

Configureer statische routes met Firewall Management Center (FMC)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft het proces voor het implementeren van statische routes in Secure Firewall Threat Defense via Firewall Management Center.

Voorwaarden

Vereisten

Cisco raadt aan kennis van deze onderwerpen te hebben:

- Firewall Management Center (FMC)
- Secure Firewall Threat Defence (FTD)
- Grondbeginselen van netwerkroutes.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

- Firewall Management Center voor VMWare v7.3
- Cisco Secure Firewall Threat Defence voor VMWare v7.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Deze procedure wordt op toestellen ondersteund:

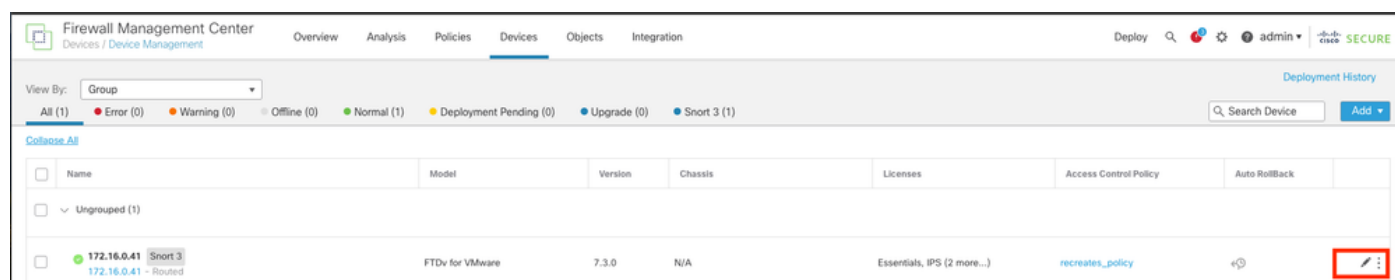
- Firewall Management Center op locatie
- Firewall Management Center voor VMWare
- cdFMC
- Cisco Secure Firewall 1000 Series-apparaten
- Cisco Secure Firewall 2100 Series-apparaten
- Cisco Secure Firewall 3100 Series-apparaten
- Cisco Secure Firewall 4100 Series-apparaten
- Cisco Secure Firewall 4200 Series-apparaten
- Cisco Secure Firewall 9300-apparaat
- Cisco Secure Firewall Threat Defense voor VMWare

Configureren

Configuraties

Stap 1. Ga in de FMC GUI naar Apparaten > Apparaatbeheer.

Stap 2. Identificeer het FTD dat moet worden geconfigureerd en klik op het potloodpictogram om de huidige configuratie van het FTD te bewerken.



Stap 2. Klik over het tabblad Routing.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

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 >| C

Stap 3. Selecteer in het linkermenu de optie Statische route

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

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	
▼ IPv4 Routes							
▼ IPv6 Routes							

No data to display |< < Page 1 of 1 >| C

Stap 4. klik op de (+) Add route optie.

Stap 5. Voer onder de sectie Statische routeconfiguratie de gewenste informatie in de velden Type, Interface, Beschikbaar netwerk, Gateway en Metric (en indien nodig ook Tunneling en Routertracing).

Type: Klik op IPv4 of IPv6 afhankelijk van het type statische route dat u toevoegt.

Interface: Kies de interface waarop deze statische route van toepassing is.

Beschikbaar netwerk: kies het doelnetwerk in de lijst Beschikbaar netwerk. Om een standaardroute te bepalen, creëer een voorwerp met het adres 0.0.0.0/0 en selecteer het hier.

Gateway: Voer in het veld Gateway of IPv6 Gateway de gatewayrouter in of kies die de volgende hop voor deze route is. U kunt een IP-adres of een Netwerken/Hosts-object opgeven.

Metric: Voer in het metriek veld het aantal hop in naar het doelnetwerk. Geldige waarden variëren van 1 tot 255; de standaardwaarde is 1.

Tunneling: (optioneel) Klik voor een standaardroute op het selectievakje Tunneling om een afzonderlijke standaardroute voor VPN-verkeer te definiëren

Route-tracking: (alleen statische IPv4-route) Om de beschikbaarheid van de route te bewaken, voert u de naam in of kiest u de naam van een SLA-monitorobject (Service Level Agreement) dat het monitoringbeleid definieert, in het veld Route Tracking.

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


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 C +

Q 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

Selected Network

10.203.18.0

Gateway*
10.203.18.100 +

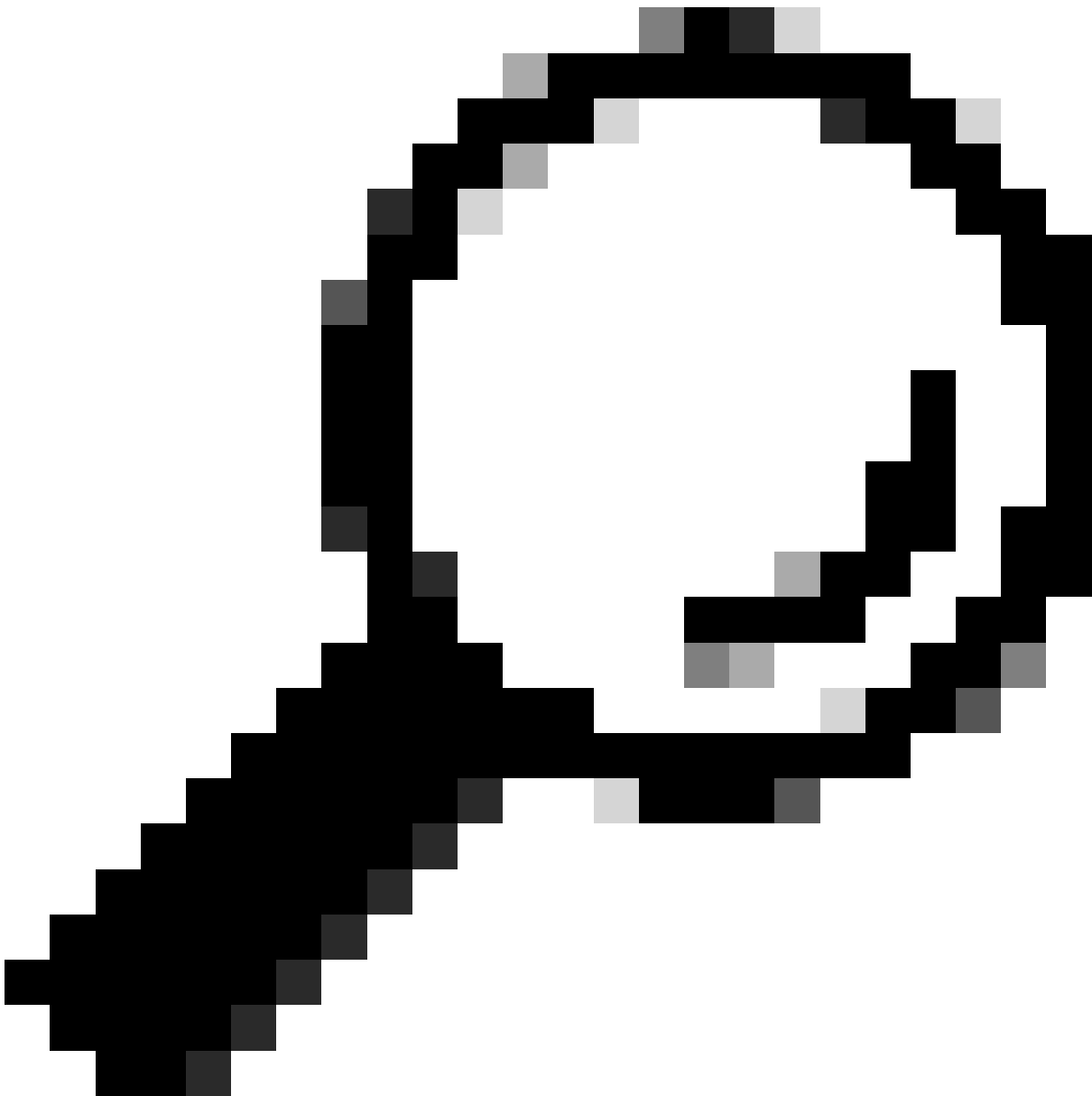
Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

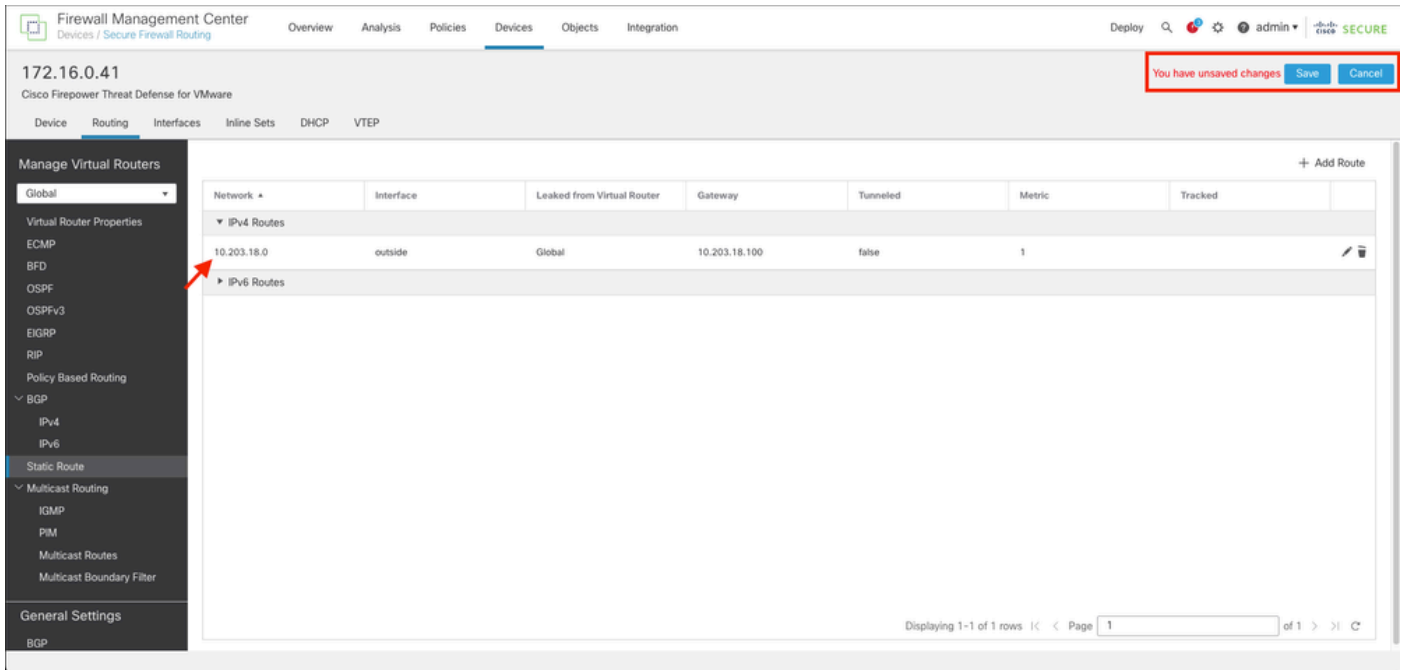
ata to display |< < Page 1 of 1 > > | C



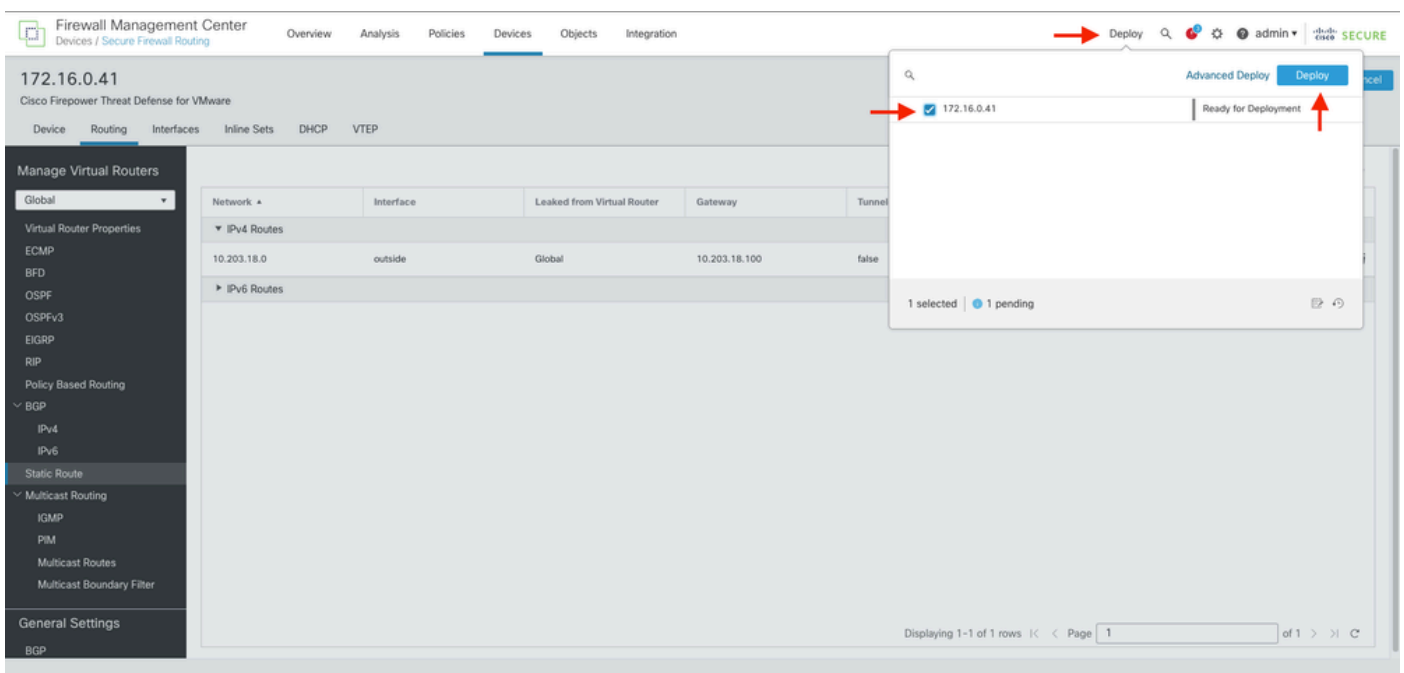
Tip: In de velden Beschikbare netwerken, gateway- en routeverkeer moeten netwerkobjecten worden gebruikt. Als de objecten nog niet zijn gemaakt, klikt u rechts van elk veld op het (+) teken om een nieuw netwerkobject te maken.

Stap 6. Klik op OK

Stap 7. Sla de configuratie op en bevestig de nieuwe statische route die zoals verwacht wordt weergegeven.



Stap 7. Navigeer om het geselecteerde FTD in Stap 2 te implementeren en aanvinkvakje aan te vinken, en klik vervolgens op het blauwe implementatiepictogram om de nieuwe configuratie te implementeren.



Stap 8. Valideren dat de implementatie wordt weergegeven als voltooid.

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	Tunnel
▼ IPv4 Routes				
10.203.18.0	outside	Global	10.203.18.100	false
▼ IPv6 Routes				

Deploy 172.16.0.41 Completed

Advanced Deploy Deploy All

1 succeeded

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

Verifiëren

1. Log met SSH, Telnet of console in op de eerder gebruikte FTD.
2. De opdracht Uitvoeren toont route en toont in werking stelt -in werking stellen-configuratie route
3. Valideren van de FTD Routing Table heeft nu de ontplooide statische route met de S vlag en die het ook toont in de lopende configuratie.

```
> 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
> █
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.