

Configurer des routes statiques avec le Centre de gestion des pare-feu (FMC)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurations](#)

[Vérifier](#)

Introduction

Ce document décrit le processus de déploiement de routes statiques dans Secure Firewall Threat Defense via Firewall Management Center.

Conditions préalables

Exigences

Cisco recommande d'avoir connaissance de ces sujets :

- Centre de gestion des pare-feu (FMC)
- Protection pare-feu et protection contre les menaces (FTD)
- Routes réseau - Notions de base.

Composants utilisés

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Firewall Management Center pour VMWare v7.3
- Cisco Secure Firewall Threat Defense pour 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cette procédure est prise en charge sur les appliances :

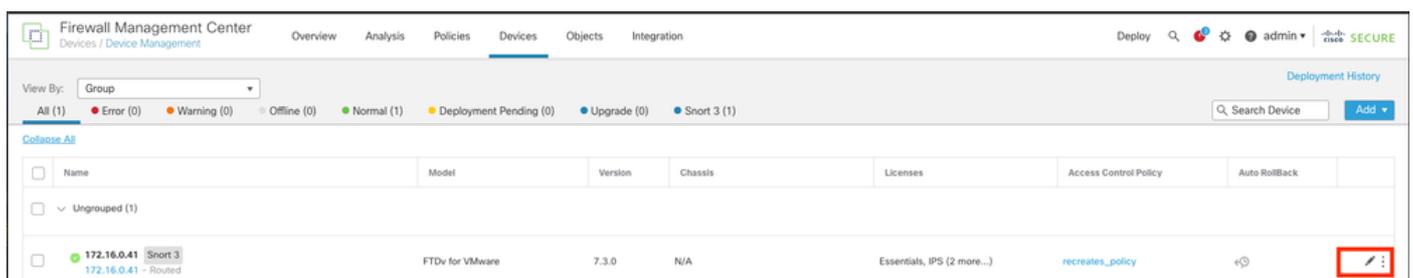
- Firewall Management Center On-Prem
- Firewall Management Center pour VMWare
- CdFMC
- Appliances Cisco Secure Firewall 1000
- Appliances Cisco Secure Firewall 2100
- Appliances Cisco Secure Firewall 3100
- Appliances Cisco Secure Firewall 4100
- Appliances Cisco Secure Firewall 4200
- Appliance Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense pour VMWare

Configurer

Configurations

Étape 1. Dans l'interface utilisateur graphique de FMC , accédez à Périphériques > Gestion des périphériques.

Étape 2. Identifiez le FTD qui va être configuré et cliquez sur l'icône de crayon afin de modifier la configuration actuelle du FTD.



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
172.16.0.41	FTDv for VMware	7.3.0	N/A	Essentials, IPS (2 more...)	recreates_policy	+S	

Étape 2. Cliquez sur l'onglet Routage.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

172.16.0.41
Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

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

Étape 3. Dans le menu de gauche, sélectionnez Static Route

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

172.16.0.41
Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

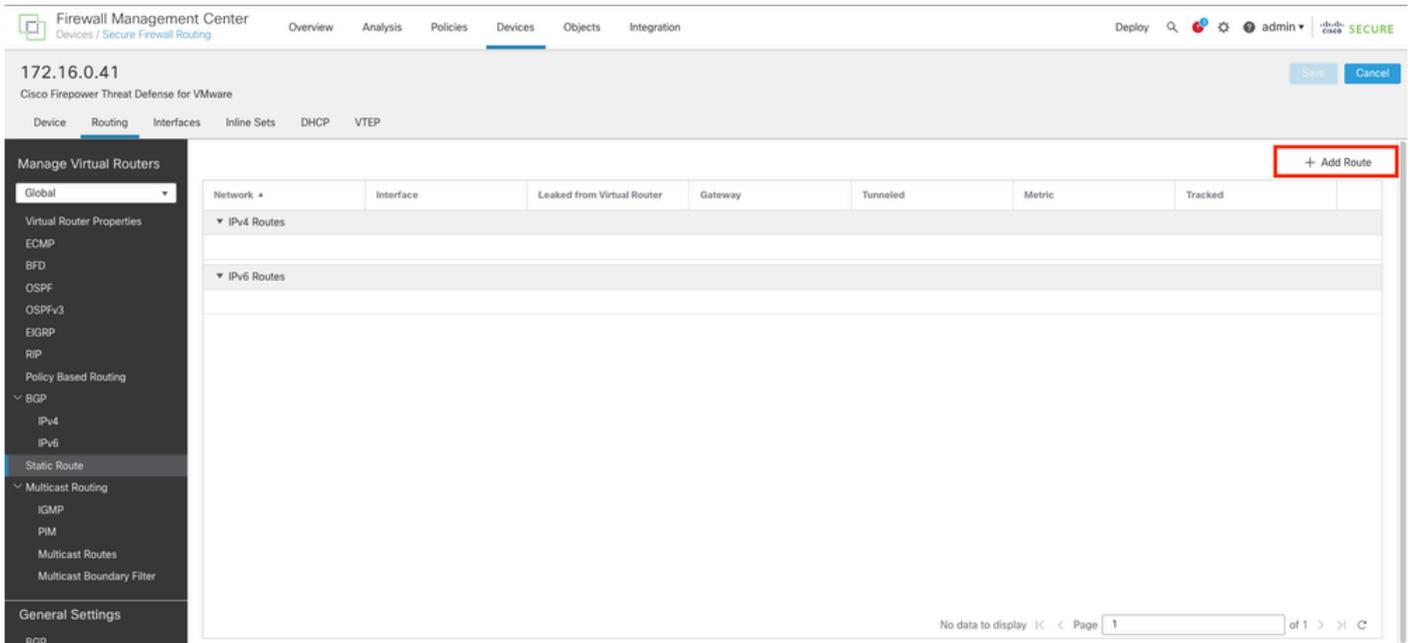
Global

- 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

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

No data to display Page 1 of 1

Étape 4. cliquez sur l'option (+) Add route.



Étape 5. Dans la section Static Route Configuration, saisissez les informations requises dans les champs Type, Interface, Available Network, Gateway, and Metric (ainsi que Tunneled et le suivi de route si nécessaire).

Type : cliquez sur IPv4 ou IPv6 selon le type de route statique que vous ajoutez.

Interface : sélectionnez l'interface à laquelle cette route statique s'applique.

Available Network : dans la liste Available Network, sélectionnez le réseau de destination. Pour définir une route par défaut, créez un objet avec l'adresse 0.0.0.0/0 et sélectionnez-le ici.

Passerelle : dans le champ Passerelle ou Passerelle IPv6, entrez ou sélectionnez le routeur de passerelle qui est le tronçon suivant pour cette route. Vous pouvez fournir une adresse IP ou un objet Réseaux/Hôtes.

Metric : dans le champ Metric, saisissez le nombre de sauts vers le réseau de destination. Les valeurs valides sont comprises entre 1 et 255 ; la valeur par défaut est 1.

Tunneled : (facultatif) pour une route par défaut, cochez la case Tunneled pour définir une route par défaut distincte pour le trafic VPN

Suivi de route : (route statique IPv4 uniquement) Pour surveiller la disponibilité de la route, saisissez ou sélectionnez le nom d'un objet de surveillance SLA (accord de niveau de service) qui définit la stratégie de surveillance, dans le champ Suivi de route.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy admin

172.16.0.41
Cisco Firepower Threat Defense for VMware

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

Network Interface

IPv4 Routes

IPv6 Routes

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

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

Available Network +

Selected Network

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

Gateway*
10.203.18.100

Metric:
1

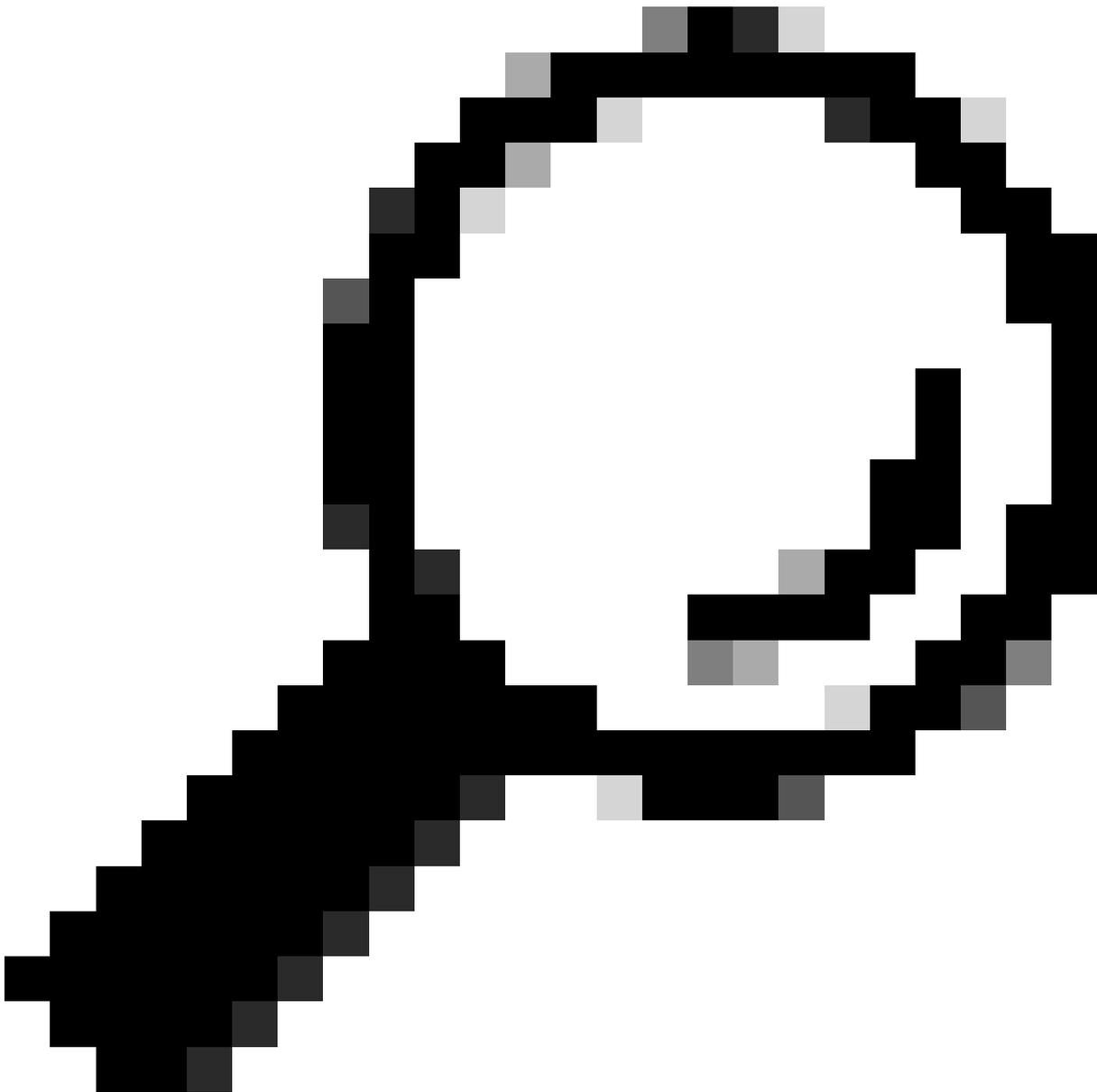
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel OK

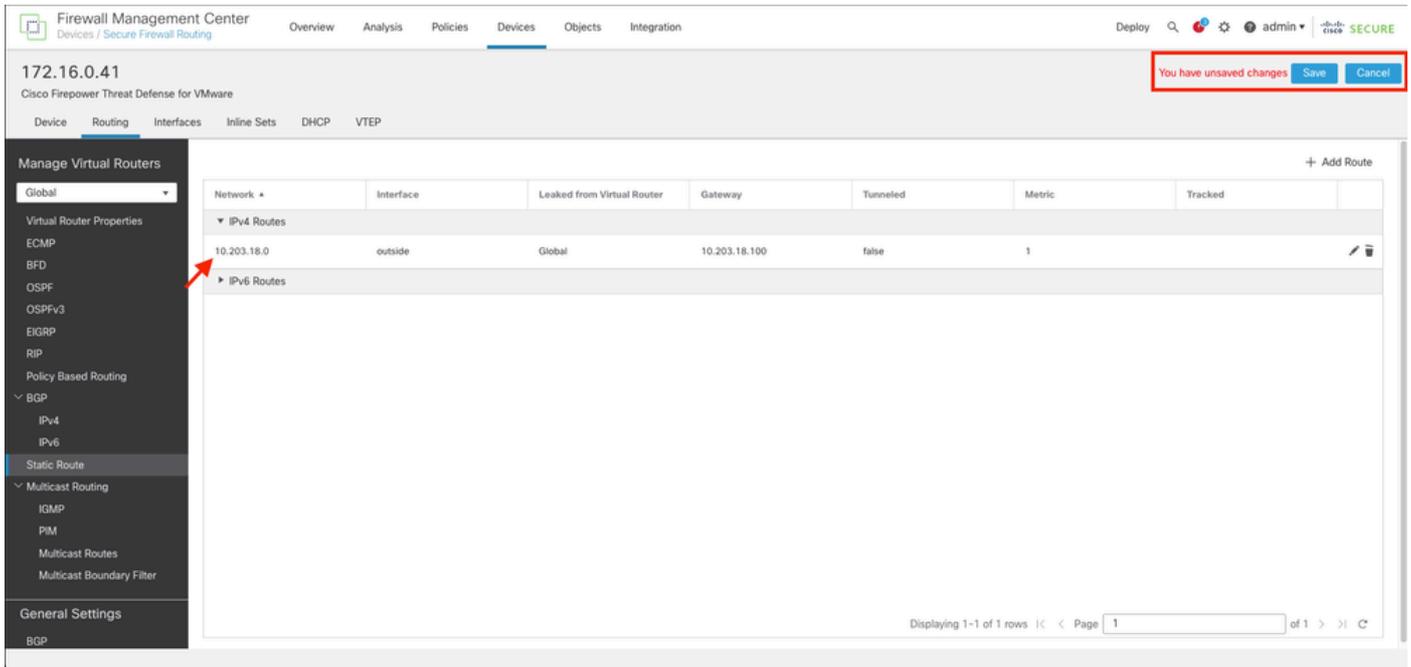
data to display Page 1 of 1



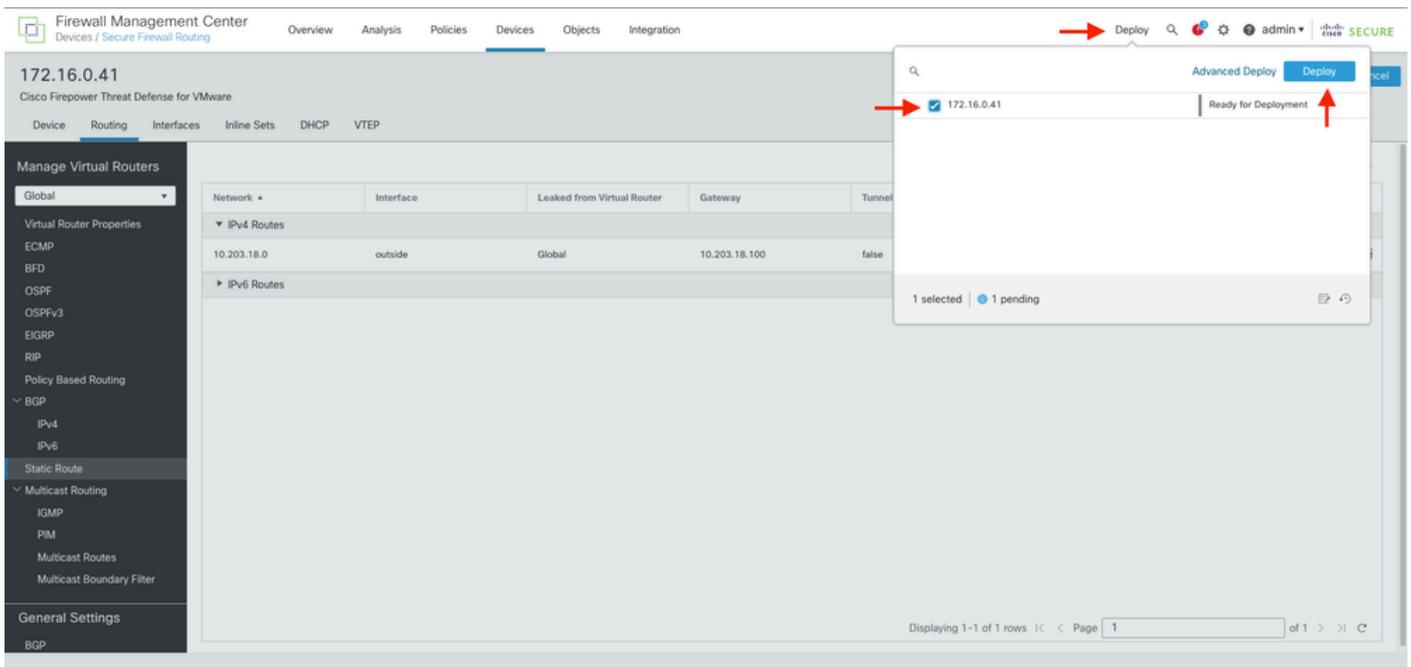
Conseil : les champs Réseau disponible , Passerelle et Trafic de route nécessitent l'utilisation d'objets réseau. Si les objets ne sont pas encore créés, cliquez sur le signe (+) à droite de chaque champ afin de créer un nouvel objet réseau.

Étape 6. Cliquez sur OK

Étape 7. Enregistrez la configuration et validez la nouvelle route statique affichée comme prévu.



Étape 7. Accédez à Déployer et cochez la case du FTD sélectionné à l'étape 2, puis cliquez sur l'icône bleue de déploiement pour déployer la nouvelle configuration.



Étape 8. Validez le déploiement comme étant terminé.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy admin

172.16.0.41
Cisco Firepower Threat Defense for VMware

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

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

172.16.0.41 Completed

1 succeeded

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

Vérifier

1. Connectez-vous à l'aide de SSH, Telnet ou console au FTD précédemment déployé.
2. Exécutez les commandes show route et show running-config route
3. Vérifiez que la table de routage FTD comporte désormais la route statique déployée avec l'indicateur S et qu'elle apparaît également dans la configuration en cours.

```
> 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
> █
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.