De herstelconfiguratiemodus gebruiken voor noodconfiguratie op het apparaat

Inhoud

Inleiding

In dit document wordt FTD 7.7 beschreven Gebruik de herstelconfiguratiemodus voor noodconfiguratie op het apparaat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD 7.7.0+
- FMC 7.7.0+

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Deze functie is geïntroduceerd in versie 7.7.0 en kan worden gebruikt om out-of-band configuratiewijzigingen aan te brengen wanneer de beheerverbinding niet beschikbaar is.

Deze configuratiewijzigingen worden rechtstreeks op de CLI van het apparaat uitgevoerd om:

- Herstel de beheerverbinding als u een gegevensinterface gebruikt voor beheerderstoegang.
- Breng bepaalde beleidswijzigingen aan die niet kunnen wachten totdat de verbinding is hersteld.

Zodra de beheerverbinding is hersteld:

1. U moet de configuratieverschillen erkennen die worden weergegeven in de waarschuwing voor configuratie buiten de band.
2. Voer dezelfde wijzigingen uit in de FMC voordat u deze implementeert, omdat lokale wijzigingen altijd worden overschreven door de FMC-implementatie.

U kunt deze functiegebieden configureren in de diagnostische CLI in de herstelconfiguratiemodus:

- Interfaces
- statische routes
- Dynamische routering: BGP en OSPF
- voorfilters
- Site-to-site VPN

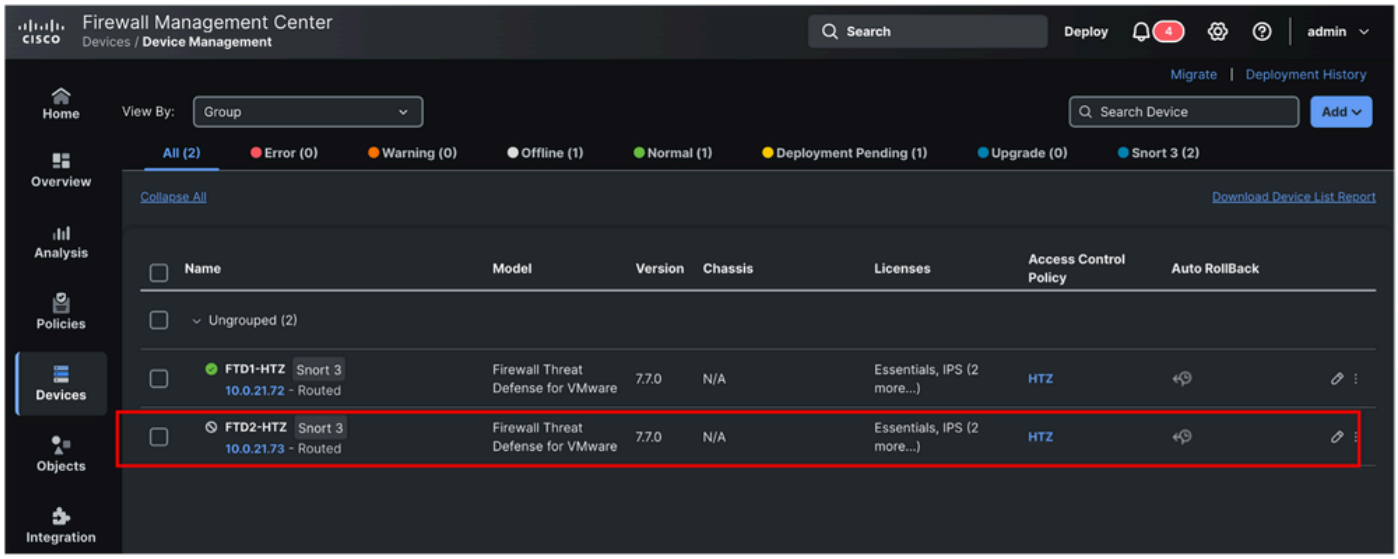
Configuratievoorbeeld

Labachtergrond

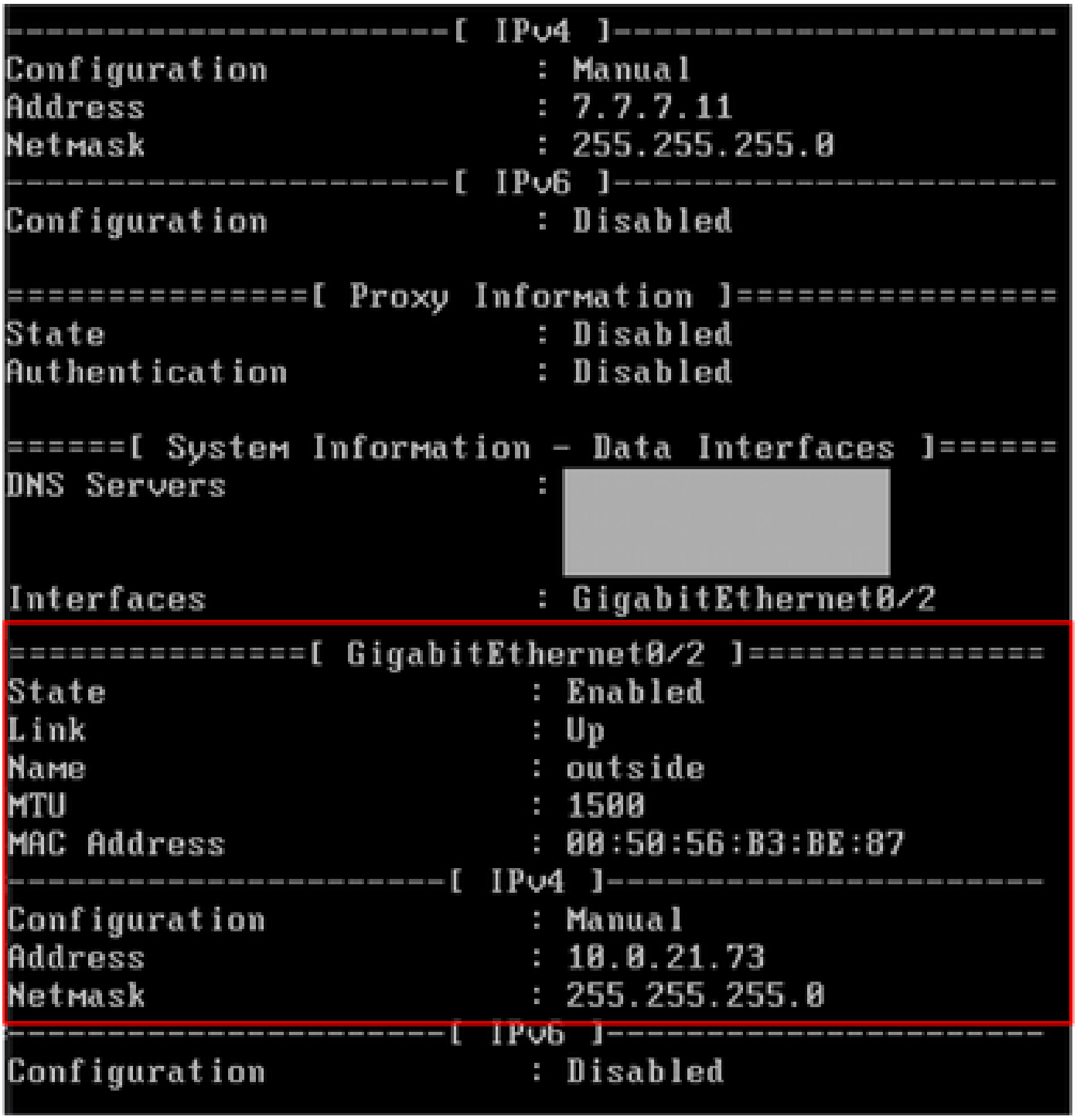
In dit scenario heeft een FTD-apparaat dat is geregistreerd bij een FMC (met behulp van data-interface als beheerinterface) de beheerverbinding verloren en om dit probleem op te lossen, wordt een statische route aan de FTD toegevoegd met behulp van de herstelconfiguratiefunctie.

FMC heeft twee bedreigingsverdedigingsapparaten geregistreerd (10.0.21.72 en 10.0.21.73), maar slechts één daarvan is bereikbaar zoals weergegeven in de volgende afbeeldingen (cli en GUI).

```
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 maakt gebruik van data-interface voor het registratieproces naar FMC.



FTD heeft ook geen verbinding met FMC via sftunnel.

```
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# _
```

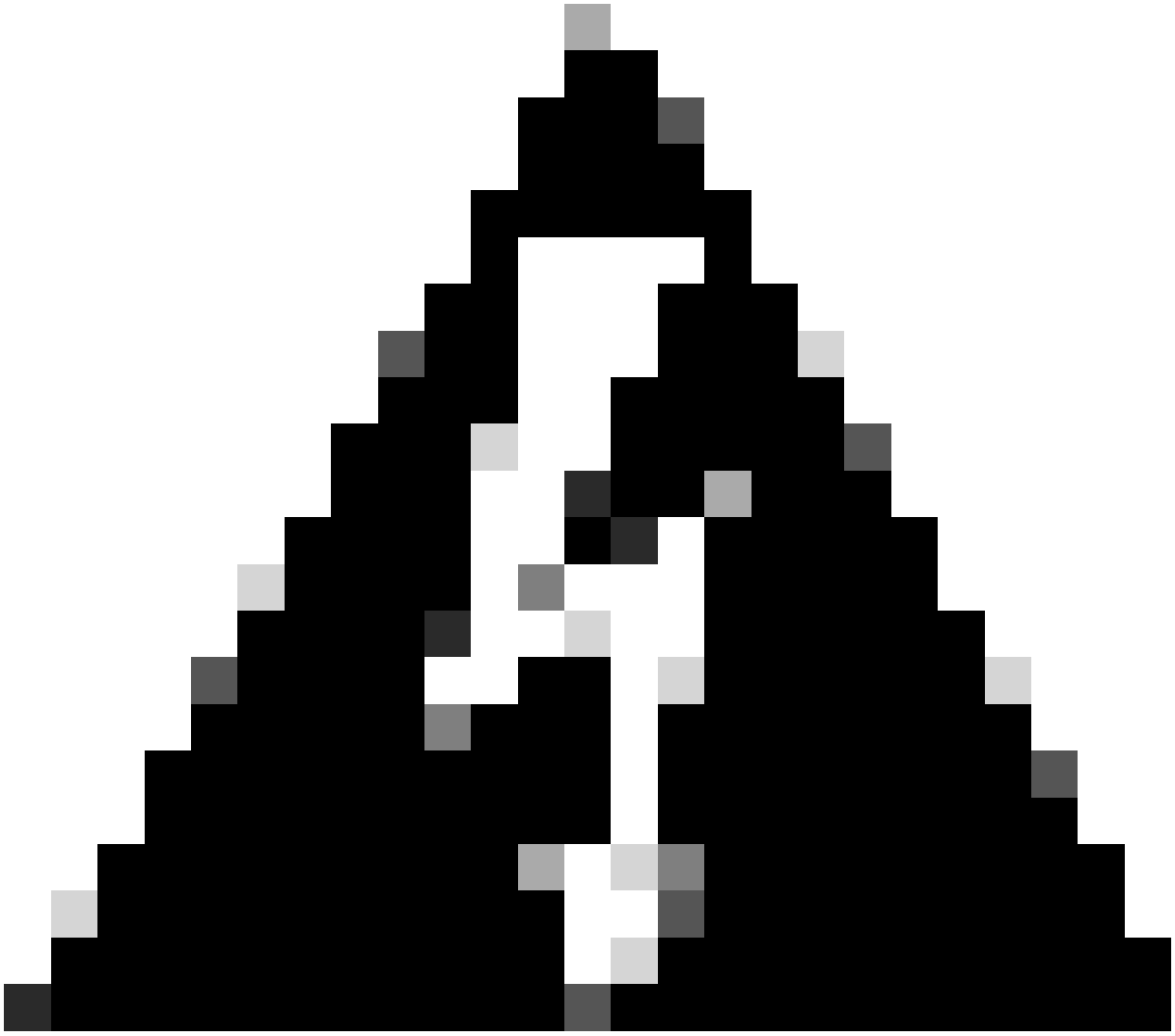
Configuratiestappen

1. Om de herstelconfiguratiefunctie te kunnen gebruiken, moet u zich aanmelden bij FTD CLI en naar de lina-modus gaan (diagnostische-cli voor systeemondersteuning).

2. Voer de opdracht recovery-config configureren uit.

3. Als u vraagteken (?) typt, worden alle ondersteunde opdrachten weergegeven, zoals wordt weergegeven in de volgende lijst.

```
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
```



Waarschuwing: u wordt geacht de opdrachten te kennen die nodig zijn voor herstel of noodgebruik. Als u niet zeker weet welke opdracht moet worden gebruikt, wordt u aangeraden contact op te nemen met Cisco TAC voor advies.

---

4. Nadat u de opdracht recovery-config configureren hebt uitgevoerd, wordt een waarschuwing weergegeven en wordt u gevraagd te bevestigen en door te gaan.

```
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. Nadat u de configuratie hebt bevestigd, kunt u de beschikbare configuratiecommando's gebruiken. In dit scenario wordt een statische route toegevoegd aan de buiteninterface. Nadat de configuratie is voltooid, voert u de opdracht Afsluiten uit om de herstelmodus te verlaten.

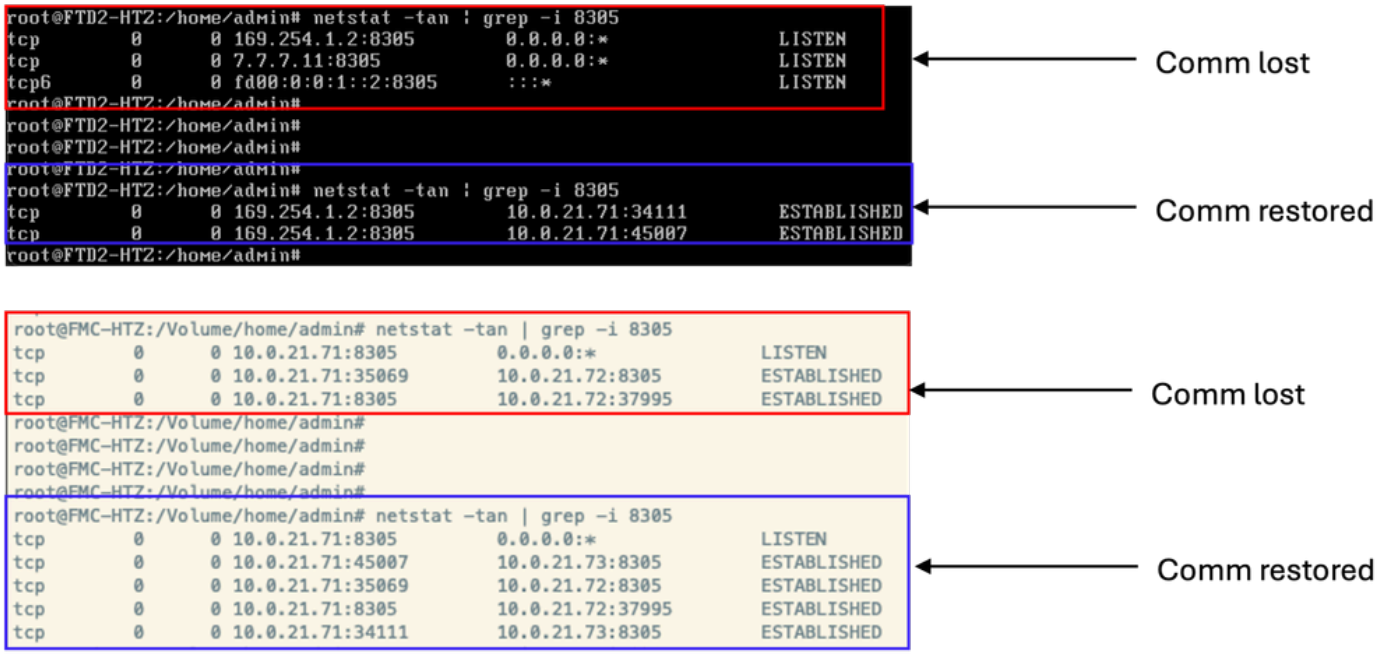
U wordt nu gevraagd om wijzigingen op te slaan en er wordt een waarschuwing weergegeven met de mededeling dat wijzigingen niet worden bewaard als het apparaat opnieuw wordt opgestart.

```
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. U kunt bevestigen dat de configuratie is toegepast. In dit geval door routes te tonen.

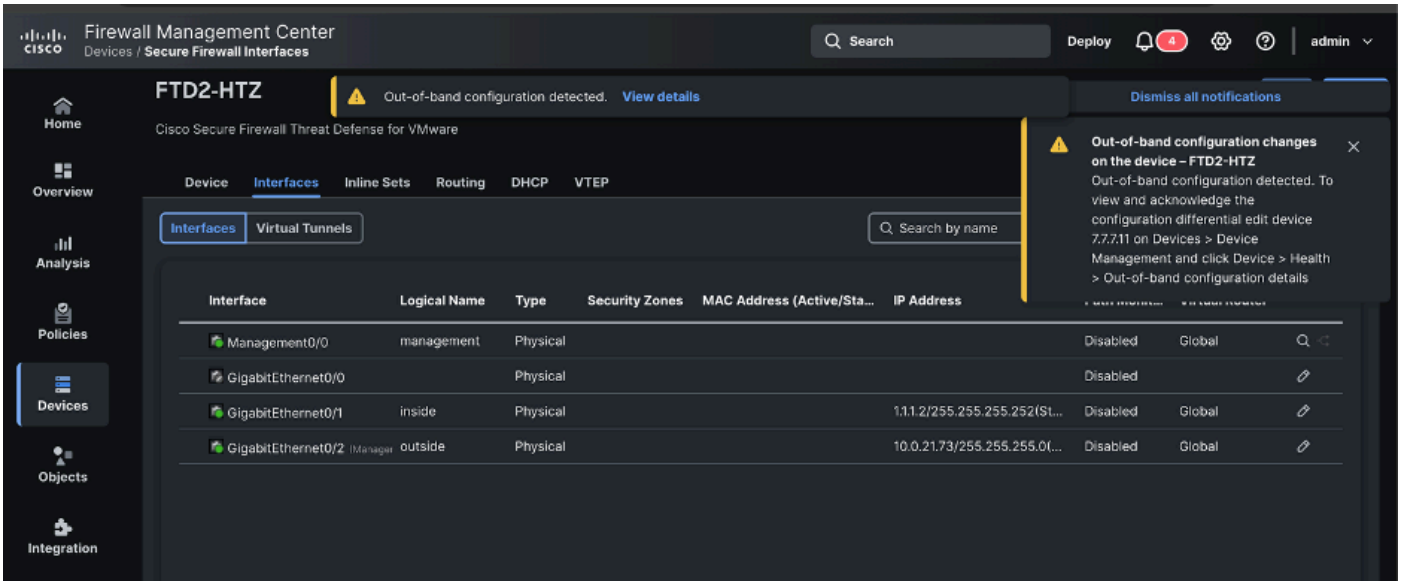
```
firepower# show route

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. Na enkele minuten herstelt deze wijziging de communicatie met het VCC. De volgende afbeeldingen tonen de verbinding die is gemaakt, eerst in FTD en vervolgens in FMC CLI.

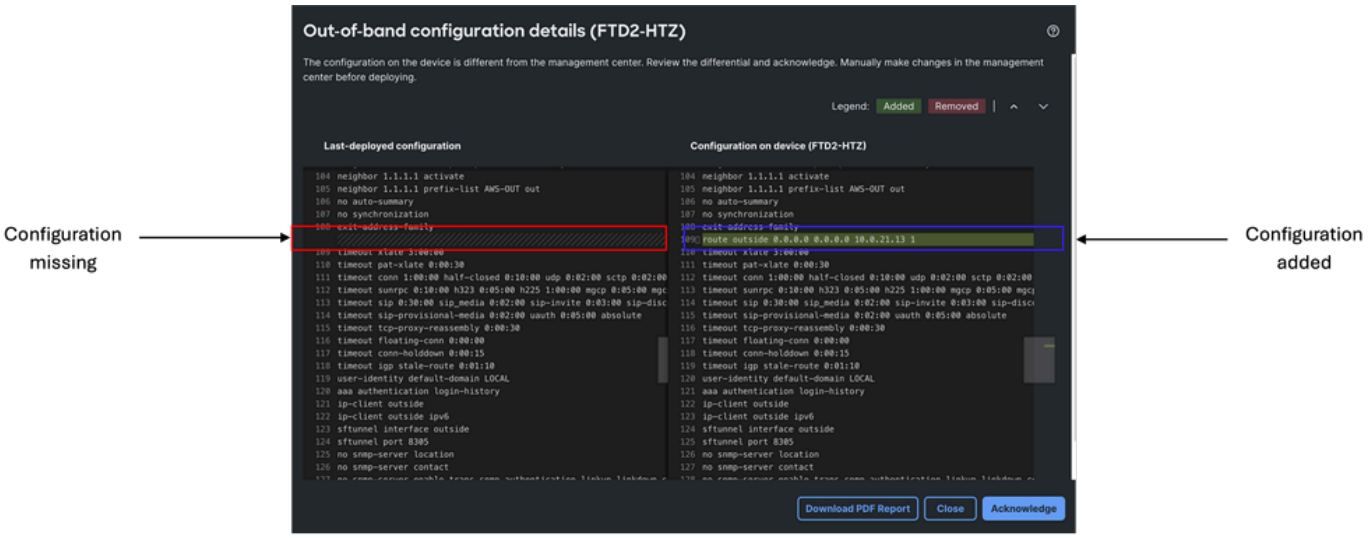


8. Nadat de configuratie is hersteld, kunt u in de FMC GUI naar Apparaat > Apparaatbeheer navigeren en op uw apparaat klikken (in dit geval is dit FTD2-HTZ).

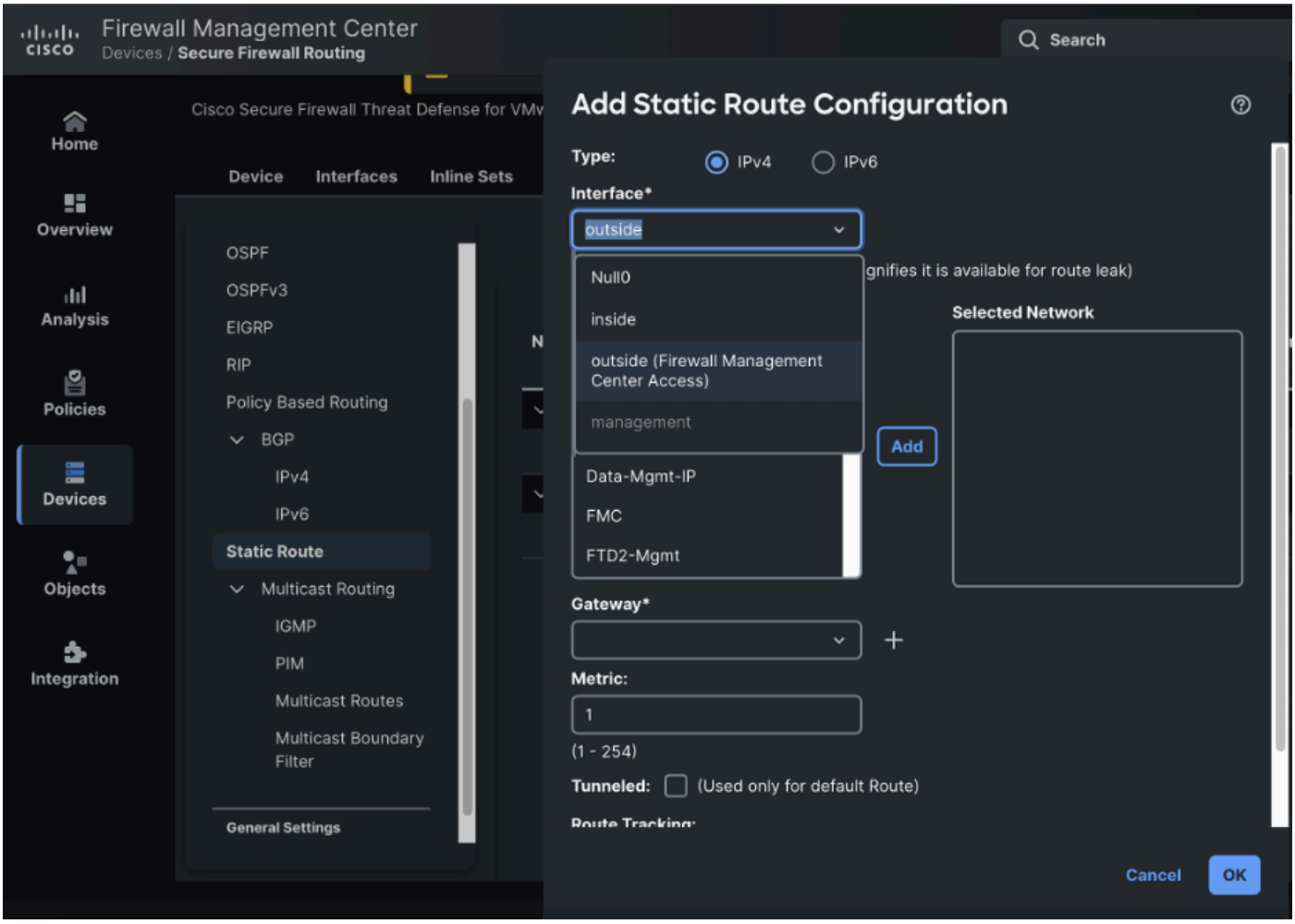
Daar ziet u de waarschuwing voor de out-of-band-configuratie die is gedetecteerd. Klik in Details weergeven om configuratieverschillen te zien.

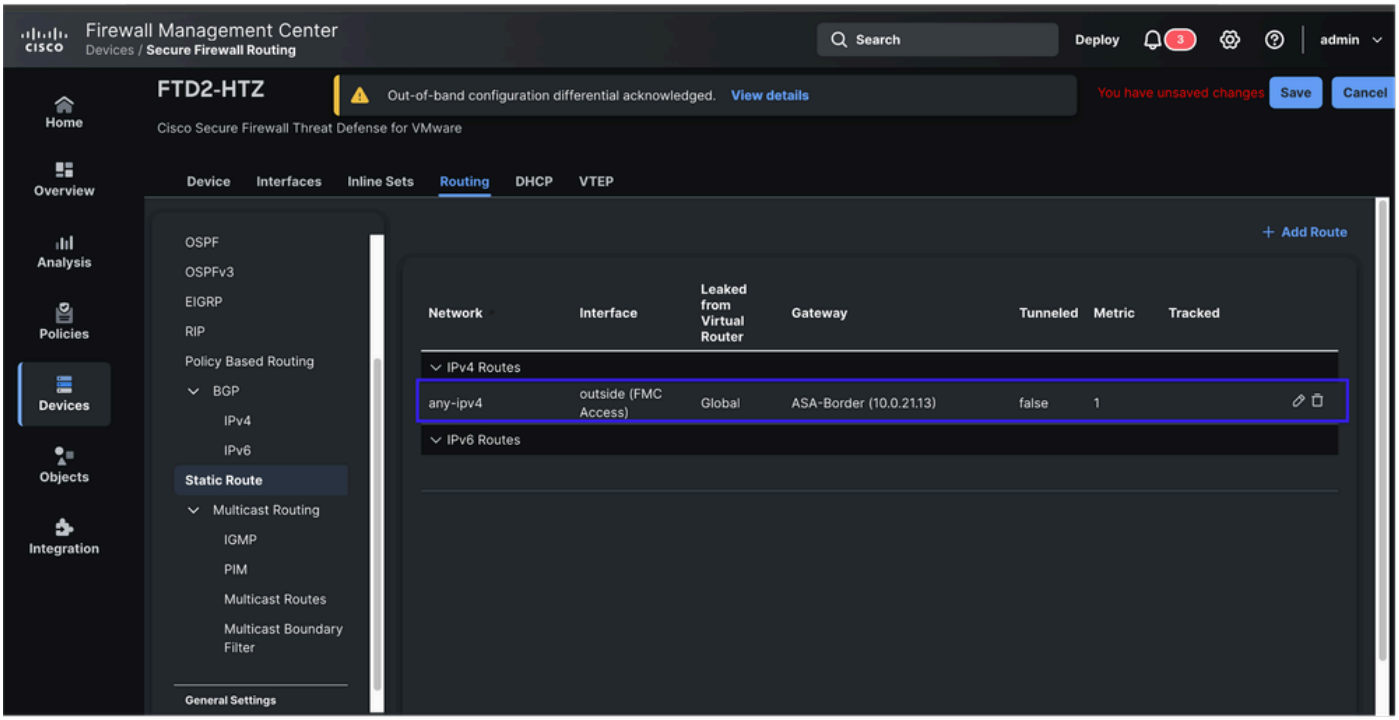


9. Bekijk details van de out-of-band configuratie en bevestig verschillen.



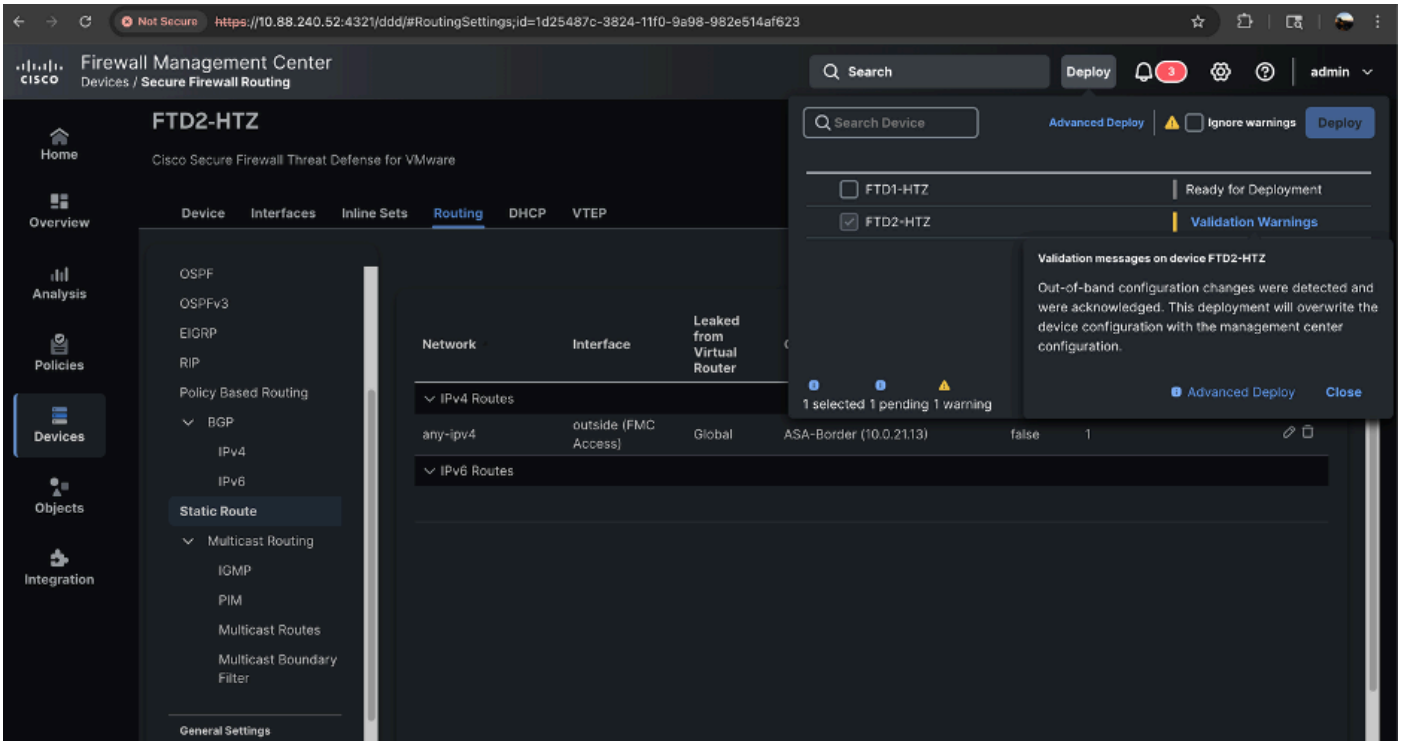
10. Nadat configuratieverschillen zijn bevestigd, configureert u dezelfde wijzigingen die in de herstelmodus zijn uitgevoerd, maar nu via de FMC GUI. In dit scenario wordt een statische route toegevoegd.

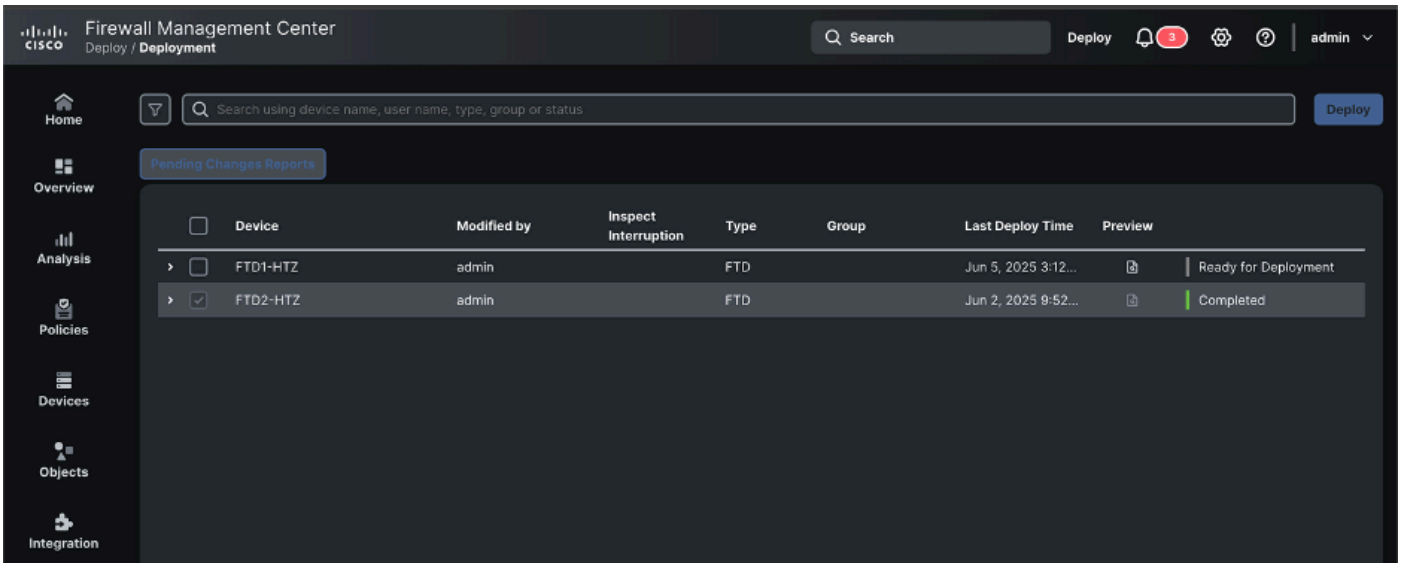




11. Zodra de configuratiewijzigingen zijn opgeslagen, gaat u verder met het implementeren van de wijzigingen. Er wordt een andere waarschuwing weergegeven die aangeeft dat wijzigingen in de out-of-band-configuratie zijn gedetecteerd en bevestigd en dat de wijzigingen worden overschreven door de huidige implementatie.

Zodra de implementatie is voltooid, wordt de configuratie opnieuw gesynchroniseerd.





Referenties

- 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.