Utiliser le mode de configuration de récupération pour la configuration d'urgence sur le périphérique

Table des matières

Introduction

Ce document décrit FTD 7.7 Utiliser le mode de configuration de récupération pour la configuration d'urgence sur le périphérique.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FTD 7.7.0+
- FMC 7.7.0+

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Cette fonctionnalité a été introduite dans la version 7.7.0 et peut être utilisée pour apporter des

modifications de configuration hors bande lorsque la connexion de gestion est désactivée.

Ces modifications de configuration sont effectuées directement sur l'interface de ligne de commande du périphérique pour :

- Restaurez la connexion de gestion si vous utilisez une interface de données pour l'accès au gestionnaire.
- Effectuez des modifications de stratégie de sélection qui ne peuvent pas attendre que la connexion soit restaurée.

Une fois la connexion de gestion restaurée :

1. Vous devez accuser réception des différences de configuration indiquées dans l'alerte de configuration hors bande.
2. Effectuez les mêmes modifications dans FMC avant le déploiement, car les modifications locales sont toujours remplacées par le déploiement FMC.

Vous pouvez configurer ces zones de fonctions à partir de l'interface de ligne de commande de diagnostic en mode de configuration de récupération :

- Interfaces
- routes statique
- Routage dynamique : BGP et OSPF
- Préfiltres
- VPN de site à site

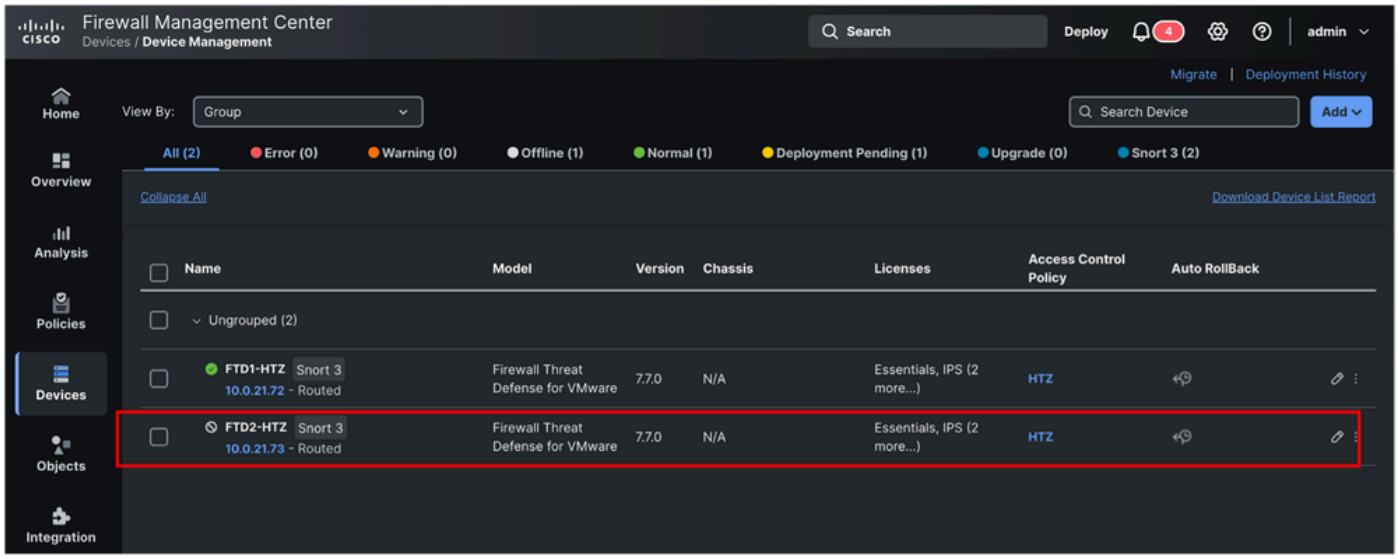
Exemple de configuration

Contexte des travaux pratiques

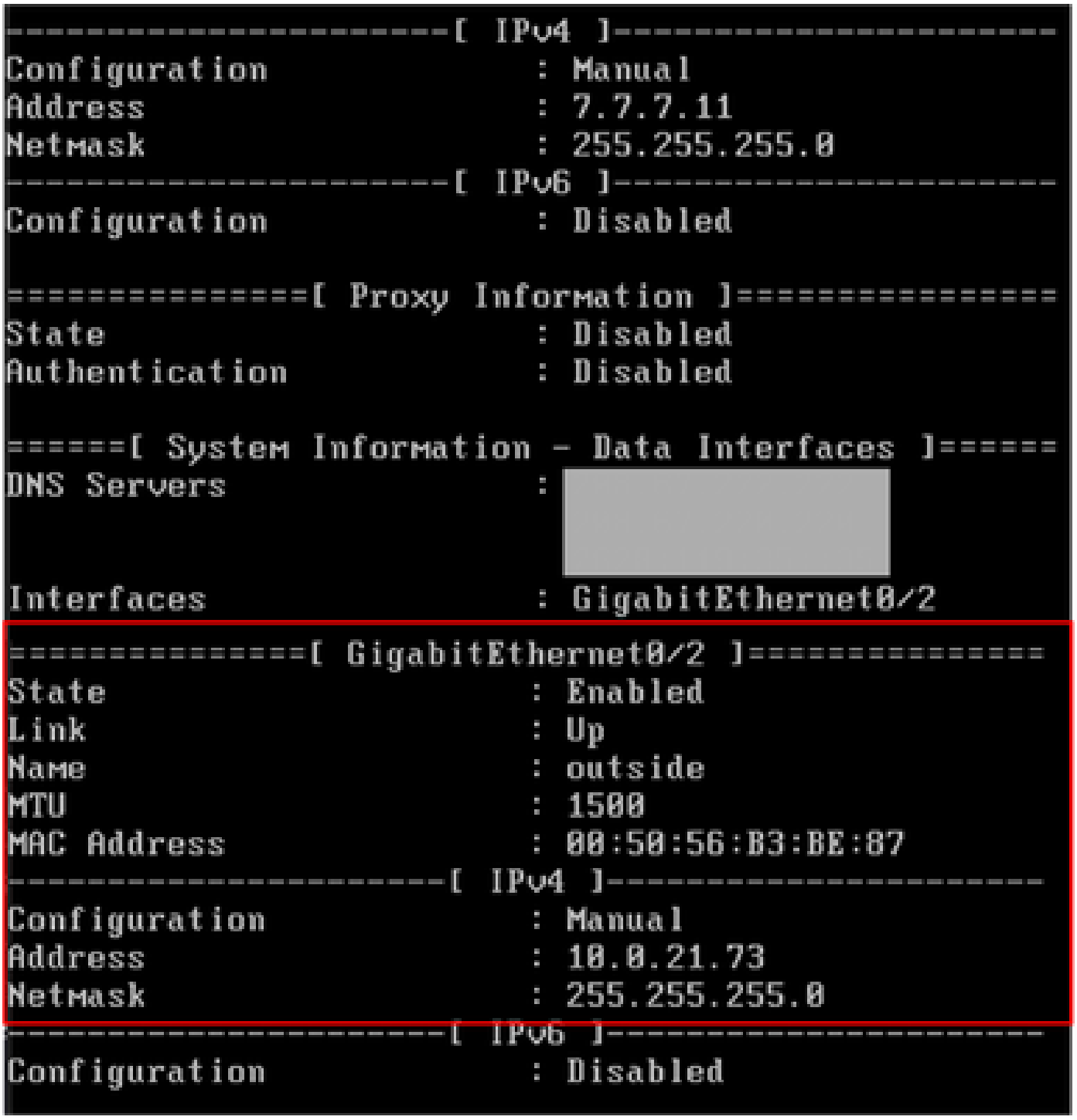
Dans ce scénario, un périphérique FTD enregistré sur un FMC (utilisant l'interface de données comme interface de gestion) a perdu la connexion de gestion et, pour résoudre ce problème, une route statique est ajoutée au FTD à l'aide de la fonctionnalité recovery-config.

FMC a enregistré deux périphériques de défense contre les menaces (10.0.21.72 et 10.0.21.73), mais un seul d'entre eux est accessible, comme illustré dans les images suivantes (interface de ligne de commande et interface graphique).

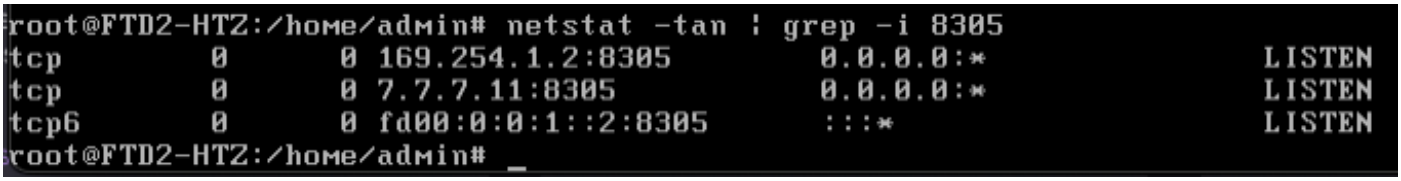
```
root@FMC-HTZ:/Volume/home/admin# netstat -tan | grep -i 8305
tcp        0      0 10.0.21.71:8305         0.0.0.0:*               LISTEN
tcp        0      0 10.0.21.71:35069        10.0.21.72:8305         ESTABLISHED
tcp        0      0 10.0.21.71:8305         10.0.21.72:37995        ESTABLISHED
root@FMC-HTZ:/Volume/home/admin#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



FTD utilise une interface de données pour le processus d'enregistrement auprès de FMC.



FTD n'a pas non plus de connexion à FMC via sftunnel .



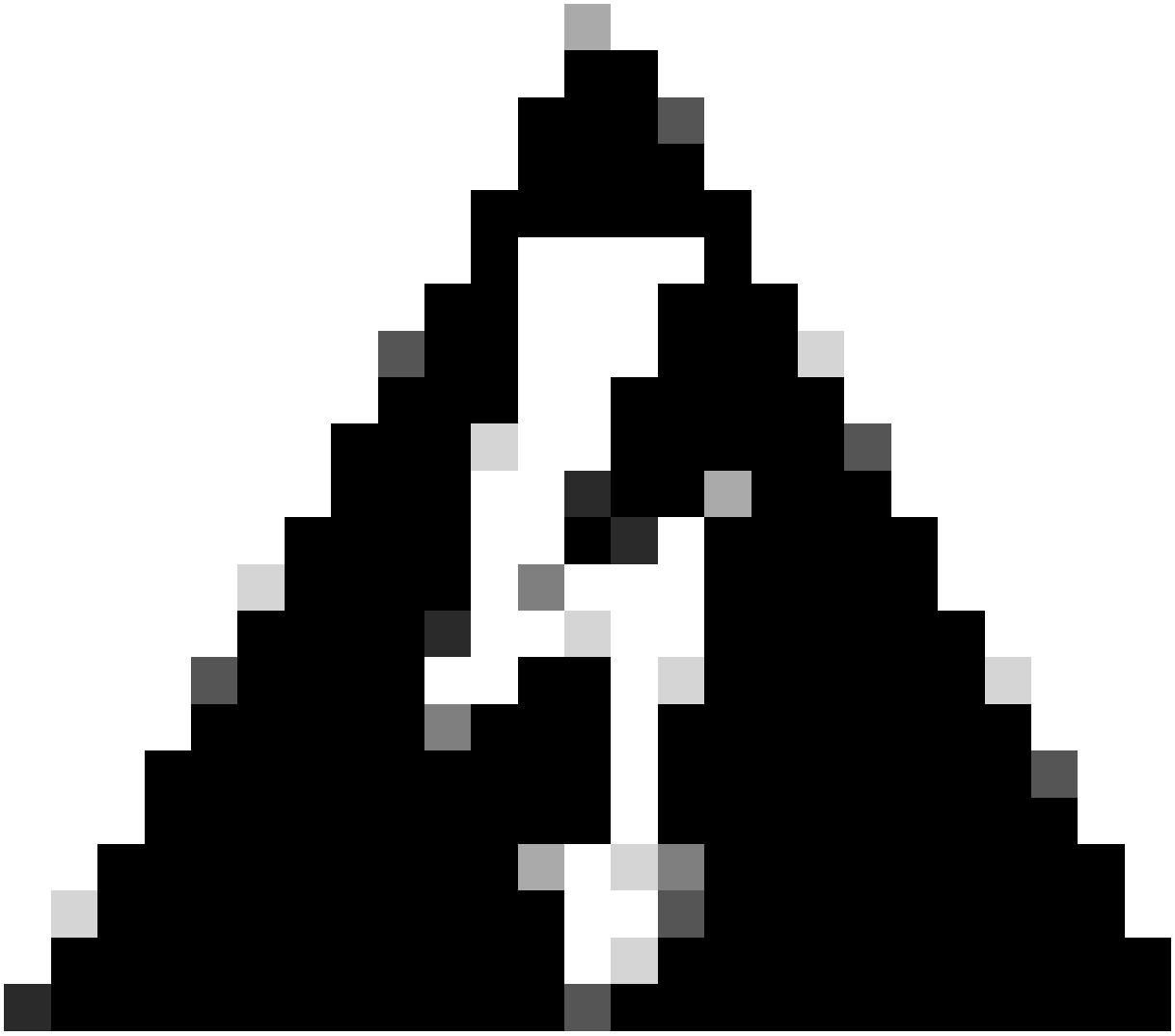
Configuration Steps

1. Pour pouvoir utiliser la fonction recovery-config, vous devez vous connecter à l'interface de ligne de commande FTD et passer en mode Lina (prise en charge système diagnostic-cli).

2. Exécutez la commande configure recovery-config.

3. Si vous tapez un point d'interrogation (?), toutes les commandes prises en charge sont répertoriées, comme indiqué dans la liste suivante.

```
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
```



Avertissement : Vous devez connaître les commandes nécessaires à la récupération ou à une utilisation d'urgence. Si vous n'êtes pas sûr de la commande à utiliser, nous vous recommandons de contacter le TAC Cisco pour obtenir des conseils.

---

4. Après avoir exécuté la commande configure recovery-config, une alerte s'affiche et vous êtes invité à confirmer et à continuer.

```
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. Une fois confirmé, vous pouvez utiliser les commandes de configuration disponibles. Dans ce scénario, une route statique est ajoutée à l'interface externe. Une fois la configuration terminée, exécutez la commande exit pour quitter le mode de récupération.

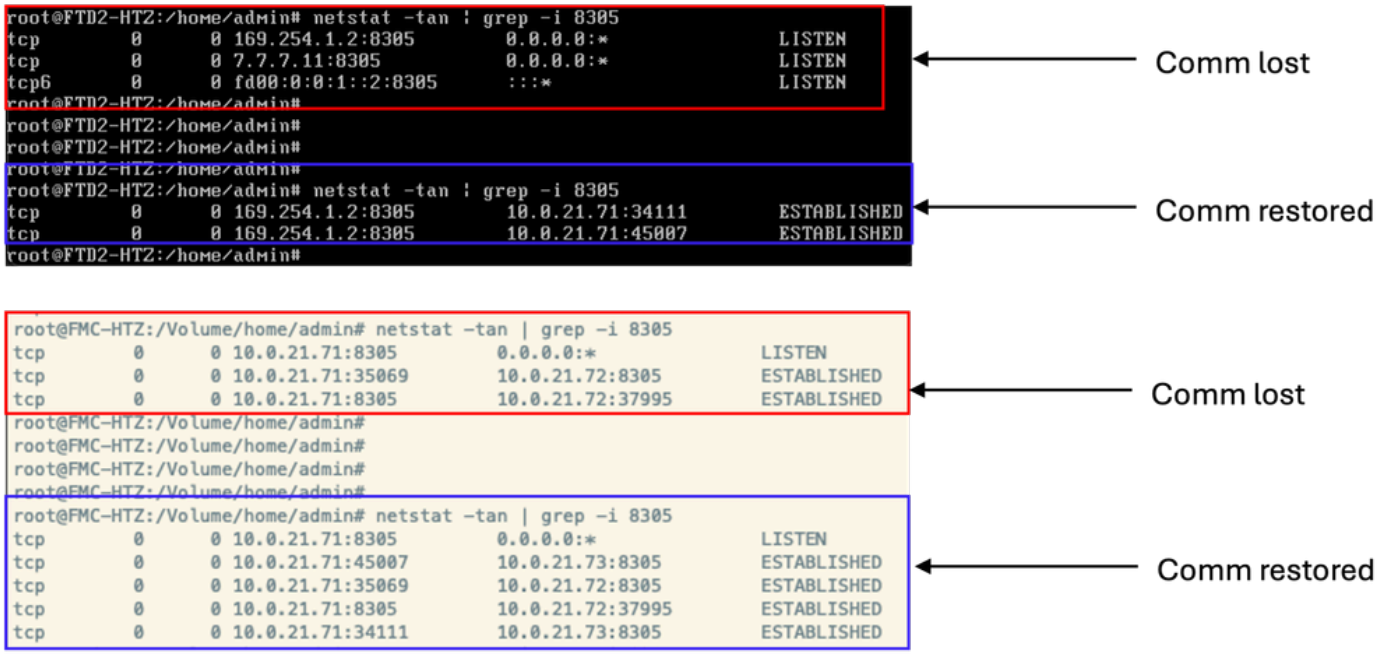
Vous êtes invité à enregistrer les modifications et une alerte s'affiche pour vous informer que les modifications ne sont pas conservées si le périphérique est redémarré.

```
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. Vous pouvez confirmer que la configuration a été appliquée. Dans le cas présent, affichage des routes.

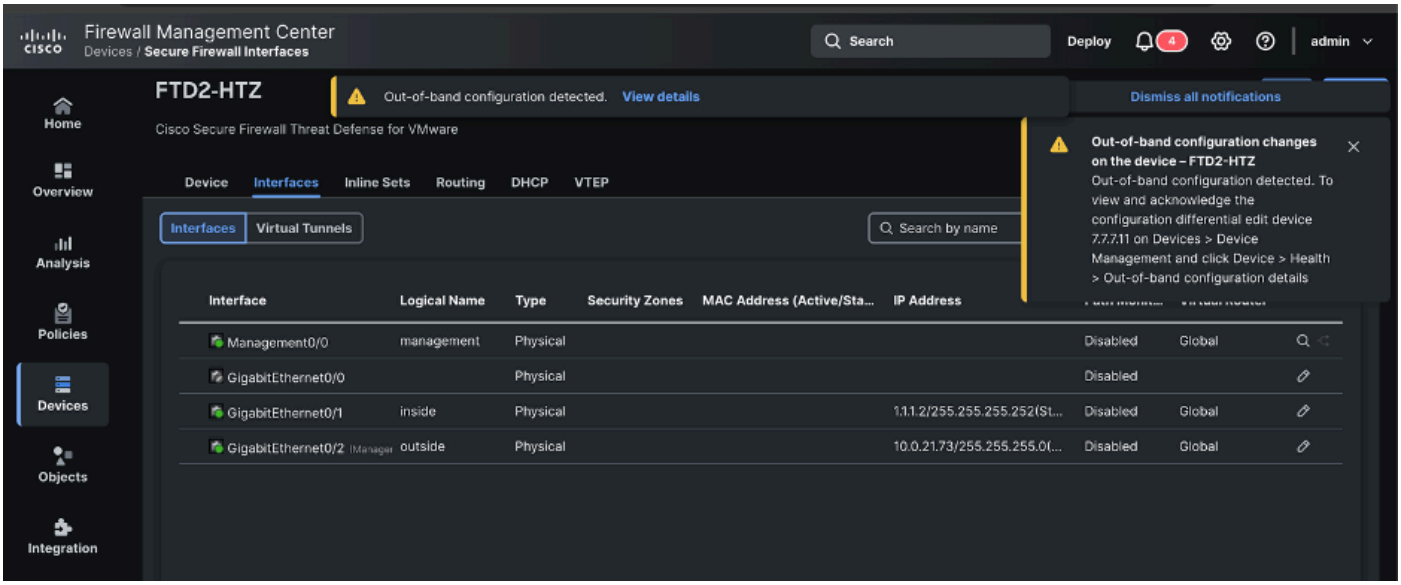
```
firepower# show route

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. Après quelques minutes, cette modification rétablit la communication avec FMC. Les images suivantes montrent la connexion établie, d'abord dans FTD et ensuite dans l'interface de ligne de commande FMC.

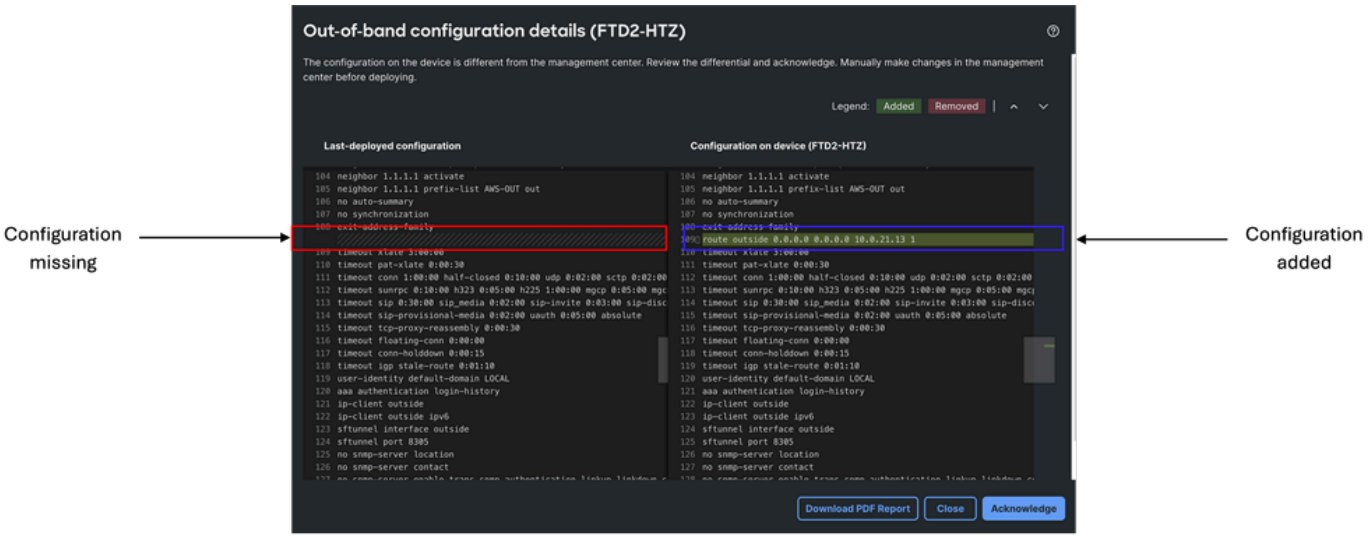


8. Une fois la configuration restaurée, dans l'interface utilisateur graphique de FMC, vous pouvez naviguer vers Device > Device Management et cliquer sur votre périphérique (dans ce cas, il s'agit de FTD2-HTZ).

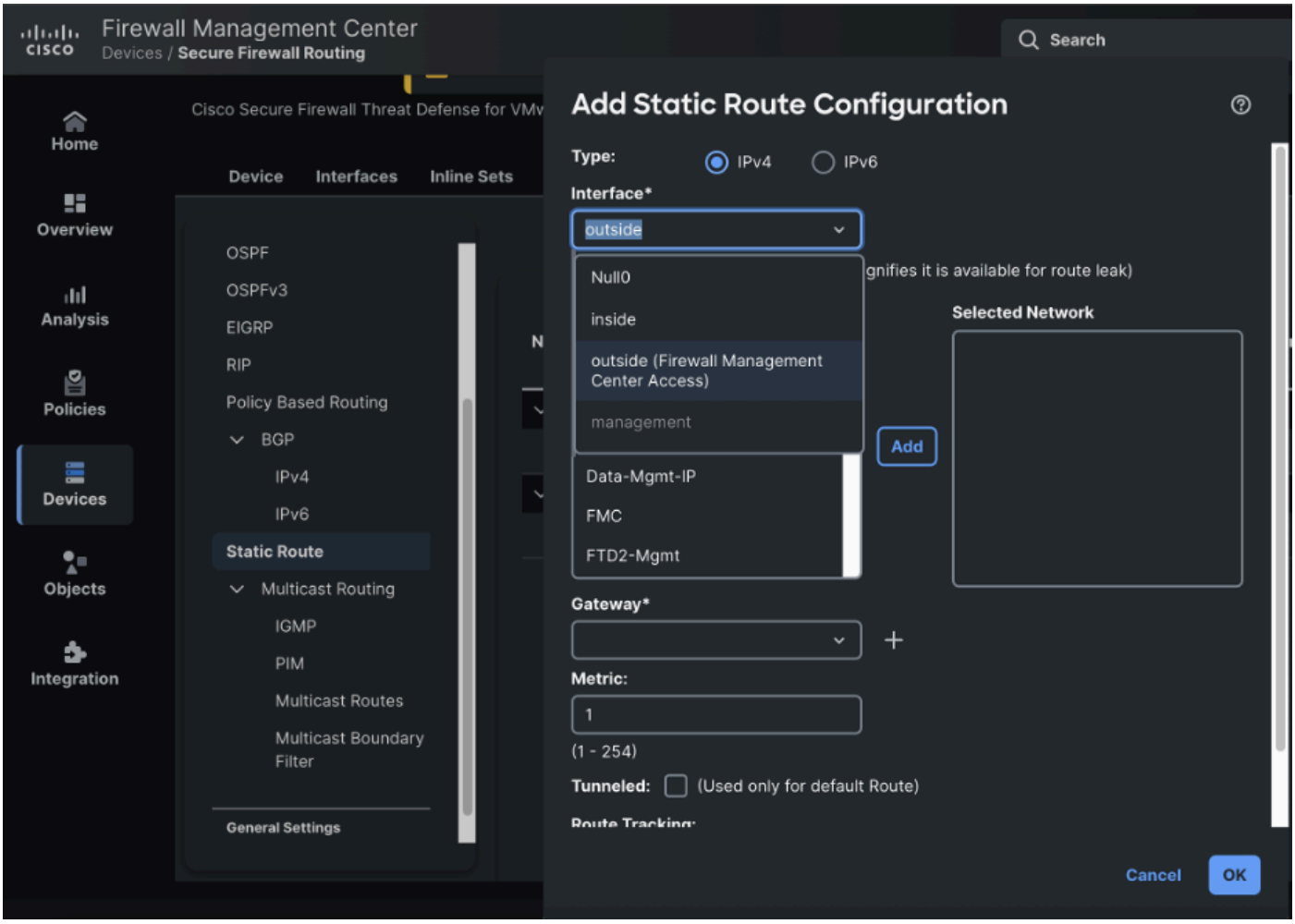
Vous pouvez y voir l'alerte de détection de configuration hors bande. Cliquez dans Afficher les détails pour voir les différences de configuration.

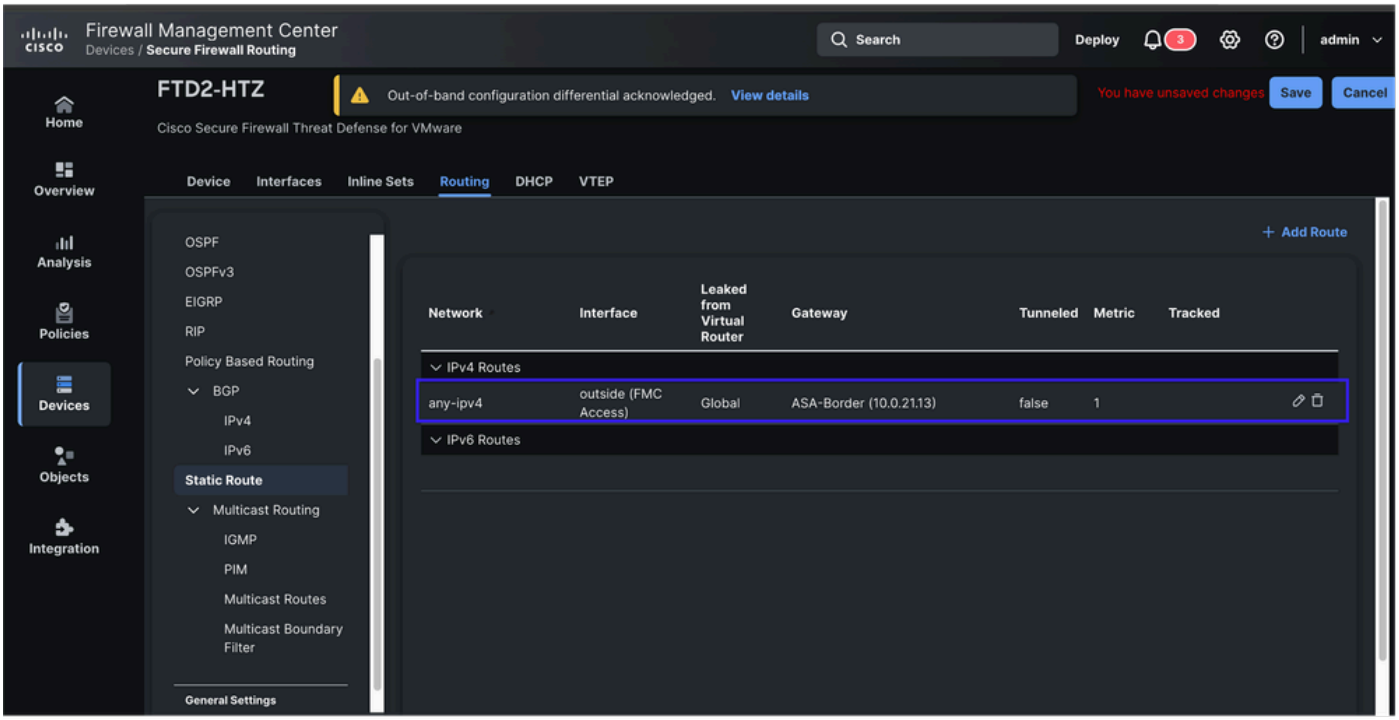


9. Consultez les détails de configuration hors bande et constatez les différences.



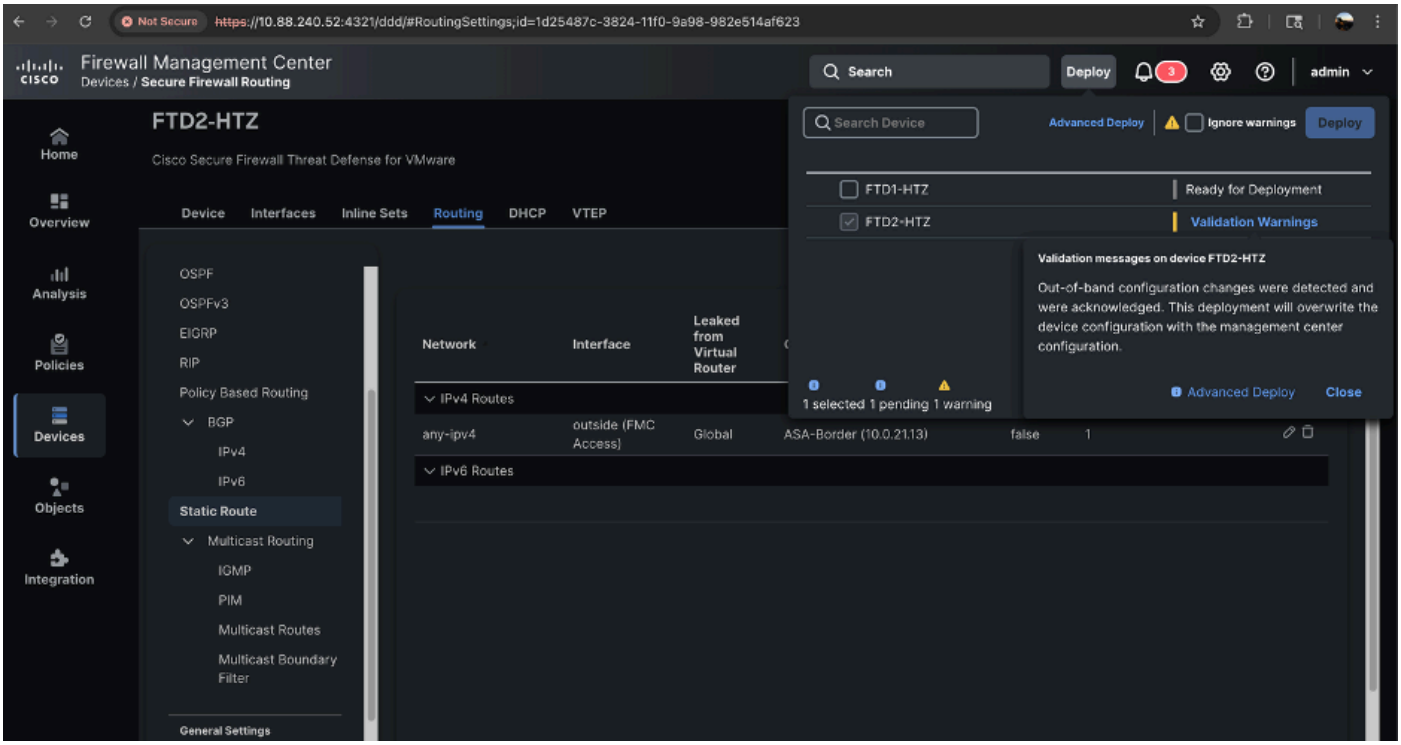
10. Une fois les différences de configuration reconnues, procédez à la configuration des mêmes modifications effectuées en mode de récupération, mais maintenant via l'interface utilisateur graphique FMC. Dans ce scénario, une route statique est ajoutée.

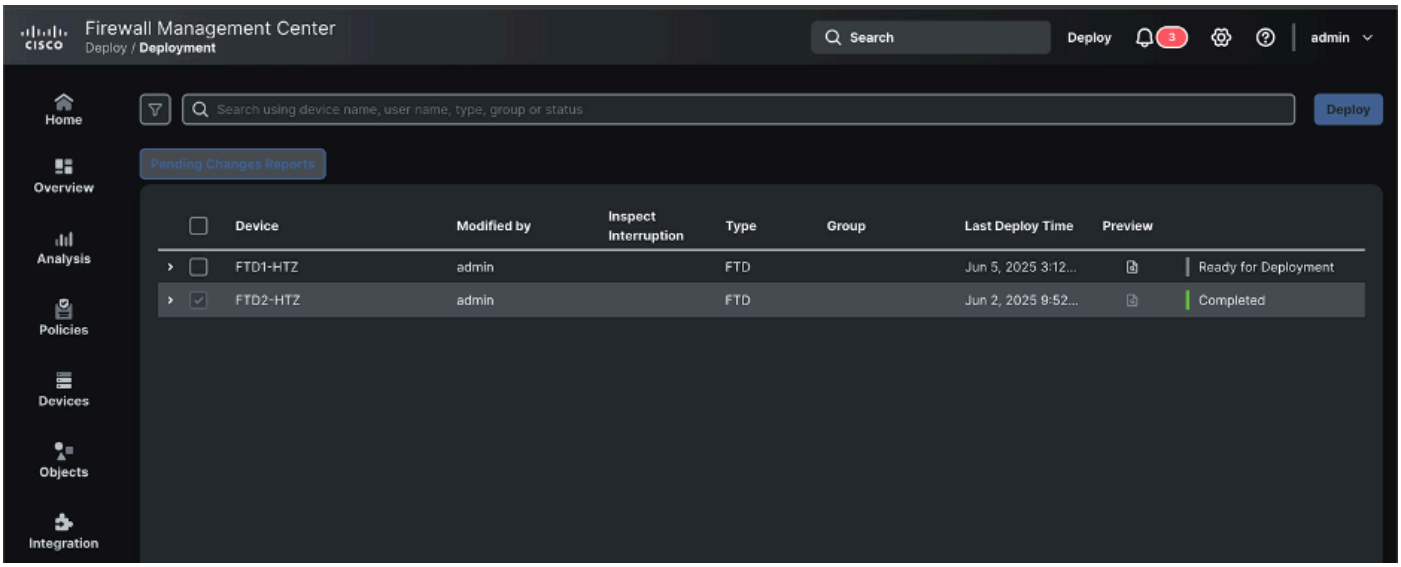




11. Une fois les modifications de configuration enregistrées, poursuivez le déploiement des modifications. Une autre alerte s'affiche pour informer que des modifications de configuration hors bande ont été détectées et reconnues, et que les modifications sont remplacées par le déploiement actuel.

Une fois le déploiement réussi, la configuration est à nouveau synchronisée.





Références

- 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.