Konfigurieren statischer Routen mit Firewall Management Center (FMC)

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Konfigurieren

- Konfigurationen

Überprüfung

Einleitung

Dieses Dokument beschreibt den Prozess, wie statische Routen in Secure Firewall Threat Defense über das Firewall Management Center bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, in den folgenden Bereichen über Kenntnisse zu verfügen:

- Firewall Management Center (FMC)
- Sicherer Firewall-Schutz vor Bedrohungen (FTD)
- Netzwerkrouten bilden die Grundlage.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Verfahren wird auf folgenden Appliances unterstützt:

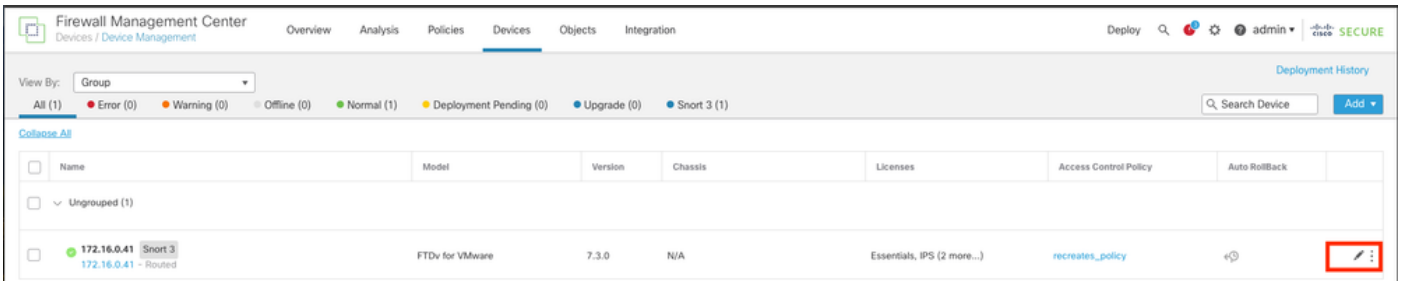
- Firewall Management Center am Standort
- Firewall Management Center für VMware
- CdFMC
- Cisco Secure Firewall Appliances der Serie 1000
- Cisco Secure Firewall Appliances der Serie 2100
- Cisco Secure Firewall Appliances der Serie 3100
- Cisco Secure Firewall Appliances der Serie 4100
- Cisco Secure Firewall Appliances der Serie 4200
- Cisco Secure Firewall der Serie 9300
- Cisco Secure Firewall Threat Defense für VMware

Konfigurieren

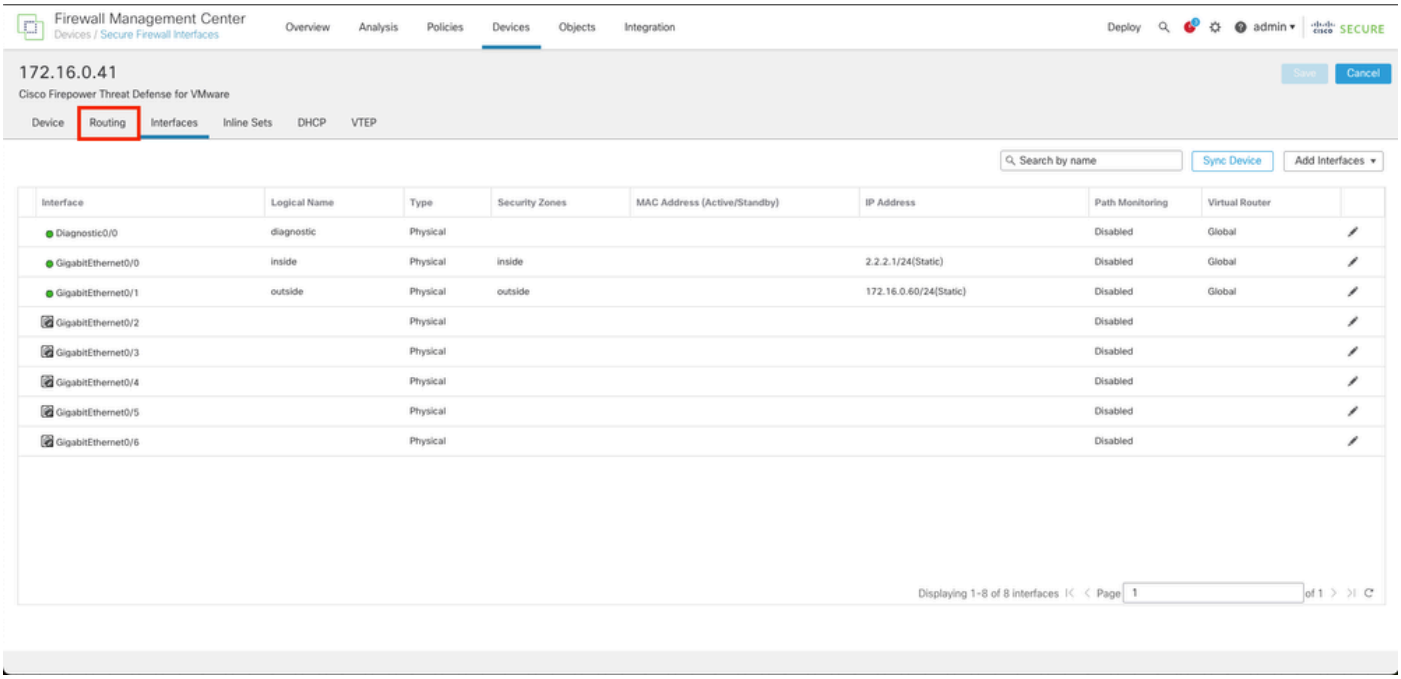
Konfigurationen

Schritt 1: Navigieren Sie in der FMC-GUI zu Geräte > Geräteverwaltung.

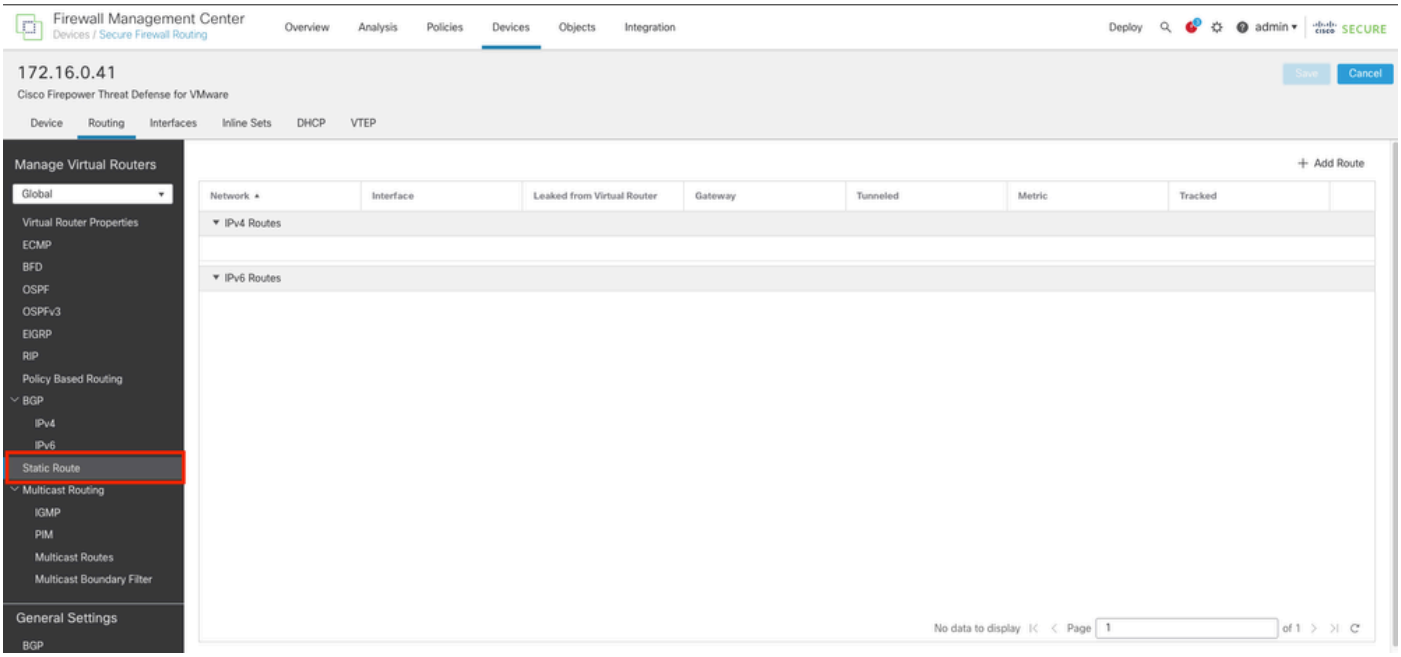
Schritt 2: Identifizieren Sie das FTD, das konfiguriert werden soll, und klicken Sie auf das Bleistiftsymbol, um die aktuelle Konfiguration des FTD zu bearbeiten.



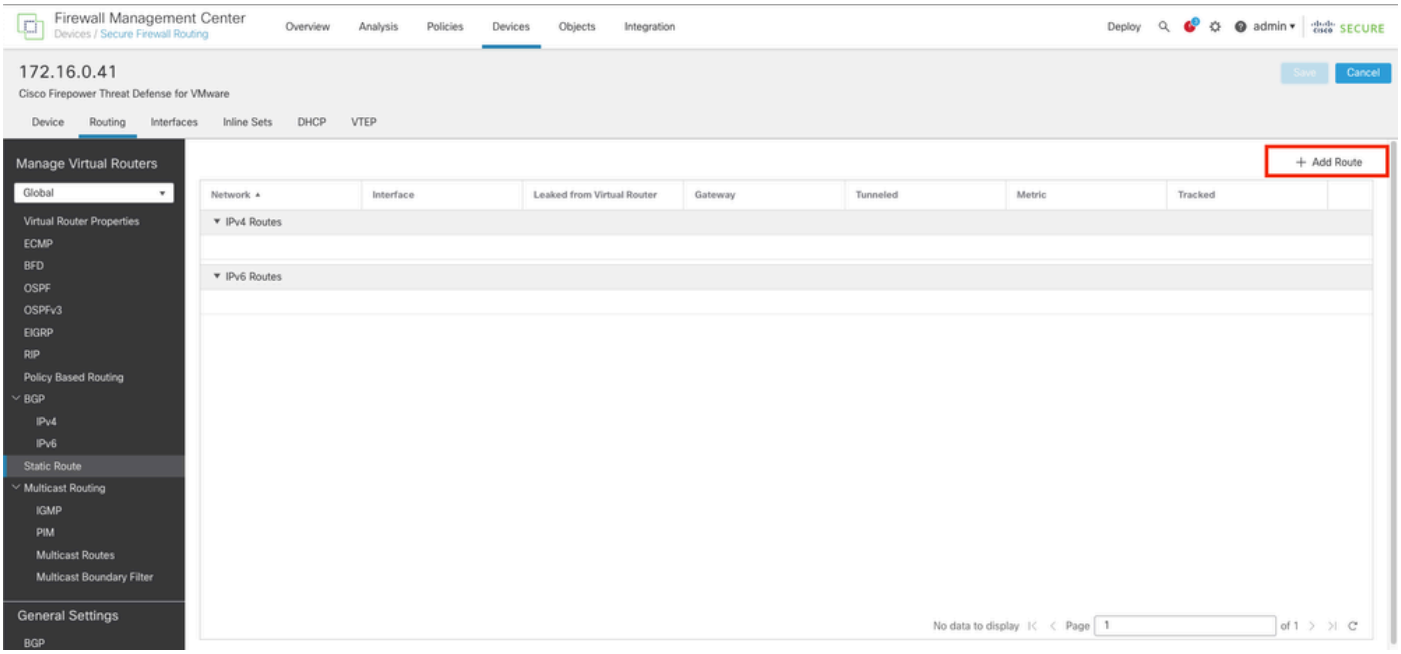
Schritt 2: Klicken Sie auf die Registerkarte Routing.



Schritt 3: Wählen Sie im Menü links die Option Static Route (Statische Route).

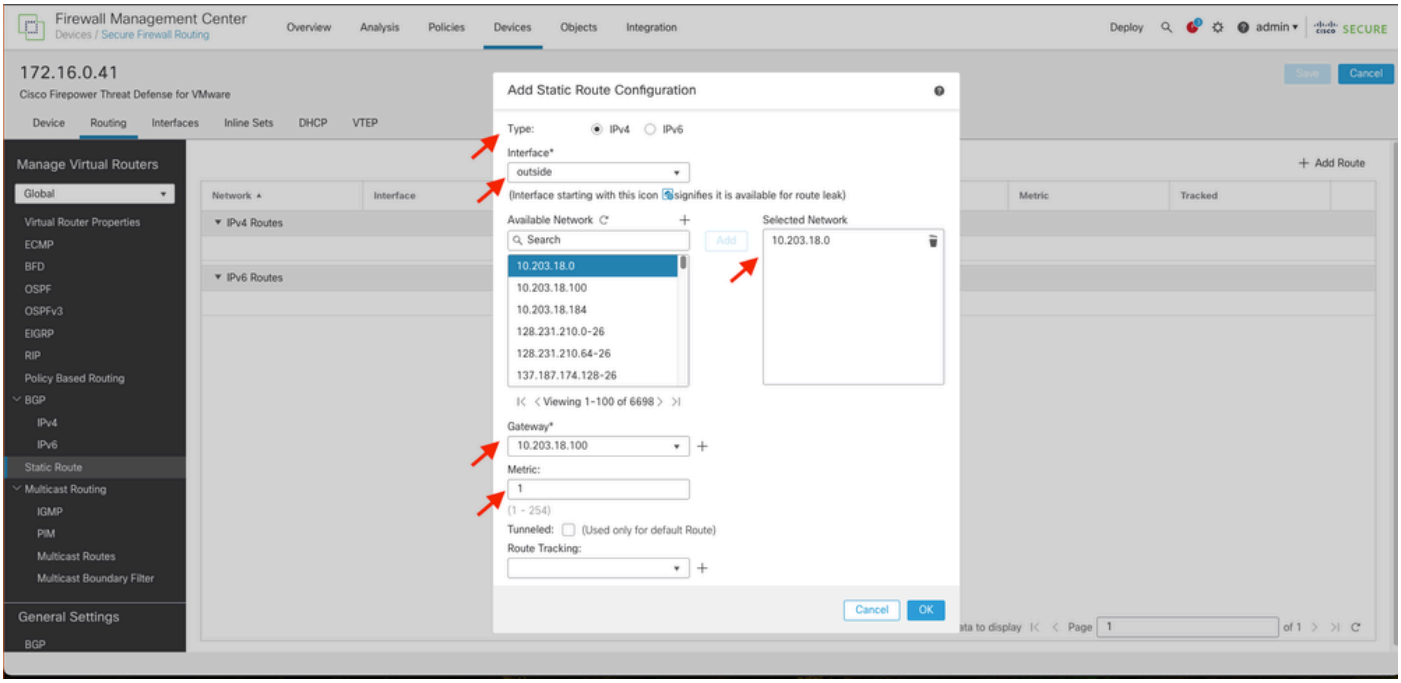


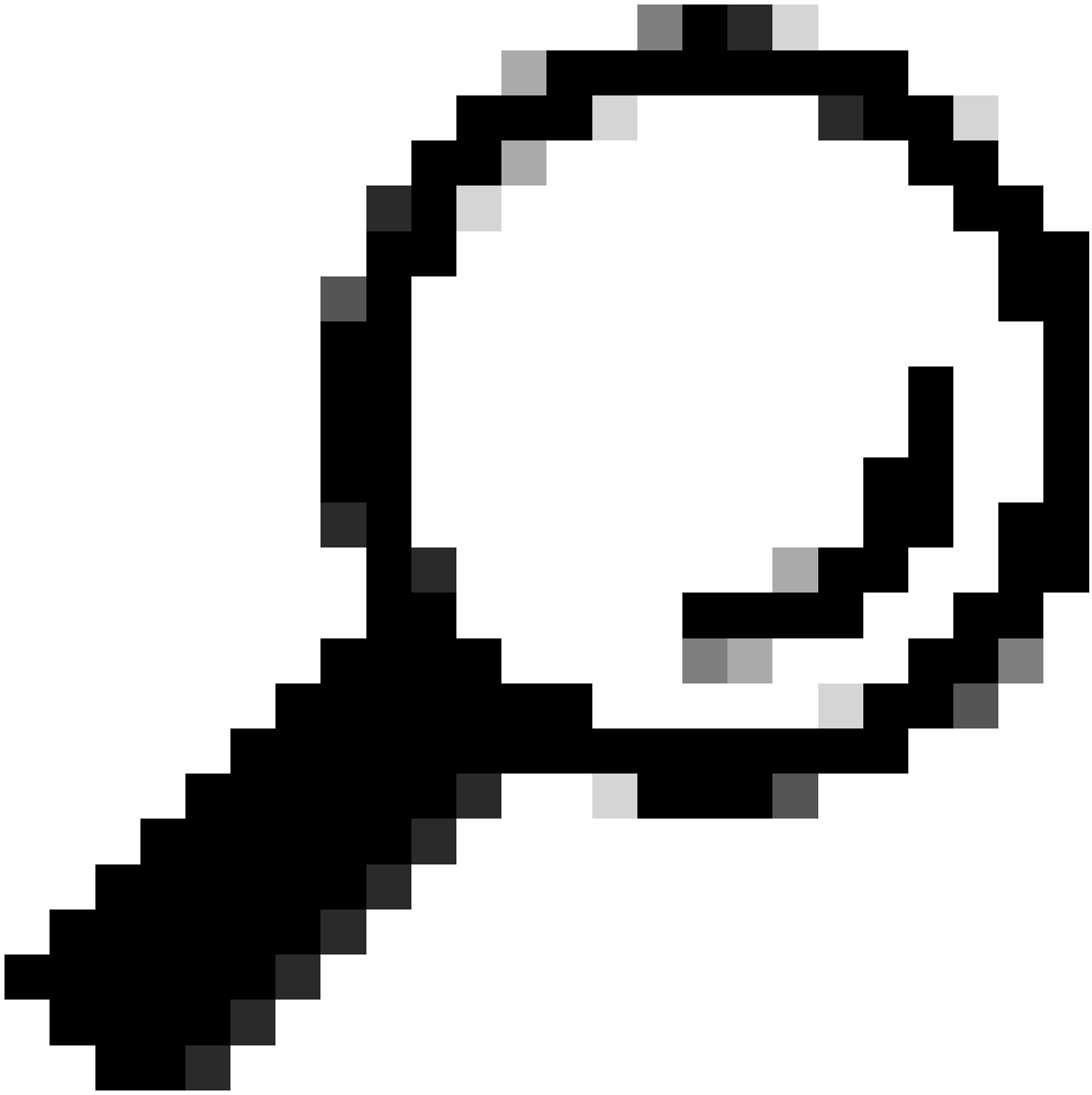
Schritt 4: Klicken Sie auf die Option (+) Route hinzufügen.



Schritt 5: Geben Sie im Abschnitt "Static Route Configuration" (Statische Routenkonfiguration) die erforderlichen Informationen in die Felder "Type" (Schnittstelle), "Available Network" (Verfügbares Netzwerk), "Gateway" (Gateway) und "Metric" (sowie bei Bedarf "Tunneled" und "Route Tracking" (Routenverfolgung) ein.

Typ: Klicken Sie je nach Art der statischen Route, die Sie hinzufügen, auf IPv4 oder IPv6.
Schnittstelle: Wählen Sie die Schnittstelle aus, auf die diese statische Route angewendet wird.
Available Network (Verfügbares Netzwerk): Wählen Sie in der Liste Available Network (Verfügbares Netzwerk) das Zielnetzwerk aus. Um eine Standardroute zu definieren, erstellen Sie ein Objekt mit der Adresse 0.0.0.0/0 und wählen es hier aus.
Gateway: Geben Sie im Feld Gateway or IPv6 Gateway (Gateway oder IPv6-Gateway) den Gateway-Router ein, der den nächsten Hop für diese Route darstellt, oder wählen Sie diesen aus. Sie können eine IP-Adresse oder ein Netzwerk-/Hosts-Objekt angeben.
Metrisch: Geben Sie im Feld "Metrisch" die Anzahl der Hops zum Zielnetzwerk ein. Gültige Werte liegen zwischen 1 und 255; der Standardwert ist 1.
Getunnelt: (Optional) Klicken Sie bei einer Standardroute auf das Kontrollkästchen Getunnelt, um eine separate Standardroute für VPN-Datenverkehr zu definieren.
Routenverfolgung: (Nur statische IPv4-Route) Geben Sie zum Überwachen der Routenverfügbarkeit den Namen eines SLA-Objekts (Service Level Agreement), das die Überwachungsrichtlinie definiert, in das Feld "Routenverfolgung" ein, oder wählen Sie diesen aus.

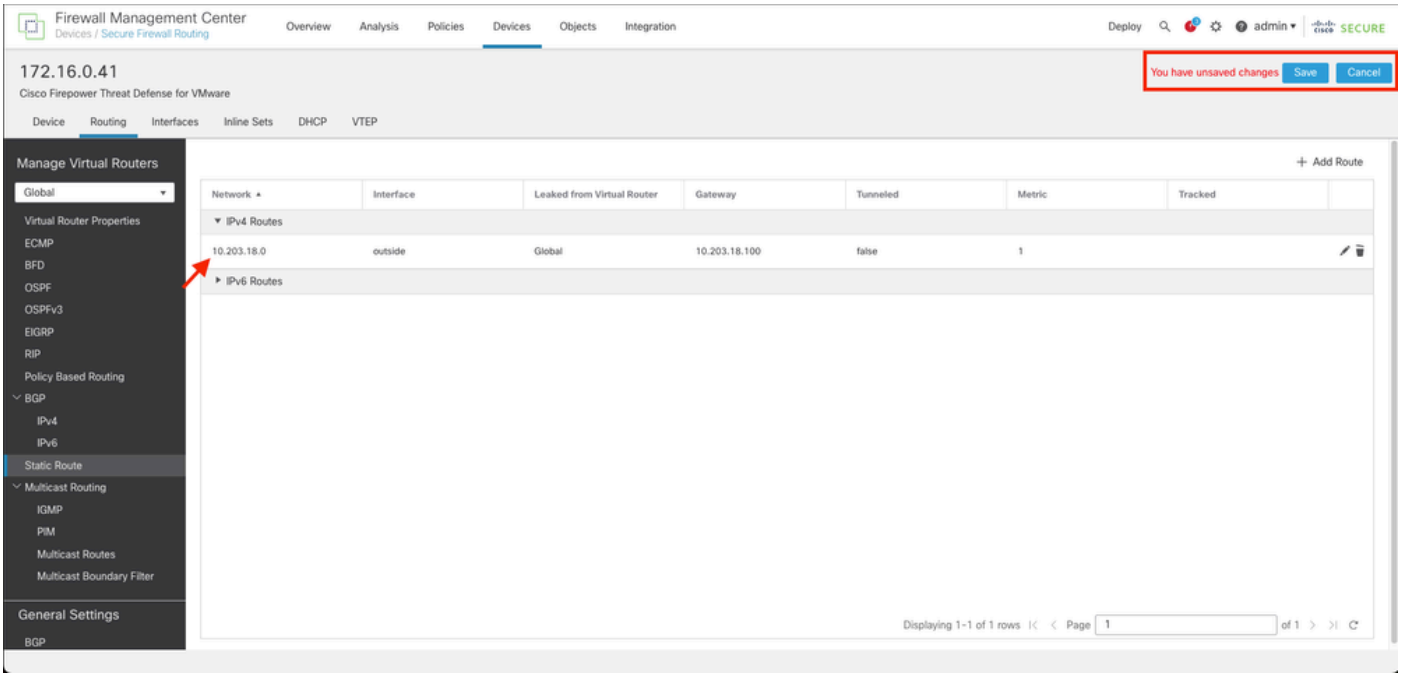

Firewall Management Center
Devices / Secure Firewall Routing
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
172.16.0.41
Cisco Firepower Threat Defense for VMware
Save
Cancel
Device
Routing
Interfaces
Inline Sets
DHCP
VTEP
Manage Virtual Routers
Global
Virtual Router Properties
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
Metric
Tracked
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
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
Page
1
of 1



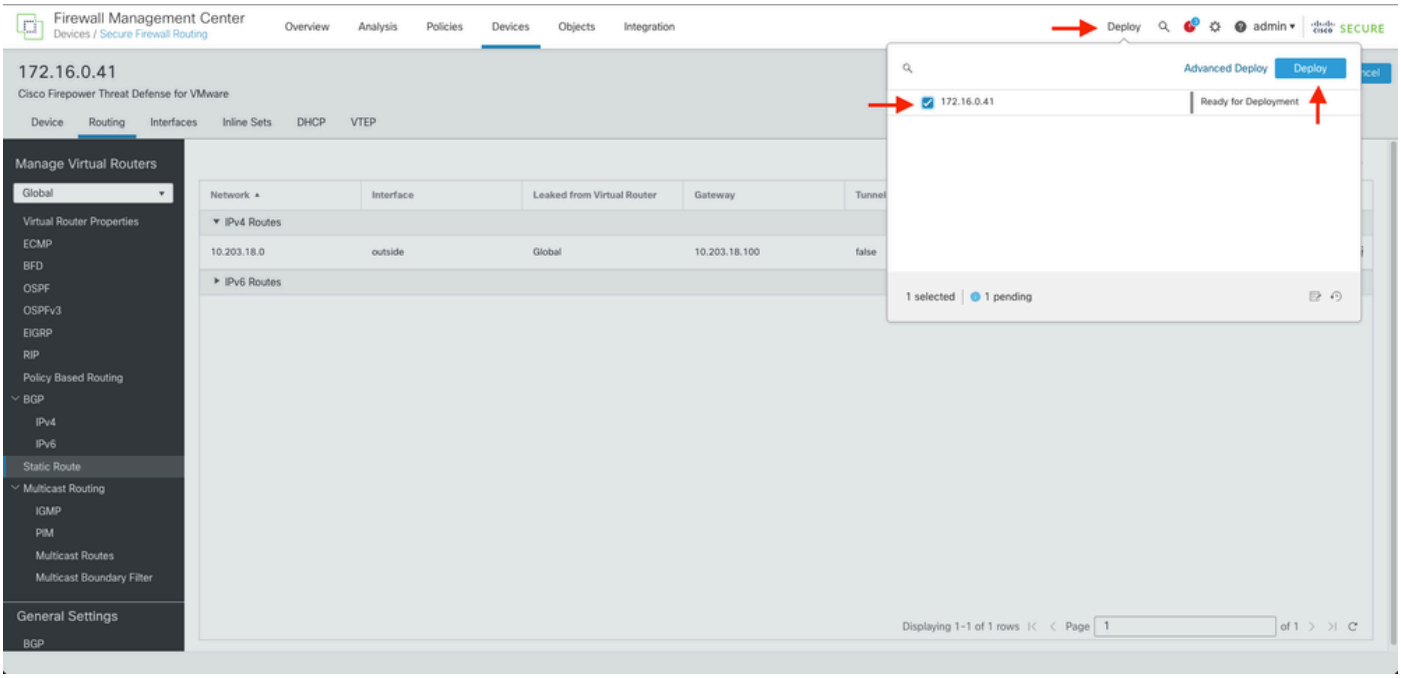
Tipp: Die Felder Available Network , Gateway und Route traffic erfordern die Verwendung von Netzwerkobjekten. Falls die Objekte noch nicht erstellt wurden, klicken Sie bitte auf das (+) Zeichen rechts von jedem Feld, um ein neues Netzwerkobjekt zu erstellen.

Schritt 6: Klicken Sie auf OK

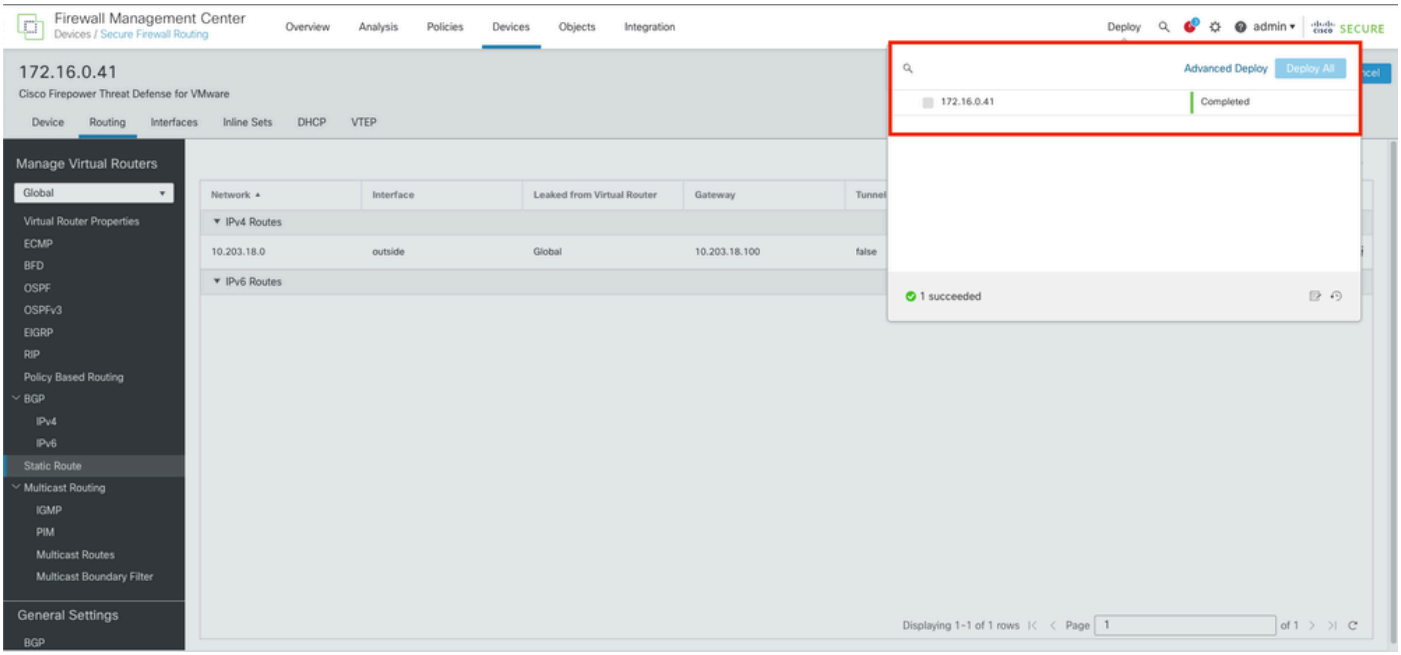
Schritt 7. Speichern Sie die Konfiguration, und validieren Sie die neue statische Route, die wie erwartet angezeigt wird.



Schritt 7: Navigieren Sie zu Deploy (Bereitstellen), und aktivieren Sie das in Schritt 2 ausgewählte FTD, und klicken Sie dann auf das blaue Symbol "Deployment" (Bereitstellung), um die neue Konfiguration bereitzustellen.



Schritt 8: Überprüfen, ob die Bereitstellung als abgeschlossen angezeigt wird



Überprüfung

1. Melden Sie sich mithilfe von SSH, Telnet oder der Konsole bei der zuvor bereitgestellten FTD an.

2. Führen Sie den Befehl show route und show running-config route aus

3. Überprüfen Sie, ob die FTD-Routing-Tabelle nun die bereitgestellte statische Route mit dem S-Flag enthält und in der aktuellen Konfiguration angezeigt wird.

```
> 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
>
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.