Configure static routes with Firewall Management Center (FMC)

Contents

Introduction

This document describes the process of how to deploy static routes in Secure Firewall Threat Defense through Firewall Management Center.

Prerequisites

Requirements

Cisco recommends having knowledge of these topics:

- Firewall Management Center (FMC)
- Secure Firewall Threat Defense (FTD)
- Network routes foundamentals.

Components Used

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

- Firewall Management Center for VMWare v7.3
- Cisco Secure Firewall Threat Defense for VMWare v7.3

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 Information

This procedure is supported on appliances:

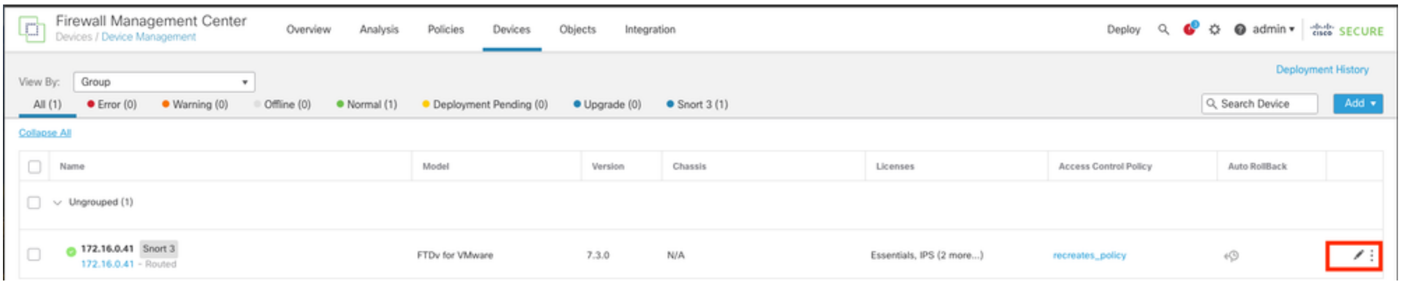
- Firewall Management Center On-Prem
- Firewall Management Center for VMWare
- cdFMC
- Cisco Secure Firewall 1000 series appliances
- Cisco Secure Firewall 2100 Series appliances
- Cisco Secure Firewall 3100 series appliances
- Cisco Secure Firewall 4100 series appliances
- Cisco Secure Firewall 4200 series appliances
- Cisco Secure Firewall 9300 appliance
- Cisco Secure Firewall Threat Defense for VMWare

Configure

Configurations

Step 1. In the FMC GUI , Navigate to **Devices > Device Managment.**

Step 2. Identify the FTD that is going to be configured and click the pencil icon in order to edit the current configuration of the FTD.

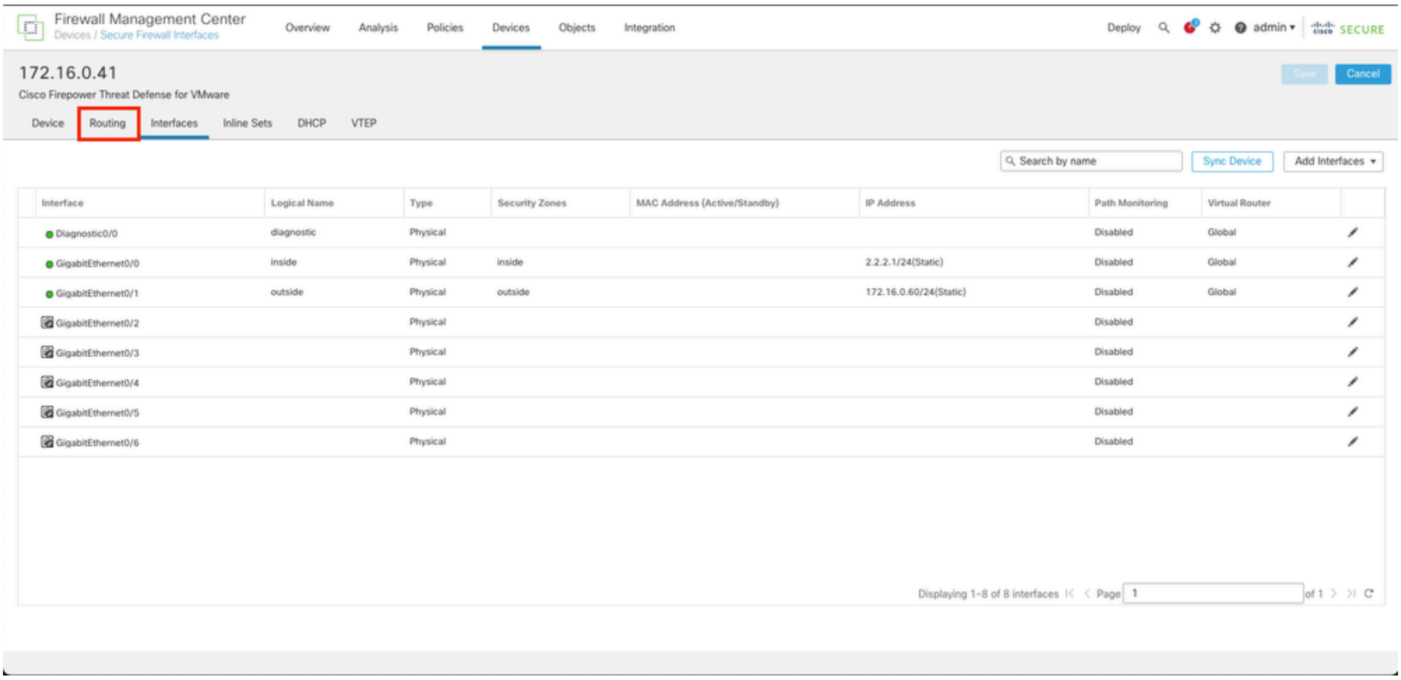


View By: Group

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

□	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
□	Ungrouped (1)							
□	172.16.0.41 Snort 3 172.16.0.41 - Routed	FTDv for VMware	7.3.0	N/A	Essentials, IPS (2 more...)	recreates_policy		✎ ⋮

Step 2. Click over the **Routing** tab.

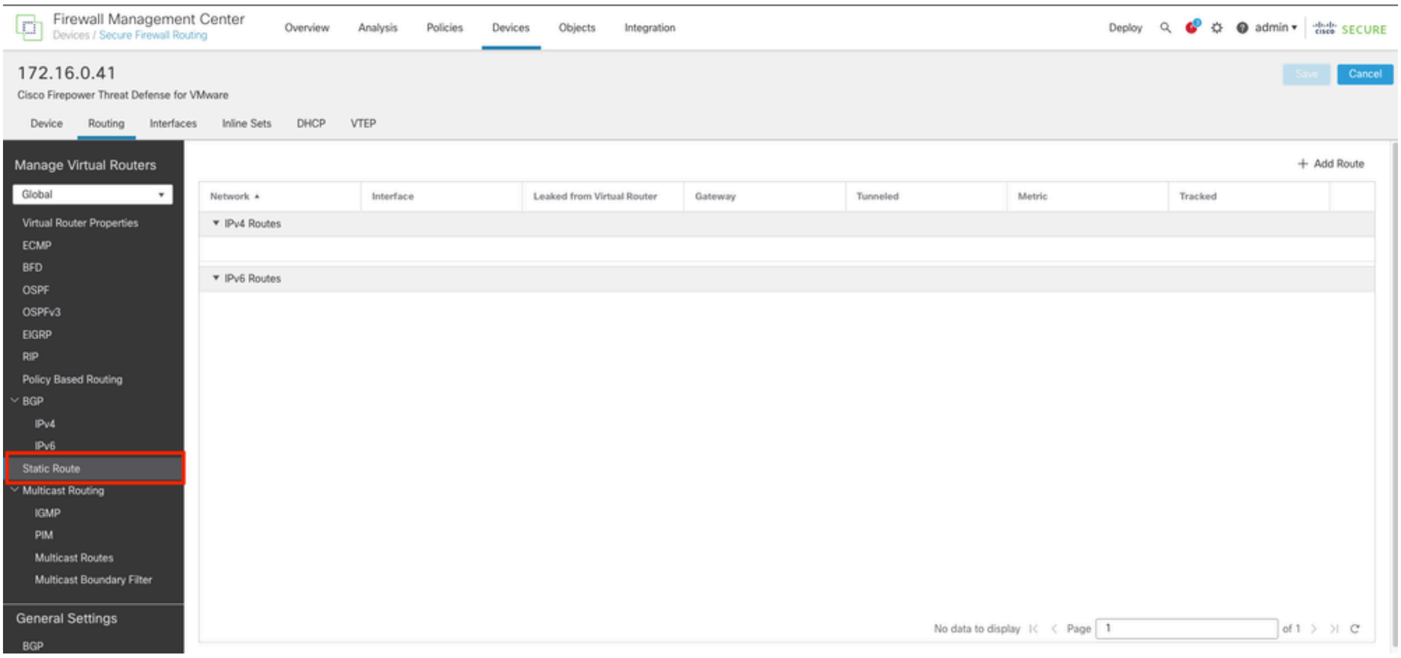


172.16.0.41
Cisco Firepower Threat Defense for VMware

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Diagnostic0/0	diagnostic	Physical				Disabled	Global
GigabitEthernet0/0	inside	Physical	inside		2.2.2.1/24(Static)	Disabled	Global
GigabitEthernet0/1	outside	Physical	outside		172.16.0.60/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
GigabitEthernet0/4		Physical				Disabled	
GigabitEthernet0/5		Physical				Disabled	
GigabitEthernet0/6		Physical				Disabled	

Displaying 1-8 of 8 interfaces Page 1 of 1

Step 3. At the left menu select **Static Route**

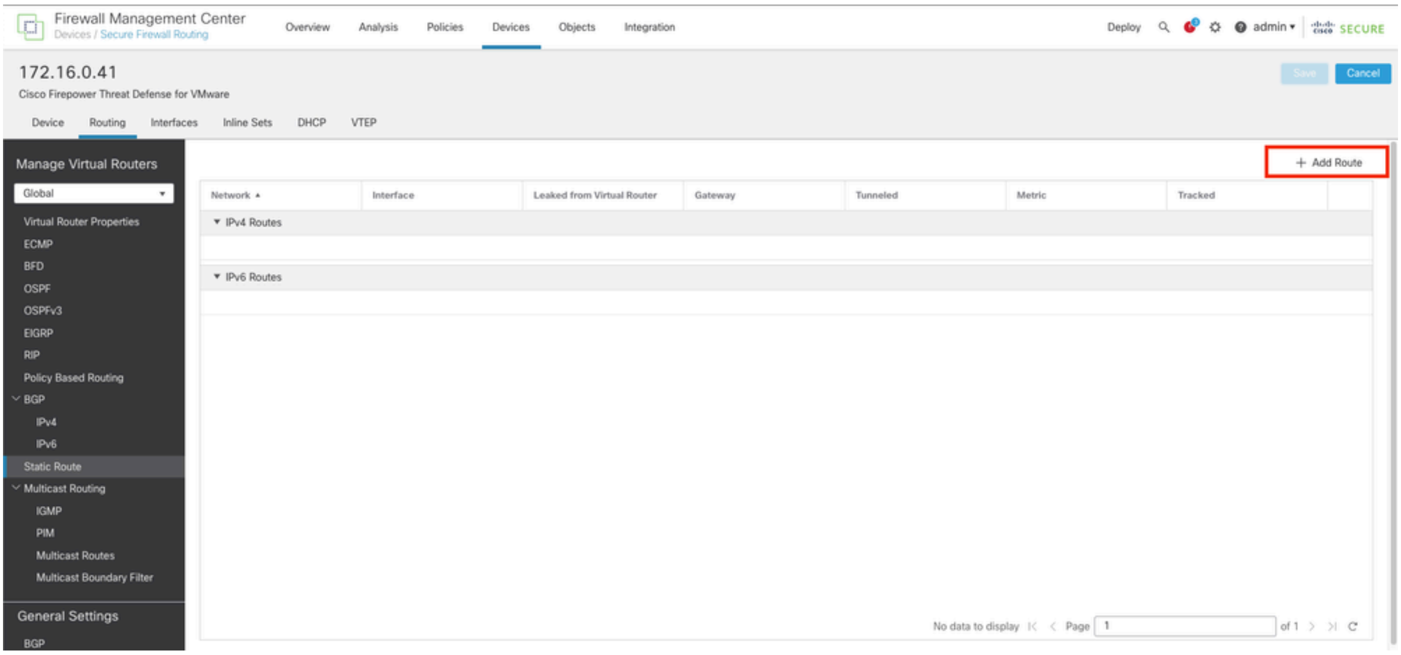


172.16.0.41
Cisco Firepower Threat Defense for VMware

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

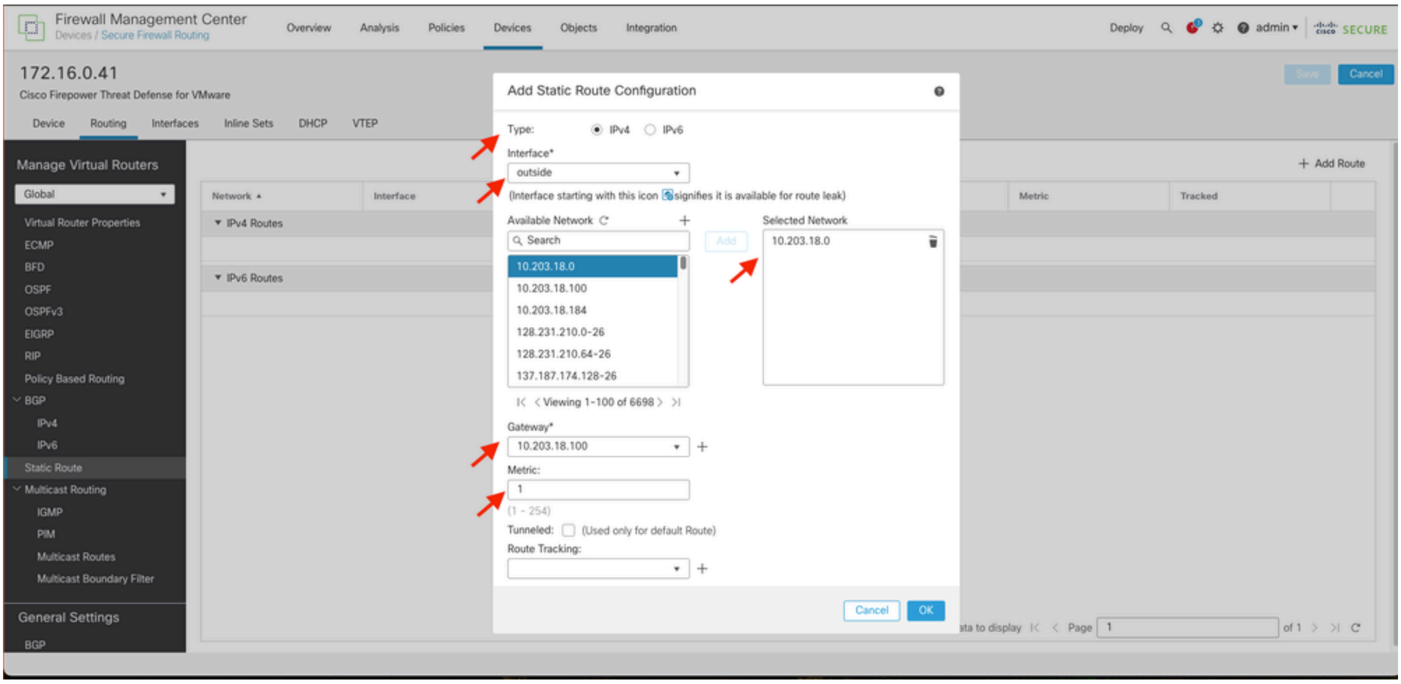
No data to display Page 1 of 1

Step 4. click the **(+) Add route** option.



Step 5. Under the **Static Route Configuration** section, enter the required information in the **Type**, **Interface**, **Available Network**, **Gateway**, and **Metric** fields (as well as **Tunneled** and **Route tracking** if needed).

Type: Click **IPv4**or **IPv6** depending on the type of static route that you are adding.
Interface: Choose the**Interface**to which this static route applies.
Available Network: In the **Available Network** list, choose the destination network. To define a default route, create an object with the address 0.0.0.0/0 and select it here.
Gateway: In the**Gateway or IPv6 Gateway** field, enter or choose the gateway router which is the next hop for this route. You can provide an IP address or a Networks/Hosts object.
Metric: In the **Metric**field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.
Tunneled: (Optional) For a default route, click the **Tunneled** checkbox to define a separate default route for VPN traffic
Route tracking: (IPv4 static route only) To monitor route availability, enter or choose the name of an SLA (service level agreement) Monitor object that defines the monitoring policy, in the **Route Tracking** field.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

(Interface starting with this icon signifies it is available for route leak)

Available Network

Search

- 10.203.18.0
- 10.203.18.100
- 10.203.18.184
- 128.231.210.0-26
- 128.231.210.64-26
- 137.187.174.128-26

Viewing 1-100 of 6698

Add

Selected Network: 10.203.18.0

Gateway*: 10.203.18.100

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

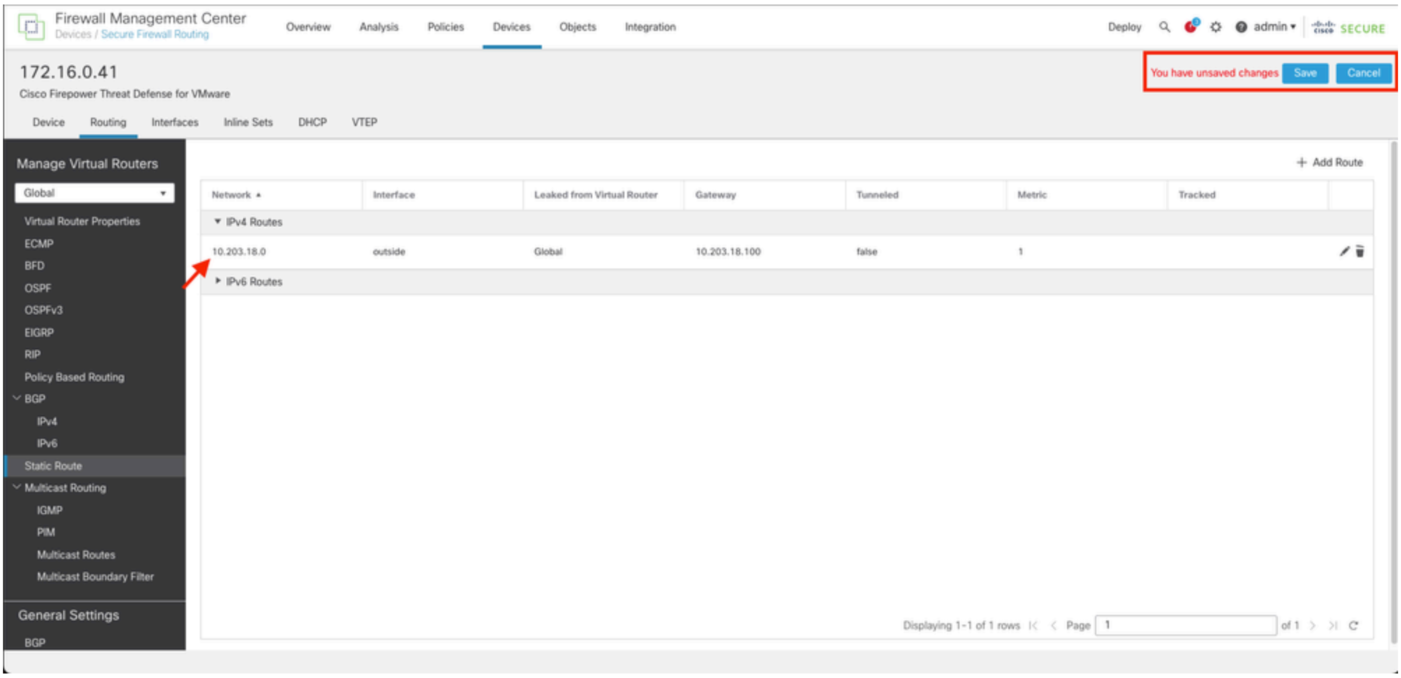
Route Tracking:

Cancel OK

Tip: Available Network , Gateway and Route traffic fields requires the use of network objects, if the objects are not created yet , please click over the **(+)** sign at the right of each filed in order to create a new network object.

Step 6. Click on **OK**

Step 7. Save the configuration and validate the new static route it is showing as expected.



Firewall Management Center
Devices / Secure Firewall Routing

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin ▾ | SECURE

172.16.0.41
Cisco Firepower Threat Defense for VMware

You have unsaved changes | Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

Manage Virtual Routers: Global

Virtual Router Properties, ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP (IPv4, IPv6), Static Route, Multicast Routing (IGMP, PIM, Multicast Routes, Multicast Boundary Filter)

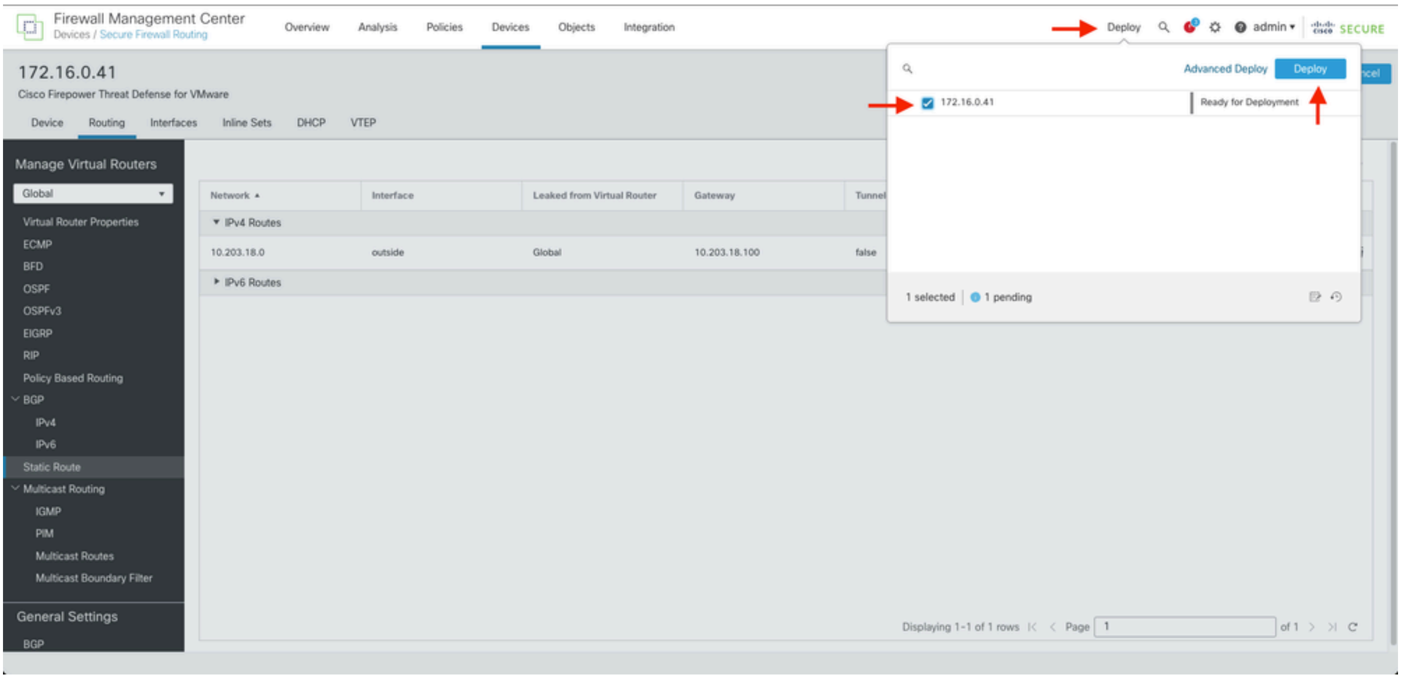
General Settings: BGP

+ Add Route

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▾ IPv4 Routes						
10.203.18.0	outside	Global	10.203.18.100	false	1	
▸ IPv6 Routes						

Displaying 1-1 of 1 rows | Page 1 of 1

Step 7. Navigate to **Deploy** and **checkbox** the selected FTD in **Step 2**, then click over the blue deploy icon to deploy the new configuration.



Firewall Management Center
Devices / Secure Firewall Routing

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin ▾ | SECURE

172.16.0.41
Cisco Firepower Threat Defense for VMware

Advanced Deploy | Deploy

☑ 172.16.0.41 | Ready for Deployment

1 selected | ● 1 pending

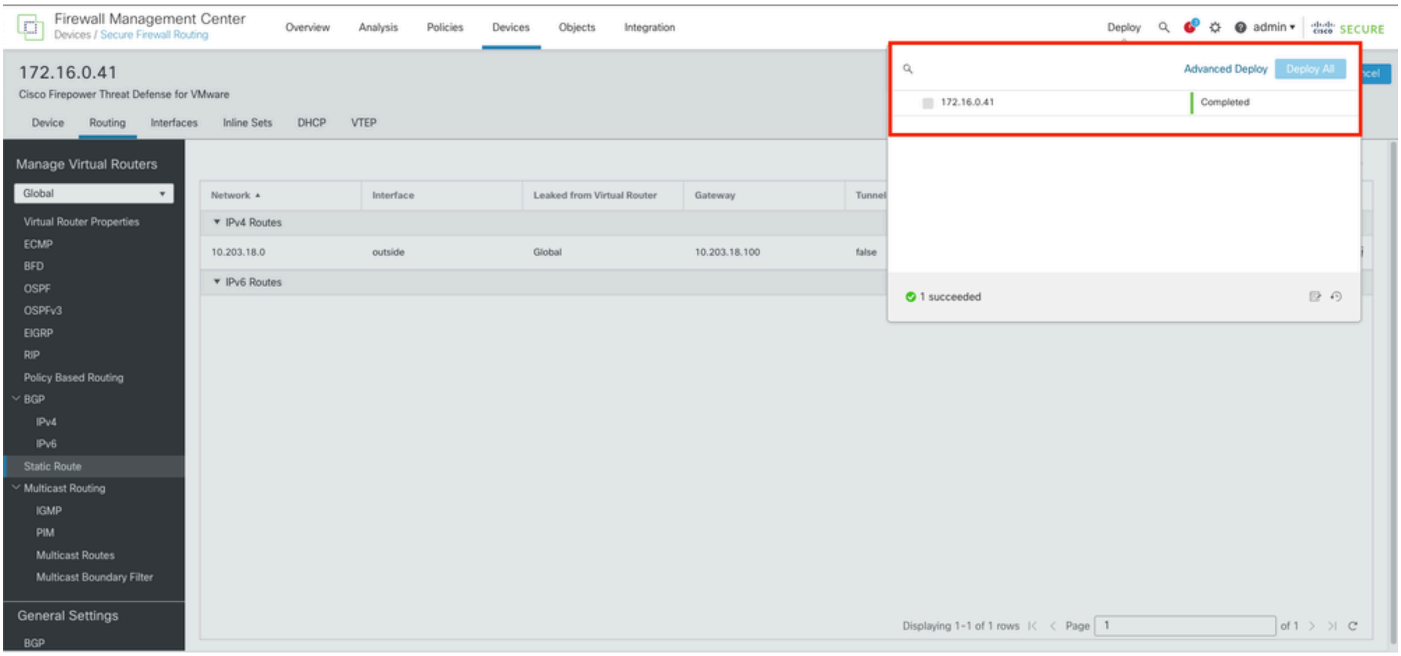
Device | Routing | Interfaces | Inline Sets | DHCP | VTEP

Manage Virtual Routers: Global

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunnel
▾ IPv4 Routes				
10.203.18.0	outside	Global	10.203.18.100	false
▸ IPv6 Routes				

Displaying 1-1 of 1 rows | Page 1 of 1

Step 8. Validate the deployment is showing as completed.



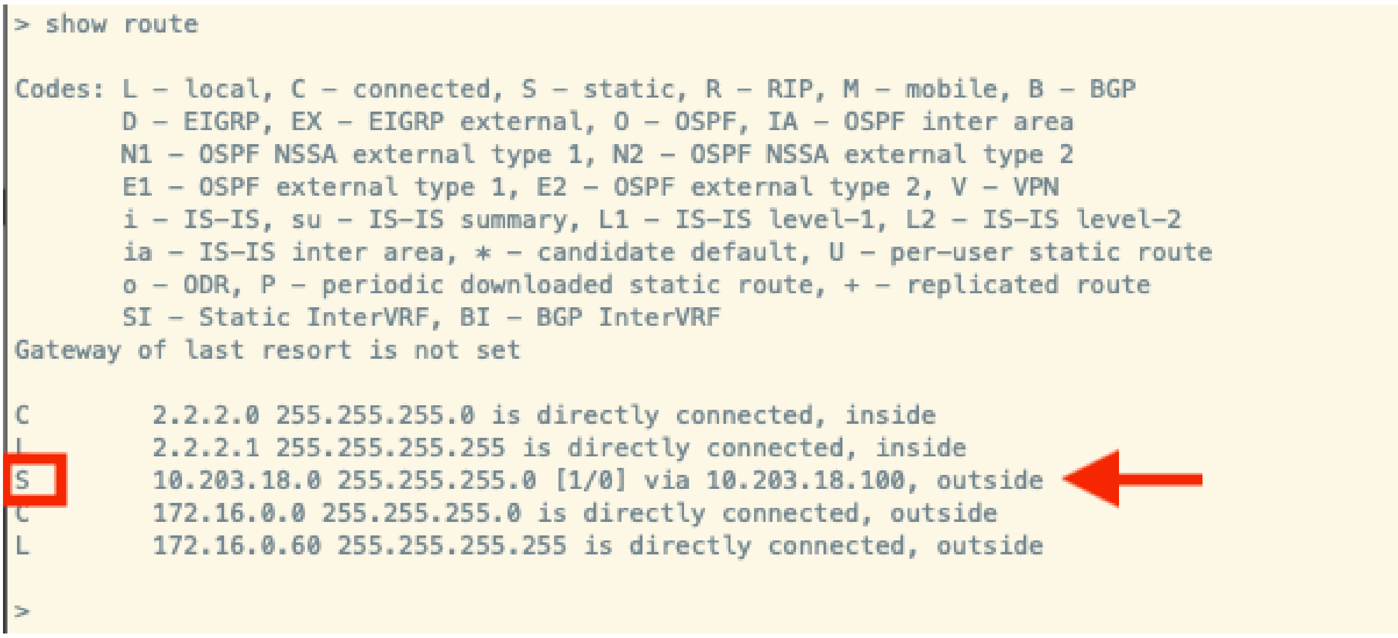
Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunnel
▼ IPv4 Routes				
10.203.18.0	outside	Global	10.203.18.100	false
▼ IPv6 Routes				

Verify

1. Log using SSH, Telnet or console to the previously deployed FTD.

2. Run command **show route** and **show running-config route**

3. Validate the FTD routing table has now the deployed static route with the **S** flag and that it is also showing in the running configuration.

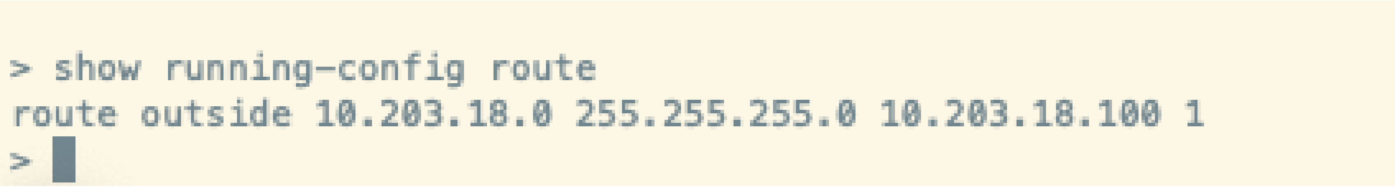


```
> show route

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 not set

C        2.2.2.0 255.255.255.0 is directly connected, inside
L        2.2.2.1 255.255.255.255 is directly connected, inside
S        10.203.18.0 255.255.255.0 [1/0] via 10.203.18.100, outside
C        172.16.0.0 255.255.255.0 is directly connected, outside
L        172.16.0.60 255.255.255.255 is directly connected, outside

>
```



```
> show running-config route
route outside 10.203.18.0 255.255.255.0 10.203.18.100 1
>
```