Usar o modo de configuração de recuperação para configuração de emergência no dispositivo

Contents

Introdução

Este documento descreve o FTD 7.7 Usar modo de configuração de recuperação para configuração de emergência no dispositivo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças (FTD) do Cisco Firepower
- Cisco Firepower Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD 7.7.0+
- FMC 7.7.0+

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Esse recurso foi introduzido na versão 7.7.0 e pode ser usado para fazer alterações de configuração fora de banda quando a conexão de gerenciamento estiver inativa.

Essas alterações de configuração são executadas diretamente na CLI do dispositivo para:

- Restaure a conexão de gerenciamento se estiver usando uma interface de dados para acesso do gerenciador.
- Faça as alterações de política selecionadas que não podem esperar até que a conexão seja restaurada.

Depois que a conexão de gerenciamento for restaurada:

1. Você precisa reconhecer as diferenças de configuração mostradas no alerta de configuração fora de banda.
2. Faça as mesmas alterações no FMC antes da implantação, pois as alterações locais são sempre substituídas pela implantação do FMC.

Você pode configurar estas áreas de recursos na CLI de diagnóstico no modo de configuração de recuperação:

- Interfaces
- rotas estáticas
- Roteamento dinâmico: BGP e OSPF
- Pré-filtros
- VPN site a site

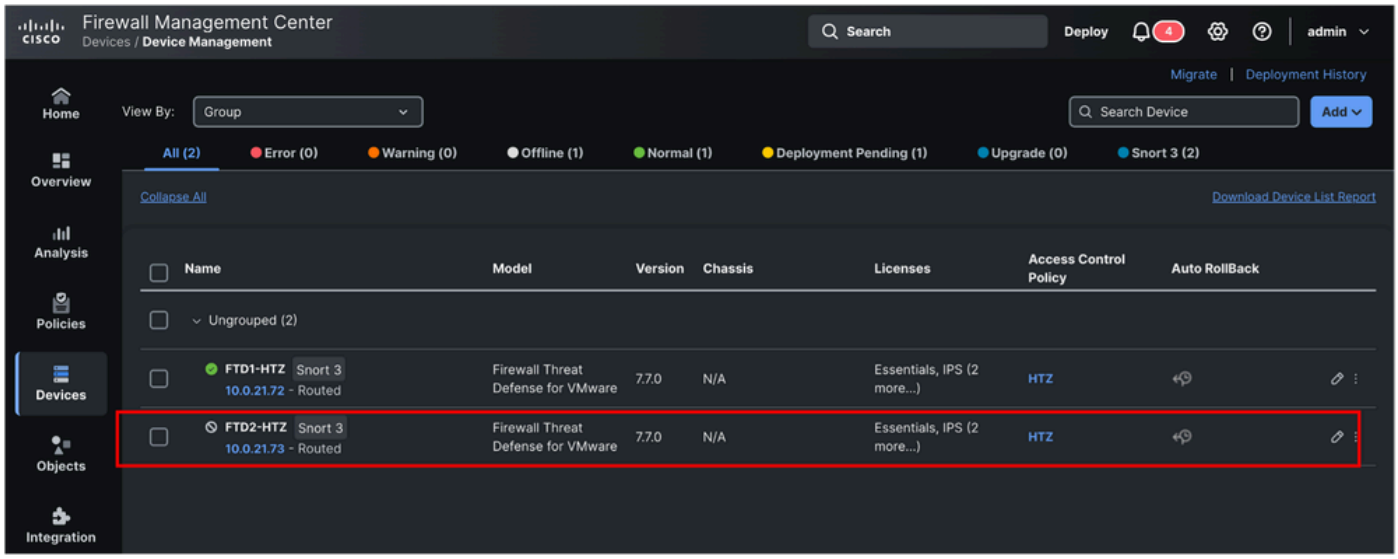
Exemplo de configuração

Plano de fundo do laboratório

Neste cenário, um dispositivo FTD registrado em um FMC (usando a interface de dados como interface de gerenciamento) perdeu a conexão de gerenciamento e, para corrigir esse problema, uma rota estática é adicionada ao FTD usando o recurso de configuração de recuperação.

O FMC tem dois dispositivos de defesa contra ameaças registrados (10.0.21.72 e 10.0.21.73), mas apenas um deles pode ser acessado conforme mostrado nas imagens seguintes (cli e 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#
```



O DTF utiliza a interface de dados para o processo de registro junto do CVP.

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

O FTD também não tem conexão com o FMC através do 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# _
```

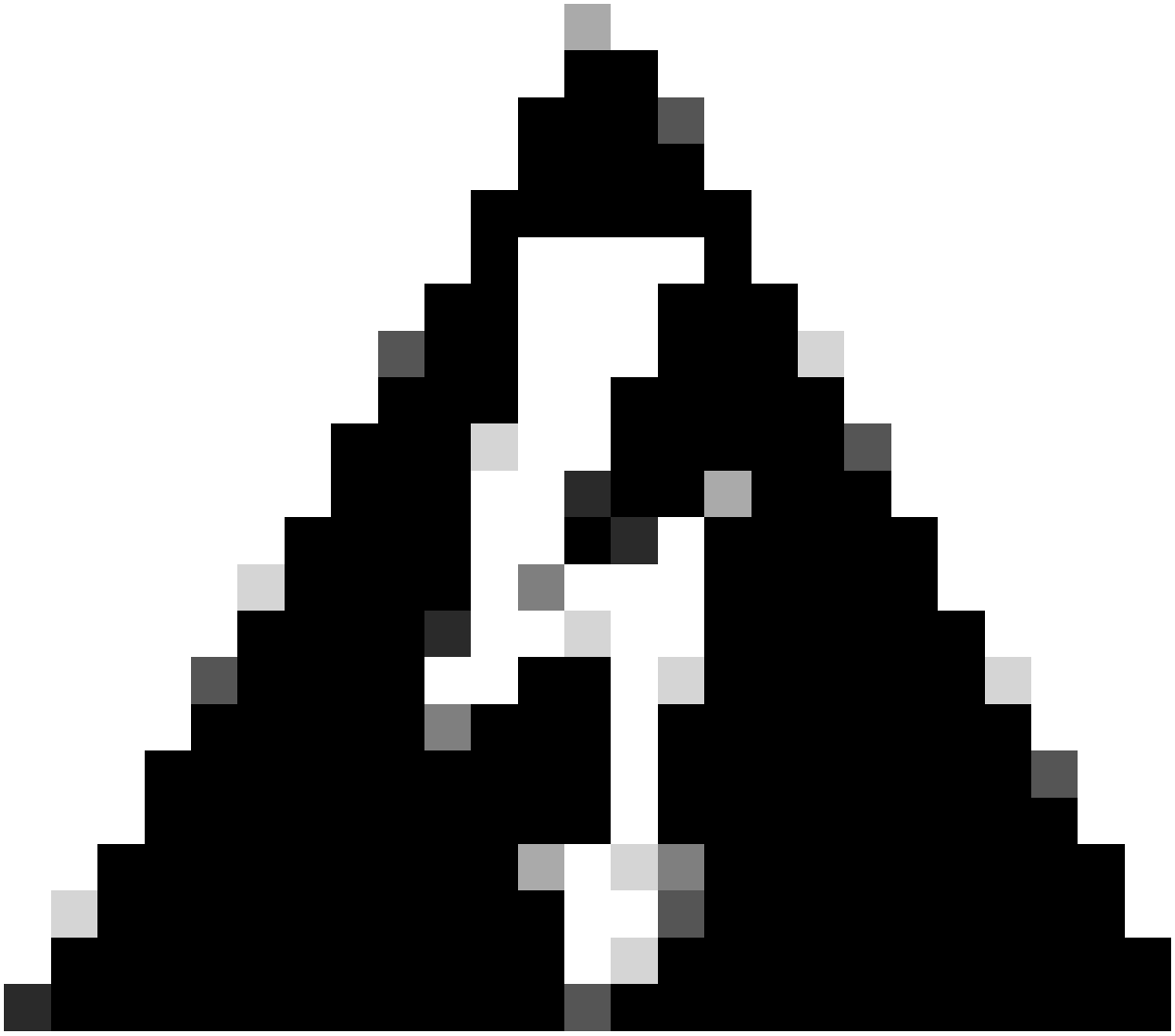
Configuration Steps

1. Para poder usar o recurso de configuração de recuperação, você precisa iniciar a sessão na CLI do FTD e ir para o modo de linha (system support diagnostic-cli).

2. Execute o comando configure recovery-config.

3. Se você digitar o ponto de interrogação (?), todos os comandos suportados serão listados, conforme mostrado na lista a seguir.

```
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
```



aviso: Espera-se que você conheça os comandos necessários para recuperação ou uso de emergência. Se você não tiver certeza sobre qual comando deve ser usado, é recomendável entrar em contato com o TAC da Cisco para obter orientação.

---

4. Após executar o comando configure recovery-config, um alerta será exibido e você será solicitado a confirmar e continuar.

```
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. Uma vez confirmado, você pode começar a usar os comandos de configuração disponíveis. Neste cenário, uma rota estática é adicionada à interface externa. Após concluir a configuração, execute o comando exit para sair do modo de recuperação.

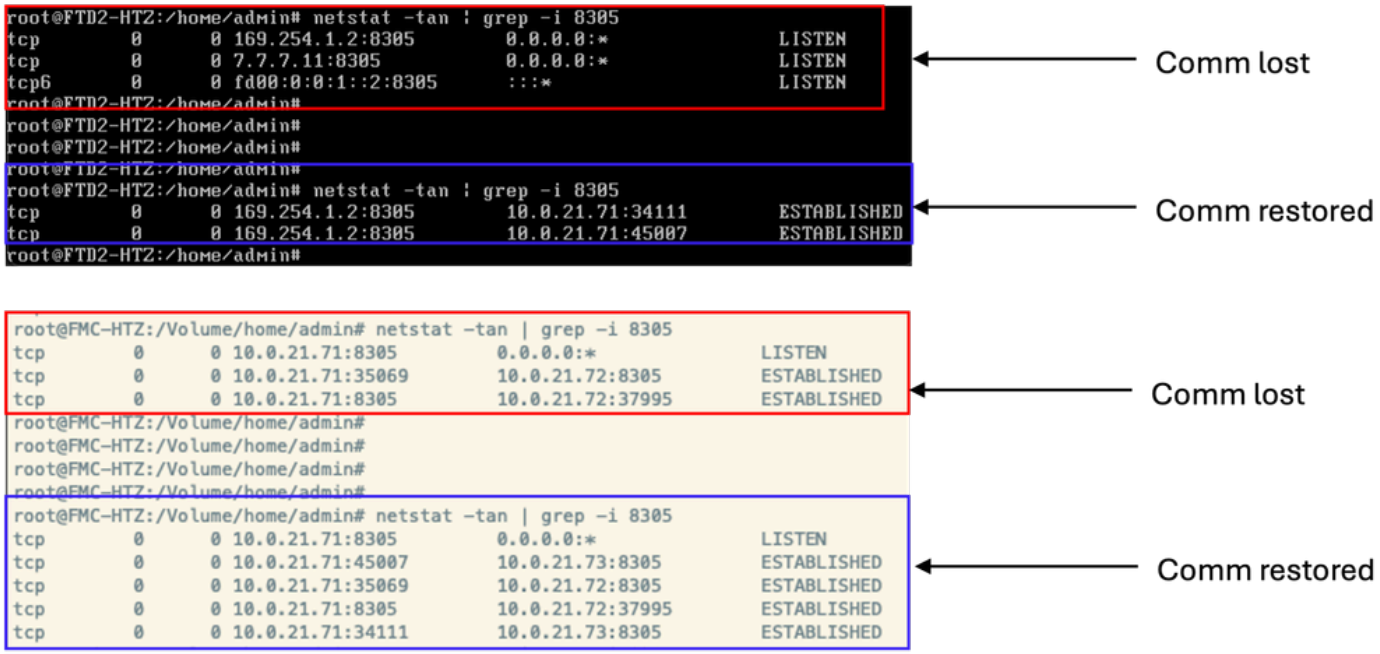
Você será solicitado a salvar as alterações e um alerta será exibido informando que as alterações não serão mantidas se o dispositivo for reinicializado.

```
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. Você pode confirmar que a configuração foi aplicada. Neste caso, mostrando rotas.

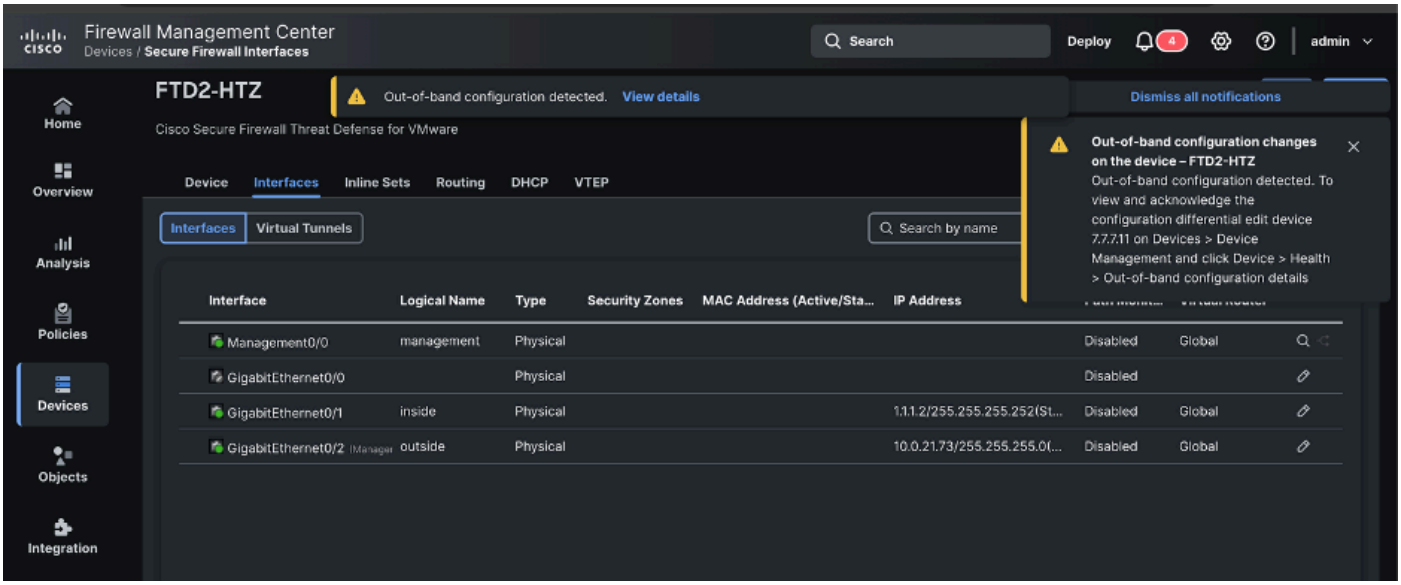
```
firepower# show route

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. Após alguns minutos, essa alteração restabelece a comunicação com o FMC. As imagens a seguir mostram a conexão estabelecida, primeiro no FTD e depois no FMC CLI.

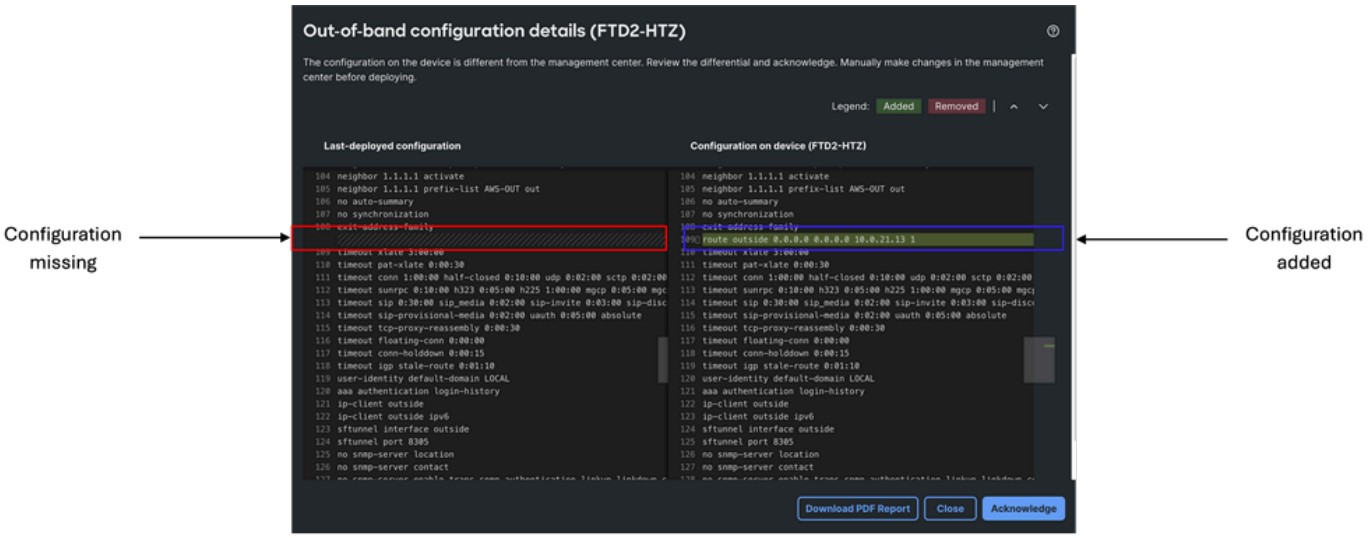


8. Depois que a configuração for restaurada, na GUI do FMC você pode navegar para Device > Device Management e clicar em seu dispositivo (neste caso é FTD2-HTZ).

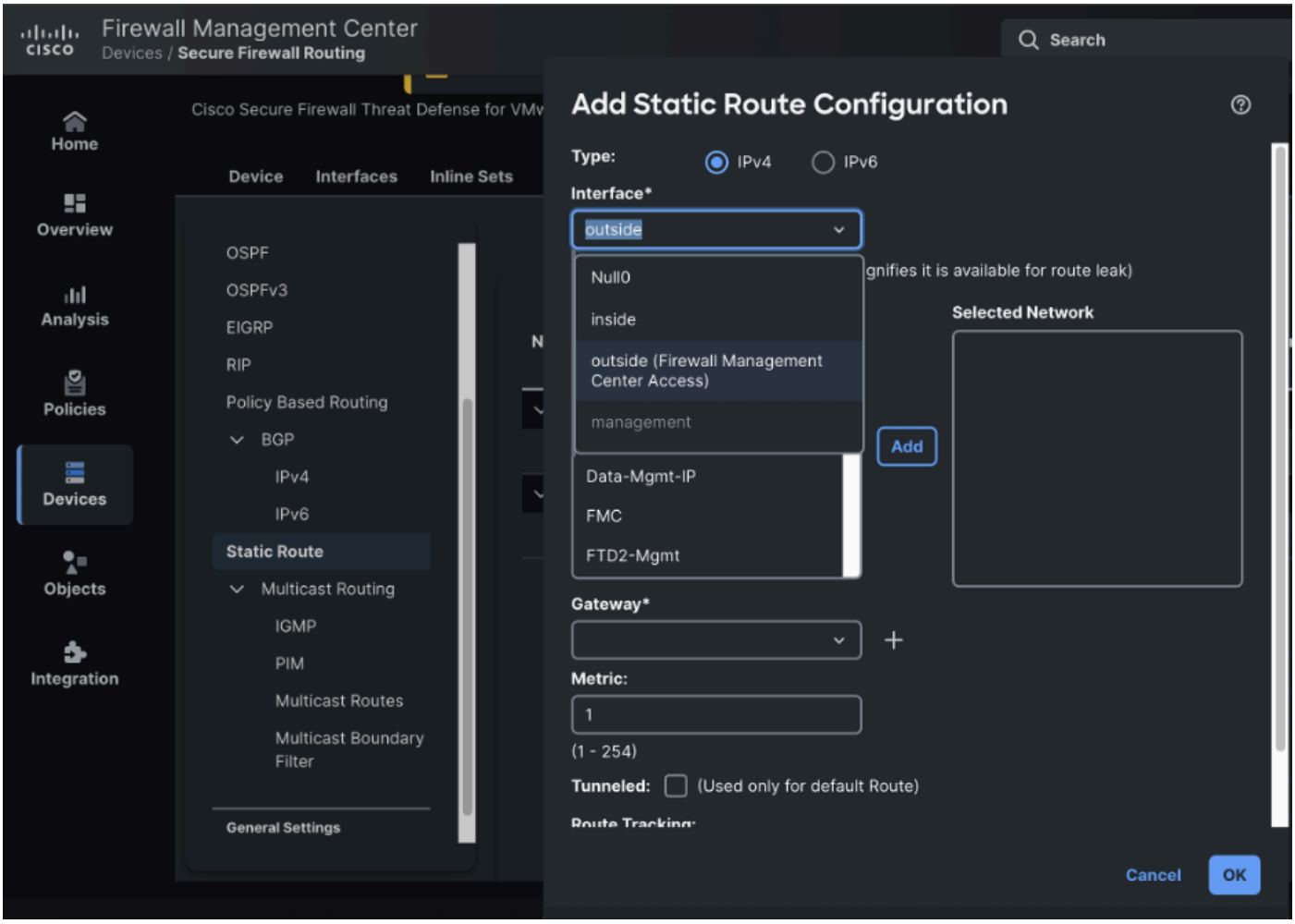
Aqui você pode ver o alerta Configuração fora de banda detectada. Clique em View details para ver as diferenças de configuração.

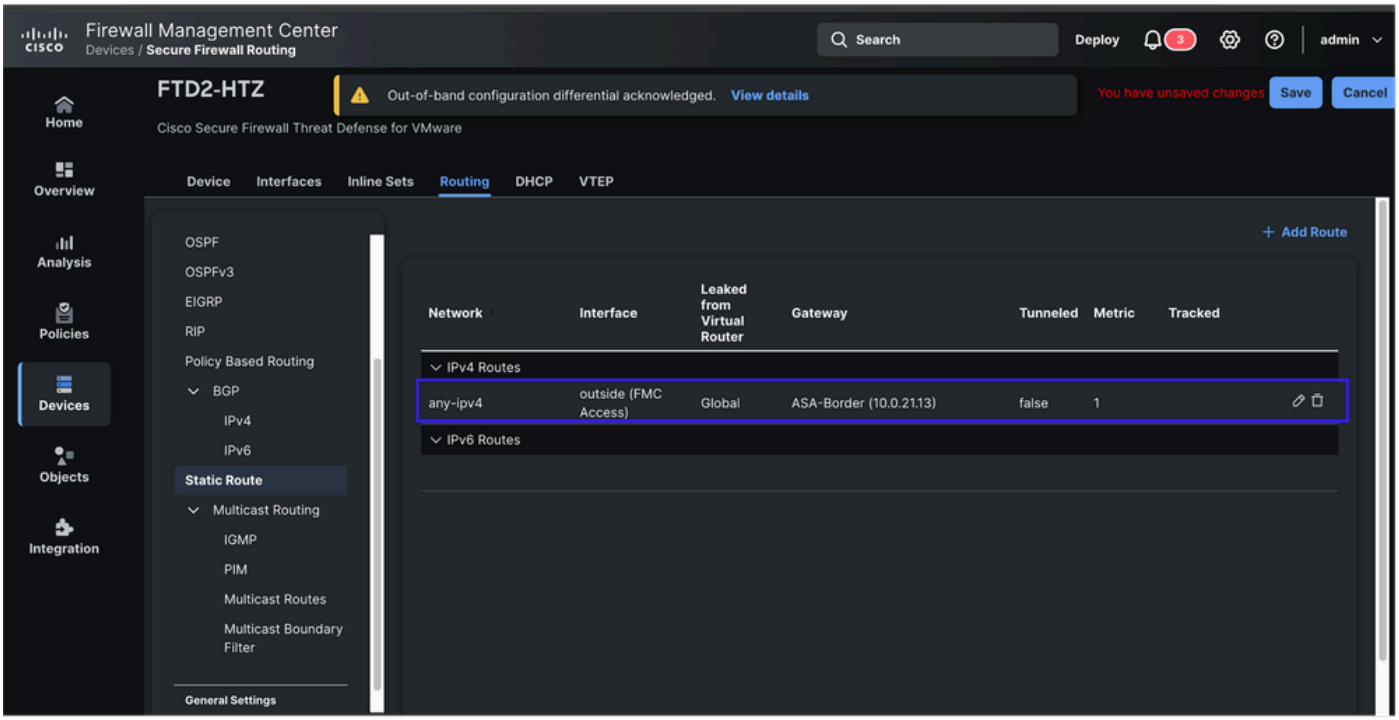


9. Reveja detalhes da configuração fora da banda e confirme as diferenças.



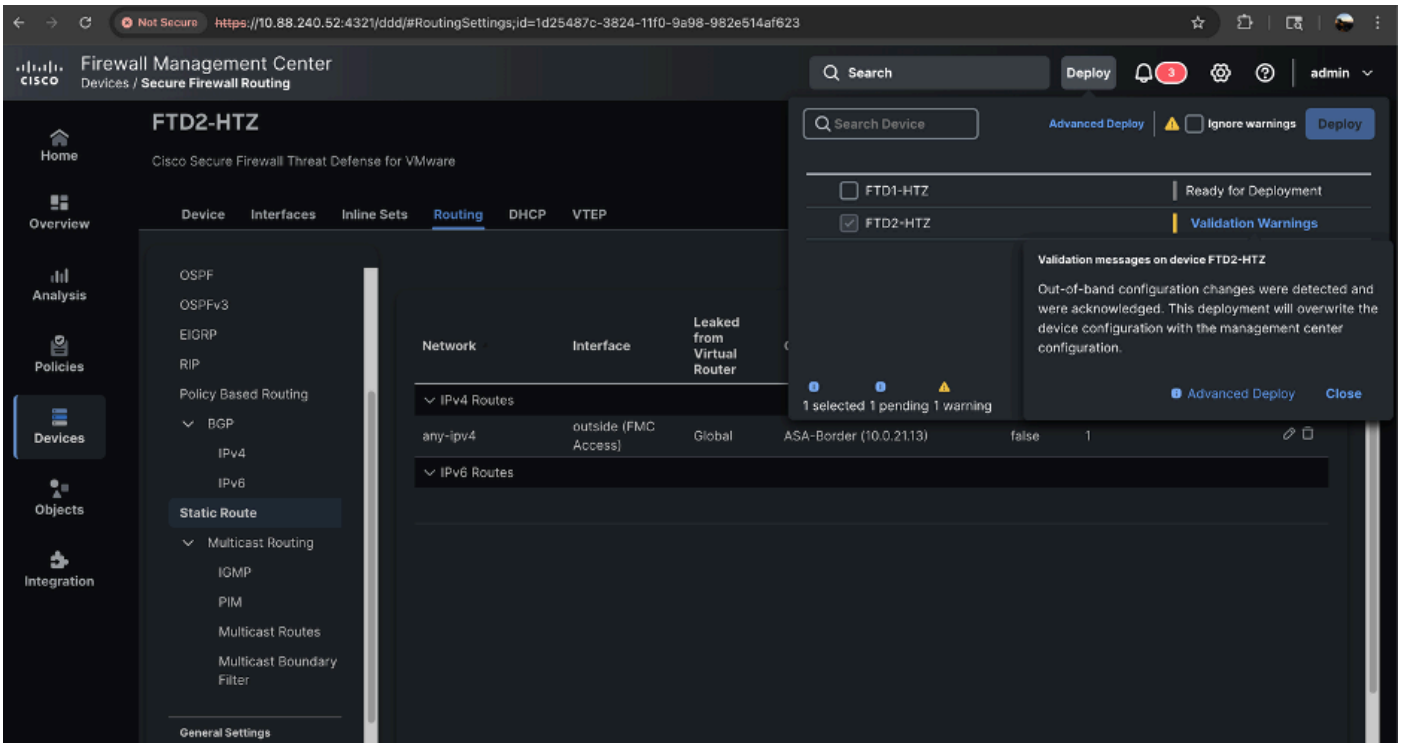
10. Depois que as diferenças de configuração forem confirmadas, continue para configurar as mesmas alterações feitas no modo de recuperação, mas agora através da GUI do FMC. Neste cenário, uma rota estática é adicionada.

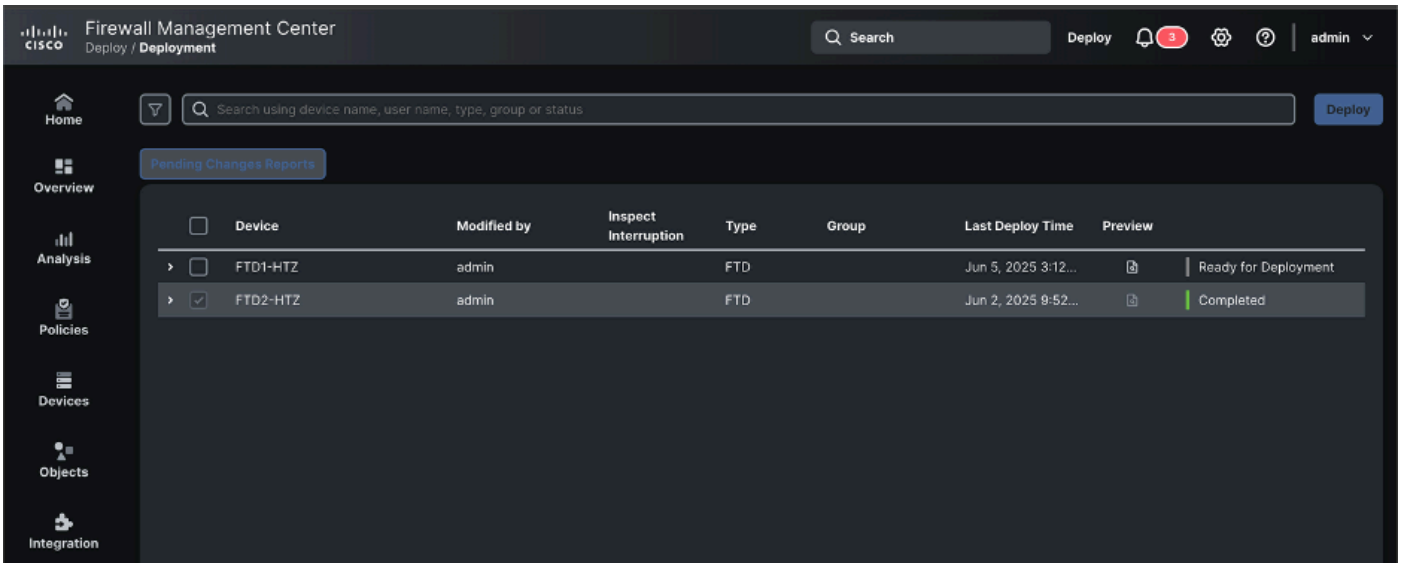




11. Depois que as alterações de configuração forem salvas, continue para implantar as alterações. Outro alerta é mostrado informando que alterações de configuração fora de banda foram detectadas e confirmadas e que as alterações foram substituídas pela implantação atual.

Quando a implantação for bem-sucedida, a configuração será sincronizada novamente.





Referências

- 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.