Use Recovery-config Mode for Emergency On-device Configuration

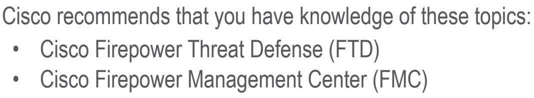
Contents

Introduction

This document describes FTD 7.7 Use Recovery-config Mode for Emergency on-device Configuration.

Prerequisites

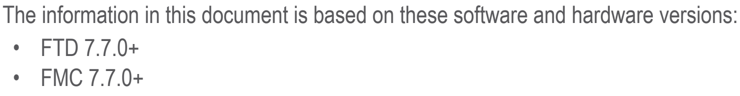
Requirements



Cisco recommends that you have knowledge of these topics:

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

Components Used



The information in this document is based on these software and hardware versions:

- FTD 7.7.0+
- FMC 7.7.0+

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

This feature has been introduced in version 7.7.0 and can be used to make out-of-band configuration changes when the management connection is down.

These configuration changes are performed directly at the device CLI to:

- Restore the management connection if you are using a data interface for manager access.
- Make select policy changes that cannot wait until the connection is restored.

Once management connection is restored:

1. You need to acknowledge the configuration differences shown in the out of band configuration alert.
2. Perform the same changes in the FMC before deploying, because local changes are always overwritten by the FMC deployment.

You can configure these feature areas at the diagnostic CLI in recovery-config mode:

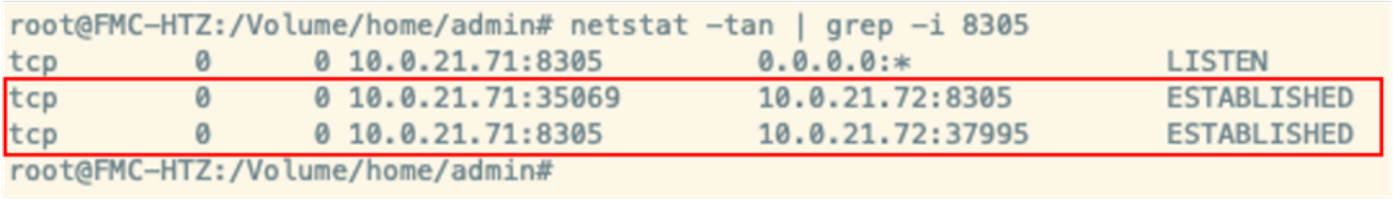
- Interfaces
- Static Routes
- Dynamic Routing: BGP and OSPF
- Prefilters
- Site-to-site VPN

Configuration Example

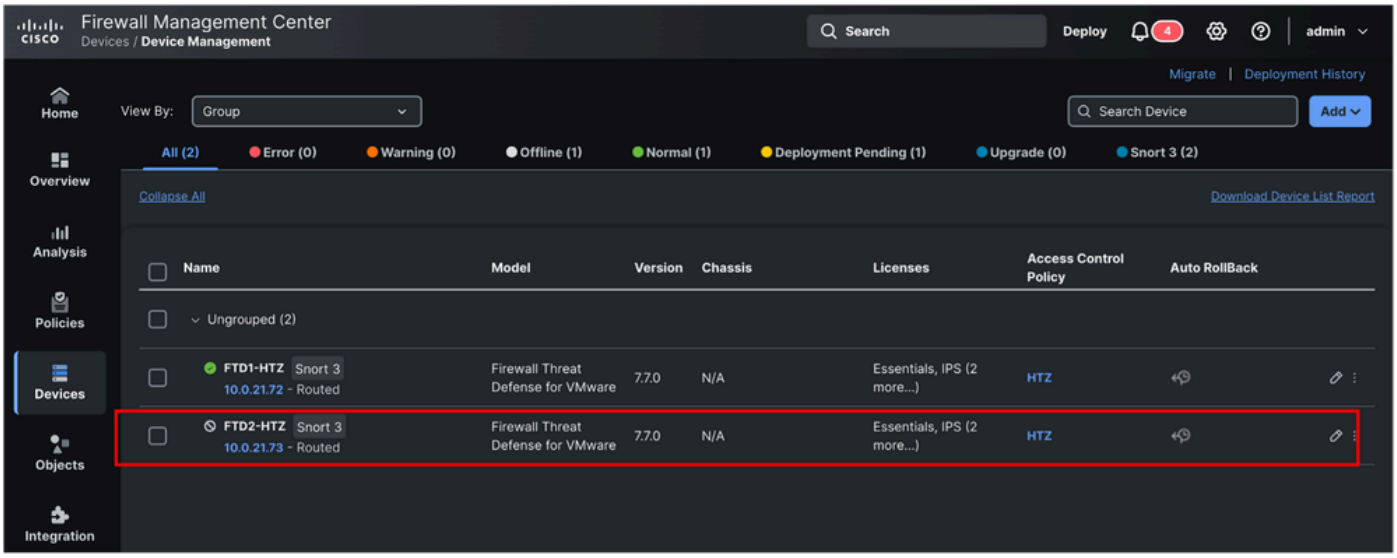
Lab background

In this scenario, an FTD device registered to an FMC (using data-interface as management interface) has lost management connection and, to fix this issue, a static route is added to the FTD using the recovery-config feature.

FMC has two threat defense devices registered (10.0.21.72 and 10.0.21.73), but only one of those is reachable as shown in the next images (cli and 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#
```



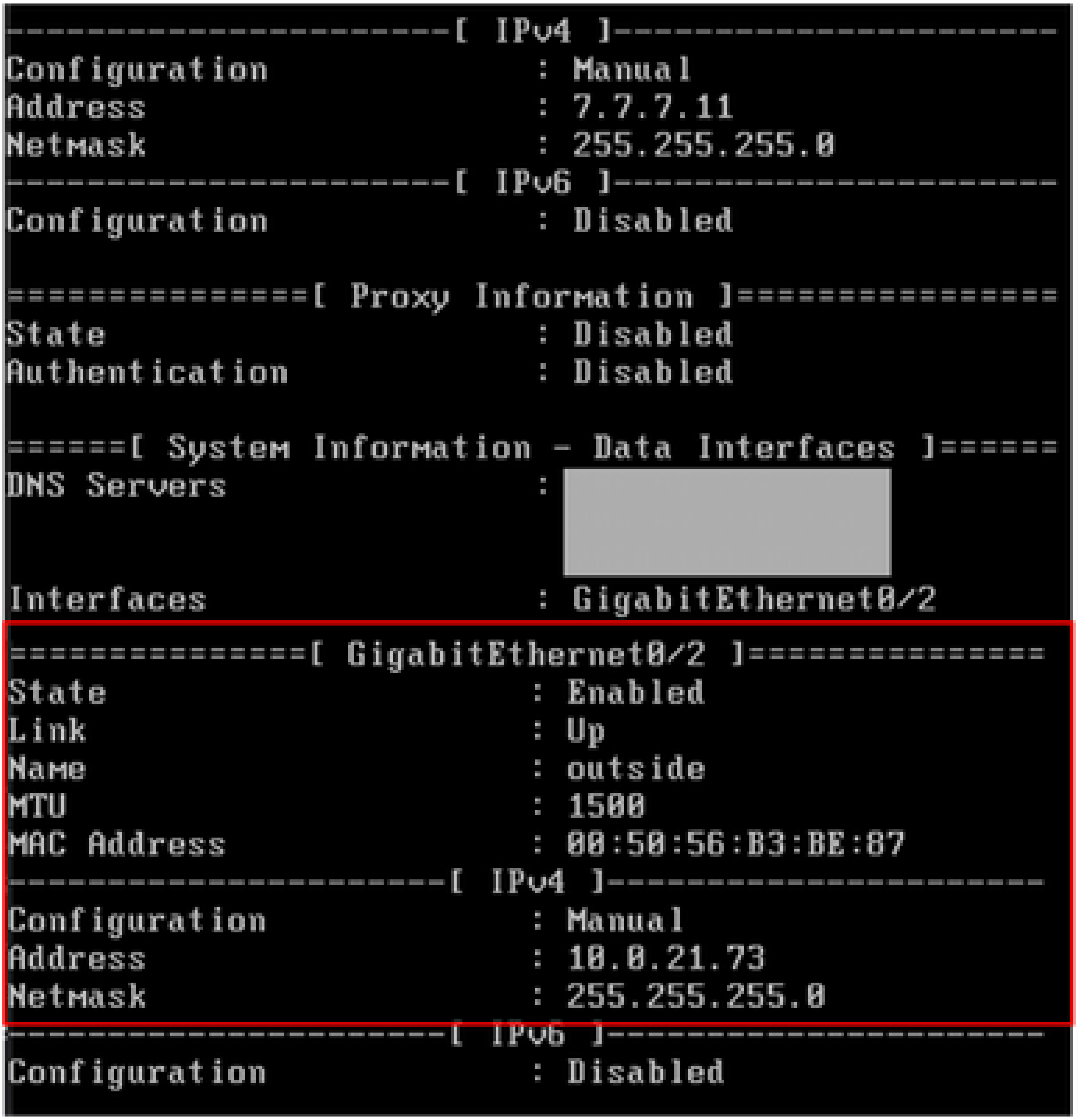
Firewall Management Center
Devices / Device Management
Search
Deploy
admin
Migrate | Deployment History
Home
Overview
Analysis
Policies
Devices
Objects
Integration
Search Device
Add
Collapse All
Download Device List Report

View By: Group

All (2) ● Error (0) ● Warning (0) ● Offline (1) ● Normal (1) ● Deployment Pending (1) ● Upgrade (0) ● Snort 3 (2)

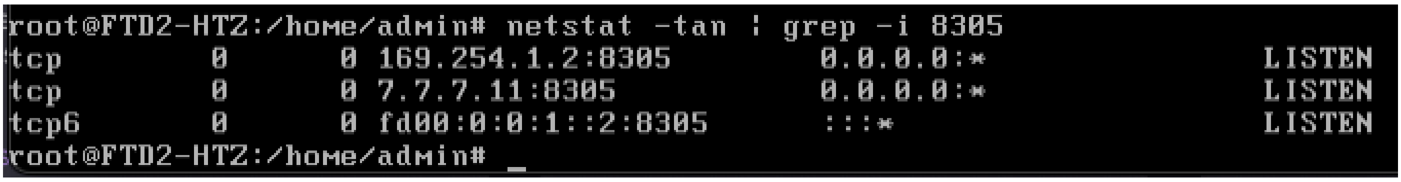
□	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
□	Ungrouped (2)						
□	FTD1-HTZ Snort 3 10.0.21.72 - Routed	Firewall Threat Defense for VMware	7.7.0	N/A	Essentials, IPS (2 more...)	HTZ	
□	FTD2-HTZ Snort 3 10.0.21.73 - Routed	Firewall Threat Defense for VMware	7.7.0	N/A	Essentials, IPS (2 more...)	HTZ	

FTD is using data interface for the registration process to FMC.



```
----------------------[ 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 also has not connection to FMC through **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. To be able to use recovery-config feature, you need to log in to FTD CLI and go to lina mode (**system support diagnostic-cli)**.

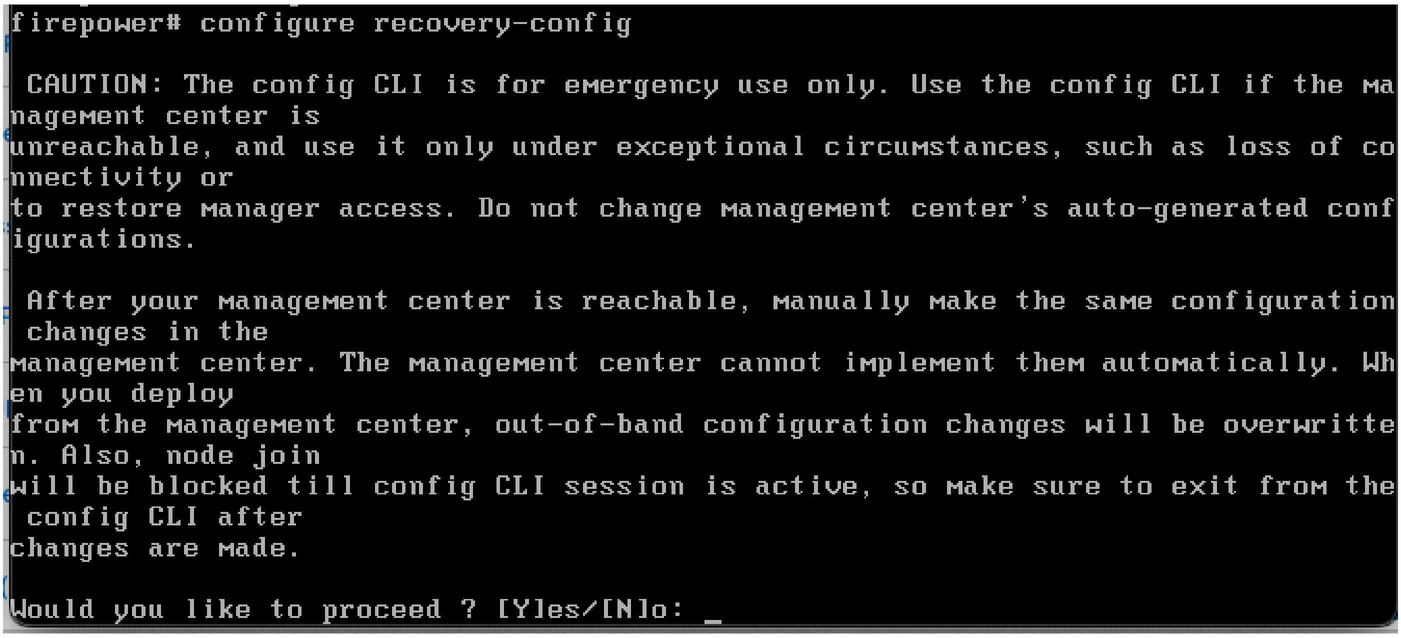
2. Run the **configure recovery-config** command.

3. If you type question mark (**?**), all the supported commands are listed, as shown in the next list.

```
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
```

Warning: You are expected to know the commands that are required for recovery or emergency use. If you are unsure about the which command must be used, it is recommended that you contact Cisco TAC for guidance.

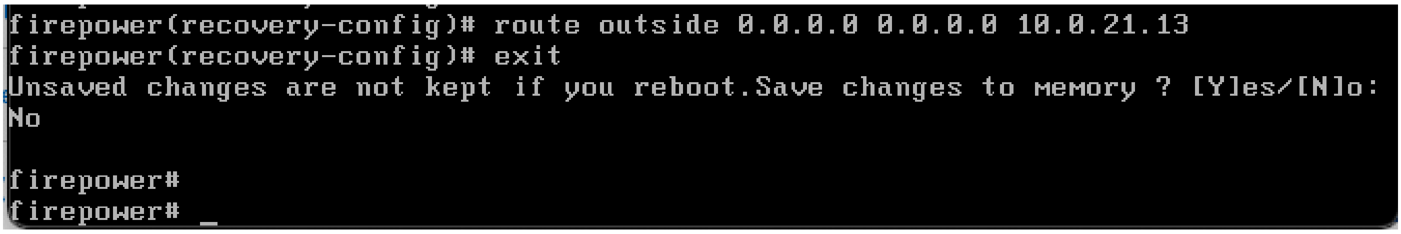
4. After you run the **configure recovery-config** command, an alert is displayed and you are asked to confirm and proceed.



```
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: _
```

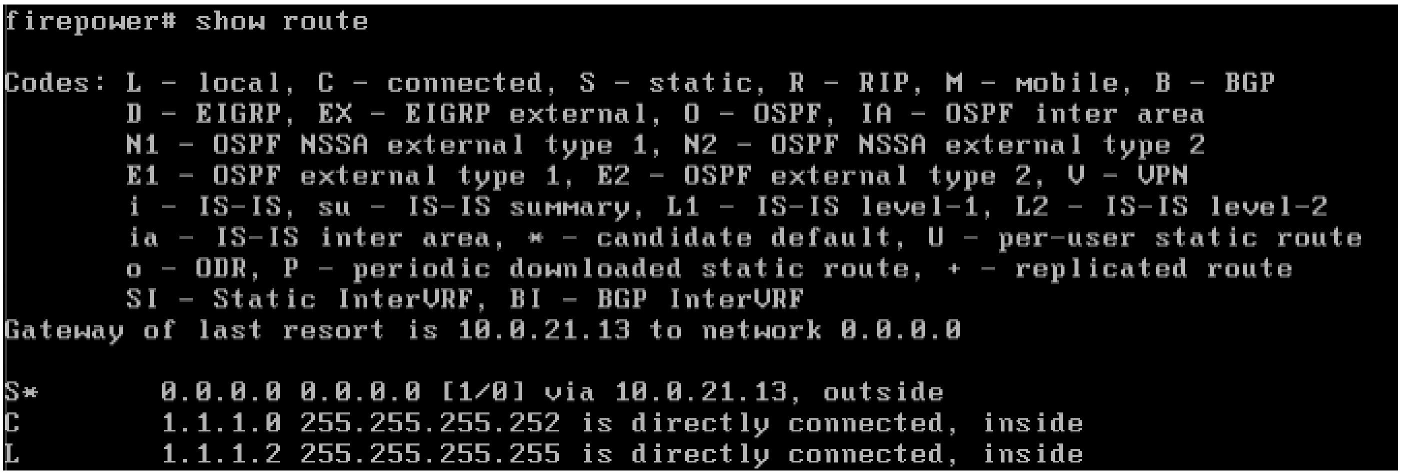
5. Once confirmed, you can start using the available config commands. In this scenario, a static route is added to the outside interface. After config is completed, run the **exit** command to exit from the recovery mode.

You are asked now to save changes and an alert is shown informing that changes are not kept if the device is rebooted.



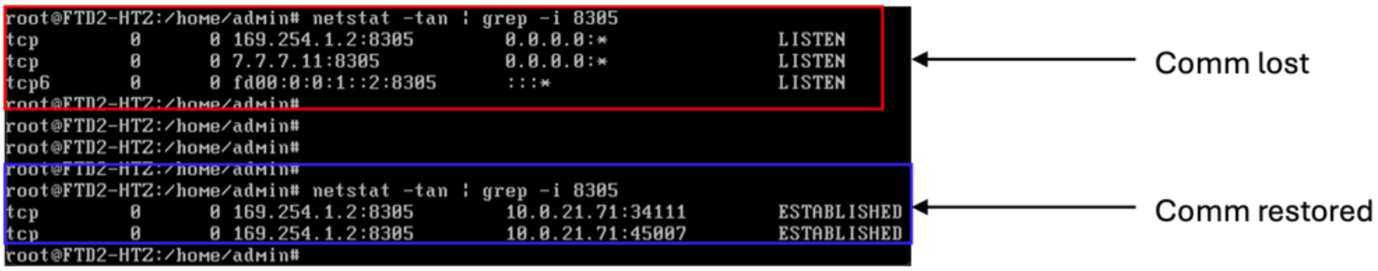
```
firepower(recovery-config)# route outside 0.0.0.0 0.0.0.0 10.0.21.13
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o:
No

firepower#
firepower# _
```

6. You can confirm the configuration has been applied. In this case, showing routes.

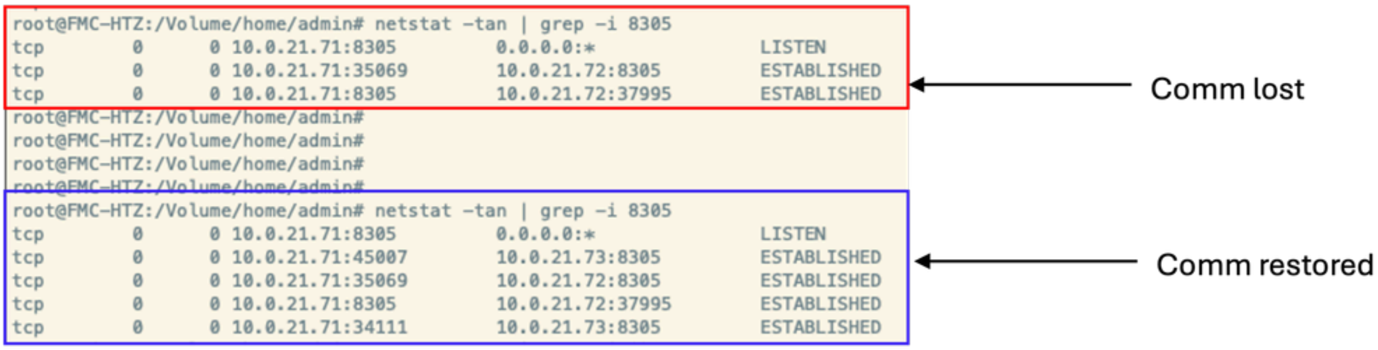


```
firepower# show route

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. After several minutes, this change restores the communication with FMC. The next images show connection established, first in FTD and next in FMC CLI.



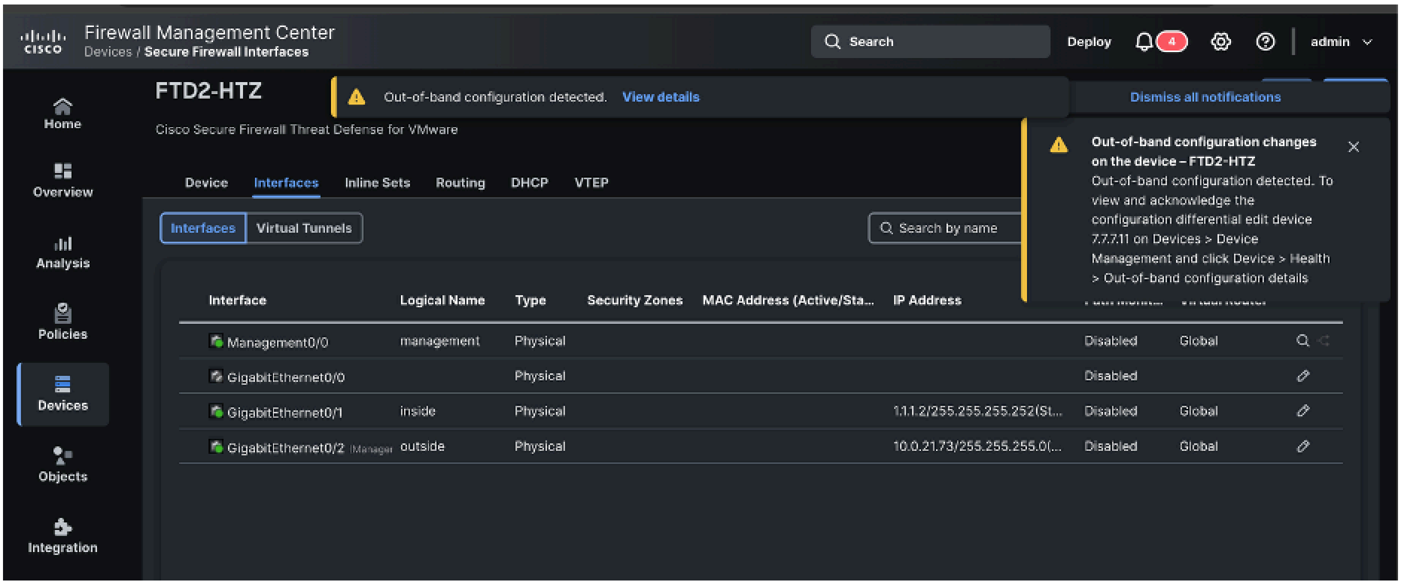
```
root@FTD2-HTZ:/home/admin# netstat -tan | grep -i 8305
tcp        0      0 169.254.1.2:8305        0.0.0.0:*               LISTEN
tcp        0      0 7.7.7.11:8305           0.0.0.0:*               LISTEN
tcp6       0      0 fd00:0:0:1::2:8305      :::*                    LISTEN
root@FTD2-HTZ:/home/admin#
root@FTD2-HTZ:/home/admin#
root@FTD2-HTZ:/home/admin#
root@FTD2-HTZ:/home/admin#
root@FTD2-HTZ:/home/admin# netstat -tan | grep -i 8305
tcp        0      0 169.254.1.2:8305        10.0.21.71:34111        ESTABLISHED
tcp        0      0 169.254.1.2:8305        10.0.21.71:45007        ESTABLISHED
root@FTD2-HTZ:/home/admin#
```



```
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#
root@FMC-HTZ:/Volume/home/admin#
root@FMC-HTZ:/Volume/home/admin#
root@FMC-HTZ:/Volume/home/admin#
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 10.0.21.71:45007        10.0.21.73:8305         ESTABLISHED
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
tcp        0      0 10.0.21.71:34111        10.0.21.73:8305         ESTABLISHED
```

8. After configuration is restored, in FMC GUI you can naviate to **Device > Device Management** and click on your device (in this case it is FTD2-HTZ).

There you can see the **Out-of-band configuration detected** alert. Click in **View details** to see configuration differences.



FTD2-HTZ

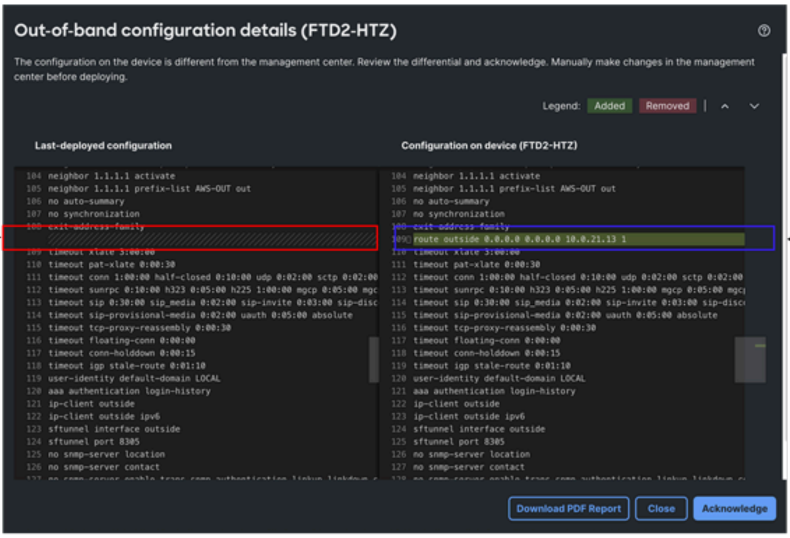
Cisco Secure Firewall Threat Defense for VMware

Out-of-band configuration detected. View details

Out-of-band configuration changes on the device – FTD2-HTZ
Out-of-band configuration detected. To view and acknowledge the configuration differential edit device 7.7.7.11 on Devices > Device Management and click Device > Health > Out-of-band configuration details

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address		
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1	inside	Physical			1.1.1.2/255.255.255.252(St...	Disabled	Global
GigabitEthernet0/2 (Manager	outside	Physical			10.0.21.73/255.255.255.0(...	Disabled	Global

9. Review **Out-of-band configuration details** and acknowledge differences.



Configuration missing

Configuration added

Out-of-band configuration details (FTD2-HTZ)

The configuration on the device is different from the management center. Review the differential and acknowledge. Manually make changes in the management center before deploying.

Legend: Added Removed

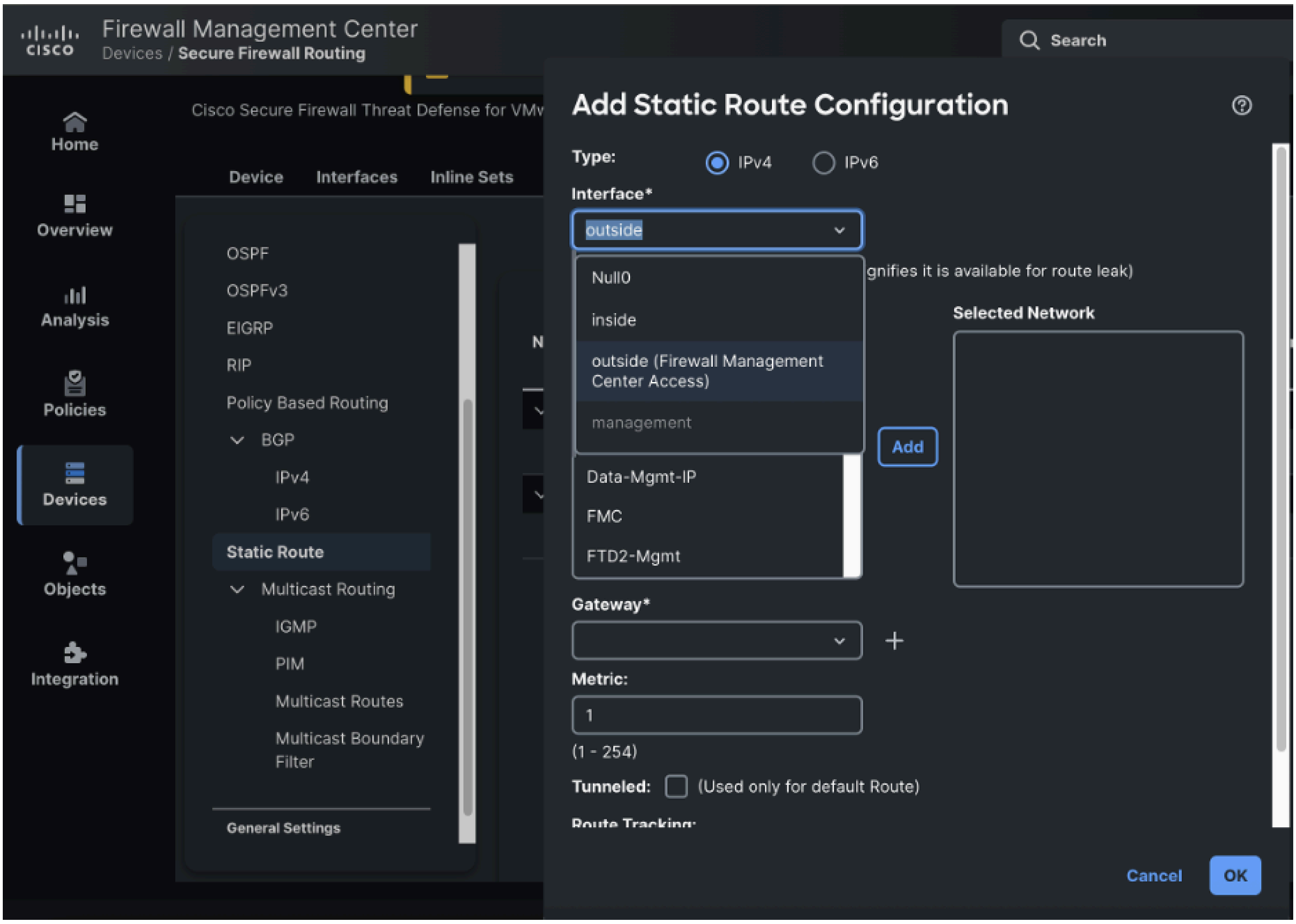
Last-deployed configuration

```
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 prefix-list AWS-OUT out
no auto-summary
no synchronization
exit-address-family

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgc
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disc
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
ip-client outside
ip-client outside ipv6
sftunnel interface outside
sftunnel port 8305
no snmp-server location
no snmp-server contact
```

Configuration on device (FTD2-HTZ)

```
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 prefix-list AWS-OUT out
no auto-summary
no synchronization
exit-address-family
route outside 0.0.0.0 0.0.0.0 10.0.21.13 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgc
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disc
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
ip-client outside
ip-client outside ipv6
sftunnel interface outside
sftunnel port 8305
no snmp-server location
no snmp-server contact
```

10. After configuration differences are acknowledge, proceed to configure the same changes done in the recovery mode, but now through FMC GUI. In this scenario, a static route is added.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

Null0
inside
outside (Firewall Management Center Access)
management
Data-Mgmt-IP
FMC
FTD2-Mgmt
gnifies it is available for route leak)
Selected Network
Add

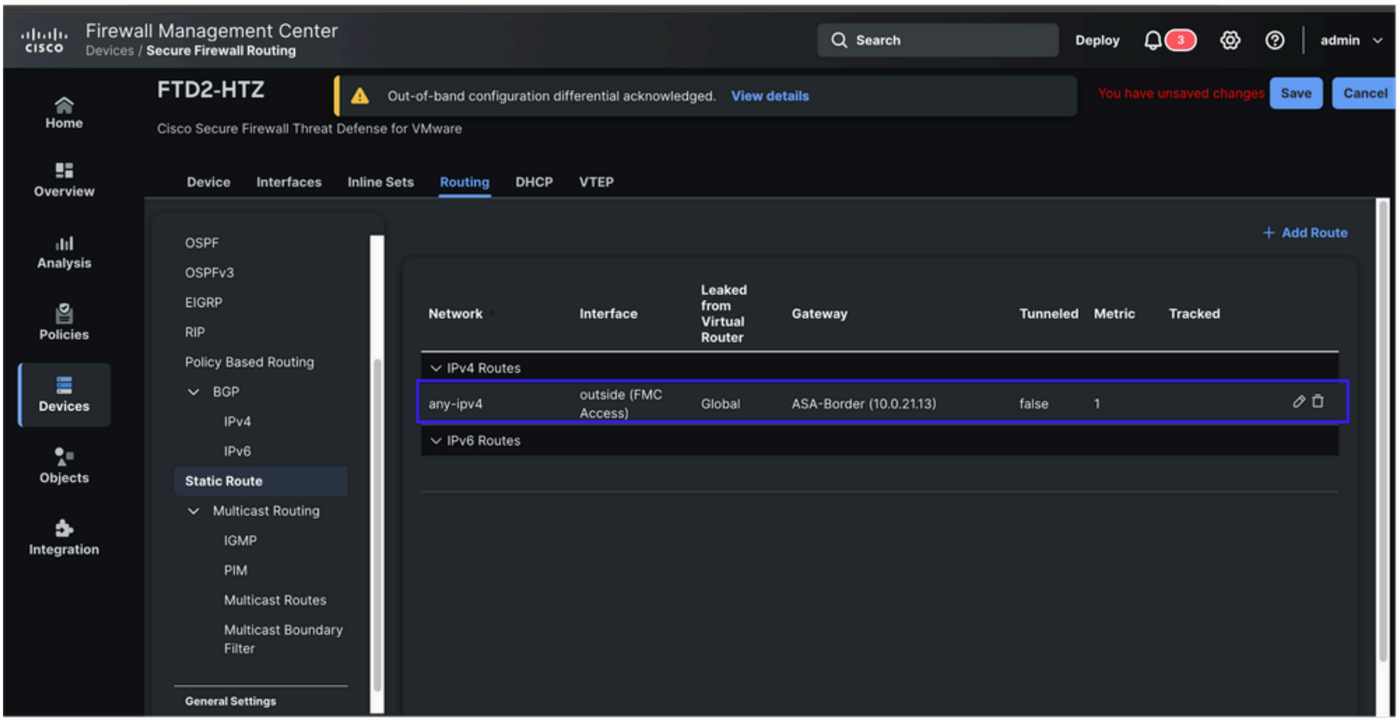
Gateway*:

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

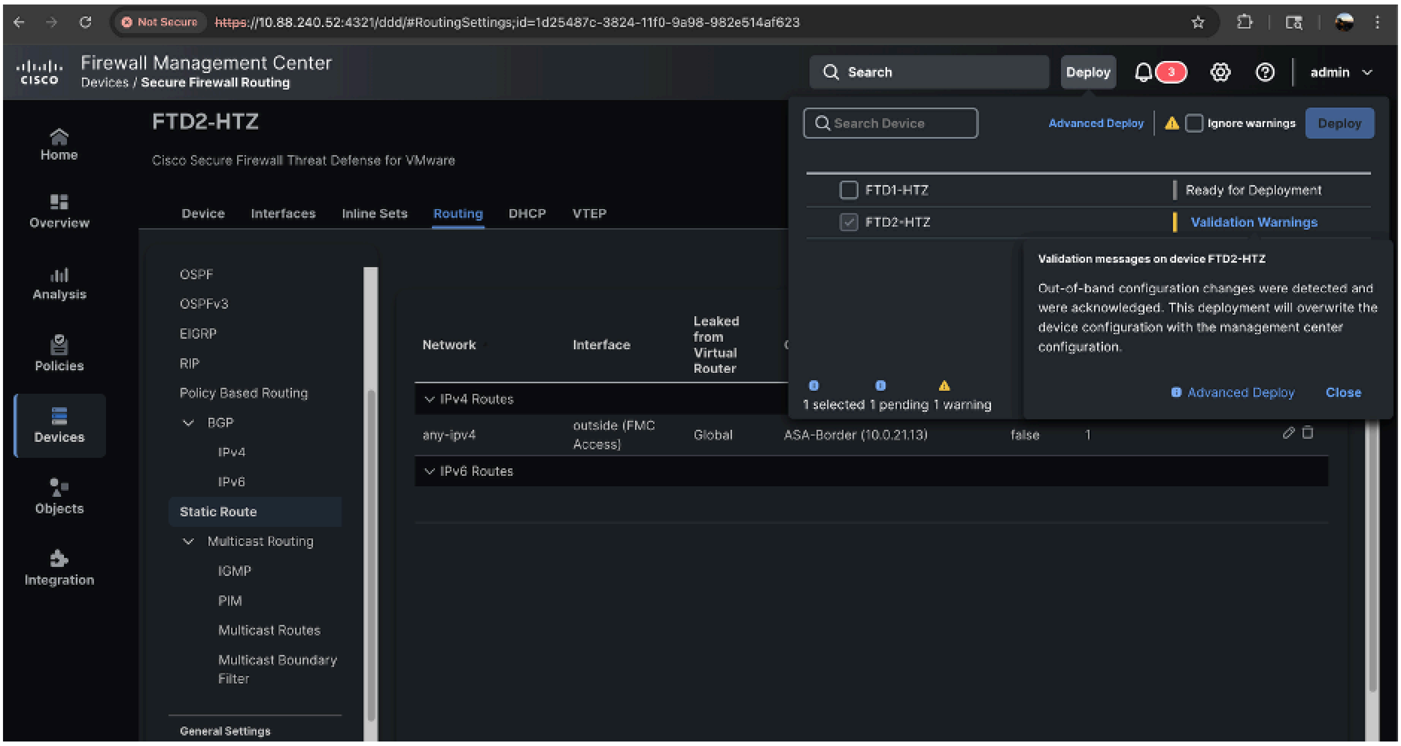


Out-of-band configuration differential acknowledged. View details

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
∨ IPv4 Routes						
any-ipv4	outside (FMC Access)	Global	ASA-Border (10.0.21.13)	false	1	
∨ IPv6 Routes						

11. Once configuration changes are saved, proceed to deploy the changes. Another alert is shown informing Out-of-band configuration changes were detected and acknowledged, and that the changes are overridden by the current deployment.

Once the deployment succeeds, the configuration is in sync again.



https://10.88.240.52:4321/ddd/#RoutingSettings;id=1d25487c-3824-11f0-9a98-982e514af623

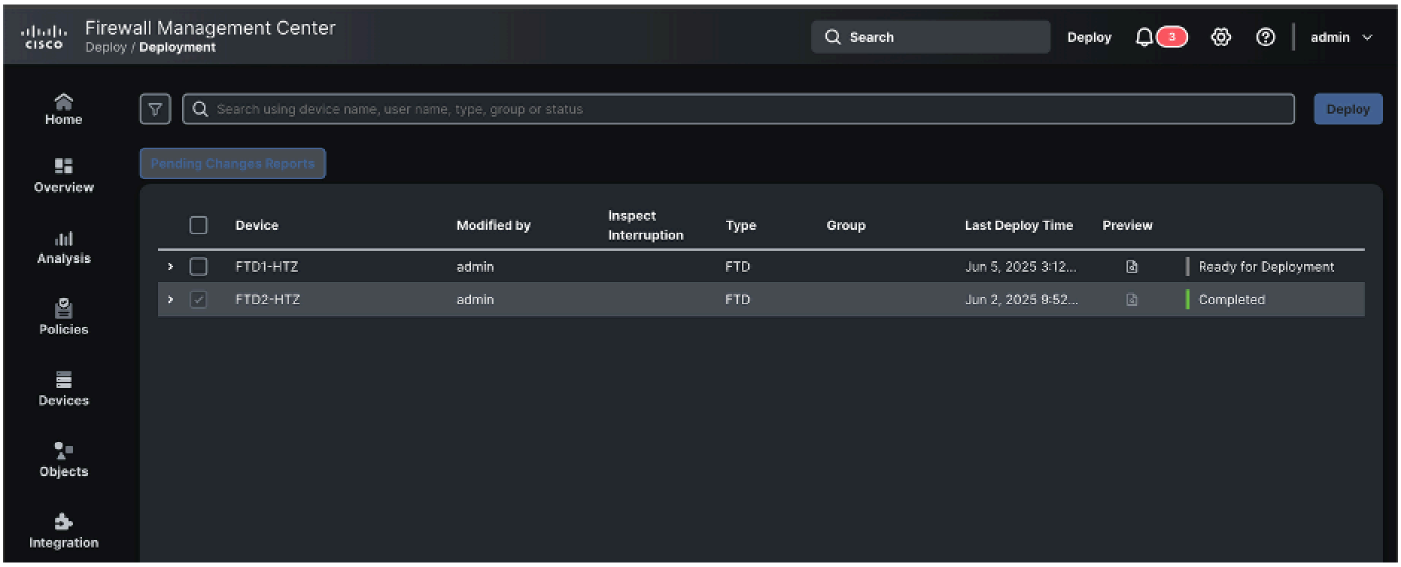
□ FTD1-HTZ	Ready for Deployment
☑ FTD2-HTZ	Validation Warnings

1 selected 1 pending 1 warning

Validation messages on device FTD2-HTZ

Out-of-band configuration changes were detected and were acknowledged. This deployment will overwrite the device configuration with the management center configuration.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
∨ IPv4 Routes					
any-ipv4	outside (FMC Access)	Global	ASA-Border (10.0.21.13)	false	1
∨ IPv6 Routes					



□	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	
› □	FTD1-HTZ	admin		FTD		Jun 5, 2025 3:12...		Ready for Deployment
› ☑	FTD2-HTZ	admin		FTD		Jun 2, 2025 9:52...		Completed

References

- 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_Firepov