使用Recovery-config模式进行紧急设备内配置

目录

简介

本文档介绍FTD 7.7使用恢复配置模式进行紧急设备内配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower威胁防御(FTD)
- 思科Firepower管理中心(FMC)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTD 7.7.0+
- FMC 7.7.0+

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

此功能已在版本7.7.0中引入，可在管理连接关闭时进行带外配置更改。

这些配置更改直接在设备CLI中执行，以便：

- 如果您使用数据接口进行管理器访问，请恢复管理连接。
- 选择在连接恢复之前无法等待的策略更改。

恢复管理连接后：

1. 您需要确认带外配置警报中显示的配置差异。
2. 在部署之前在FMC中执行相同的更改，因为本地更改始终被FMC部署覆盖。

您可以在恢复配置模式下的诊断CLI中配置以下功能区域：

- 接口
- 静态路由
- 动态路由：BGP和OSPF
- 预过滤器
- 站点到站点 VPN

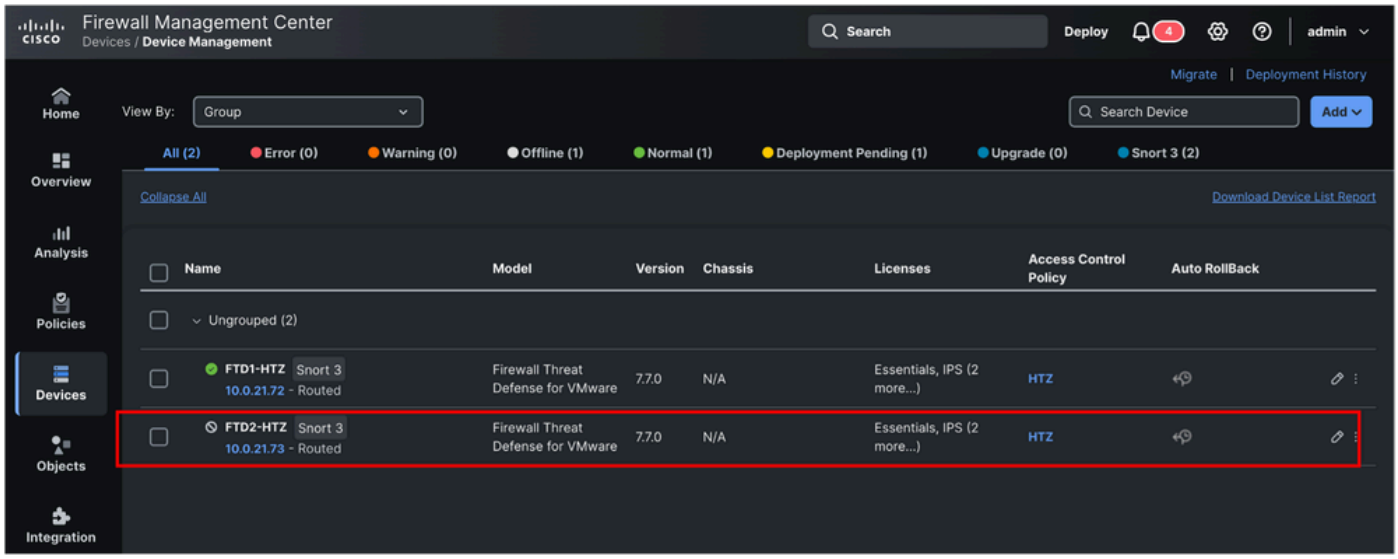
配置示例

实验背景

在此场景中，注册到FMC（使用数据接口作为管理接口）的FTD设备丢失了管理连接，为了解决此问题，将使用恢复配置功能向FTD添加静态路由。

FMC注册了两台威胁防御设备（10.0.21.72和10.0.21.73），但仅其中一台可访问，如下面的映像（cli和GUI）所示。

```
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使用数据接口向FMC进行注册过程。

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

FTD也没有通过sftunnel连接到FMC。

```
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# _
```

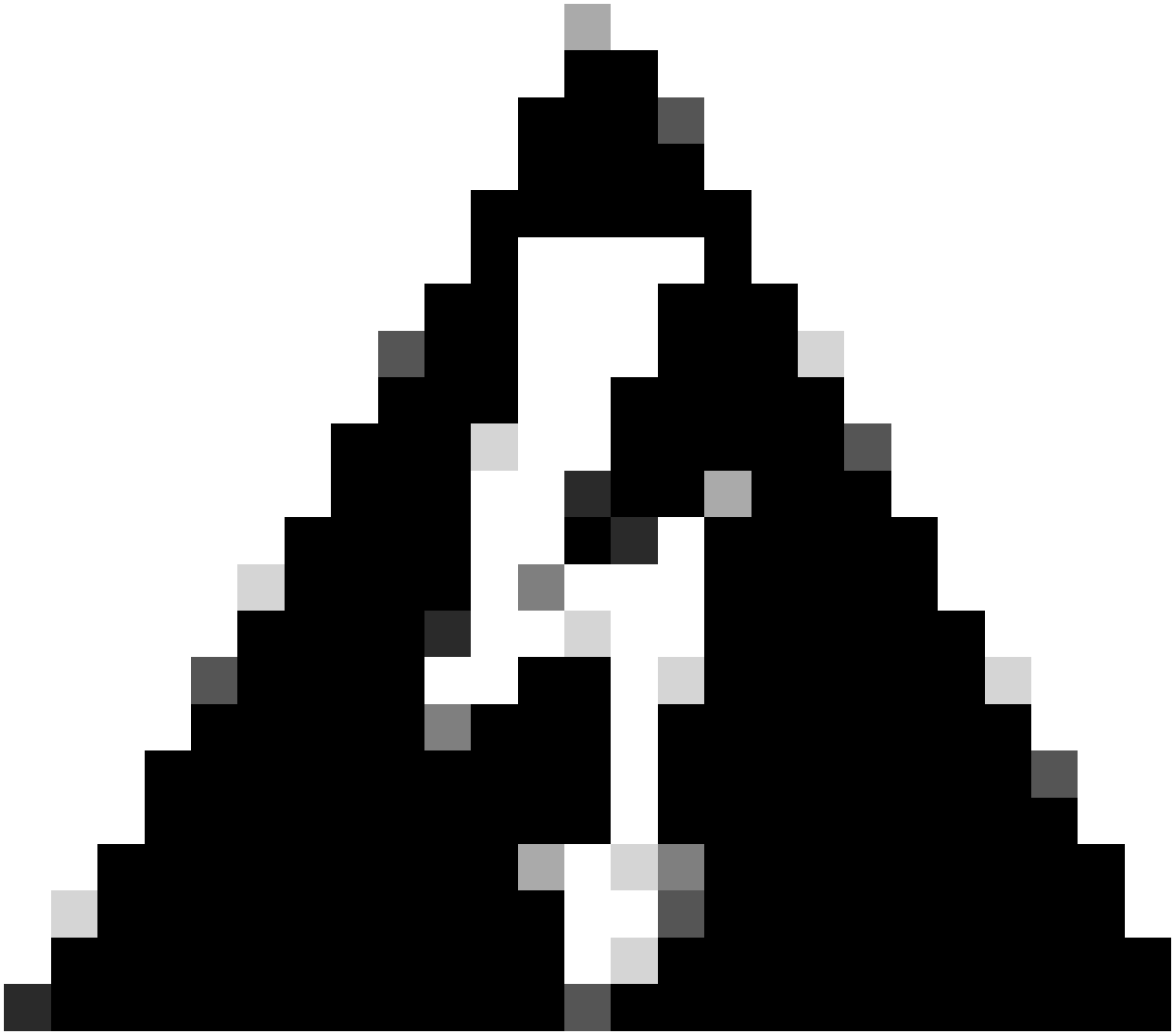
配置步骤

1.为了能够使用恢复配置功能，您需要登录到FTD CLI并进入lina模式(system support diagnostic-cli)。

2.运行configure recovery-config命令。

3.如果键入问号(?)，则会列出所有支持的命令，如下表所示。

```
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：您需要了解恢复或紧急使用所需的命令。如果您不确定必须使用哪条命令，建议您联系Cisco TAC寻求指导。

4.在运行configure recovery-config命令后，将显示警报，并要求您确认并继续。

```
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.确认后，您可以开始使用可用的config命令。在这种情况下，静态路由会添加到外部接口。配置完成后，运行exit命令退出恢复模式。

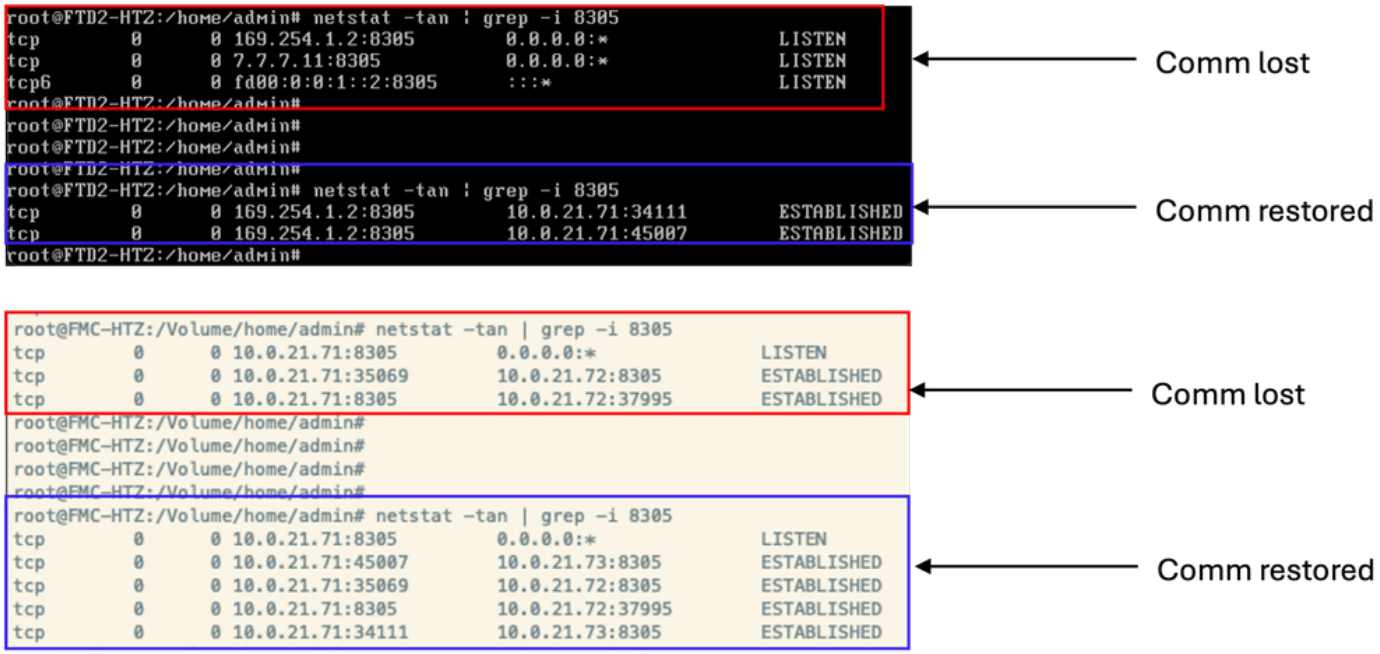
系统会要求您保存更改，并显示一个警报，通知您在设备重新启动后不会保留更改。

```
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.您可以确认配置已应用。在本例中，显示路由。

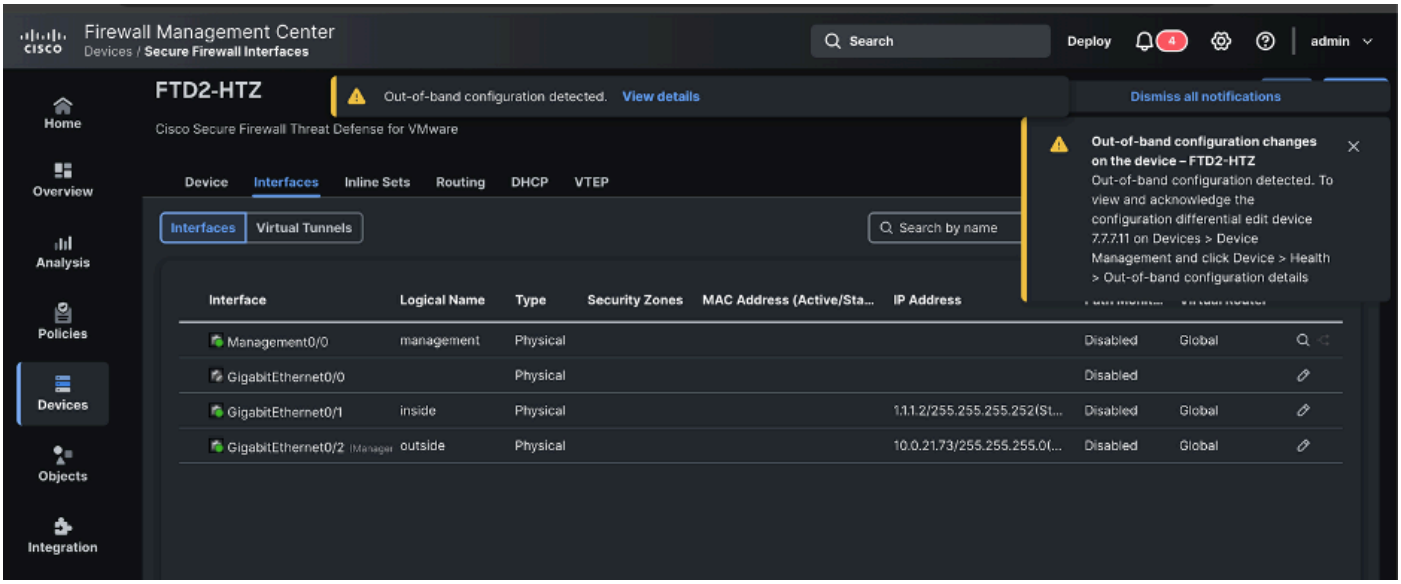
```
firepower# show route

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.几分钟后，此更改将恢复与FMC的通信。接下来的图像显示connection established，首先在FTD中，然后在FMC CLI中。

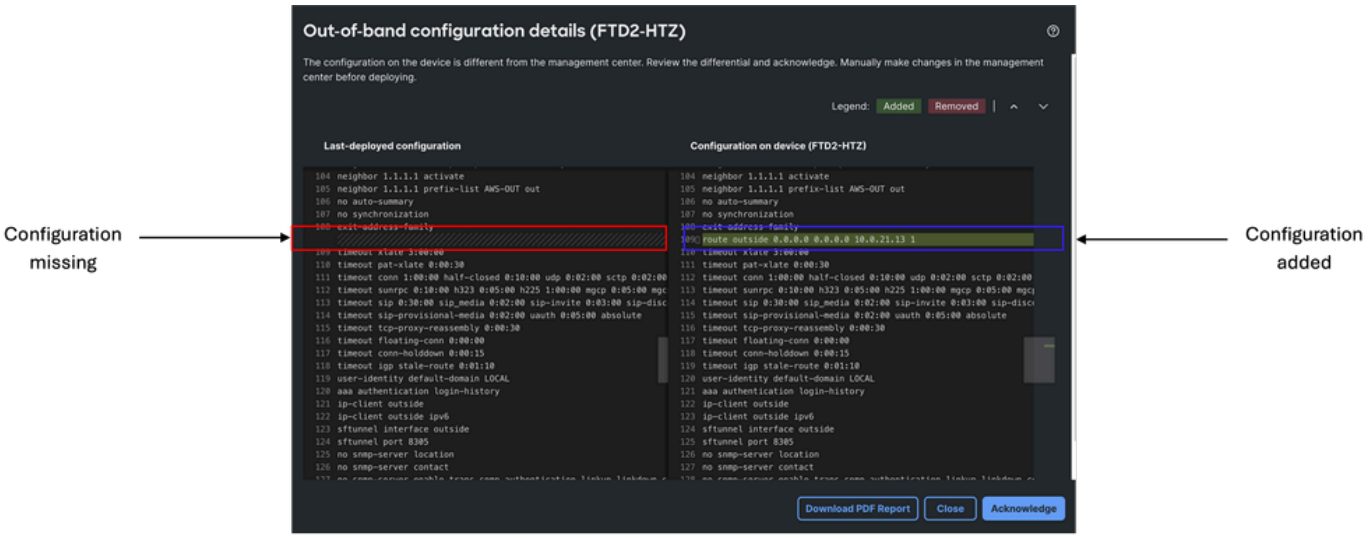


8.恢复配置后，在FMC GUI中，您可以导航到Device > Device Management，然后点击设备（本例中为FTD2-HTZ）。

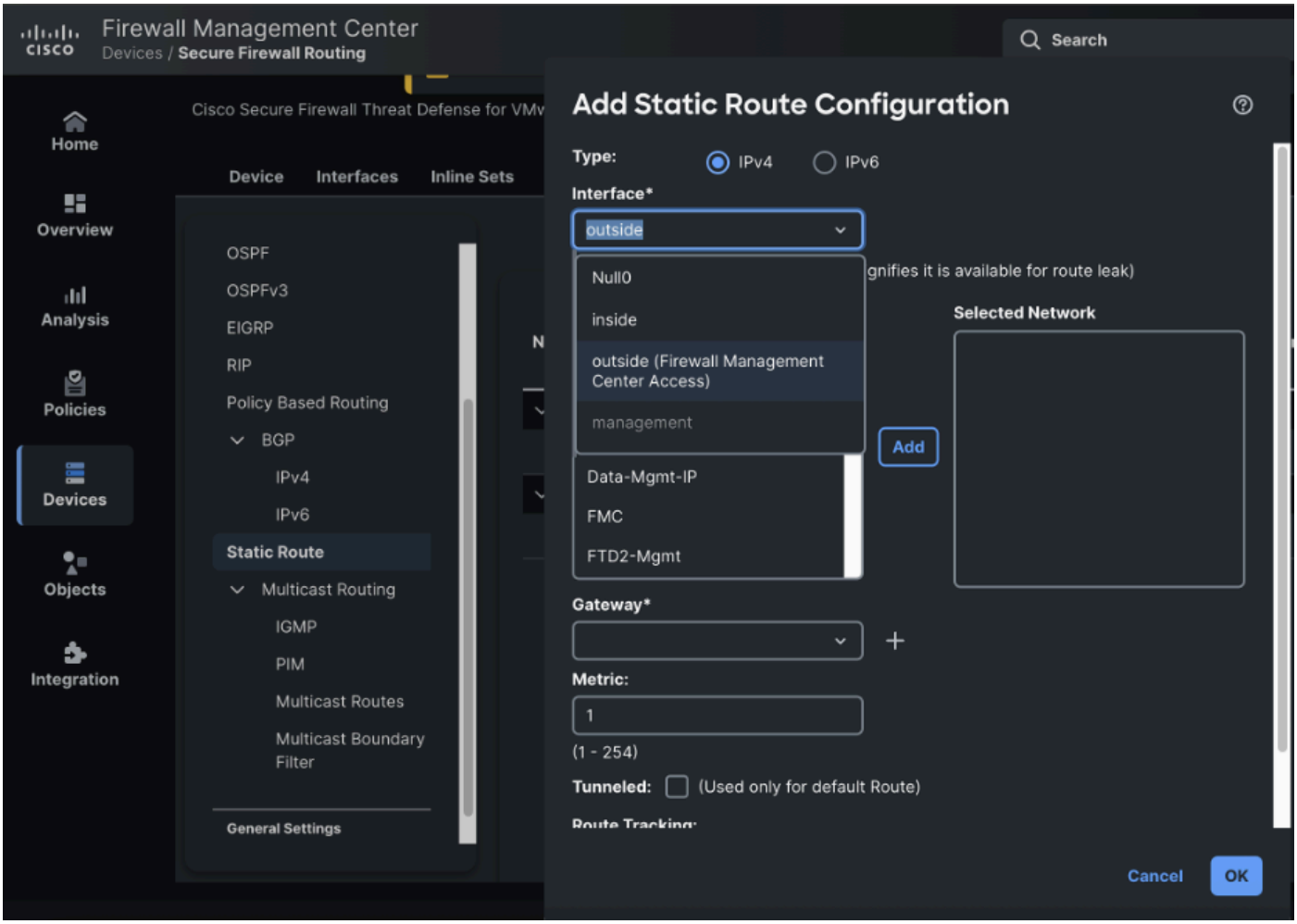
您可以在此处看到检测到带外配置警报。单击查看详细信息查看配置差异。

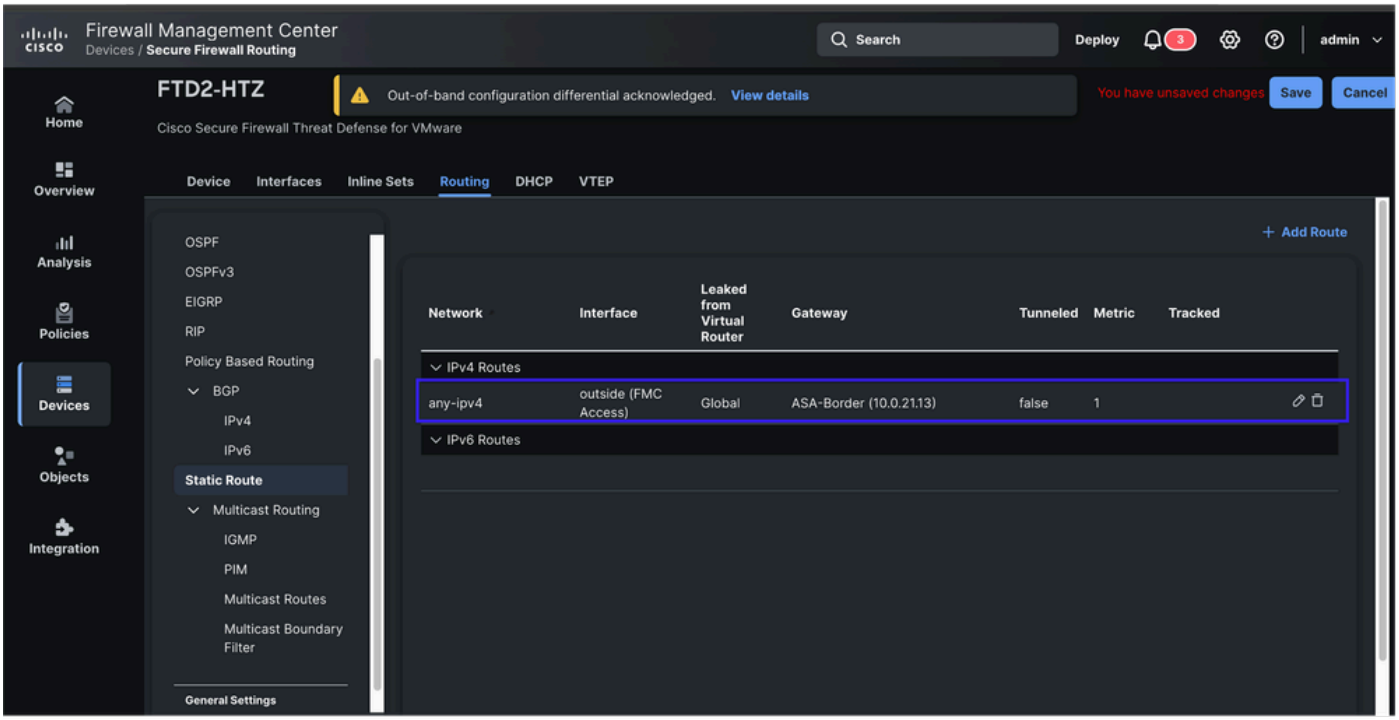


9.查看带外配置详细信息并确认差异。



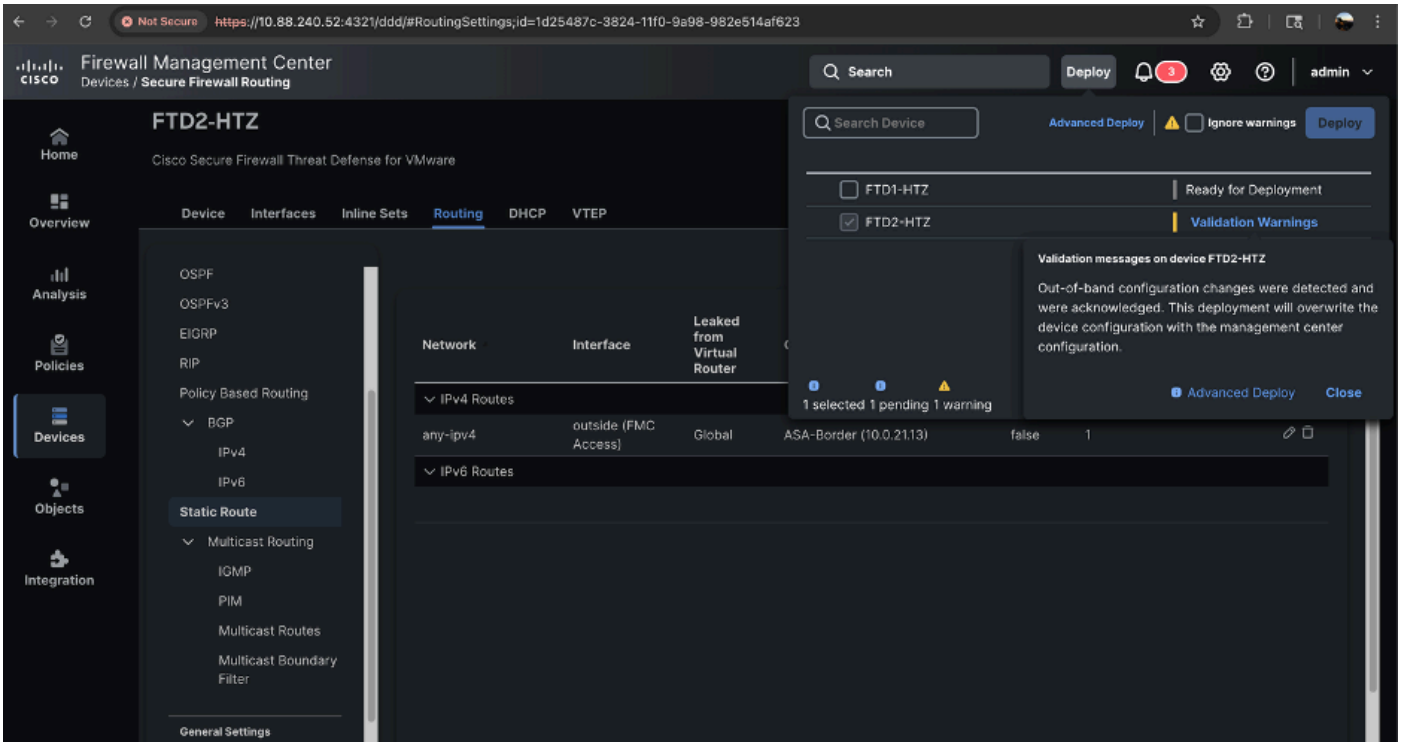
10.确认配置差异后，继续配置在恢复模式下执行的相同更改，但现在通过FMC GUI进行配置。在此场景中，添加了一条静态路由。

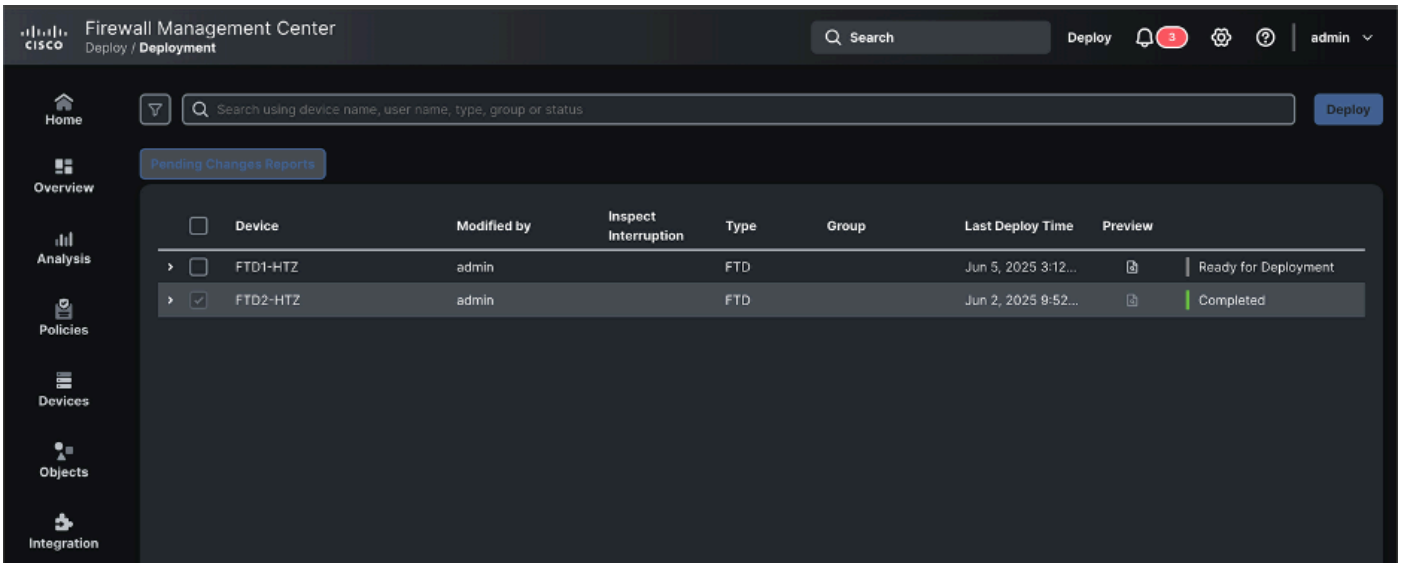




11.保存配置更改后，继续部署更改。显示另一个警报，通知检测到并确认带外配置更改，且更改被当前部署覆盖。

部署成功后，配置将再次同步。





参考

- 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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。