Utilizar el modo de configuración de recuperación para la configuración de emergencia en el dispositivo

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Background

Ejemplo de configuración

- Experiencia de laboratorio
- Configuration Steps

Referencias

Introducción

Este documento describe FTD 7.7 Use Recovery-config Mode for Emergency on-device Configuration.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD 7.7.0+
- FMC 7.7.0+

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Esta función se ha introducido en la versión 7.7.0 y se puede utilizar para realizar cambios de configuración fuera de banda cuando la conexión de administración está inactiva.

Estos cambios de configuración se realizan directamente en la CLI del dispositivo para:

- Restaure la conexión de administración si está utilizando una interfaz de datos para el acceso del administrador.
- Realice cambios en la directiva de selección que no puedan esperar hasta que se restaure la conexión.

Una vez restaurada la conexión de administración:

1. Debe reconocer las diferencias de configuración que se muestran en la alerta de configuración fuera de banda.
2. Realice los mismos cambios en el FMC antes de realizar la implementación, ya que los cambios locales siempre se sobrescriben con la implementación de FMC.

Puede configurar estas áreas de funciones en la CLI de diagnóstico en el modo recovery-config:

- Interfaces
- rutas estáticas
- Routing dinámico: BGP y OSPF
- Prefiltros
- VPN de sitio a sitio

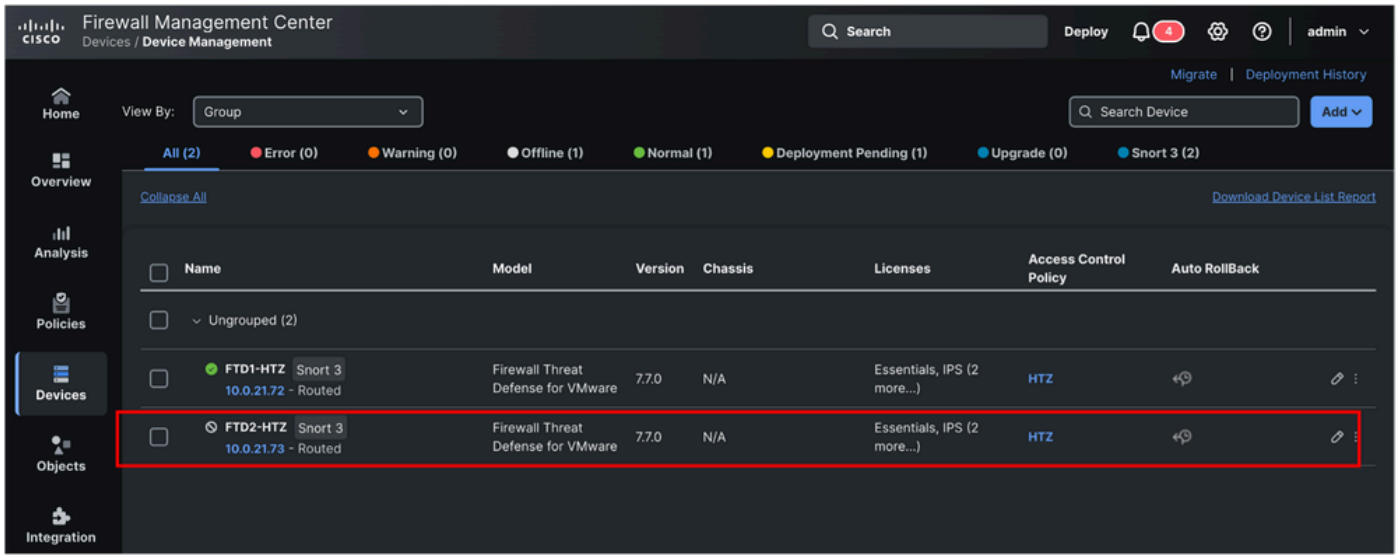
Ejemplo de configuración

Experiencia de laboratorio

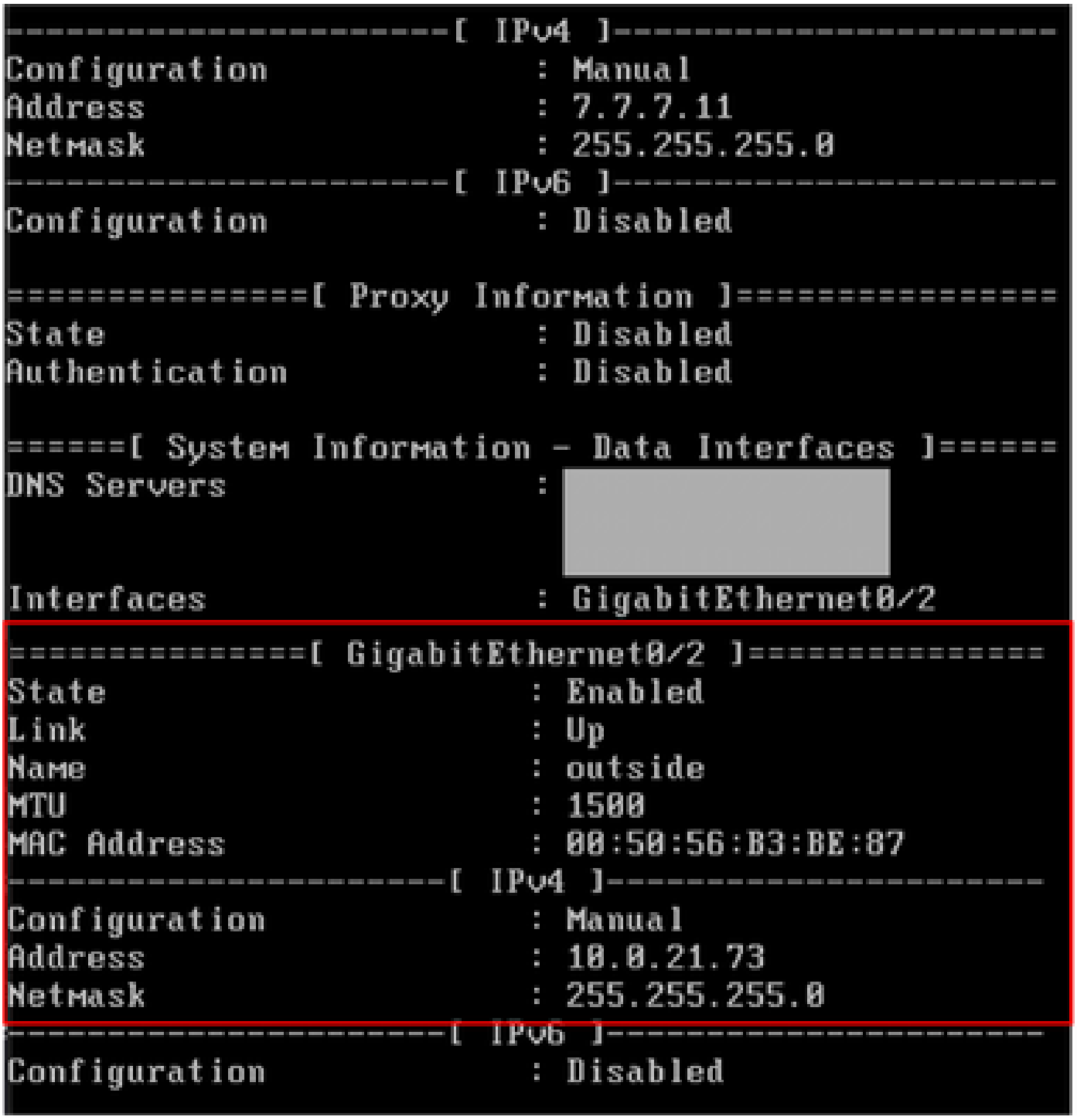
En esta situación, un dispositivo FTD registrado en un FMC (que utiliza una interfaz de datos como interfaz de gestión) ha perdido la conexión de gestión y, para solucionar este problema, se agrega una ruta estática al FTD mediante la función recovery-config (configuración de recuperación).

FMC tiene registrados dos dispositivos de defensa frente a amenazas (10.0.21.72 y 10.0.21.73), pero solo uno de ellos es accesible, como se muestra en las imágenes siguientes (cli y GUI).

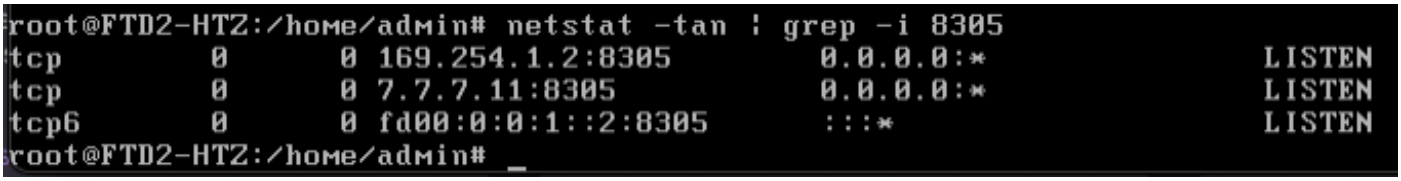
```
root@FMC-HTZ:/Volume/home/admin# netstat -tan | grep -i 8305
tcp        0      0 10.0.21.71:8305         0.0.0.0:*               LISTEN
tcp        0      0 10.0.21.71:35069        10.0.21.72:8305         ESTABLISHED
tcp        0      0 10.0.21.71:8305         10.0.21.72:37995        ESTABLISHED
root@FMC-HTZ:/Volume/home/admin#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



FTD utiliza la interfaz de datos para el proceso de registro en FMC.



FTD tampoco tiene conexión con FMC a través de sftunnel .



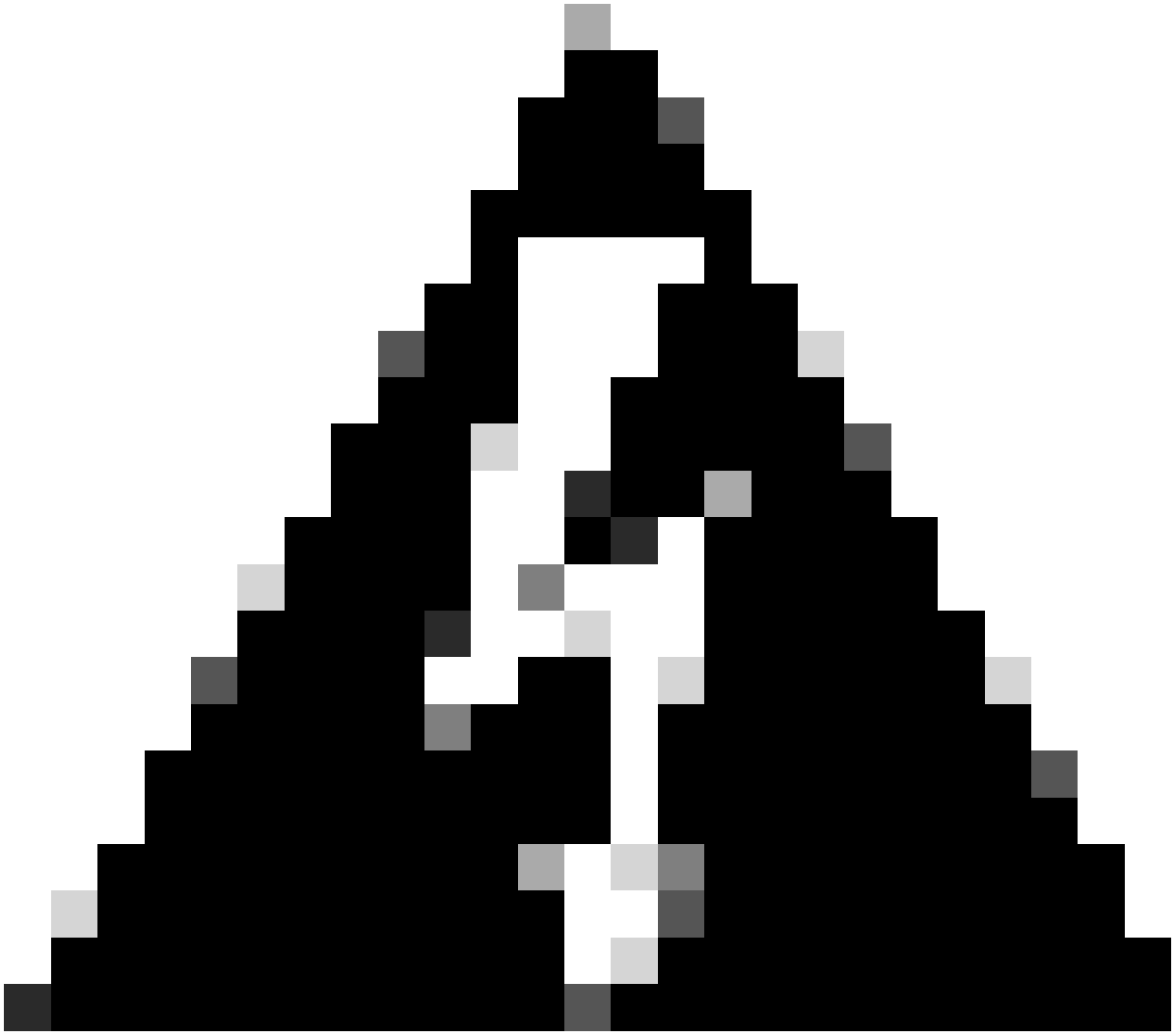
Configuration Steps

1. Para poder utilizar la función recovery-config, debe iniciar sesión en la CLI de FTD e ir al modo de línea (system support diagnostic-cli).

2. Ejecute el comando configure recovery-config.

3. Si escribe el signo de interrogación (?), se enumeran todos los comandos admitidos, como se muestra en la siguiente lista.

```
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
```



Advertencia: Se espera que conozca los comandos que se requieren para la recuperación o el uso de emergencia. Si no está seguro de qué comando debe utilizarse, se recomienda que se ponga en contacto con el TAC de Cisco para obtener orientación.

---

4. Después de ejecutar el comando configure recovery-config, se muestra una alerta y se le solicita que confirme y continúe.

```
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. Una vez confirmado, puede comenzar a utilizar los comandos de configuración disponibles. En este escenario, se agrega una ruta estática a la interfaz externa. Una vez completada la configuración, ejecute el comando exit para salir del modo de recuperación.

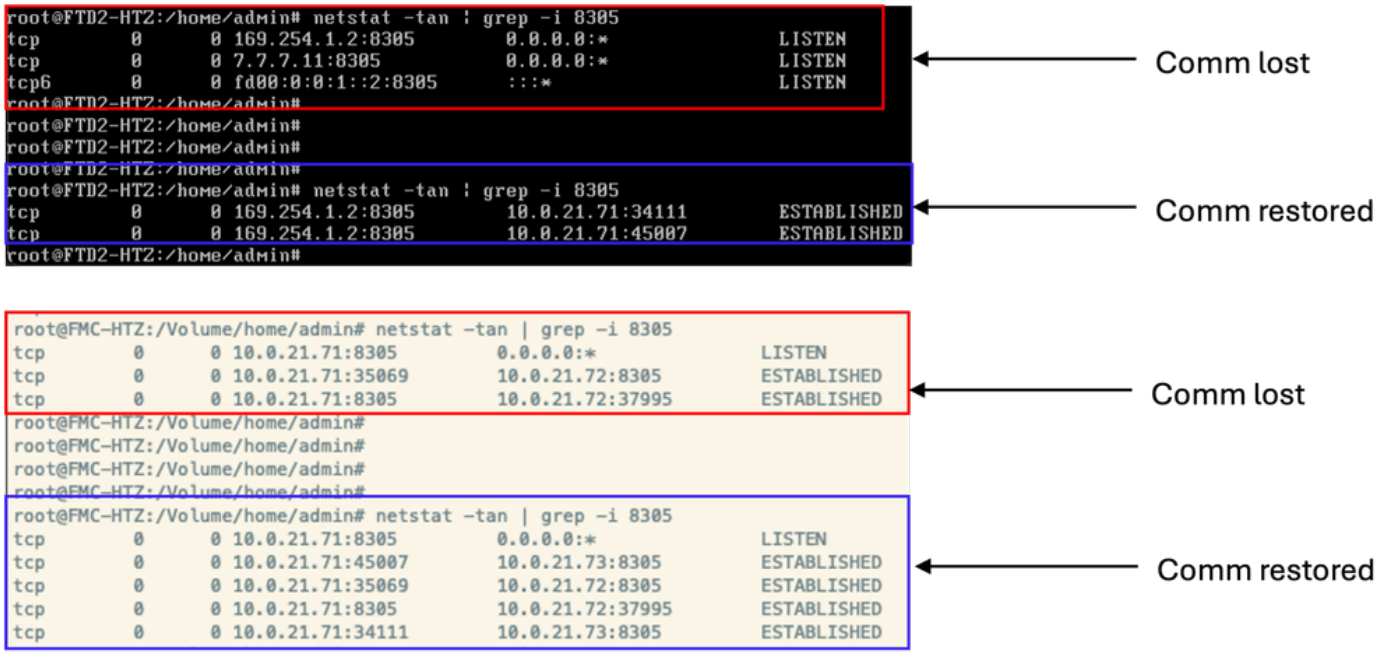
Ahora se le solicita que guarde los cambios y se muestra una alerta que informa de que los cambios no se conservan si se reinicia el dispositivo.

```
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. Puede confirmar que la configuración se ha aplicado. En este caso, se muestran las rutas.

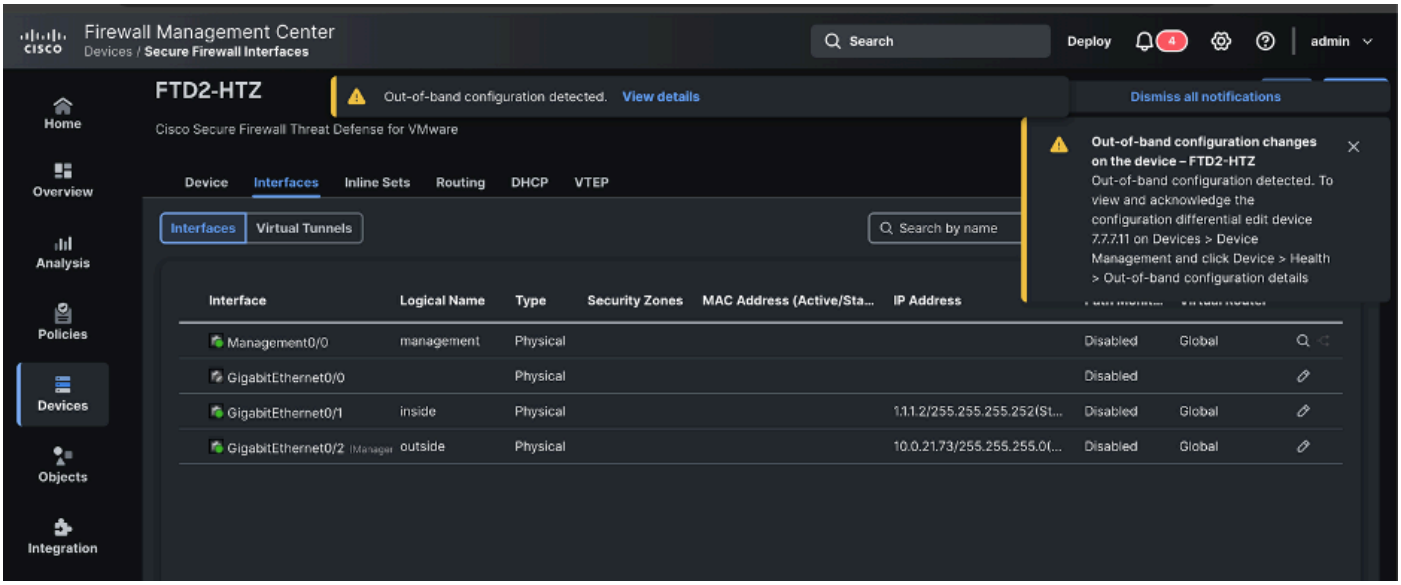
```
firepower# show route

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. Después de varios minutos, este cambio restablece la comunicación con el CSP. Las siguientes imágenes muestran la conexión establecida, primero en FTD y después en FMC CLI.

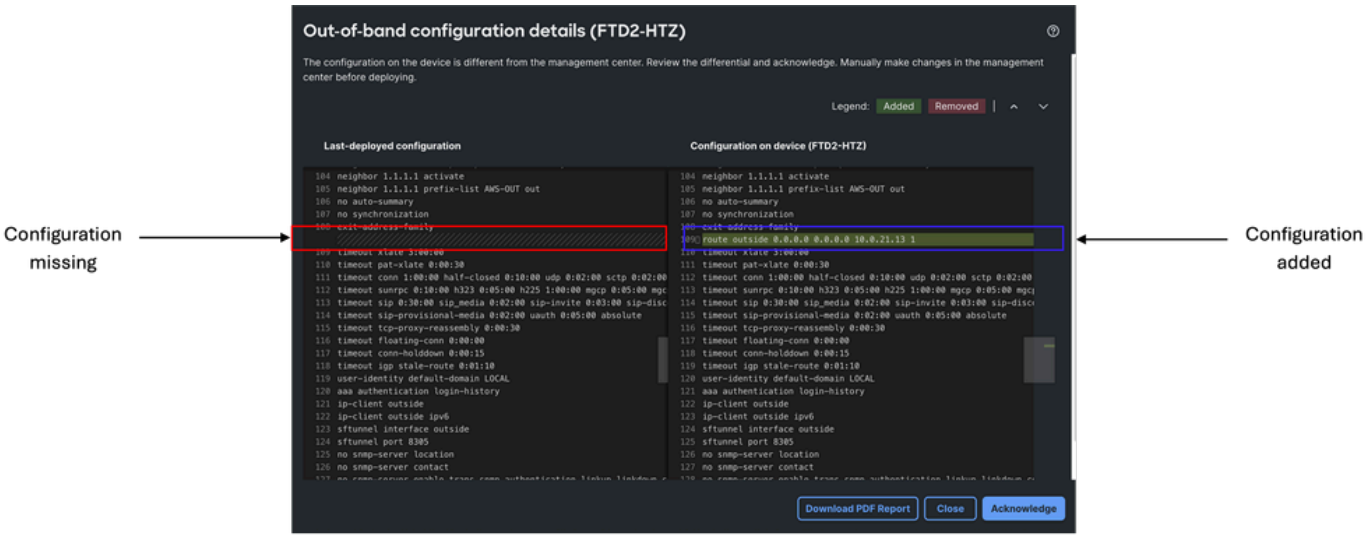


8. Después de restaurar la configuración, en FMC GUI puede navegar a Device > Device Management y haga clic en su dispositivo (en este caso es FTD2-HTZ).

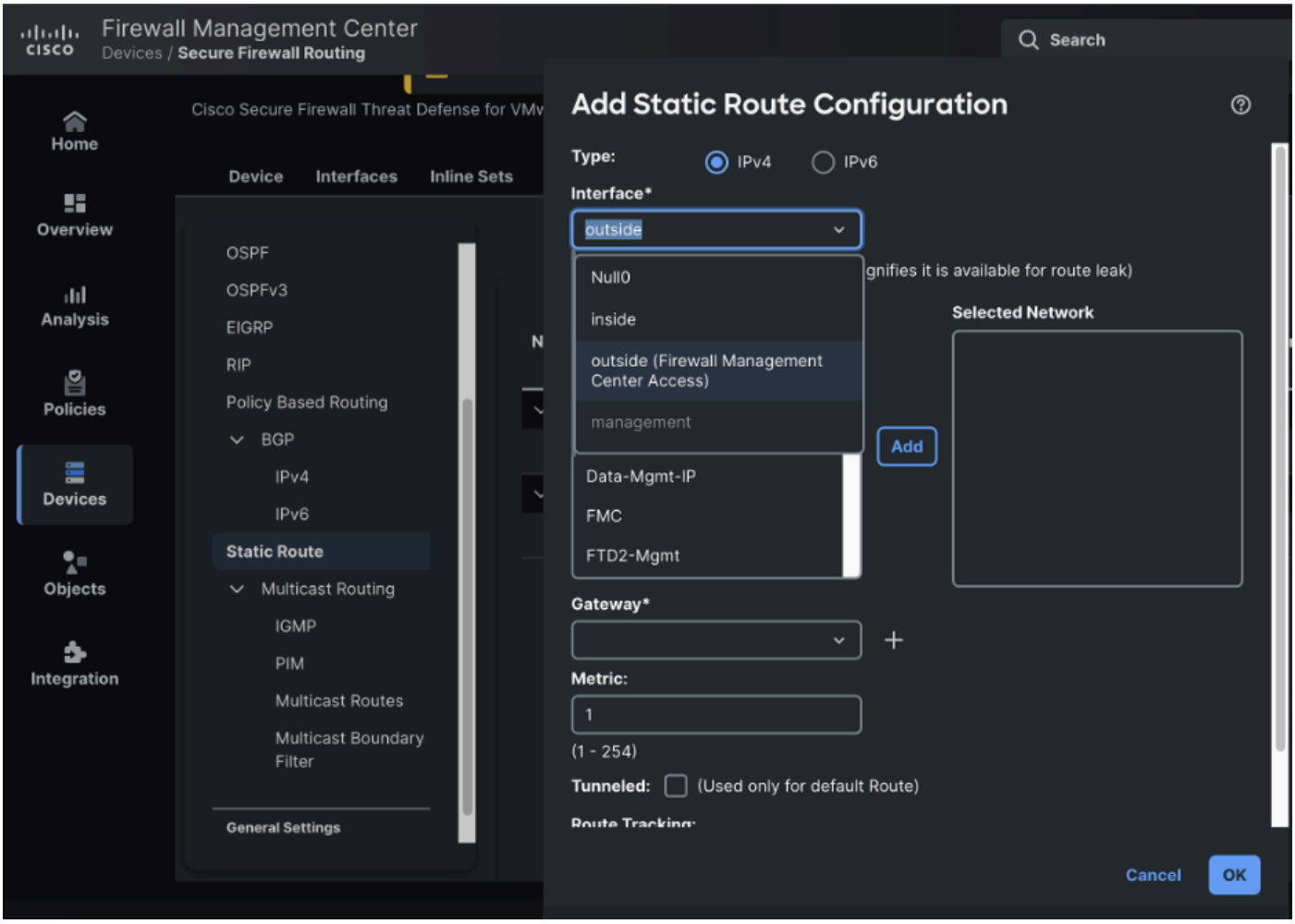
Allí puede ver la alerta de configuración fuera de banda detectada. Haga clic en Ver detalles para ver las diferencias de configuración.

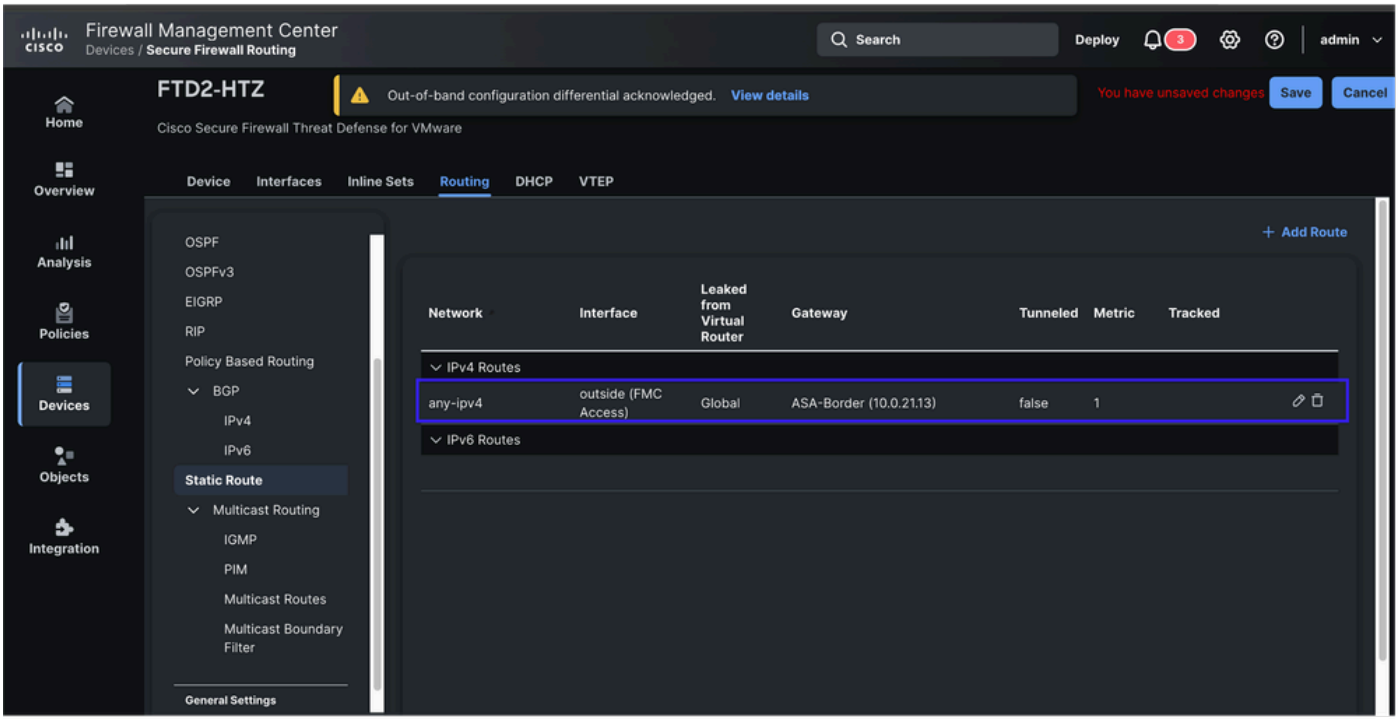


9. Revise los detalles de la configuración fuera de banda y confirme las diferencias.



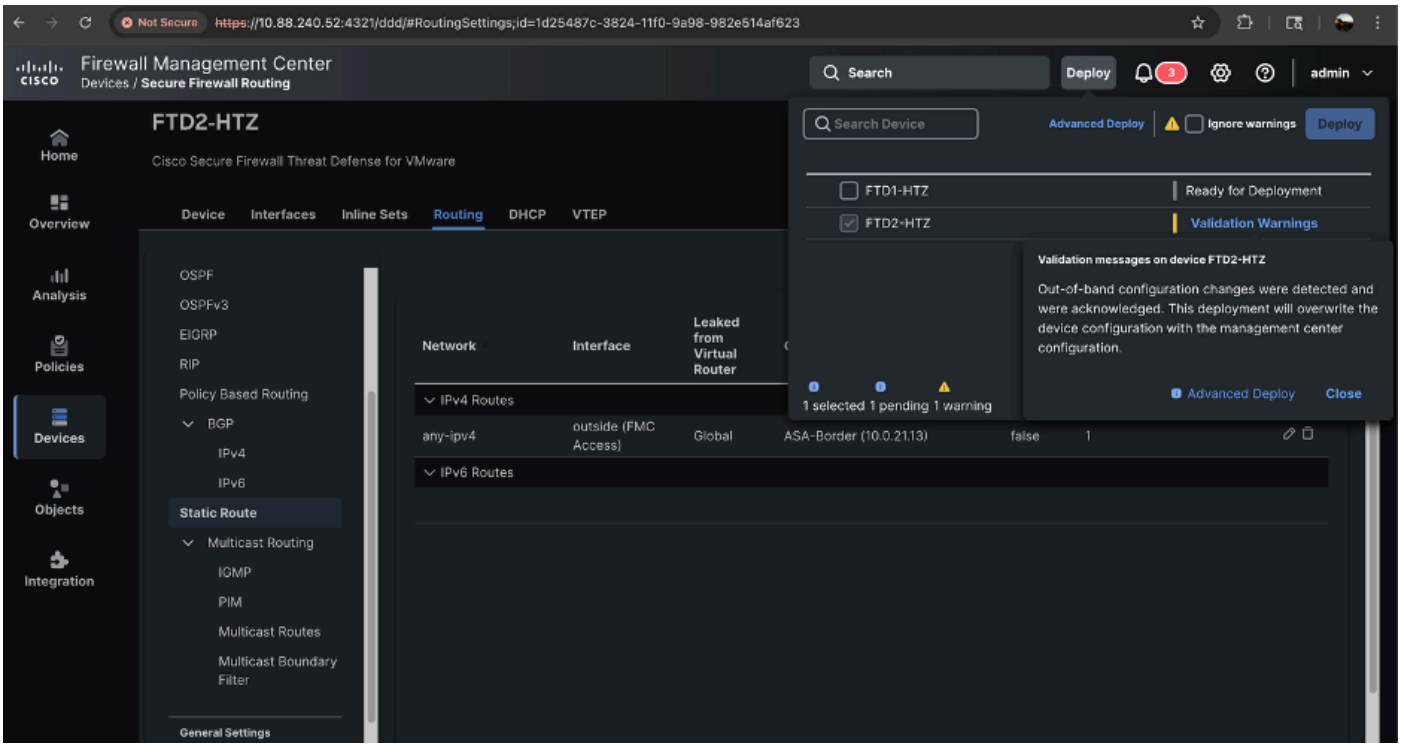
10. Después de reconocer las diferencias de configuración, continúe configurando los mismos cambios realizados en el modo de recuperación, pero ahora a través de la GUI de FMC. En este escenario, se agrega una ruta estática.

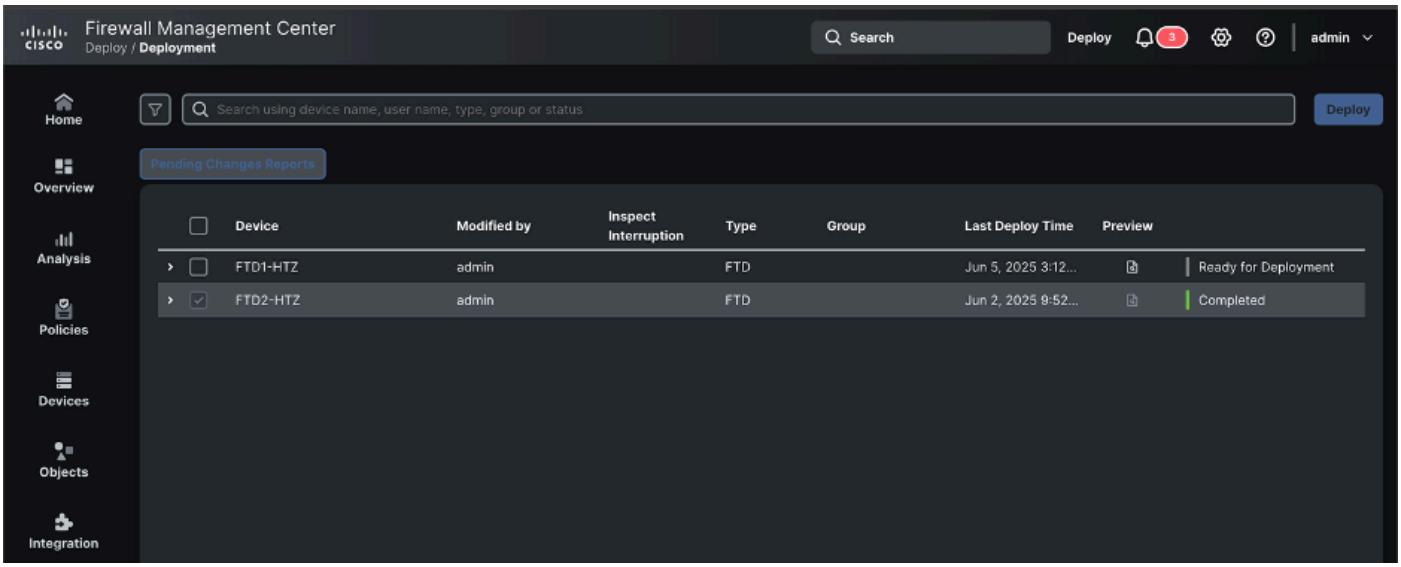




11. Una vez guardados los cambios de configuración, proceda a implementarlos. Se muestra otra alerta que informa que se detectaron y reconocieron los cambios de configuración fuera de banda y que la implementación actual anula los cambios.

Cuando la implementación se realiza correctamente, la configuración vuelve a estar sincronizada.





Referencias

- 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).