Verwenden des Wiederherstellungskonfigurationsmodus für die Konfiguration im Notfall

Inhalt

Einleitung

Dieses Dokument beschreibt FTD 7.7 Verwenden des Wiederherstellungskonfigurationsmodus für die geräteinterne Notfallkonfiguration.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD 7.7.0+
- FMC 7.7.0+

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

Diese Funktion wurde in Version 7.7.0 eingeführt und kann verwendet werden, um Out-of-Band-Konfigurationsänderungen durchzuführen, wenn die Managementverbindung ausfällt.

Diese Konfigurationsänderungen werden direkt in der Geräte-CLI durchgeführt, um:

- Stellen Sie die Verwaltungsverbindung wieder her, wenn Sie eine Datenschnittstelle für den Manager-Zugriff verwenden.
- Nehmen Sie ausgewählte Richtlinienänderungen vor, die nicht warten können, bis die Verbindung wiederhergestellt ist.

Sobald die Managementverbindung wiederhergestellt ist:

1. Sie müssen die Konfigurationsunterschiede berücksichtigen, die in der Out-of-Band-Konfigurationswarnung angezeigt werden.
2. Führen Sie vor der Bereitstellung die gleichen Änderungen im FMC durch, da lokale Änderungen immer von der FMC-Bereitstellung überschrieben werden.

Sie können diese Funktionsbereiche in der Diagnose-CLI im Wiederherstellungskonfigurationsmodus konfigurieren:

- Schnittstellen
- Statische Routen
- Dynamisches Routing: BGP und OSPF
- Vorfilter
- Standortübergreifendes VPN

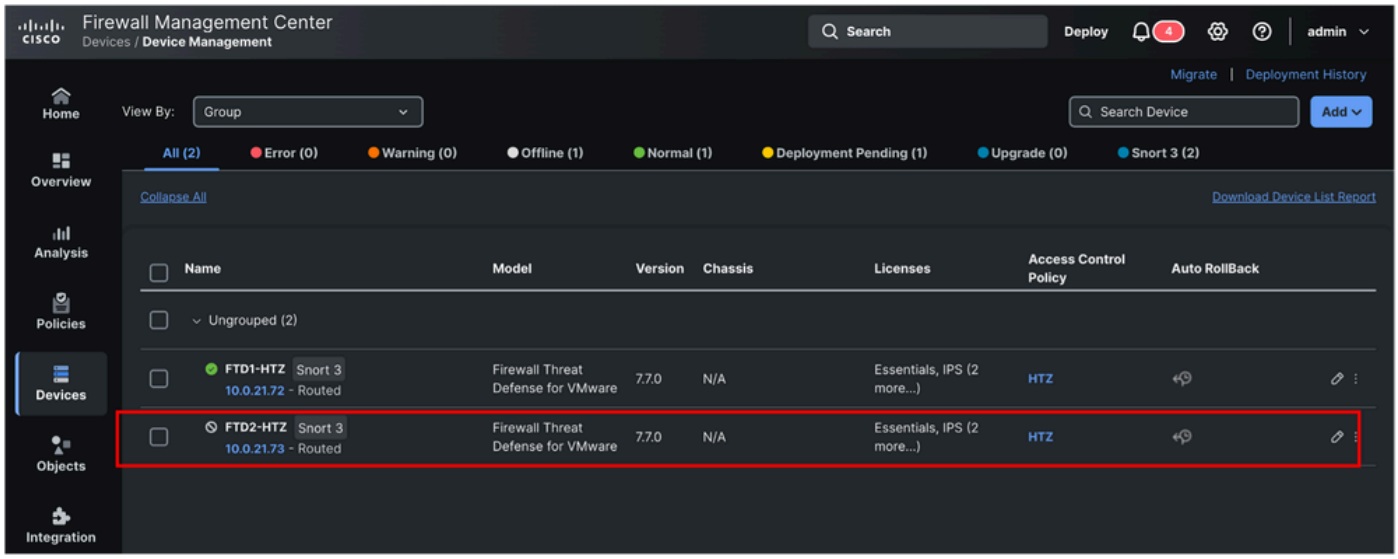
Konfigurationsbeispiel

Laborhintergrund

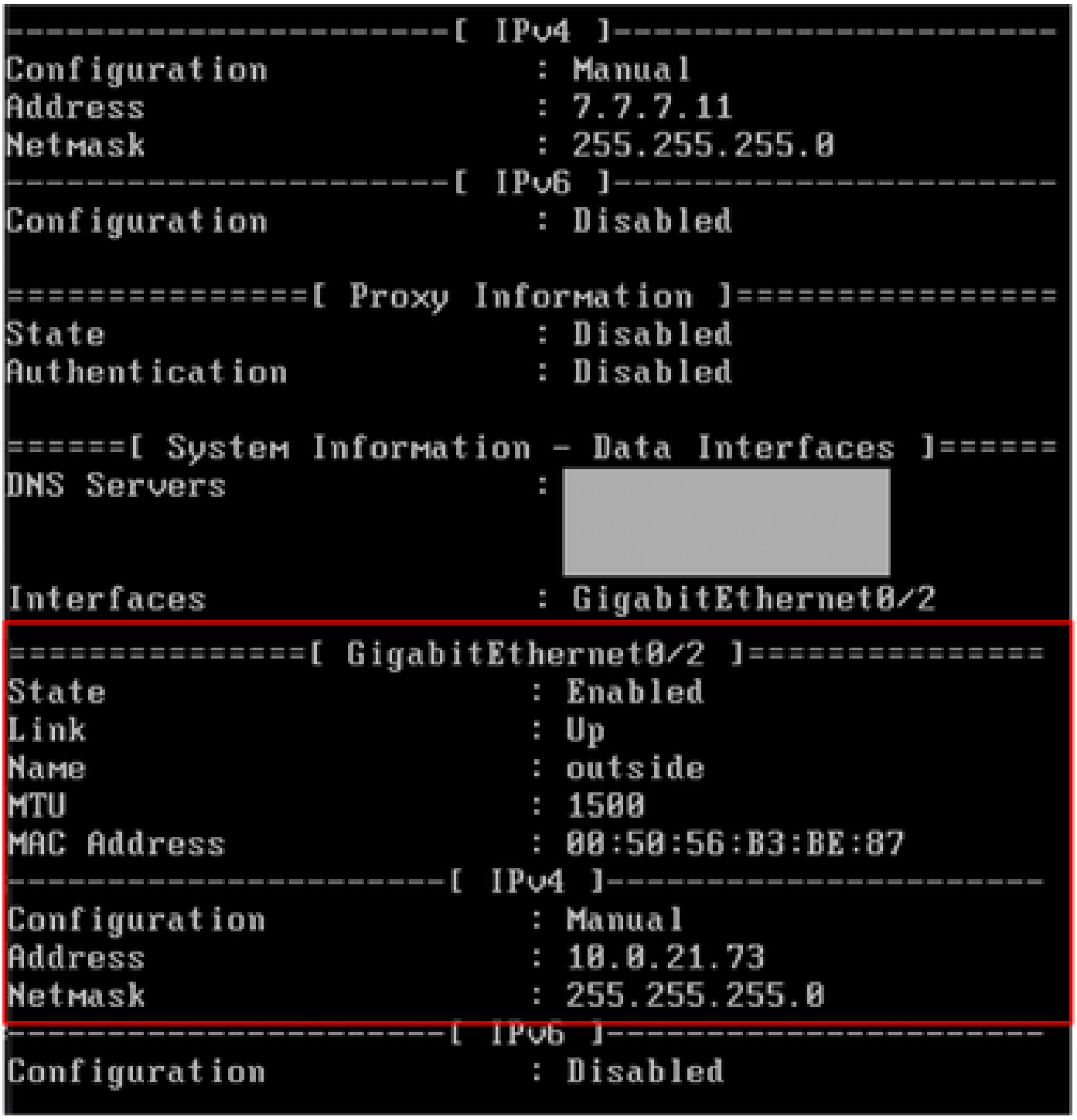
In diesem Szenario hat ein FTD-Gerät, das bei einem FMC registriert ist (und die Datenschnittstelle als Managementschnittstelle verwendet), die Managementverbindung verloren, und zur Behebung dieses Problems wird dem FTD mithilfe der Funktion zur Wiederherstellungskonfiguration eine statische Route hinzugefügt.

FMC verfügt über zwei registrierte Threat Defence-Geräte (10.0.21.72 und 10.0.21.73), von denen jedoch nur eines erreichbar ist, wie in den folgenden Bildern (CLI und GUI) dargestellt.

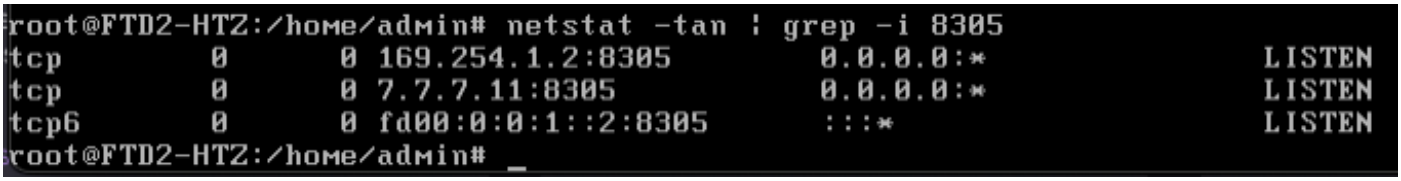
```
root@FMC-HTZ:/Volume/home/admin# netstat -tan | grep -i 8305
tcp        0      0 10.0.21.71:8305         0.0.0.0:*               LISTEN
tcp        0      0 10.0.21.71:35069        10.0.21.72:8305         ESTABLISHED
tcp        0      0 10.0.21.71:8305         10.0.21.72:37995        ESTABLISHED
root@FMC-HTZ:/Volume/home/admin#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



FTD nutzt die Datenschnittstelle für den Registrierungsprozess bei FMC.



FTD hat auch keine Verbindung zu FMC über sftunnel .



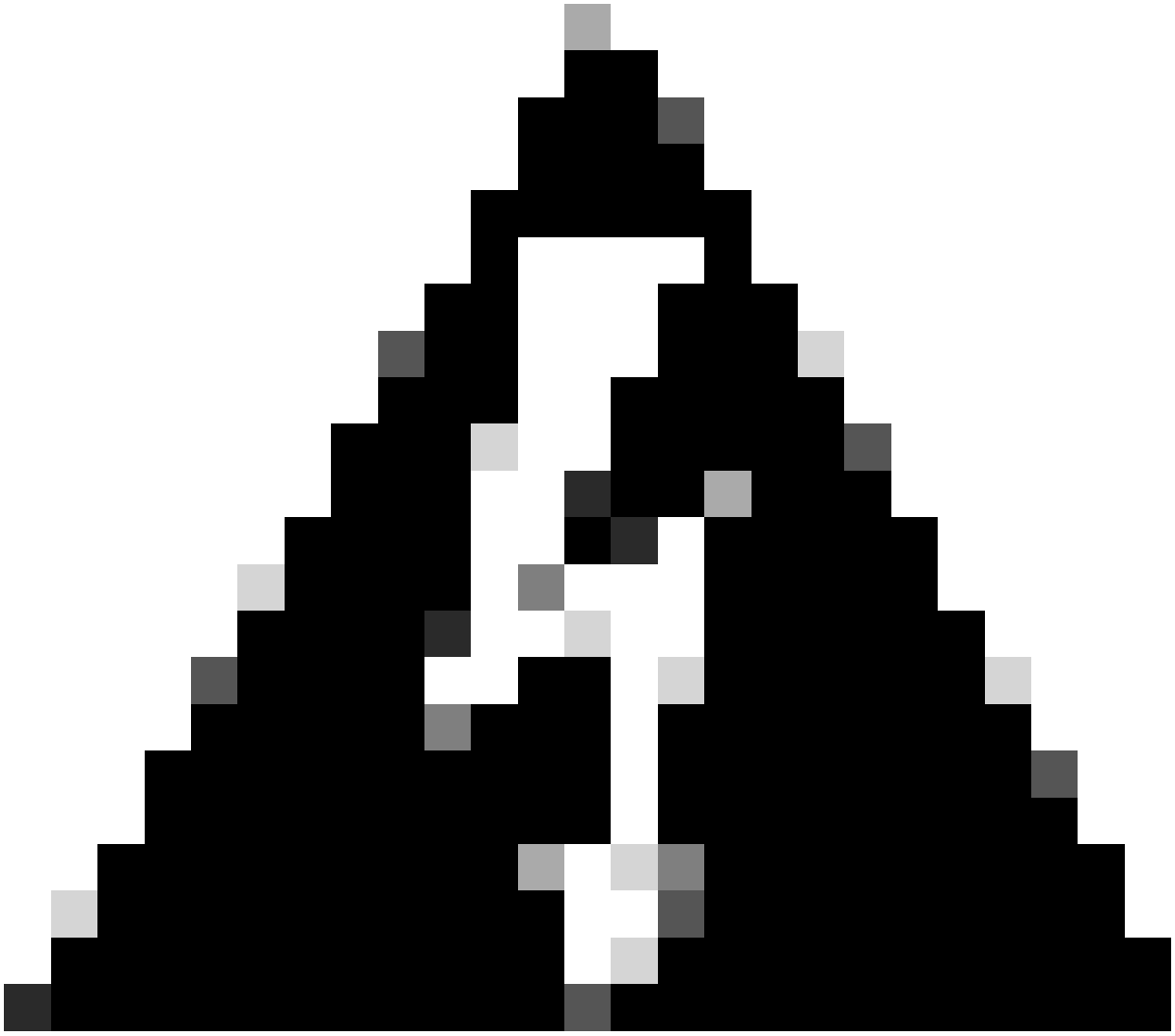
Konfigurationsschritte

1. Um die Funktion "recovery-config" verwenden zu können, müssen Sie sich bei FTD CLI anmelden und in den Lina-Modus wechseln (System support diagnostic-cli).

2. Führen Sie den Befehl configure recovery-config aus.

3. Wenn Sie Fragezeichen (?) eingeben, werden alle unterstützten Befehle aufgelistet, wie in der nächsten Liste gezeigt.

```
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
```



Warnung: Es wird erwartet, dass Sie die Befehle kennen, die für die Wiederherstellung oder den Notfall erforderlich sind. Wenn Sie unsicher sind, welcher Befehl verwendet werden muss, wenden Sie sich an das Cisco TAC.

---

4. Nachdem Sie den Befehl configure recovery-config ausgeführt haben, wird eine Warnung angezeigt, und Sie werden aufgefordert, den Vorgang zu bestätigen und fortzufahren.

```
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. Nach der Bestätigung können Sie mit den verfügbaren Konfigurationsbefehlen beginnen. In diesem Szenario wird der externen Schnittstelle eine statische Route hinzugefügt. Nachdem die Konfiguration abgeschlossen ist, führen Sie den Befehl exit aus, um den Wiederherstellungsmodus zu beenden.

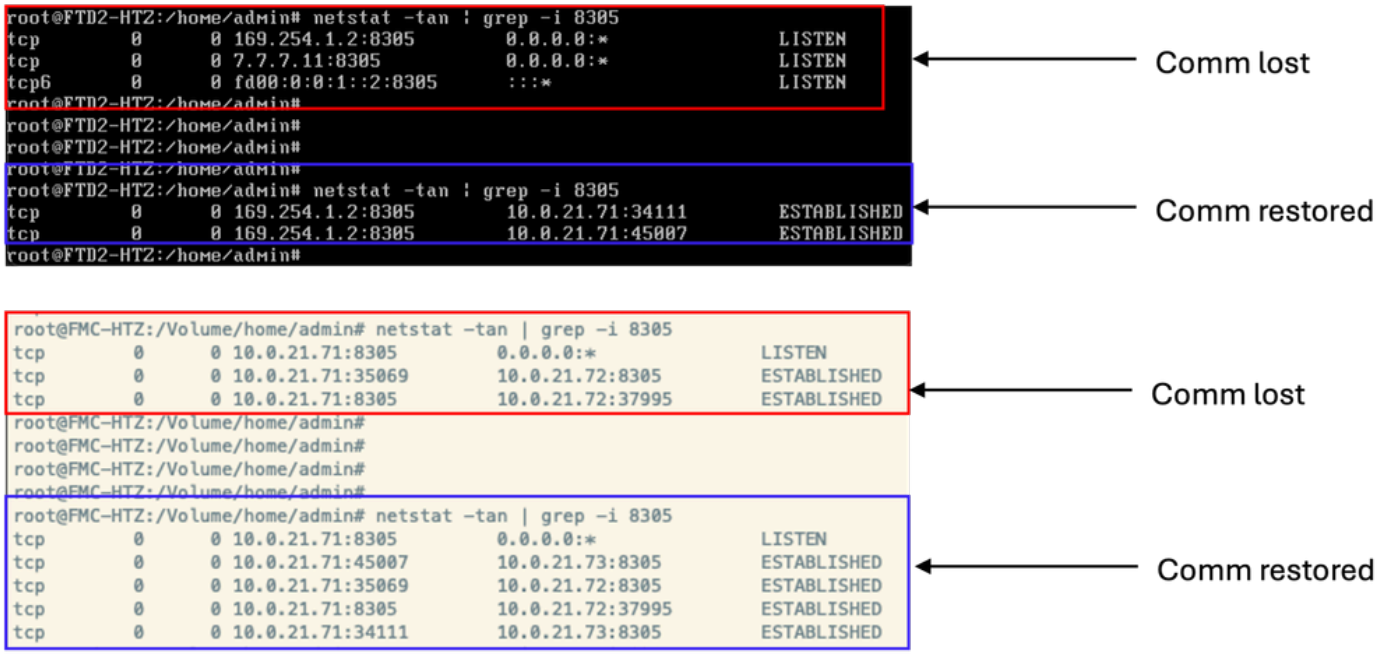
Sie werden nun aufgefordert, die Änderungen zu speichern, und es wird eine Warnung angezeigt, dass die Änderungen beim Neustart des Geräts nicht übernommen werden.

```
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. Sie können bestätigen, dass die Konfiguration angewendet wurde. In diesem Fall Routen anzeigen.

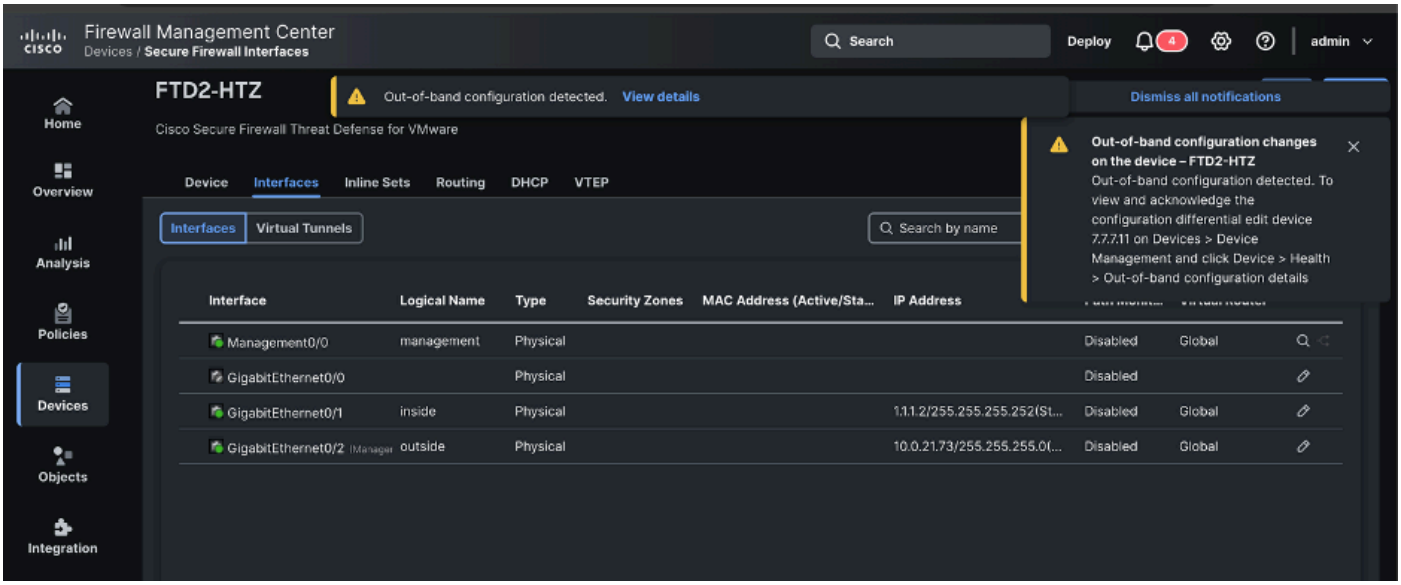
```
firepower# show route

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. Nach einigen Minuten stellt diese Änderung die Kommunikation mit FMC wieder her. Die nächsten Bilder zeigen die Verbindung hergestellt, zuerst in FTD und dann in FMC CLI.

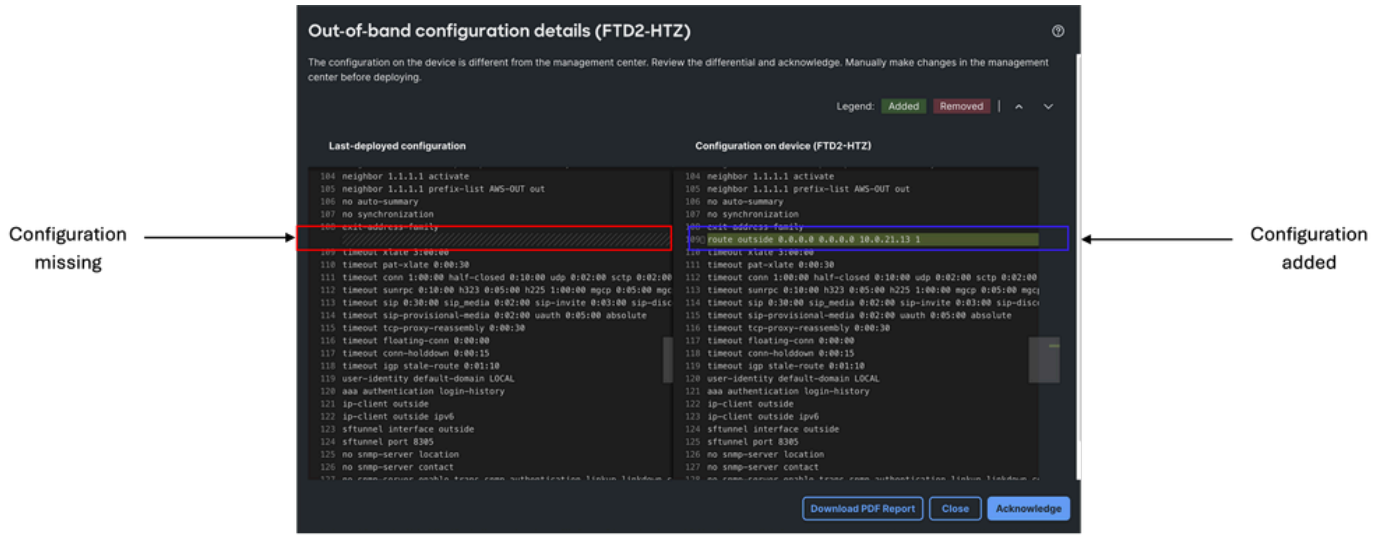


8. Nachdem die Konfiguration wiederhergestellt ist, können Sie in der FMC GUI zu Device > Device Management navigieren und auf Ihr Gerät klicken (in diesem Fall FTD2-HTZ).

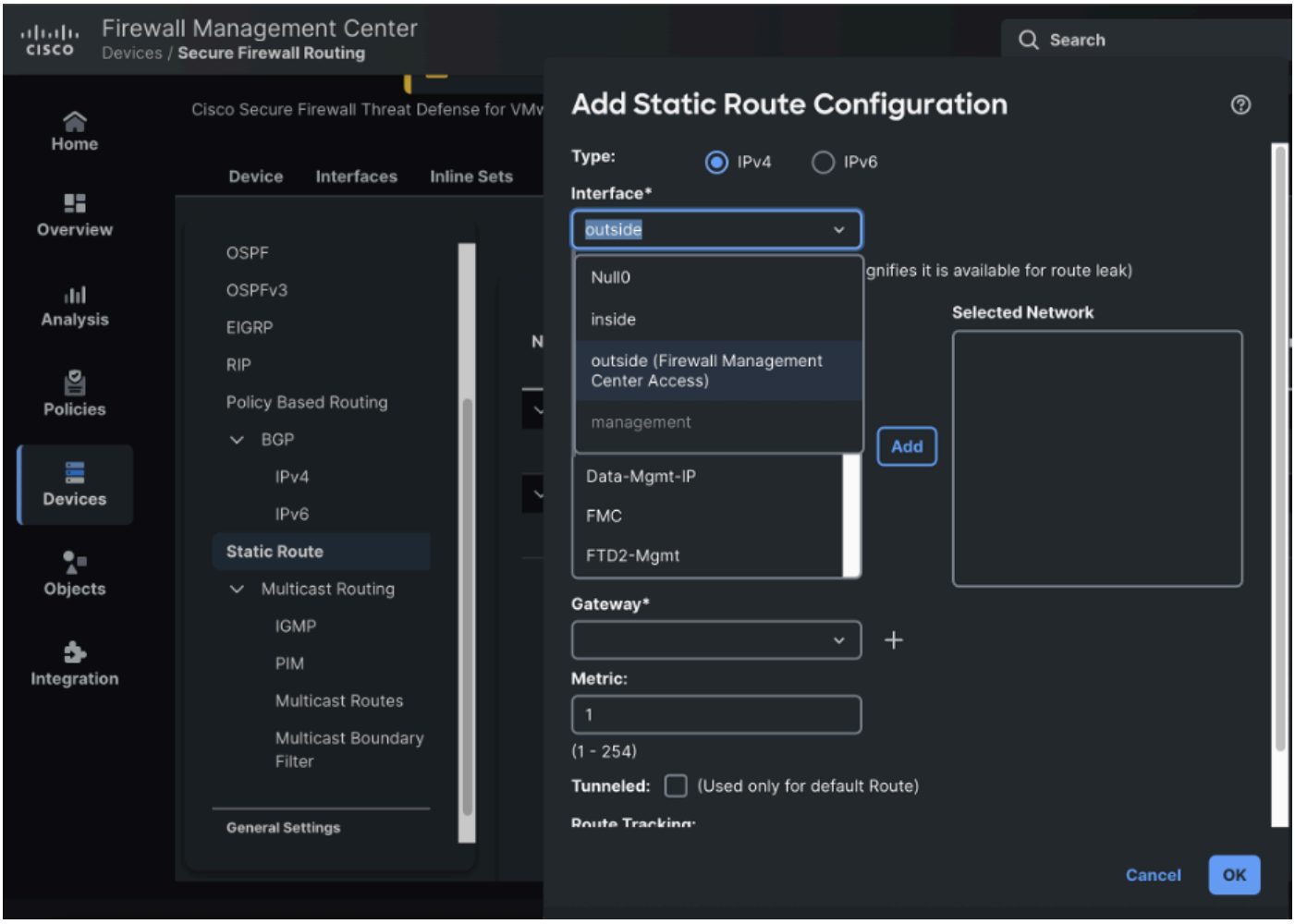
Hier sehen Sie die Warnung zur Out-of-Band-Konfiguration erkannt. Klicken Sie in Details anzeigen, um Konfigurationsunterschiede anzuzeigen.

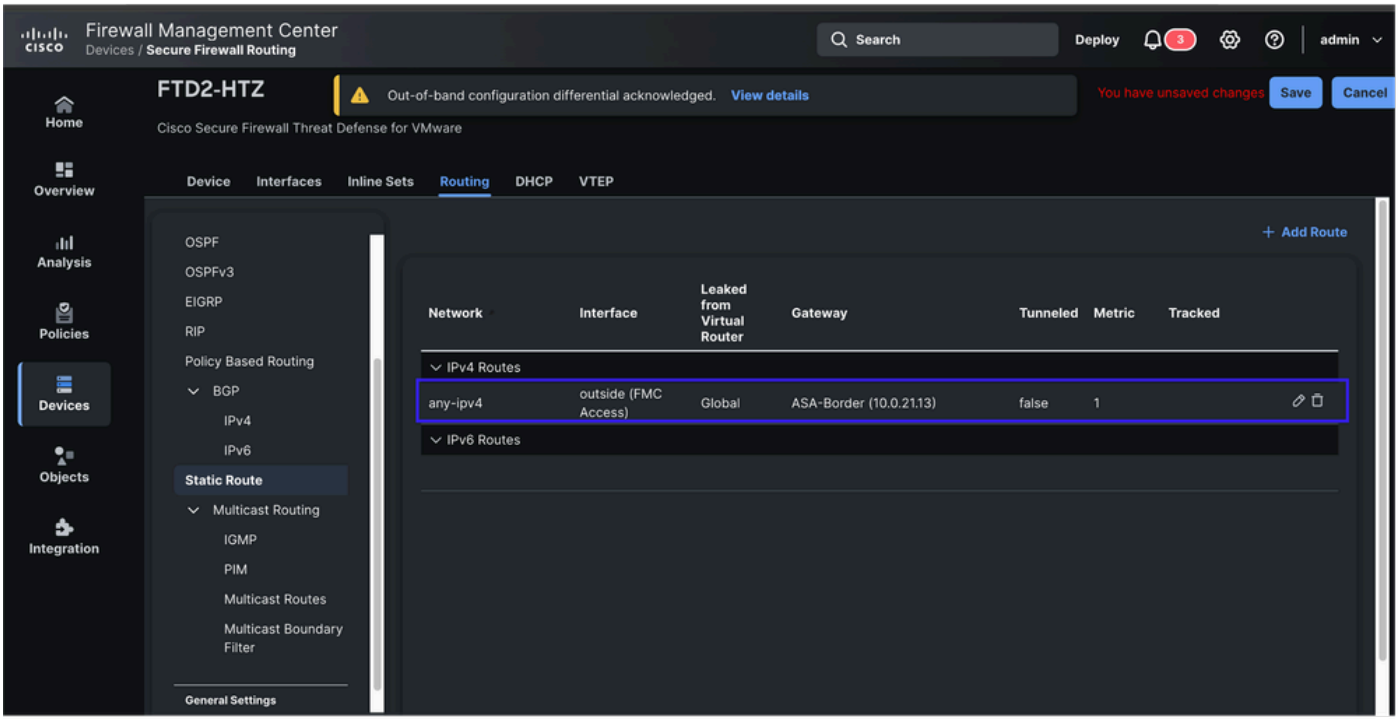


9. Überprüfen Sie die Out-of-Band-Konfigurationsdetails, und bestätigen Sie die Unterschiede.



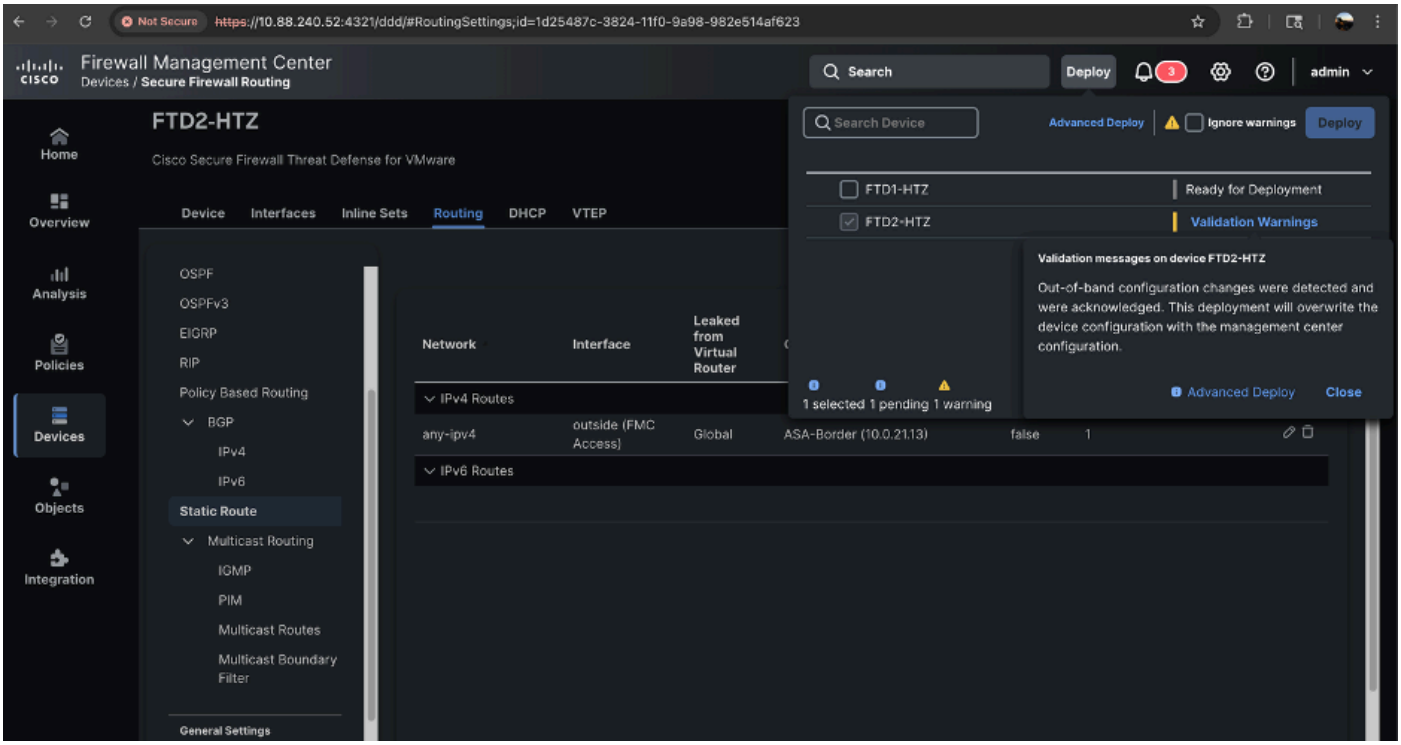
10. Nachdem Konfigurationsunterschiede bestätigt wurden, fahren Sie mit der Konfiguration der gleichen Änderungen fort, die im Wiederherstellungsmodus vorgenommen wurden, jetzt jedoch über die FMC-GUI. In diesem Szenario wird eine statische Route hinzugefügt.

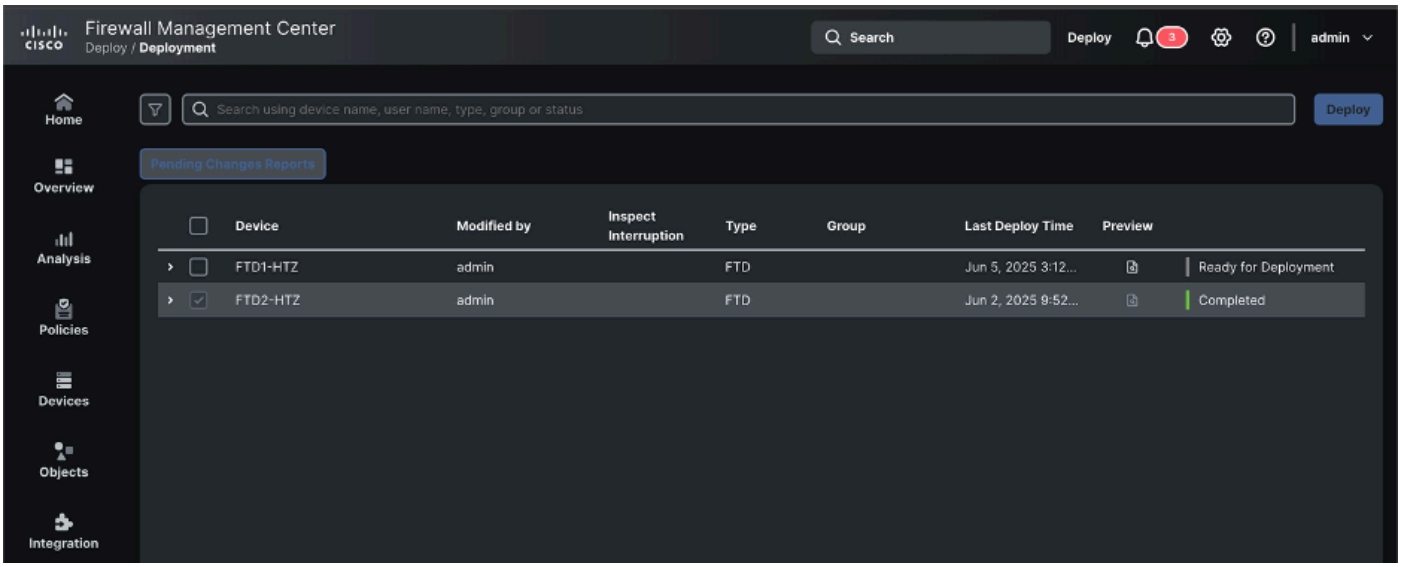




11. Sobald die Konfigurationsänderungen gespeichert wurden, fahren Sie mit der Bereitstellung der Änderungen fort. Eine weitere Warnmeldung informiert Sie darüber, dass Out-of-Band-Konfigurationsänderungen erkannt und bestätigt wurden und dass die Änderungen von der aktuellen Bereitstellung überschrieben werden.

Sobald die Bereitstellung erfolgreich war, wird die Konfiguration erneut synchronisiert.





Referenzen

- 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.