

ファイアウォール管理センター(FMC)を使用したスタティックルートの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[コンフィギュレーション](#)

[確認](#)

はじめに

このドキュメントでは、Firewall Management Center(FMC)を介したセキュアファイアウォール脅威防御にスタティックルートを展開する方法のプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ファイアウォール管理センター(FMC)
- セキュアファイアウォール脅威防御(FTD)
- ネットワークルーティングの基礎

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VMWare v7.3向けFirewall Management Center
- VMWare v7.3向けシスコセキュアファイアウォール脅威対策

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この手順はアプライアンスでサポートされています。

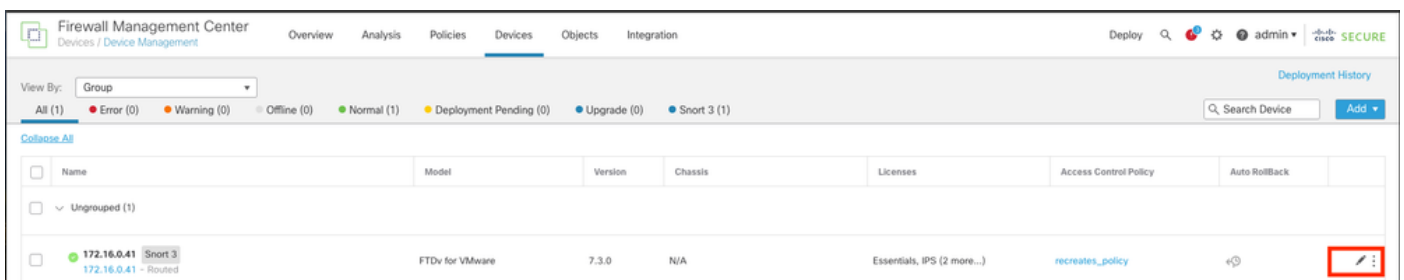
- ファイアウォール管理センターオンプレミス
- VMWare用ファイアウォール管理センター
- cdFMC (入手可能)
- Cisco Secure Firewall 1000シリーズアプライアンス
- Cisco Secure Firewall 2100シリーズアプライアンス
- Cisco Secure Firewall 3100シリーズアプライアンス
- Cisco Secure Firewall 4100シリーズアプライアンス
- Cisco Secure Firewall 4200シリーズアプライアンス
- Cisco Secure Firewall 9300アプライアンス
- VMWare向けシスコセキュアファイアウォール脅威対策

設定

コンフィギュレーション

ステップ 1 : FMCのGUI (グラフィカルユーザインターフェイス) で、Devices > Device Managmentの順に移動します。

ステップ 2 : 設定するFTDを識別し、鉛筆アイコンをクリックして、FTDの現在の設定を編集します。



ステップ 2 : Routingタブをクリックします。

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

ステップ 3 : 左側のメニューでStatic Routeを選択します。

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

ステップ4:(+) Add routeオプションをクリックします。

ステップ 5 : Static Route Configurationセクションで、Type、Interface、Available Network、Gateway、およびMetricフィールドに必要な情報(さらに必要に応じてTunneledおよびRoute trackingフィールドも入力)を入力します。

タイプ : 追加するスタティックルートのタイプに応じて、IPv4またはIPv6をクリックします。

Interface : このスタティックルートを適用するインターフェイスを選択します。

使用可能なネットワーク : [使用可能なネットワーク]リストで、宛先ネットワークを選択します。デフォルトルートを定義するには、アドレス0.0.0.0/0のオブジェクトを作成し、ここで選択します。

ゲートウェイ : ゲートウェイまたはIPv6ゲートウェイフィールドで、このルートのネクストホップであるゲートウェイルータを入力または選択します。IPアドレスまたはNetworks/Hostsオブジェクトを指定できます。

Metric:Metricfieldに、宛先ネットワークへのホップ数を入力します。有効な値の範囲は1 ~ 255です。デフォルト値は1です。

Tunneled: (オプション) デフォルトルートの場合は、Tunneledチェックボックスをクリックして、VPNトラフィック用に別のデフォルトルートを定義します

ルートトラッキング : (IPv4スタティックルートのみ) ルートの可用性を監視するには、監視ポリシーを定義するSLA(Service Level Agreement)監視オブジェクトの名前をルートトラッキングフィールドで入力または選択します。

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 +

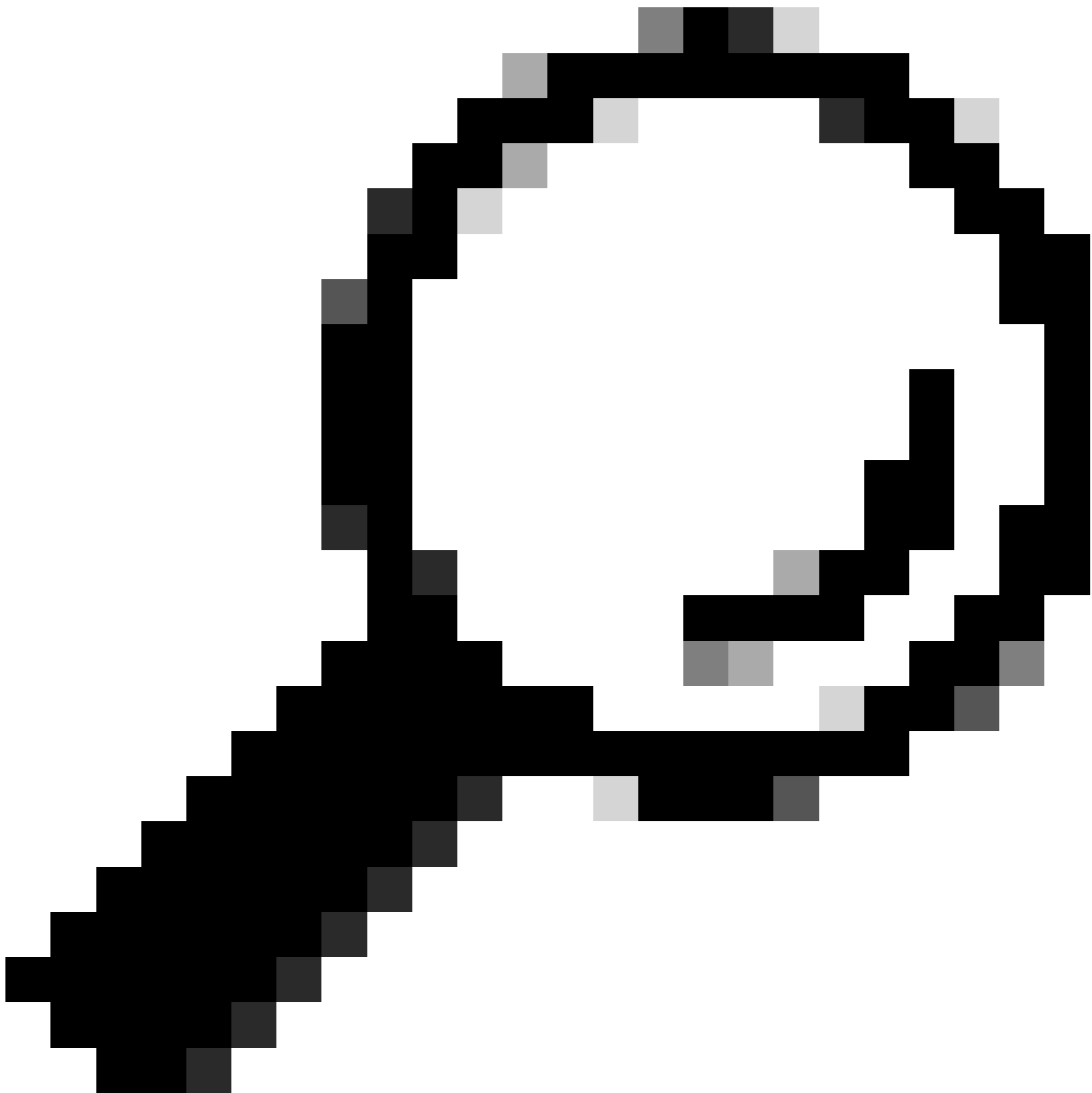
Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

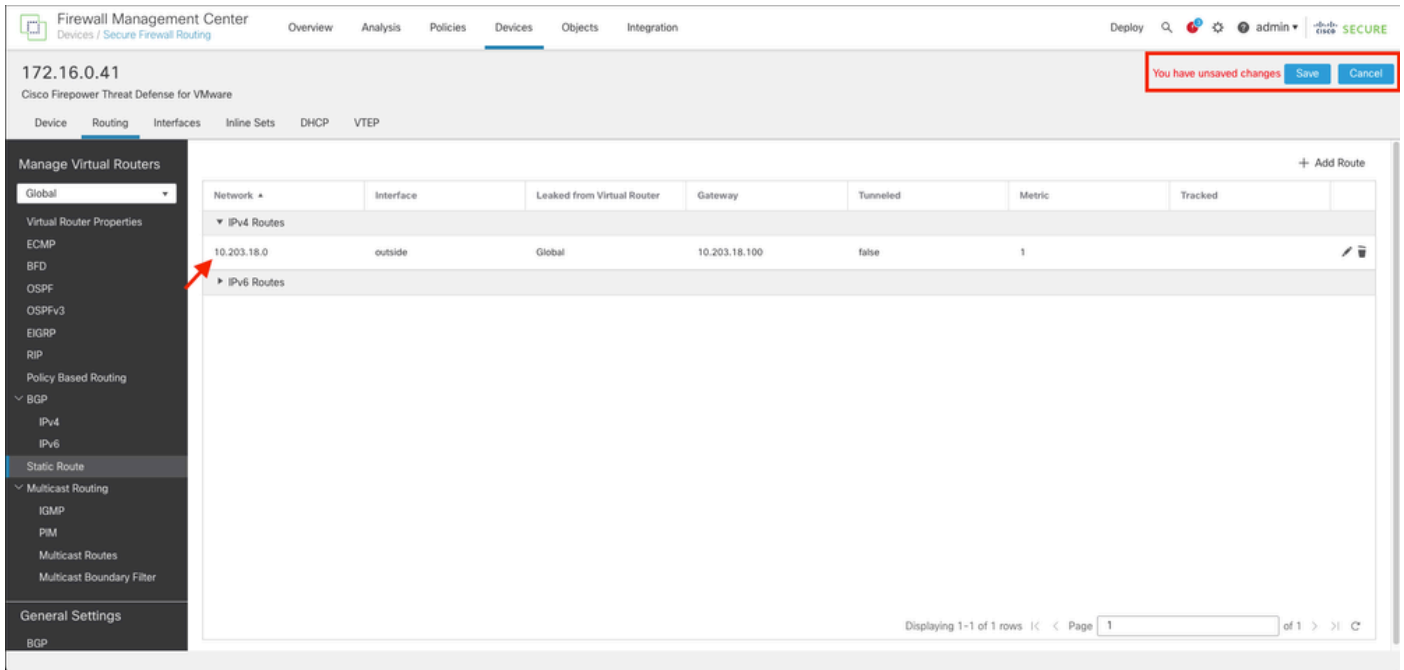
data to display | Page 1 of 1



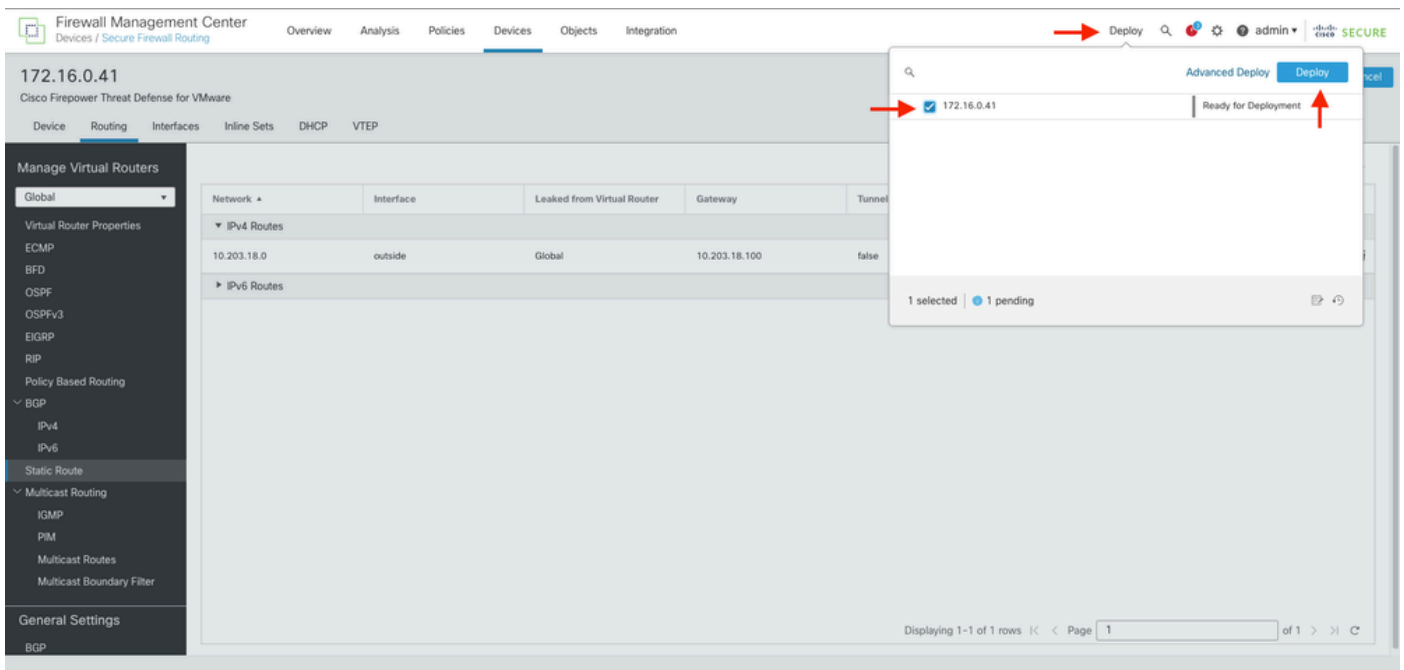
ヒント：使用可能なネットワーク(VLAN)、ゲートウェイ、およびルートトラフィックのフィールドでは、ネットワークオブジェクトを使用する必要があります。オブジェクトがまだ作成されていない場合（つまり、作成されていない場合）は、新しいネットワークオブジェクトを作成するために各フィールドの右側にある(+)記号をクリックします。

手順 6：OKをクリックします。

手順 7：設定を保存し、新しいスタティックルートが期待どおりに表示されていることを検証します。



ステップ7:ステップ2で選択したFTDを展開してチェックボックスをオンにし、青色の展開アイコンをクリックして新しい設定を展開します。



ステップ8:導入が完了済みとして表示されていることを検証します。

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

確認

1. 以前に展開したFTDに対し、SSH、Telnet、またはコンソールを使用してログを記録します。
2. コマンドshow routeおよびshow running-config routeを実行します。
3. FTDルーティングテーブルに、Sフラグが付いたスタティックルートが展開され、それが実行コンフィギュレーションにも表示されていることを確認します。

```
> 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
> █
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。