

使用防火墙管理中心(FMC)配置静态路由

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[配置](#)

[验证](#)

简介

本文档介绍如何通过防火墙管理中心在安全防火墙威胁防御中部署静态路由的过程。

先决条件

要求

思科建议了解以下主题：

- 防火墙管理中心(FMC)
- 安全防火墙威胁防御(FTD)
- 网络路由基础。

使用的组件

本文档的信息基于以下软件和硬件版本：

- VMWare v7.3防火墙管理中心
- 适用于VMWare v7.3的思科安全防火墙威胁防御

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

以下设备支持此过程：

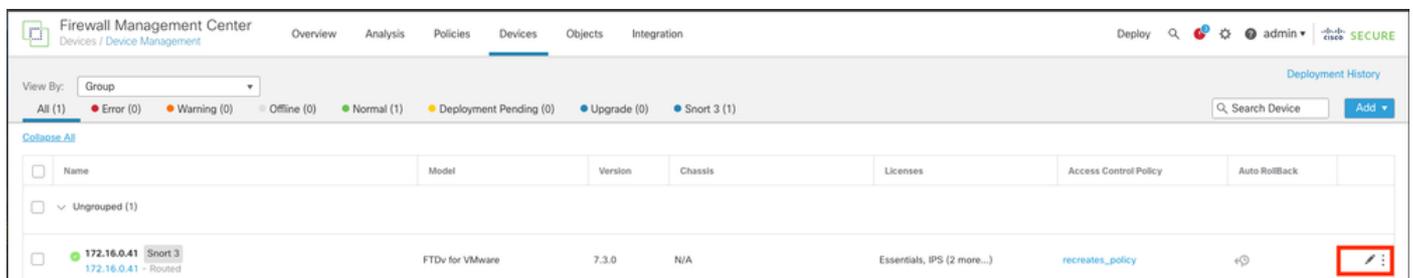
- 内部防火墙管理中心
- 适用于VMWare的防火墙管理中心
- cdFMC
- 思科安全防火墙1000系列设备
- 思科安全防火墙2100系列设备
- 思科安全防火墙3100系列设备
- 思科安全防火墙4100系列设备
- 思科安全防火墙4200系列设备
- 思科安全防火墙9300设备
- 适用于VMWare的思科安全防火墙威胁防御

配置

配置

步骤1:在FMC GUI中，导航到设备>设备管理。

第二步：确定要配置的FTD，然后点击铅笔图标以编辑FTD的当前配置。



第二步：点击路由选项卡。

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

第三步：在左侧菜单中选择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

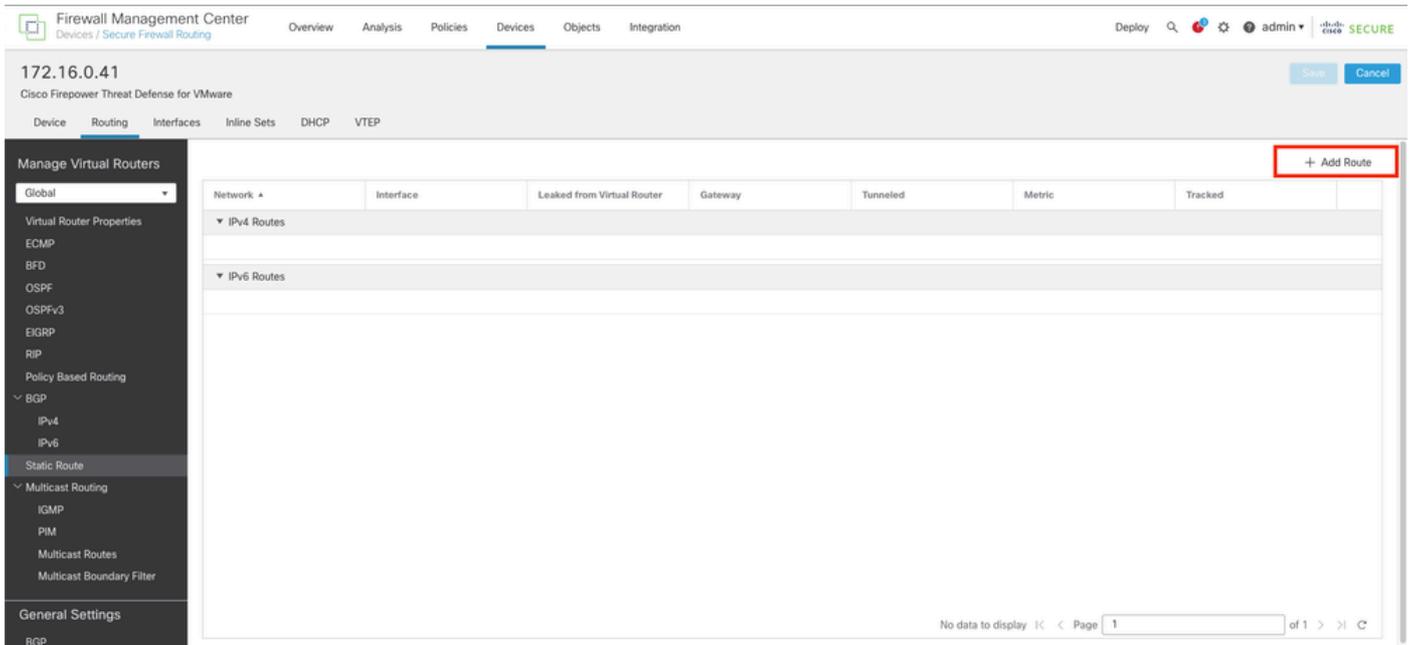
- Virtual Router Properties
- ECMP
- BFD
- OSPF
- OSPFV3
- EIGRP
- RIP
- Policy Based Routing
- BGP
 - IPv4
 - IPv6
 - Static Route**
- Multicast Routing
 - IGMP
 - PIM
 - Multicast Routes
 - Multicast Boundary Filter
- General Settings
- BGP

+ Add Route

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

No data to display Page 1 of 1

步骤4. 点击(+) Add route选项。



第五步：在Static Route Configuration部分下，在Type、Interface、Available Network、Gateway和Metric字段中输入所需的信息(以及Tunneled和Route tracking，如需要)。

类型：根据您添加的静态路由类型，单击IPv4或IPv6。

Interface：选择此静态路由所应用的接口。

可用网络(Available Network)：在可用网络(Available Network)列表中，选择目标网络。要定义默认路由，请创建一个地址为0.0.0.0/0的对象，然后在此处将其选中。

网关：在网关或IPv6网关字段中，输入或选择作为此路由的下一跳的网关路由器。可以提供IP地址或网络/主机对象。

度量：在度量字段中，输入到目标网络的跳数。有效值范围为1到255；默认值为1。

隧道化：(可选)对于默认路由，点击Tunneled复选框以为VPN流量定义单独的默认路由

路由跟踪：(仅限IPv4静态路由)要监控路由可用性，请在路由跟踪字段中输入或选择定义监控策略的SLA(服务级别协议)监控对象名称。

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

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+ + Selected Network

Q Search + Add

- 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

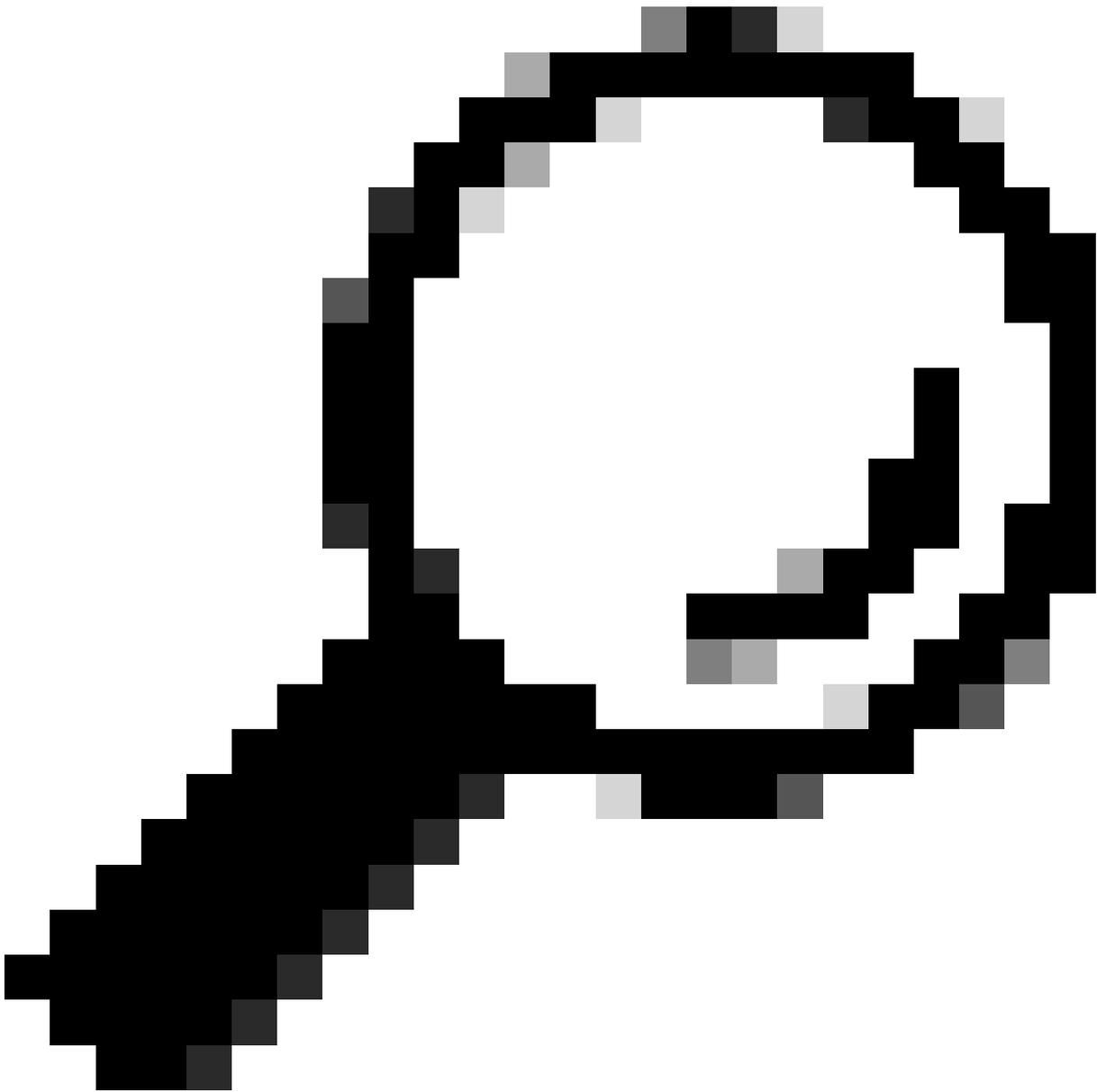
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

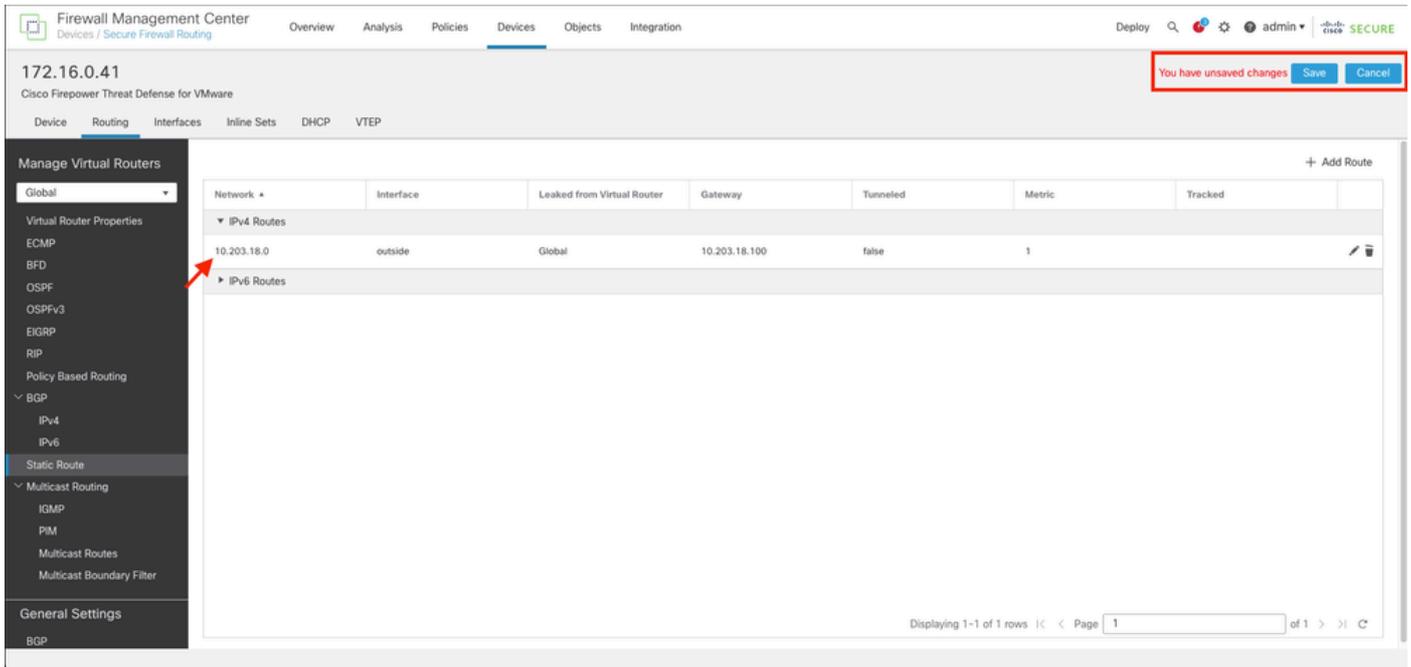
data to display | < < Page 1 of 1 > > | C



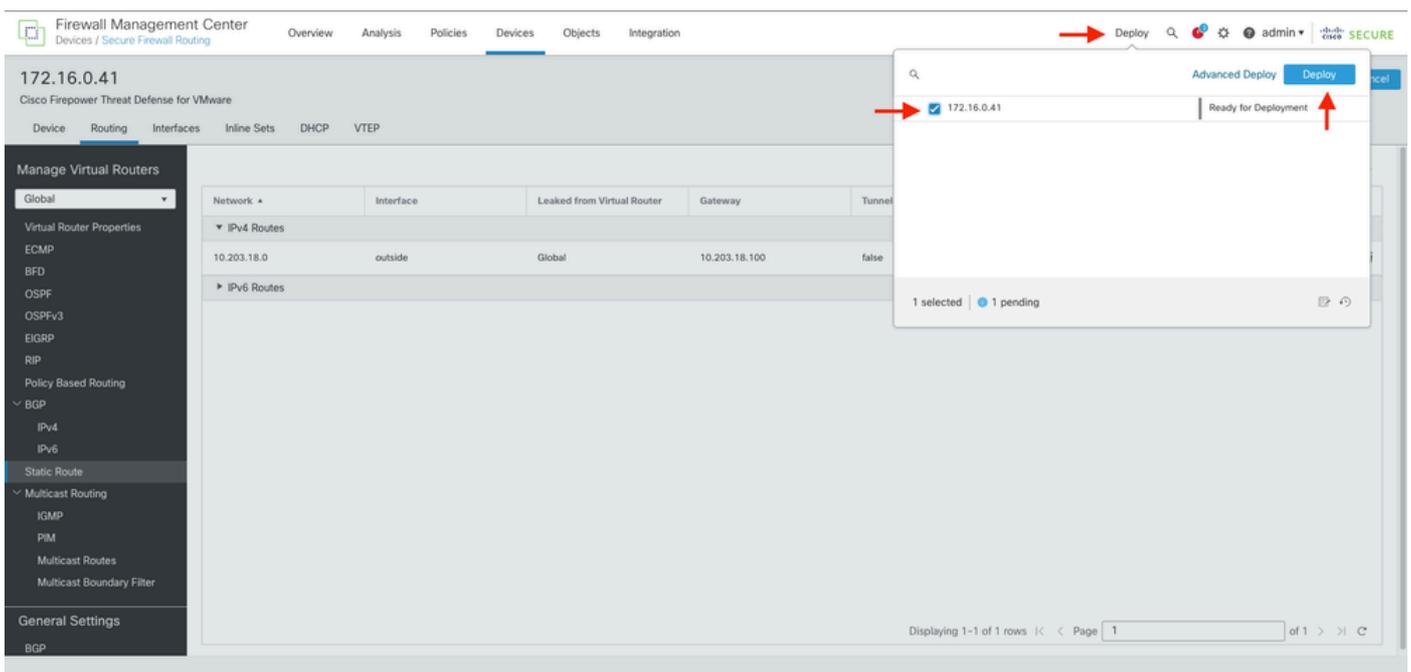
提示：可用的网络(Available Network)、网关(Gateway)和路由流量(Route traffic)字段需要使用网络对象，如果对象尚未创建，请点击每个字段右侧的(+)符号以创建新的网络对象。

第六步：点击确定

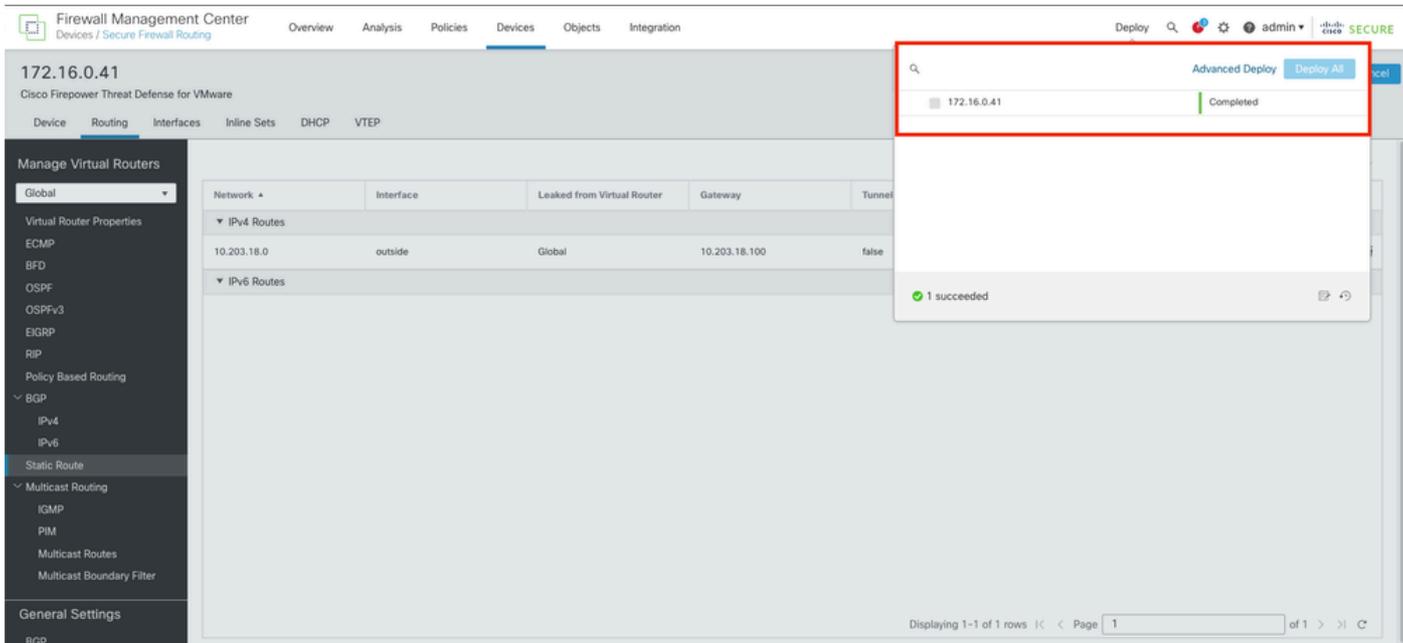
步骤 7.保存配置并验证它显示的新静态路由是否与预期一致。



第7步：导航到部署并选中第2步中选定的FTD的复选框，然后点击蓝色部署图标以部署新配置。



第8步：验证部署是否显示为已完成。



验证

1. 使用SSH、Telnet或控制台记录以前部署的FTD。
2. 运行命令show route和show running-config route
3. 验证FTD路由表是否已部署带有S标志的静态路由，以及该路由是否还显示在运行配置中。

```
> 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
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。