Configurar rotas estáticas com o Firewall Management Center (FMC)

Contents

Introdução

Este documento descreve o processo de como implantar rotas estáticas no Secure Firewall Threat Defense através do Firewall Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento destes tópicos:

- Centro de gerenciamento de firewall (FMC)
- Defesa contra ameaças (FTD) com firewall seguro
- A rede roteia os fundamentos.

Componentes Utilizados

As informações deste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este procedimento é compatível com dispositivos:

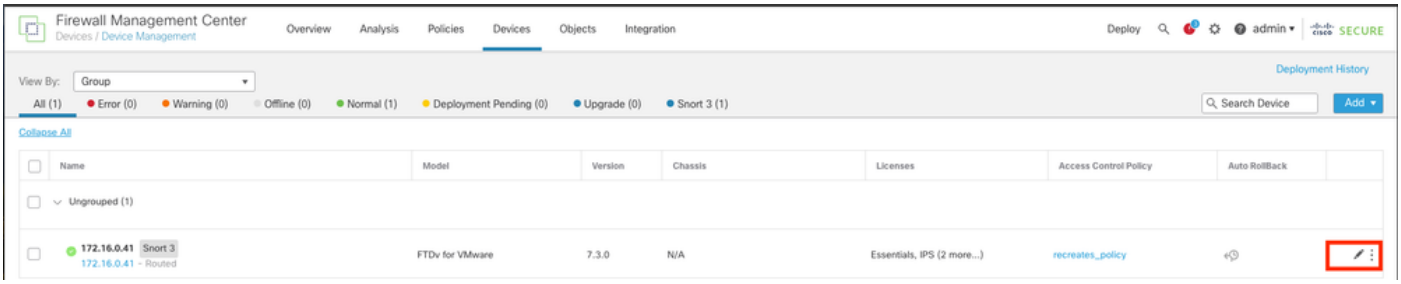
- Centro de gerenciamento de firewall local
- Centro de gerenciamento de firewall para VMWare
- cdFMC
- Dispositivos Cisco Secure Firewall 1000 Series
- Dispositivos Cisco Secure Firewall 2100 Series
- Dispositivos Cisco Secure Firewall 3100 Series
- Dispositivos Cisco Secure Firewall 4100 Series
- Dispositivos Cisco Secure Firewall 4200 Series
- Dispositivo Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense para VMWare

Configurar

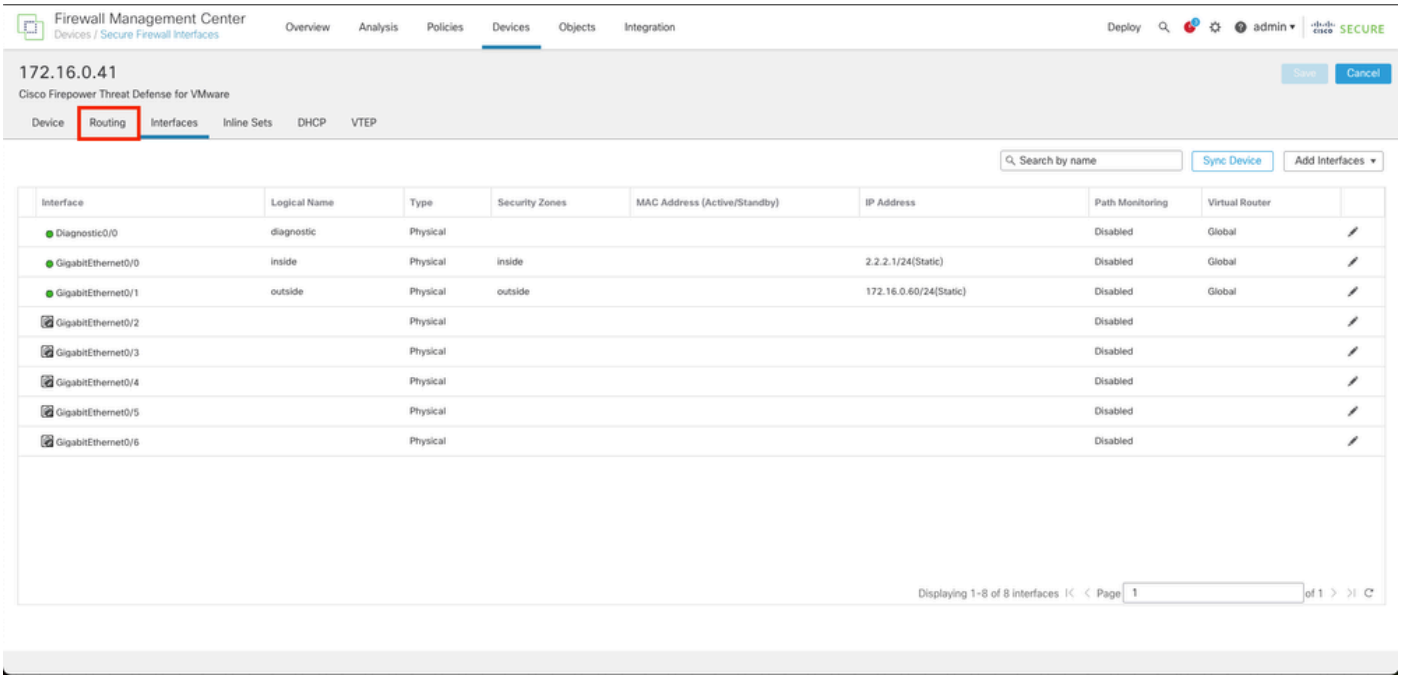
Configurações

Etapa 1. Na GUI do FMC , navegue até Devices > Device Management.

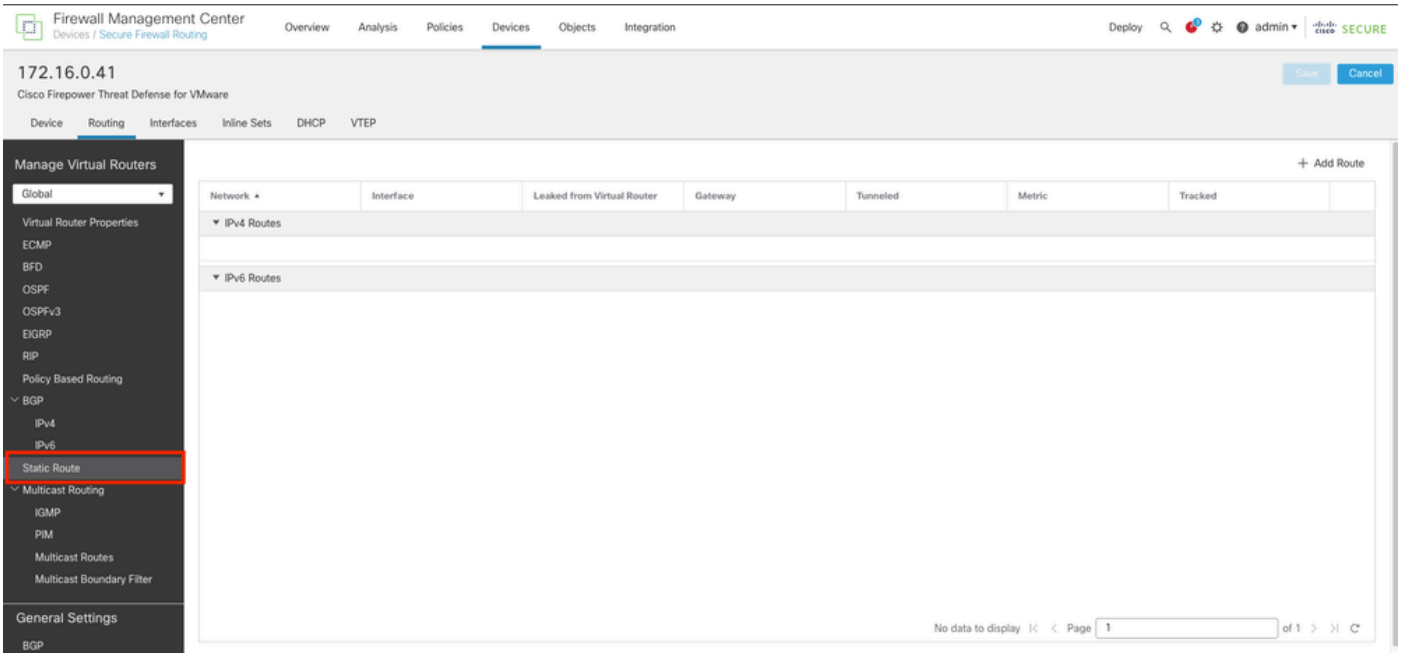
Etapa 2. Identifique o FTD que será configurado e clique no ícone do lápis para editar a configuração atual do FTD.



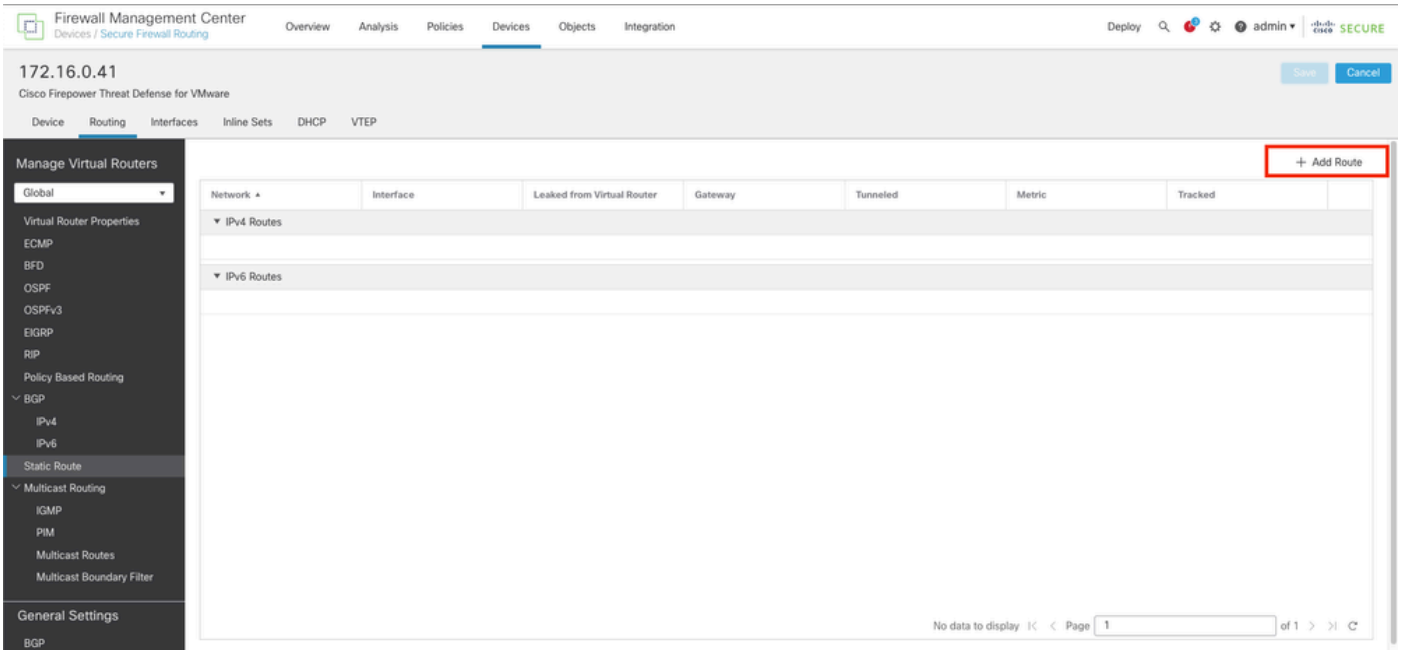
Etapa 2. Clique sobre a guia Roteamento.



Etapa 3. No menu esquerdo, selecione Static Route (Rota estática)

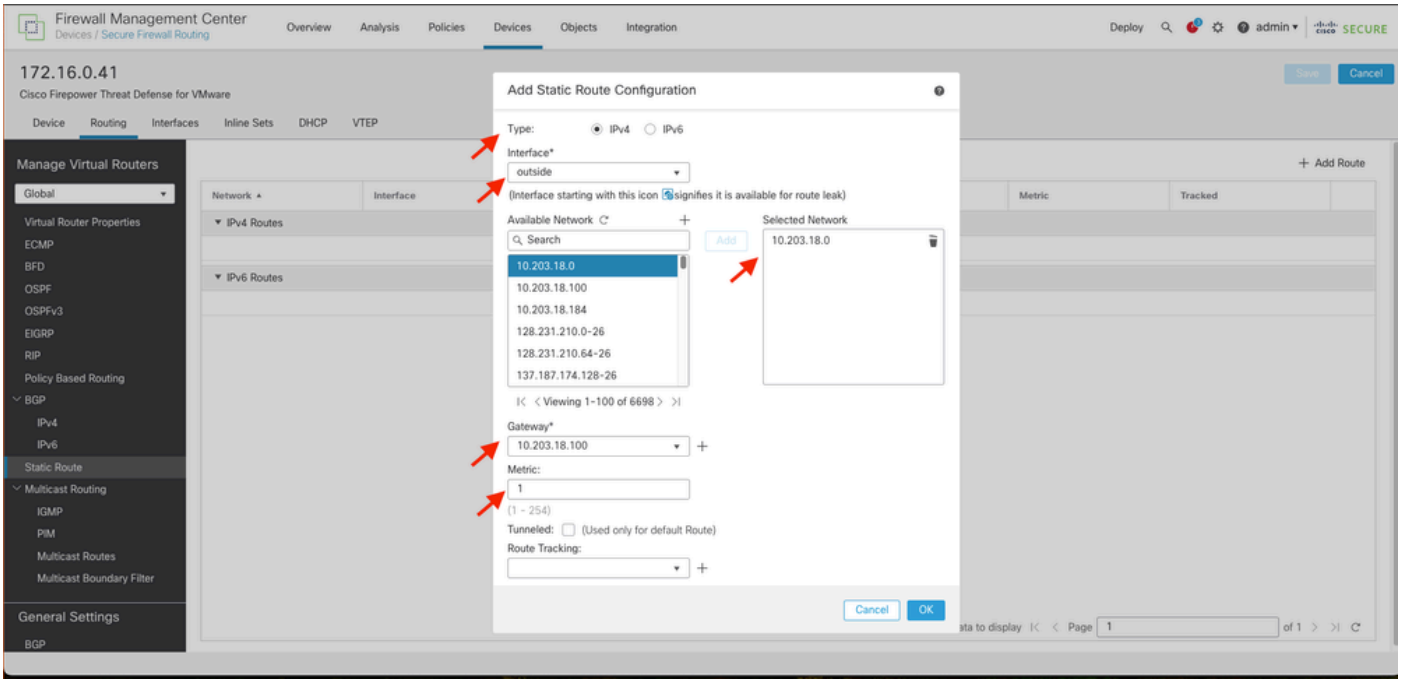


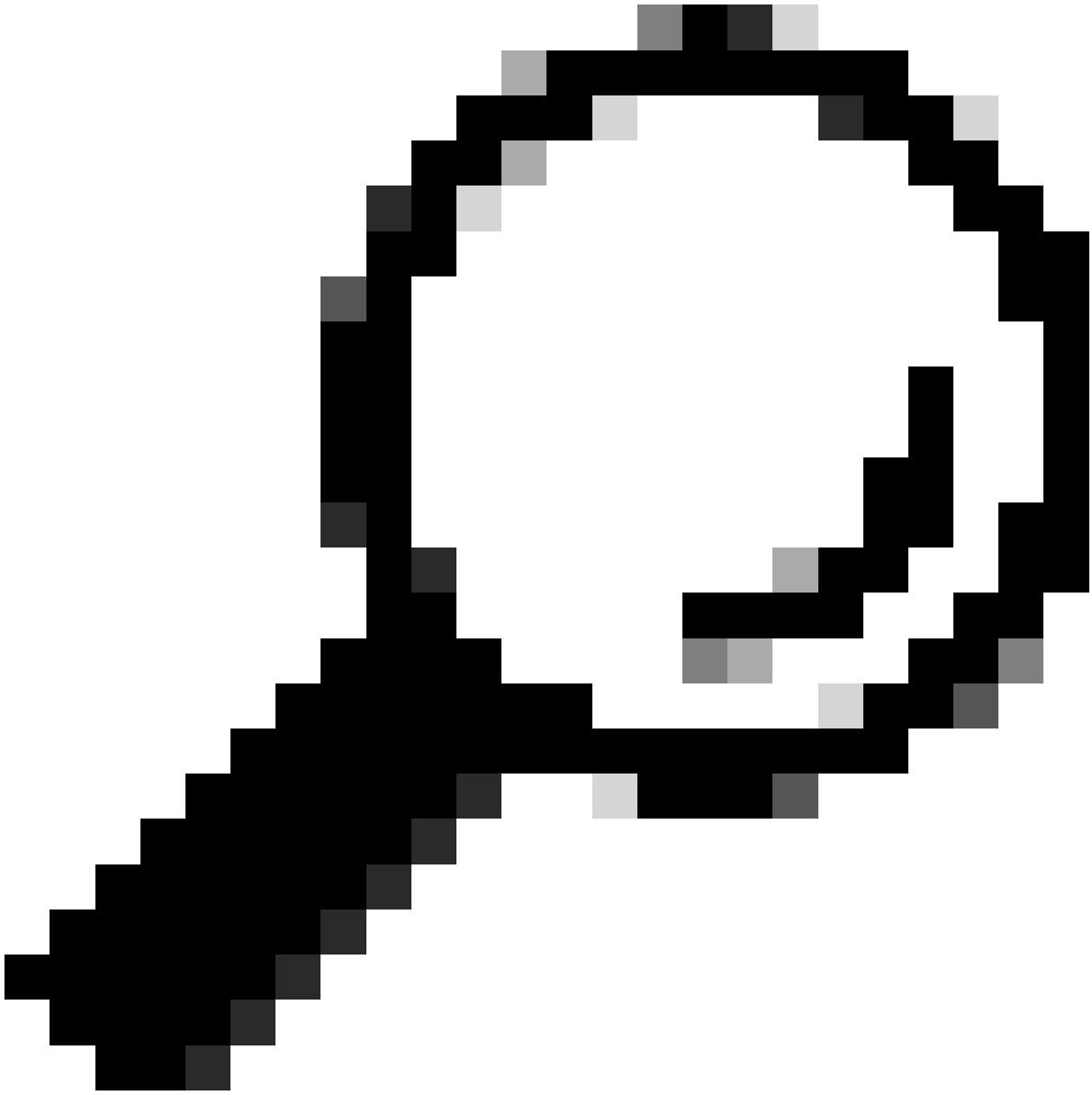
Etapa 4. clique na opção (+) Adicionar rota.



Etapa 5. Na seção Static Route Configuration, insira as informações necessárias nos campos Type, Interface, Available Network, Gateway e Metric (bem como Tunneled e Route tracking se necessário).

Tipo: Clique em IPv4ou IPv6, dependendo do tipo de rota estática que você está adicionando.
Interface: Escolha a interface à qual esta rota estática se aplica.
Available Network: na lista Available Network, escolha a rede de destino. Para definir uma rota padrão, crie um objeto com o endereço 0.0.0.0/0 e selecione-o aqui.
Gateway: no campo Gateway ou IPv6 Gateway, insira ou escolha o roteador do gateway que é o próximo salto para essa rota. Você pode fornecer um endereço IP ou um objeto Redes/Hosts.
Métrica: No campo Métrica, insira o número de saltos para a rede destino. Os valores válidos variam de 1 a 255; o valor padrão é 1.
Encapsulado: (Opcional) Para uma rota padrão, clique na caixa de seleção Encapsulado para definir uma rota padrão separada para o tráfego VPN
Rastreamento de rota: (somente rota estática IPv4) Para monitorar a disponibilidade da rota, insira ou escolha o nome de um objeto Monitor SLA (contrato de nível de serviço) que define a política de monitoramento, no campo Rastreamento de rota.

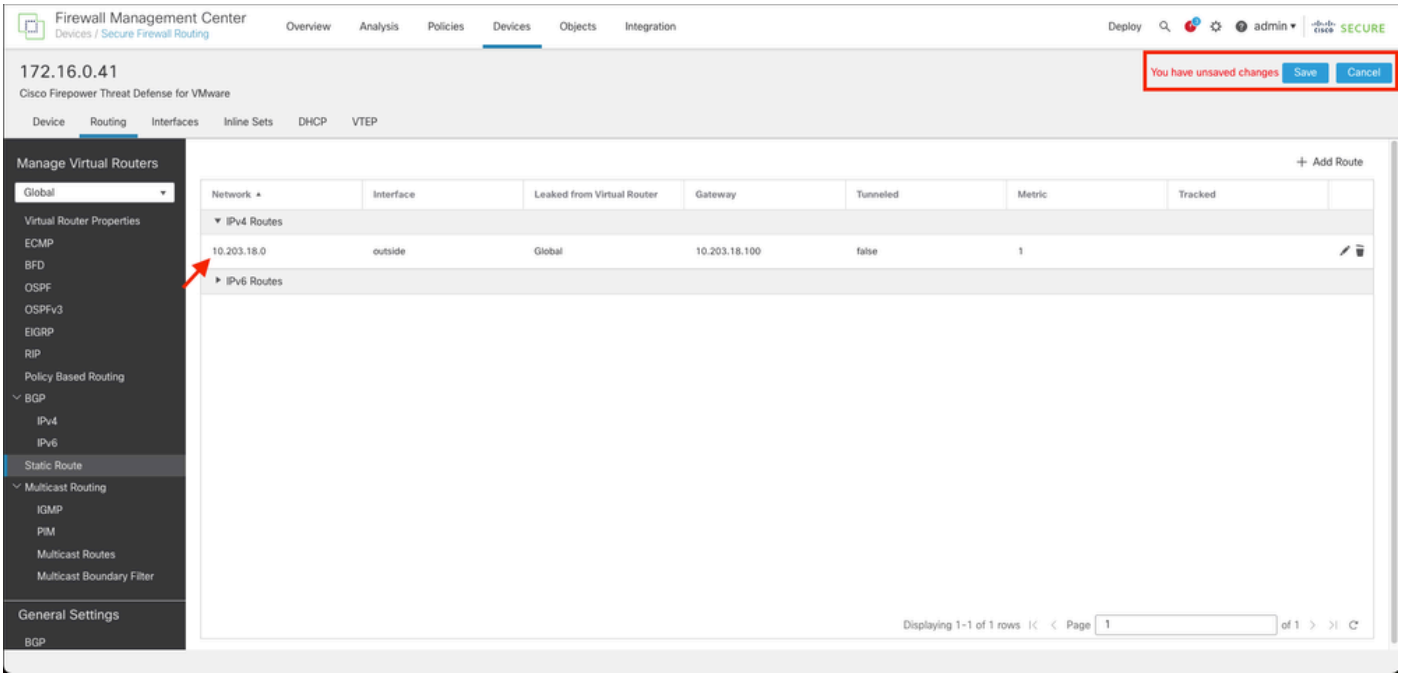

Firewall Management Center
Devices / Secure Firewall Routing
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
172.16.0.41
Cisco Firepower Threat Defense for VMware
Save
Cancel
Device
Routing
Interfaces
Inline Sets
DHCP
VTEP
Manage Virtual Routers
Global
Virtual Router Properties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



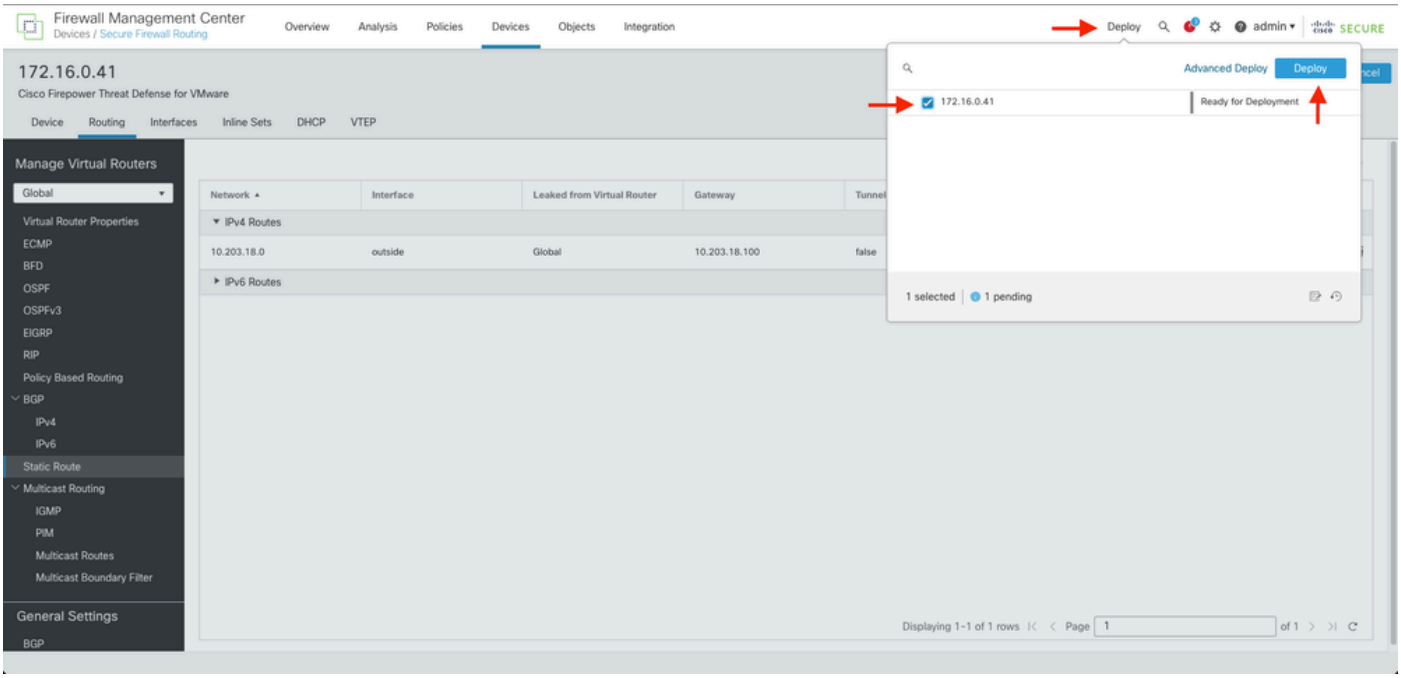
Dica: os campos Available Network , Gateway and Route traffic exigem o uso de objetos de rede. Se os objetos ainda não tiverem sido criados, clique sobre o sinal (+) à direita de cada campo para criar um novo objeto de rede.

Etapa 6. Clique em OK

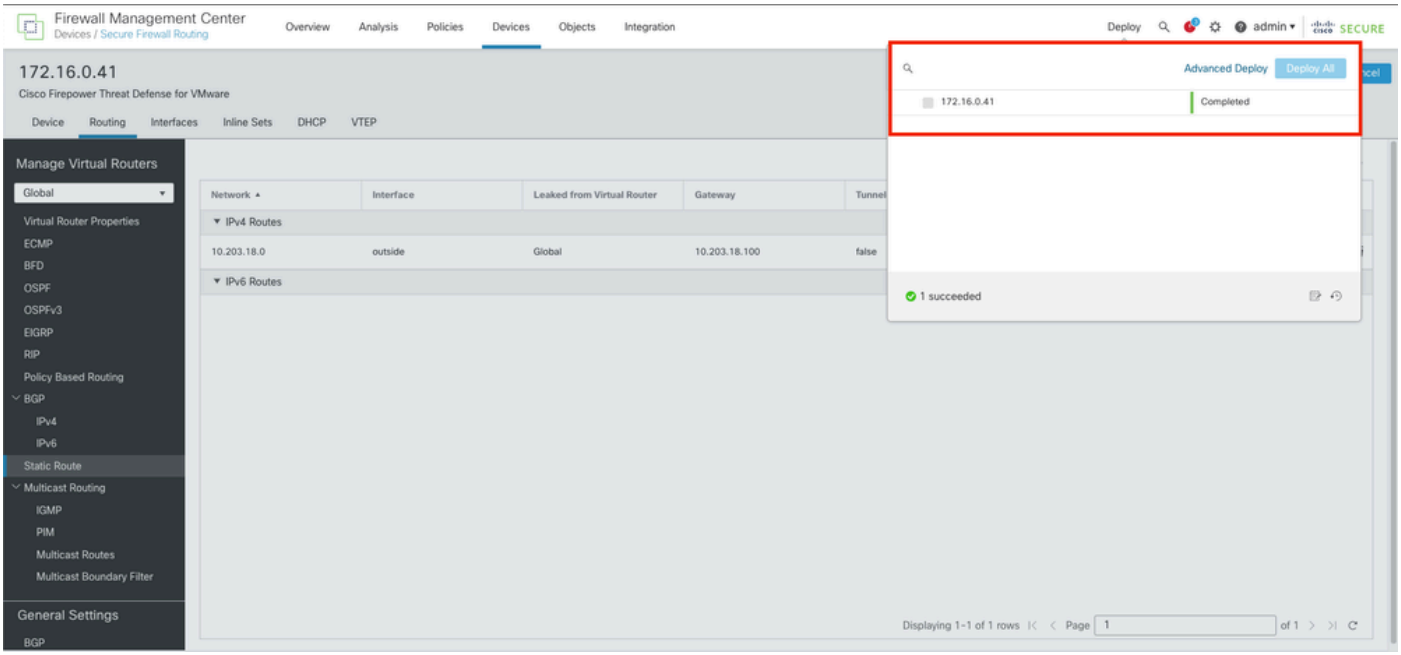
Passo 7. Salve a configuração e valide a nova rota estática que ela está mostrando como esperado.



Etapa 7. Navegue até a caixa de seleção Implantar e do FTD selecionado na Etapa 2 e clique sobre o ícone azul de implantação para implantar a nova configuração.



Etapa 8. Validar que a implantação está sendo mostrada como concluída.



Verificar

1. Registre usando SSH, Telnet ou console no FTD anteriormente implantado.

2. Execute o comando show route e show running-config route

3. Verifique se a tabela de roteamento FTD possui agora a rota estática implantada com o sinalizador S e se ela também está sendo exibida na configuração de execução.

```
> 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
>
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.