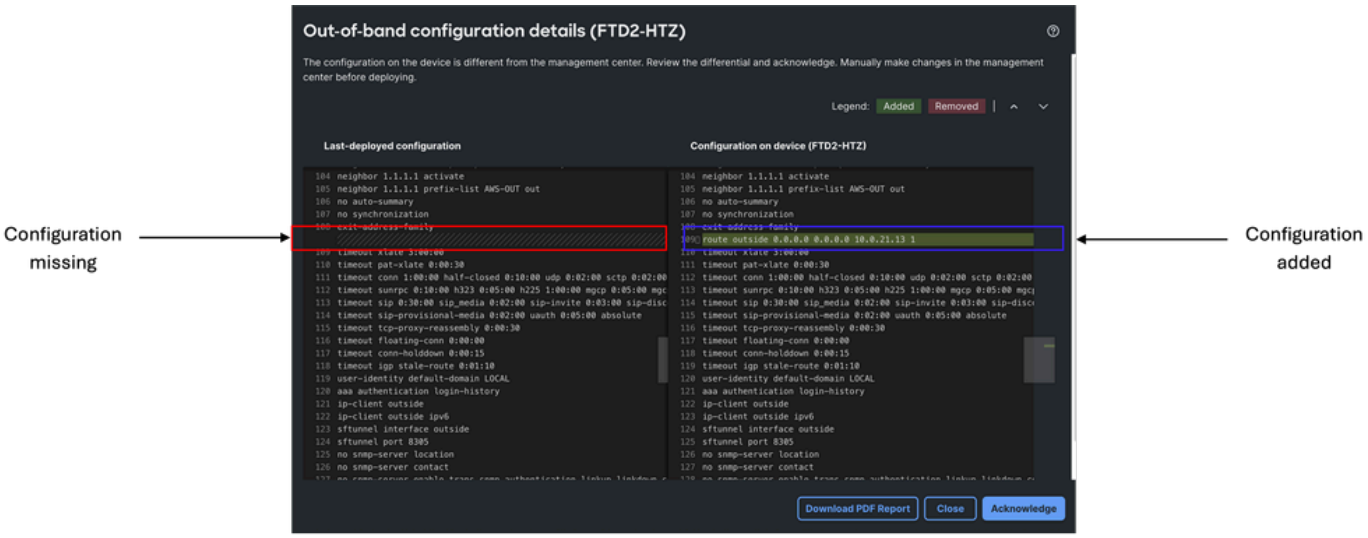


8. 設定が復元された後、FMC GUIでDevice > Device Managementに移動し、デバイス（この場合はFTD2-HTZ）をクリックできます。

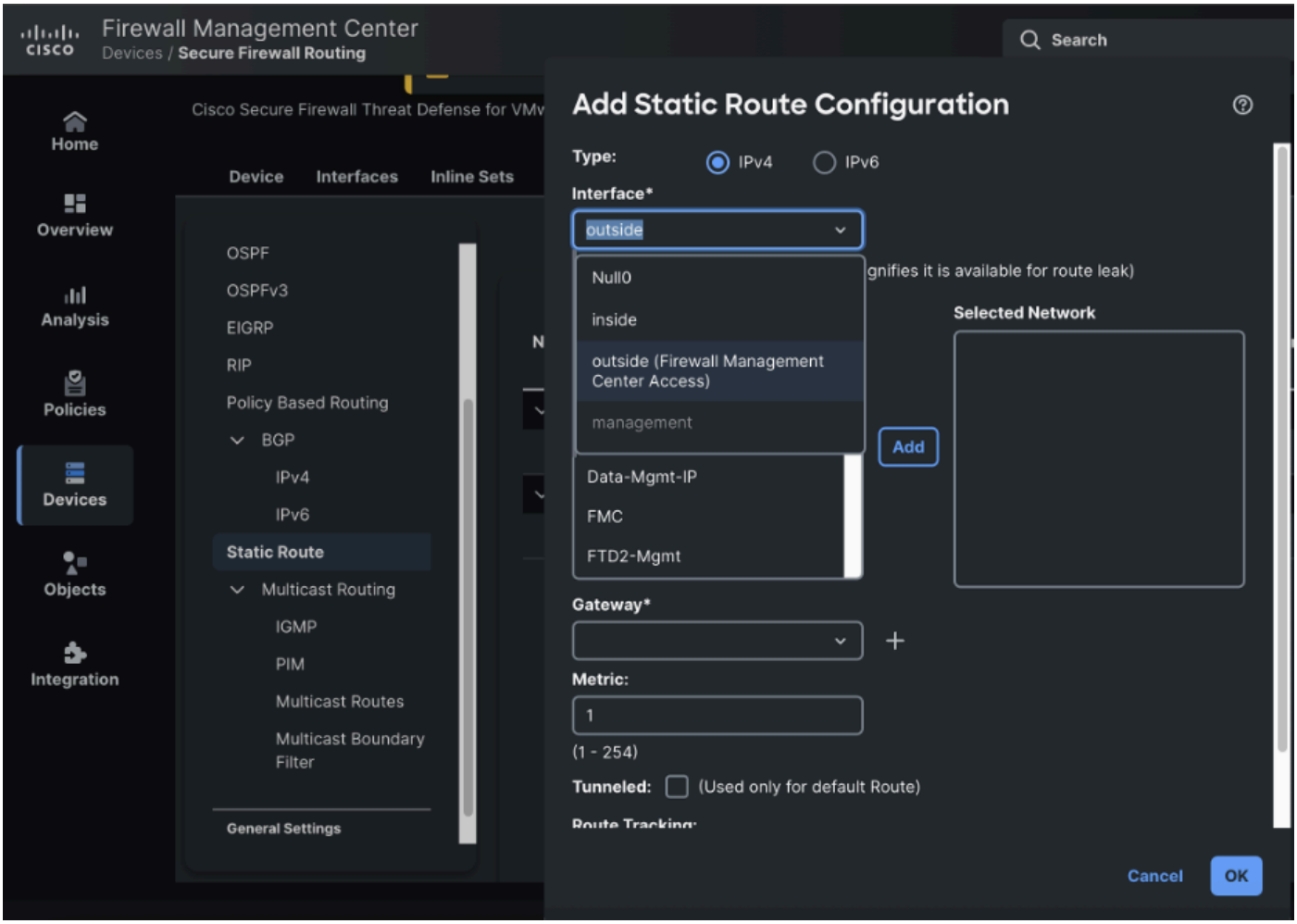
この画面で、Out-of-band configuration detectedアラートを確認できます。詳細の表示内をクリックして、設定の違いを確認します。

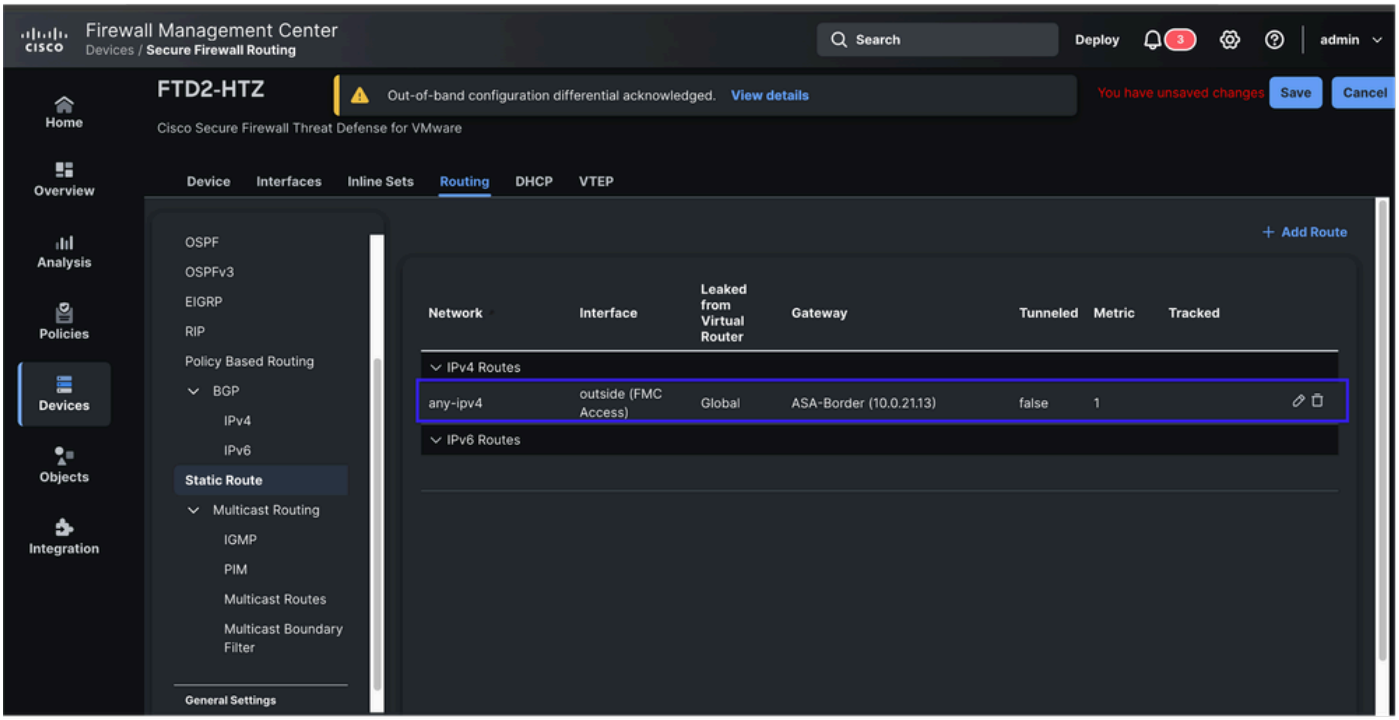


9. アウトオブバンド(OOB)設定の詳細を確認し、違いを認識します。



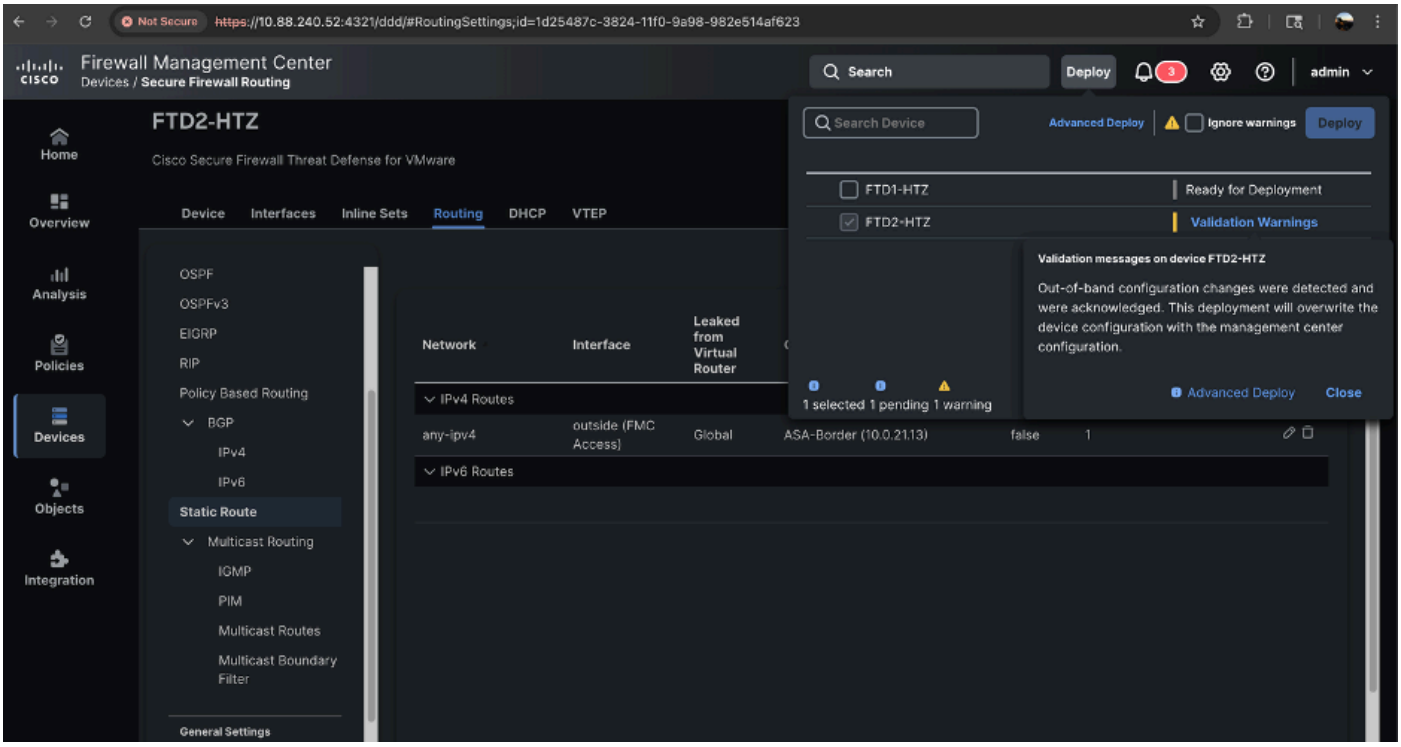
10. 設定の違いを確認した後、リカバリモードで行われた同じ変更の設定に進みますが、ここではFMC GUIを使用します。このシナリオでは、スタティックルートが追加されます。

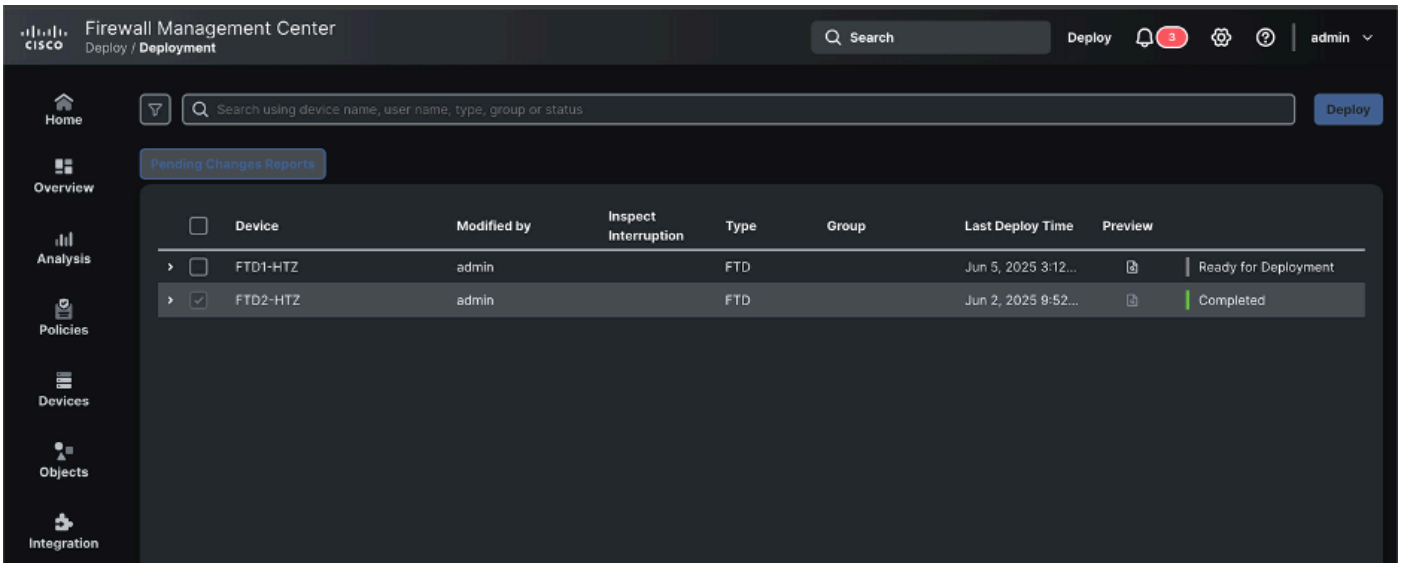




11. 構成の変更を保存したら、変更の展開に進みます。別のアラートが表示され、アウトオブバンド設定の変更が検出および確認応答され、その変更が現在の展開によって上書きされたことを通知します。

導入が成功すると、設定は再度同期されます。





参考資料

- 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。