使用恢復配置模式進行緊急裝置上配置

目錄

簡介

本檔案介紹FTD 7.7使用復原設定模式進行緊急裝置上組態。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower威脅防禦(FTD)
- Cisco Firepower Management Center(FMC)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FTD 7.7.0+
- FMC 7.7.0+

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

此功能已在7.7.0版中引入，可用於在管理連線關閉時進行帶外配置更改。

這些配置更改直接在裝置CLI上執行，以：

- 如果使用資料介面進行Manager訪問，請恢復管理連線。
- 進行選擇策略更改，這些更改不能等到連線恢復後才進行。

恢復管理連線後：

1. 您需要確認帶外配置警報中顯示的配置差異。
2. 在部署之前在FMC中執行相同的更改，因為FMC部署始終覆蓋本地更改。

您可以在恢復配置模式下的診斷CLI中配置以下功能區域：

- 介面
- 靜態路由
- 動態路由：BGP和OSPF
- 預過濾器
- 站點到站點VPN

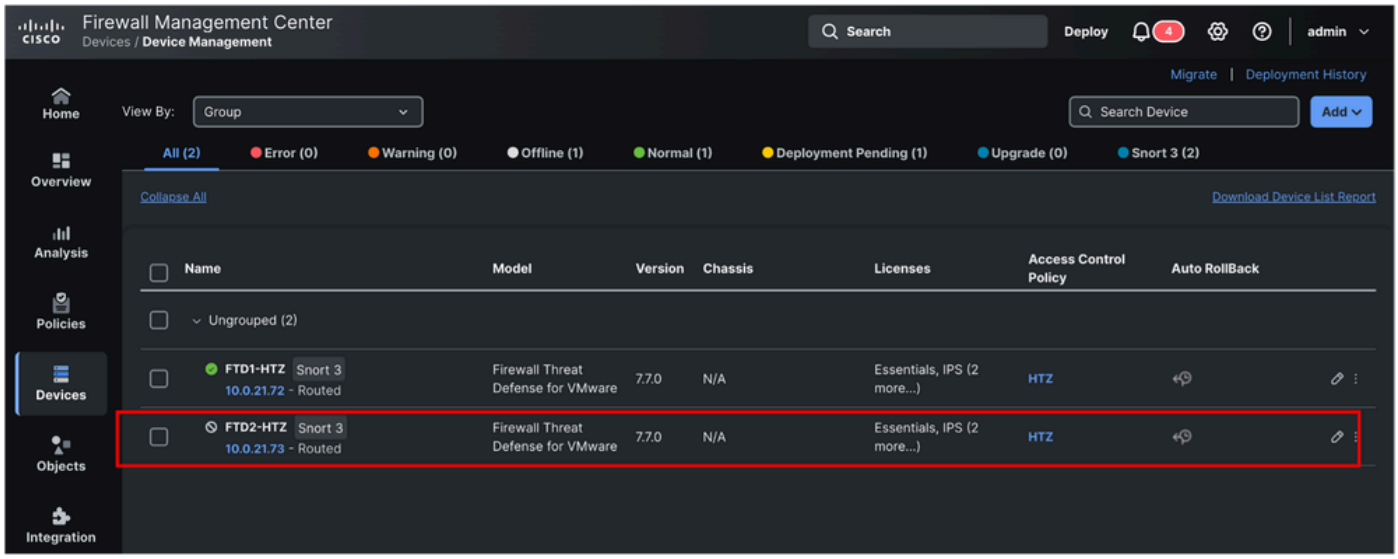
組態範例

實驗室背景

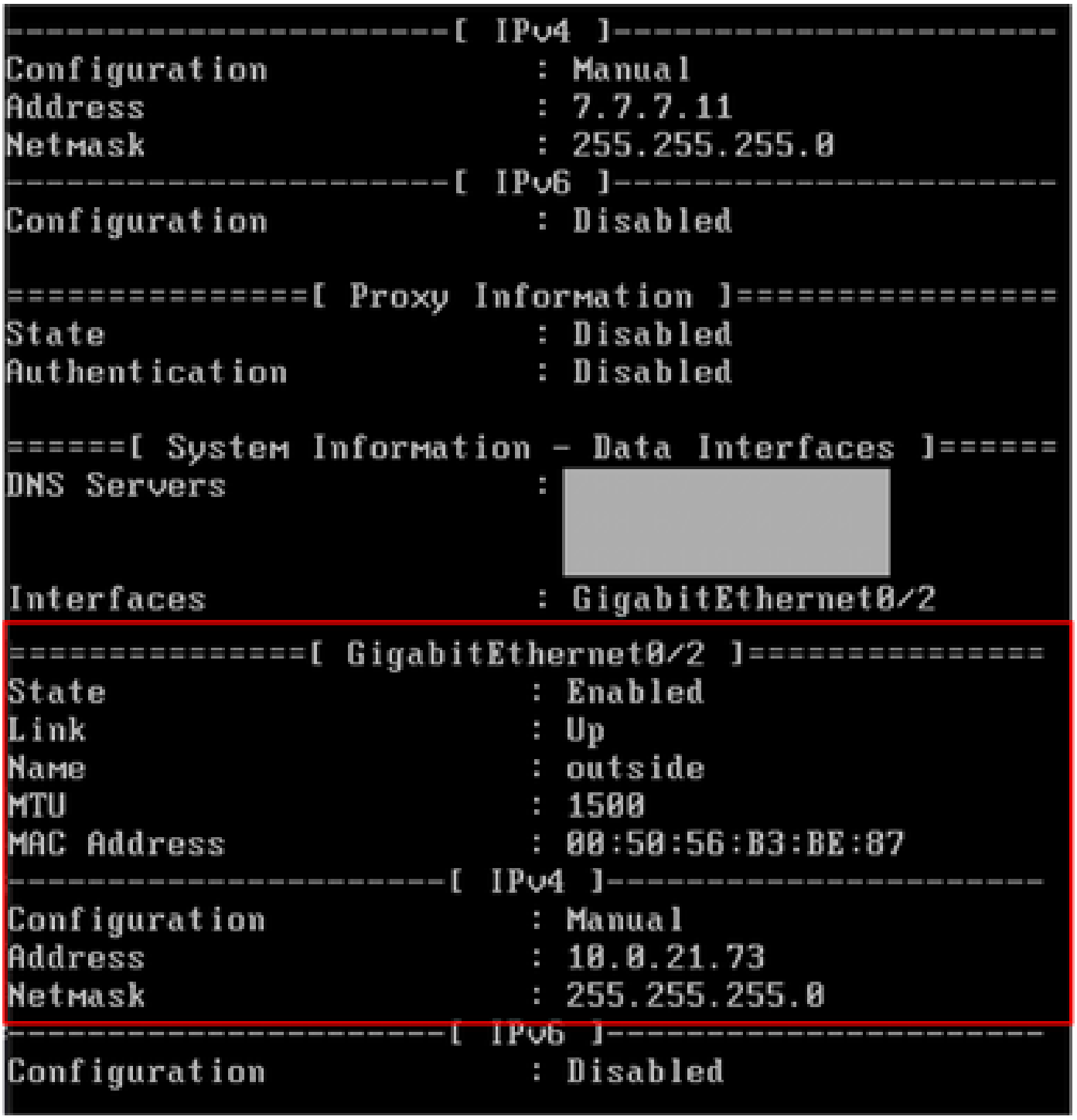
在此案例中，註冊到FMC（使用資料介面作為管理介面）的FTD裝置已遺失管理連線，為了解決此問題，會使用復原設定功能將靜態路由新增到FTD。

FMC註冊了兩台威脅防禦裝置（10.0.21.72和10.0.21.73），但只有一台裝置可訪問，如下圖所示（cli和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使用資料介面將註冊程式傳送到FMC。



FTD也沒有透過sftunnel連線至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# _
```

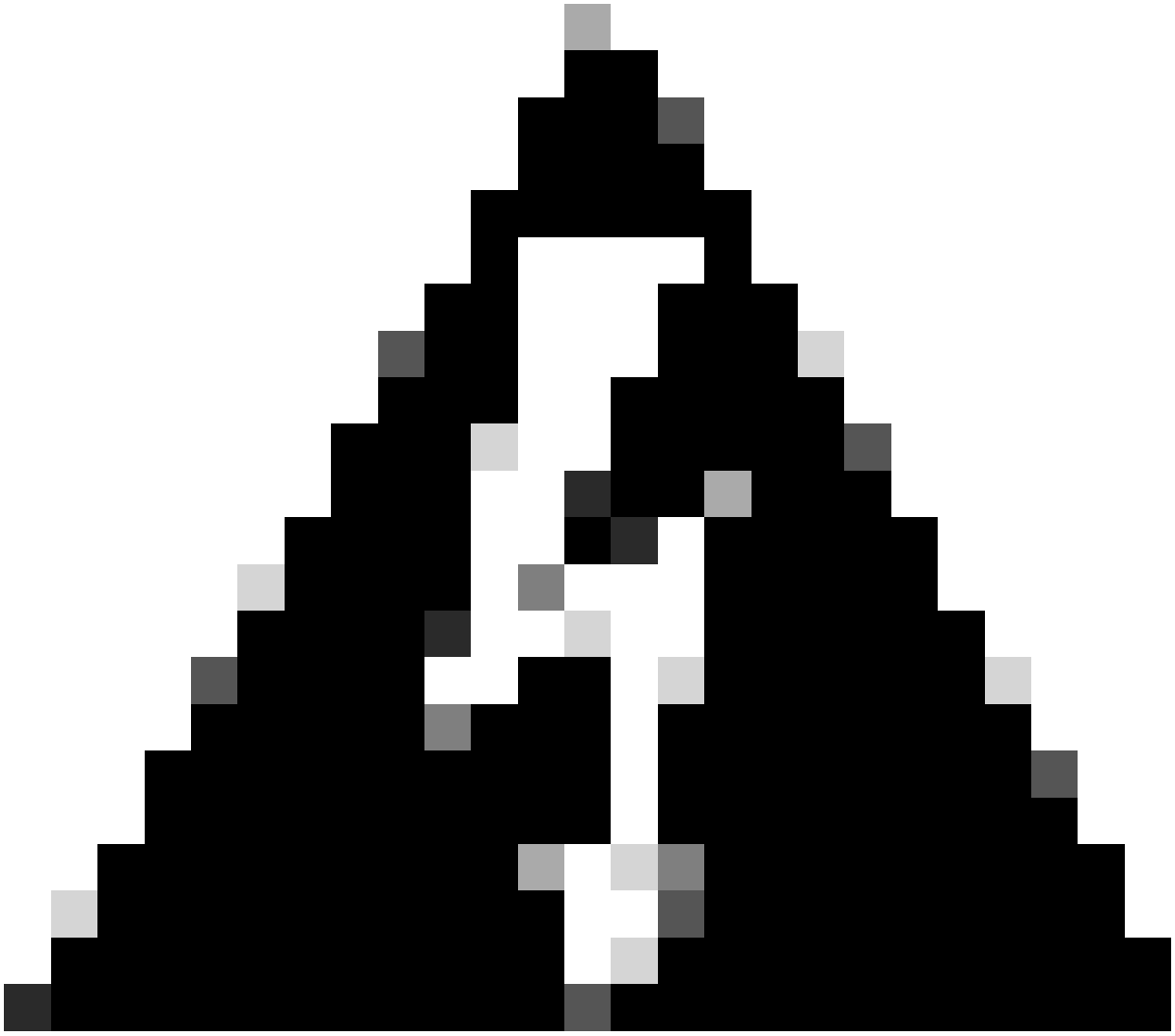
設定步驟

1.為了能夠使用恢復配置功能，您需要登入FTD CLI並進入lina模式(系統支援diagnostic-cli)。

2.運行configure recovery-config命令。

3.如果鍵入問號(?)，則會列出所有支援的命令，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：您需要瞭解恢復或緊急使用所需的命令。如果您不確定必須使用哪條命令，建議您聯絡Cisco TAC獲取指導。

4.運行configure recovery-config命令後，將顯示一個警報，要求您確認並繼續。

```
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.確認後，您可以開始使用可用的config命令。在此場景中，將靜態路由新增到外部介面。配置完成後，運行exit命令退出恢復模式。

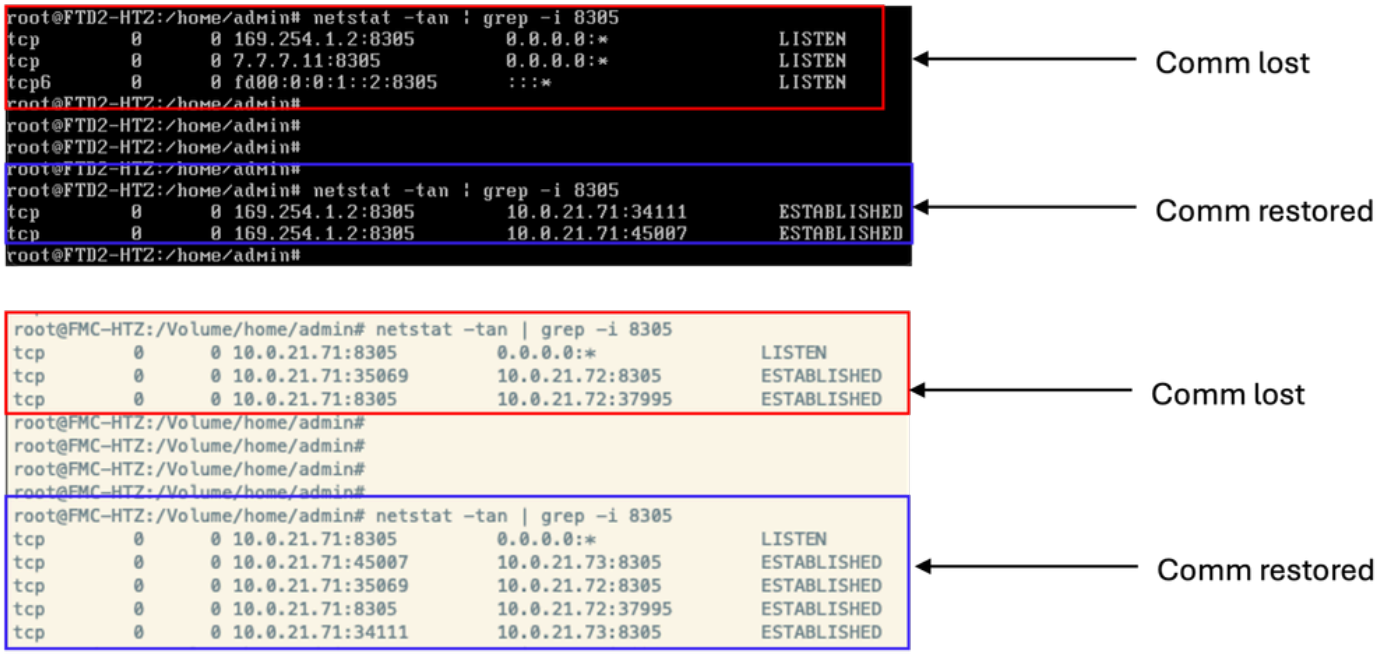
系統會要求您儲存更改，並且系統會顯示一條警報，通知在裝置重新啟動後不會保留更改。

```
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.您可以確認配置已應用。在本例中，顯示路由。

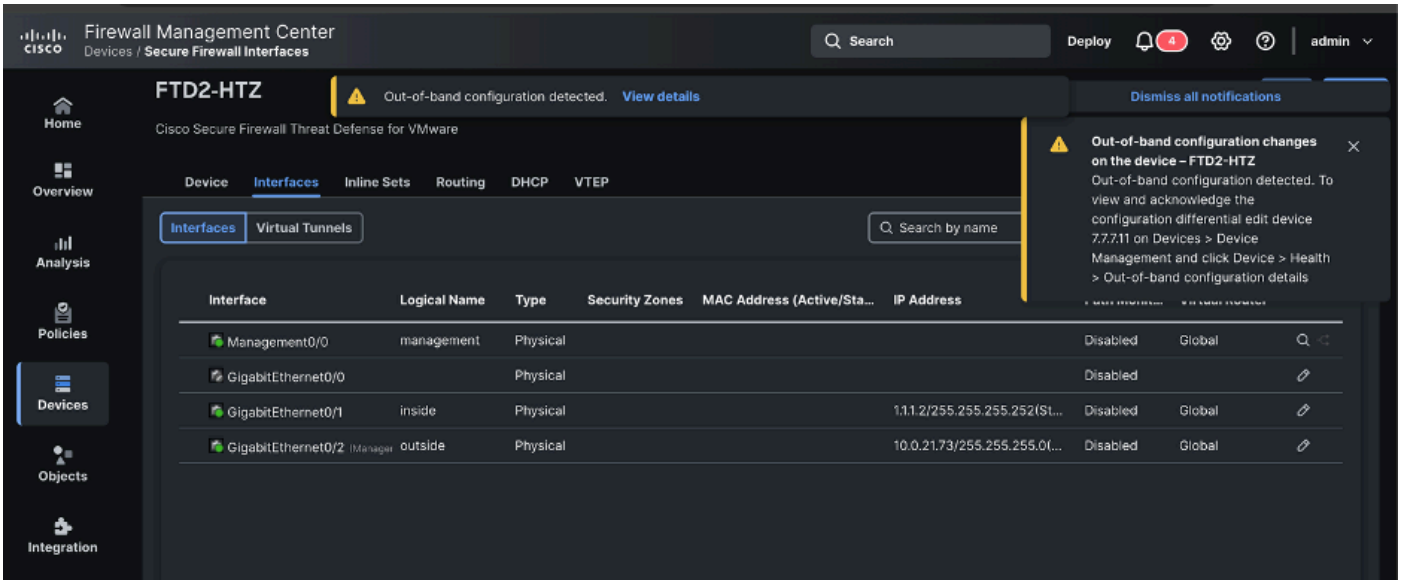
```
firepower# show route

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.幾分鐘後，此更改將恢復與FMC的通訊。下一張圖顯示已建立的連線，先在FTD中，然後在FMC CLI中。

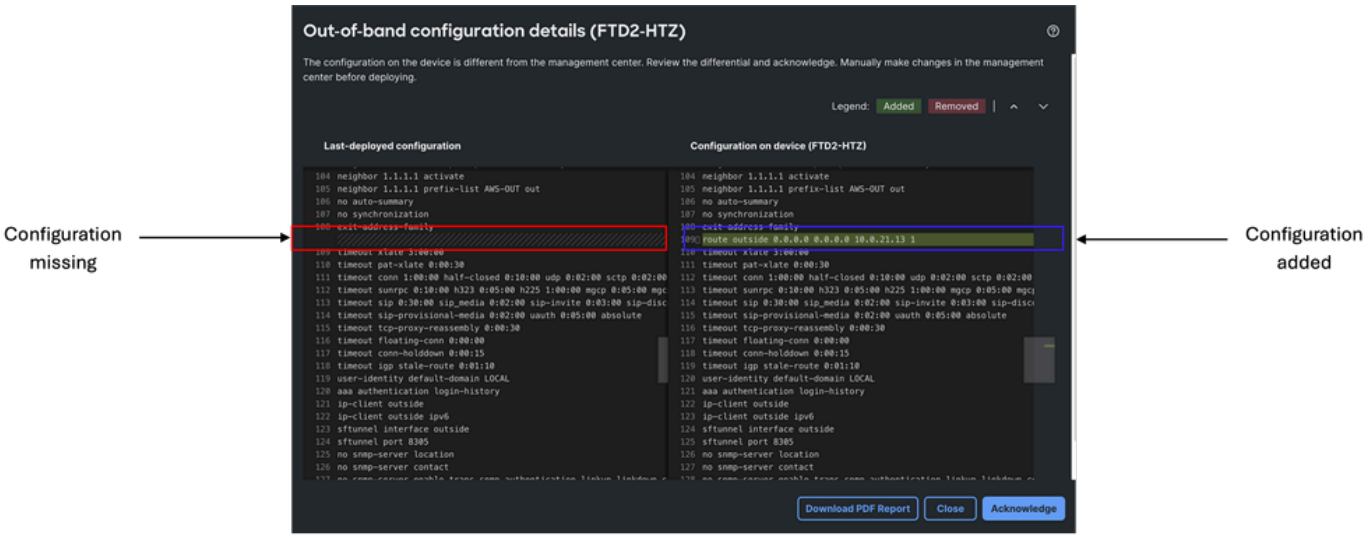


8.恢復配置後，在FMC GUI中，您可以導航到Device > Device Management，然後按一下您的裝置（在本例中為FTD2-HTZ）。

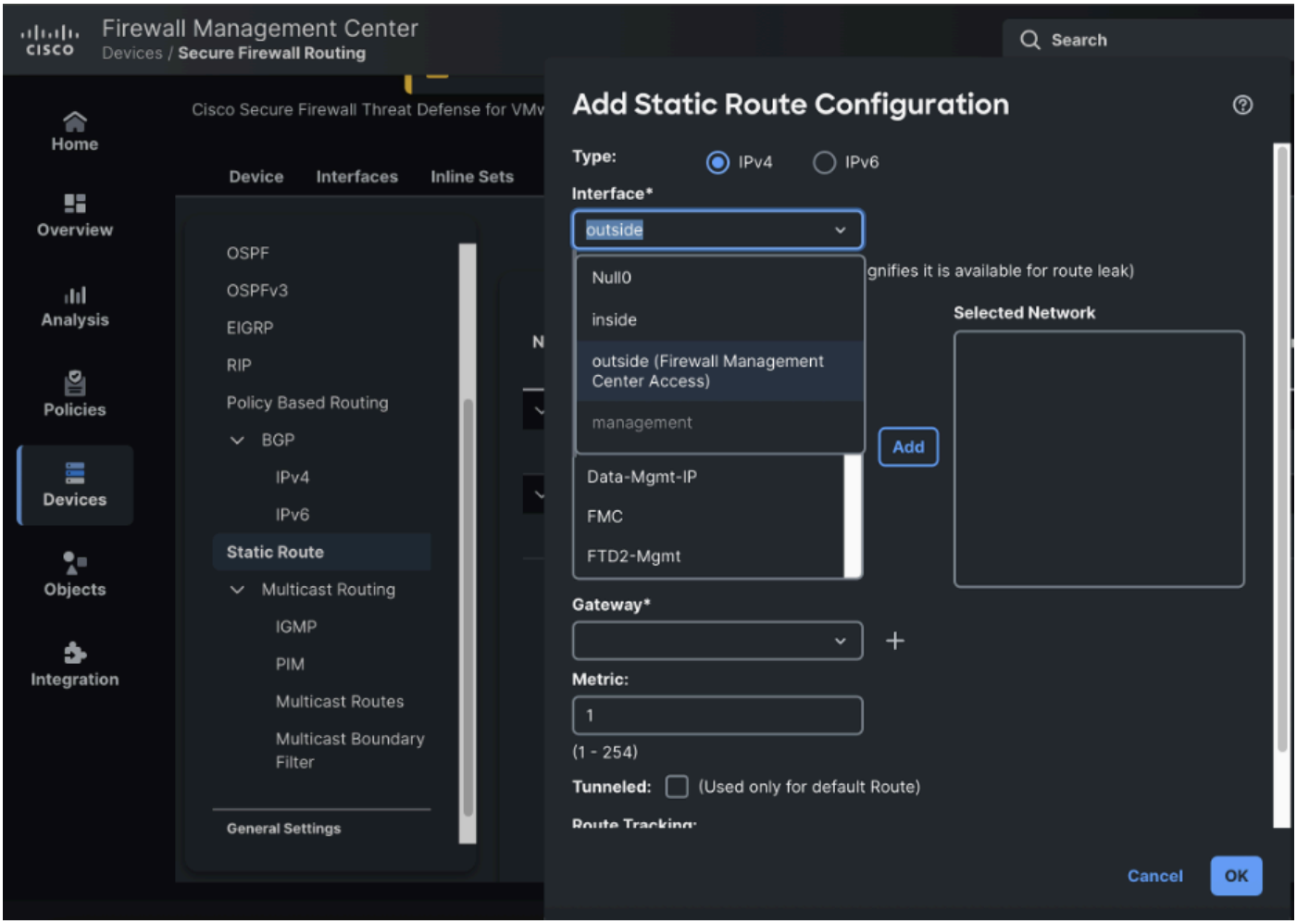
您可以在此處看到檢測到帶外配置警報。按一下View details檢視配置差異。

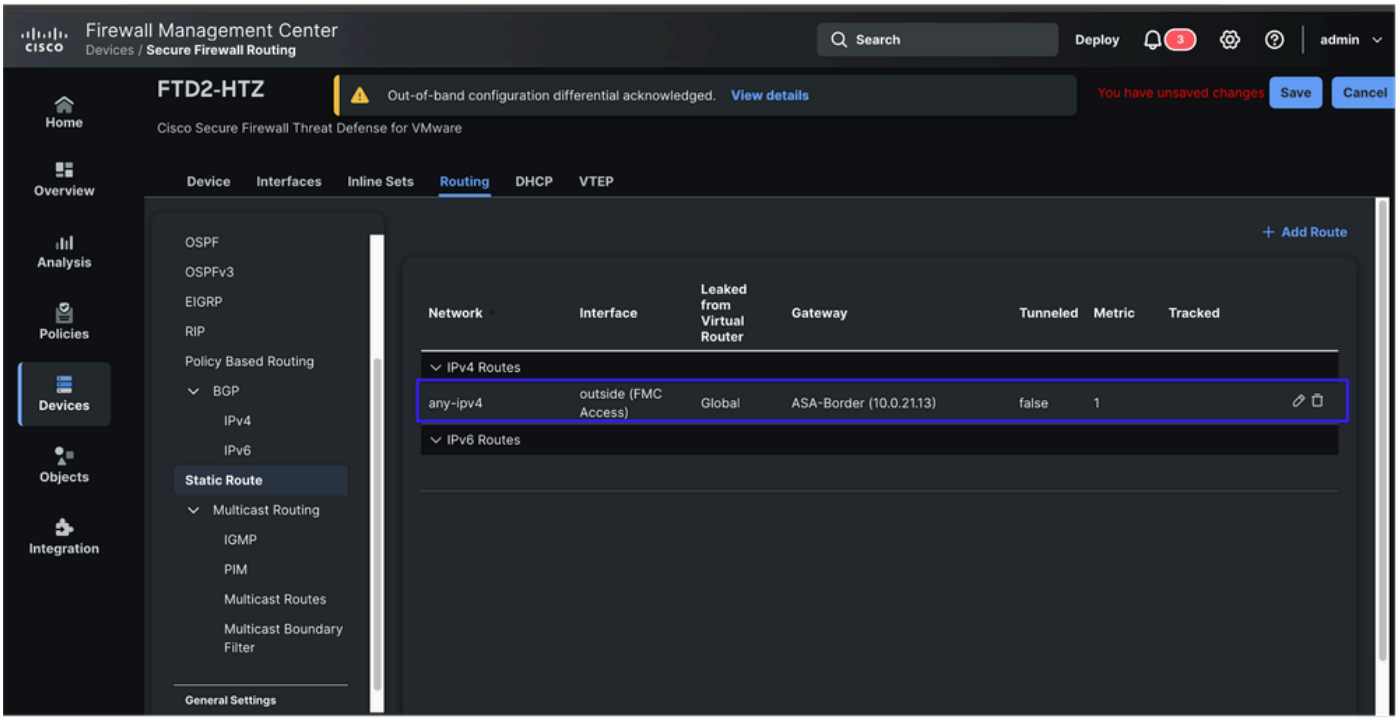


9.檢視帶外配置詳細資訊並確認差異。



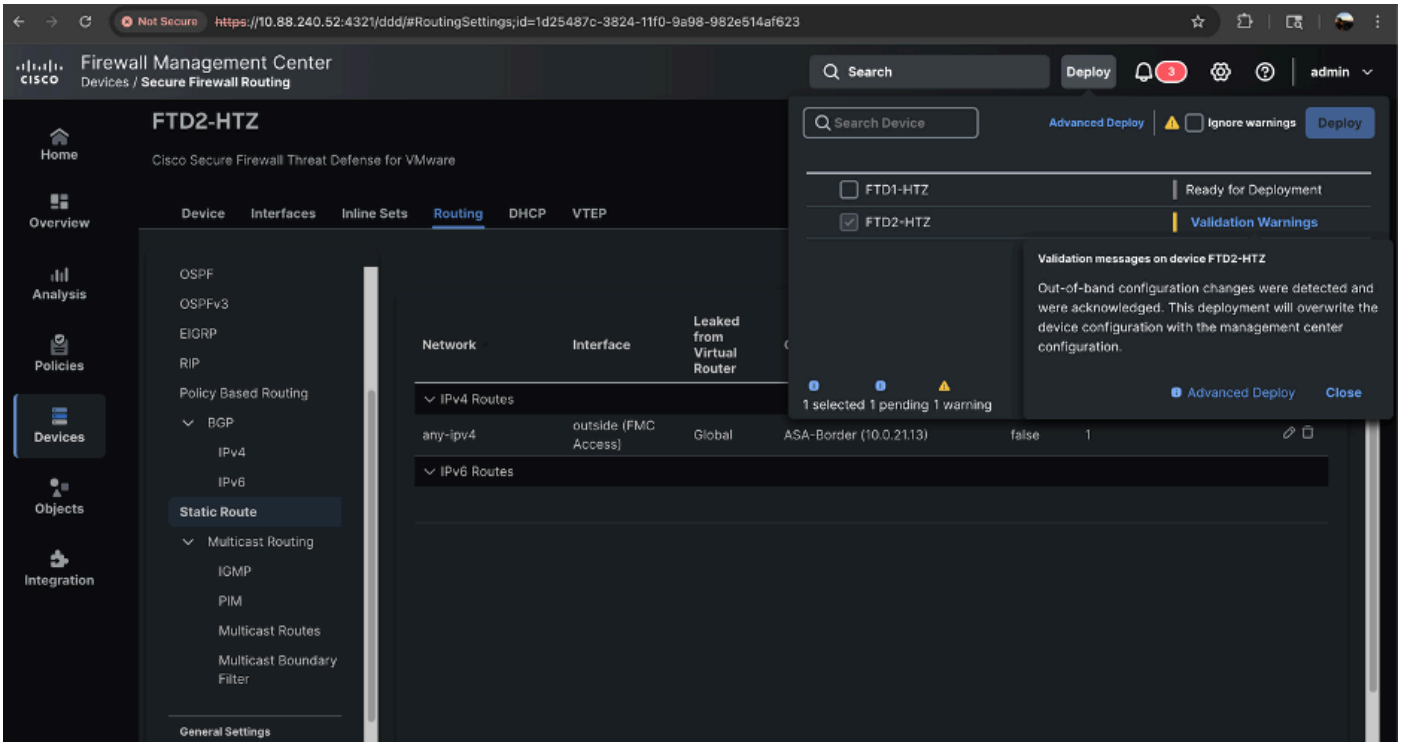
10.確認配置差異後，繼續配置在恢復模式下執行的相同更改，但現在通過FMC GUI進行配置。在此案例中，新增了一條靜態路由。

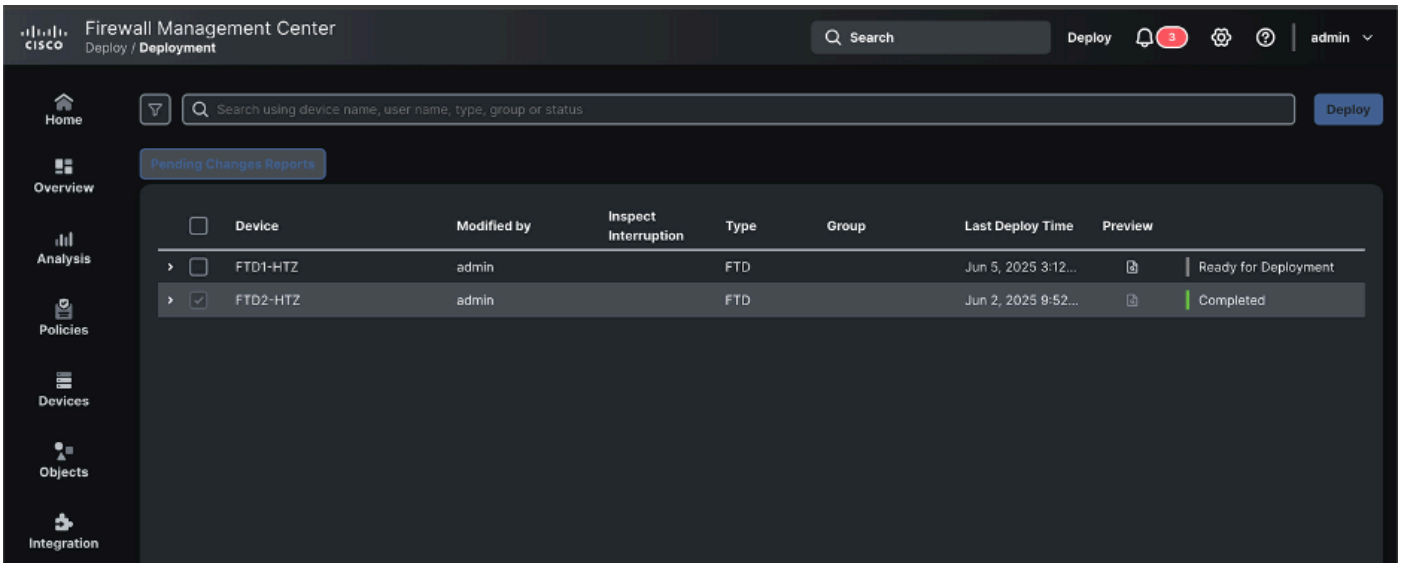




11.儲存配置更改後，繼續部署更改。顯示另一個警報，通知檢測到並確認了帶外配置更改，且當前部署覆蓋了這些更改。

部署成功後，配置將再次同步。





參考資料

- 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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。