

# FMCによって管理されるFTDに対するデュアルISPフェールオーバーの設定

## 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](#)

[スタティックルートトラッキング機能の概要](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、FMCによって管理されるFTDでPBRとIP SLAを使用してデュアルISPフェールオーバーを設定する方法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。

- ポリシーベースルーティング ( PBR )
- インターネットプロトコルサービスレベル契約(IP SLA)
- Firepower Management Center ( FMC )
- Firepower Threat Defense ( FTD )

### 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。

- FMCv 7.3.0
- FTDv 7.3.0

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

### スタティック ルート トラッキング機能の概要

スタティックルートトラッキング機能を使用すると、プライマリ専用回線が使用不能になった場合に、FTDがセカンダリISPへの接続を使用できるようになります。この冗長性を実現するために、FTDはスタティックルートを、ユーザが定義したモニタリングターゲットに関連付けます。SSLA動作では、定期的なICMPエコー要求によってターゲットが監視されます。

エコー応答が返されない場合、そのオブジェクトはダウンしているものと見なされ、そのオブジェクトに関連付けられているルートがルーティングテーブルから削除されます。そして、削除されたルートに代わって、すでに定義されているバックアップルートが使用されます。バックアップルートが使用中の場合、SLA モニタ操作は監視ターゲットへのアクセス試行を続けます。

再度、ターゲットに到達できるようになると、最初のルートがルーティングテーブルに置き換えられ、バックアップルートは削除されます。

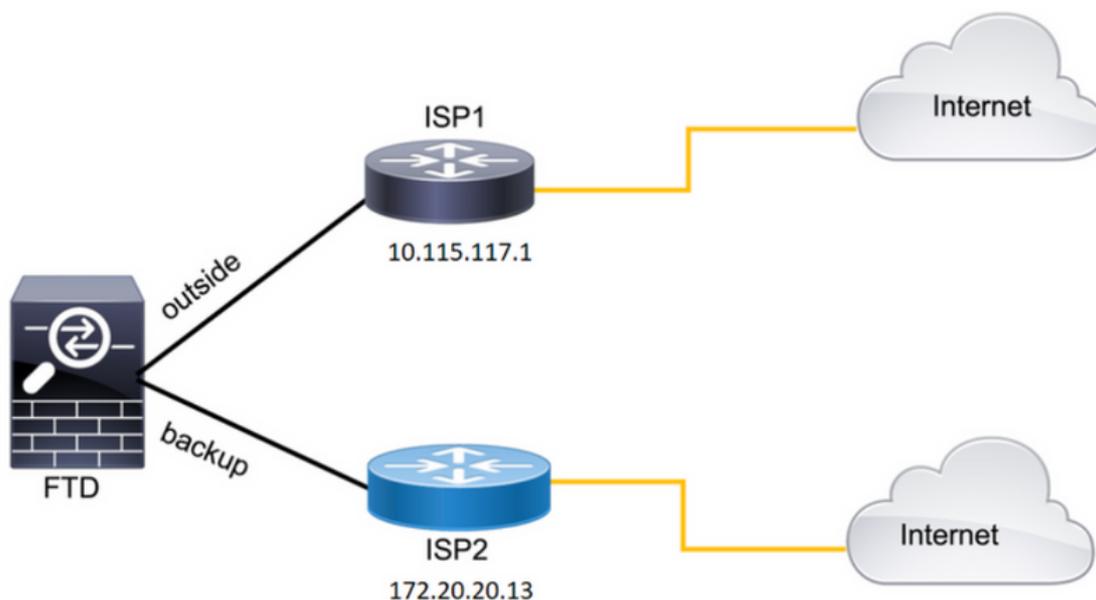
複数のネクストホップとポリシーベースのルーティング転送アクションを同時に設定できるようになりました。トラフィックがルートの基準に一致すると、システムは成功するまで、指定した順序でIPアドレスにトラフィックを転送しようとします。

この機能は、バージョン7.1以降を実行しているFTDデバイスで使用でき、FMCバージョン7.3以降で管理されています。

## 設定

### ネットワーク図

次の図に、ネットワークダイアグラムの例を示します。



画像 1.図の例。

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

## コンフィギュレーション

ステップ 1 : SLAモニタオブジェクトを設定します。

FMCで、Object > Object Management > SLA Monitor > Add SLA Monitorに移動し、ISPのIPアドレスのSLAモニタオブジェクトを追加します。

プライマリデフォルトゲートウェイ(ISP1)のSLAモニタ。

### Edit SLA Monitor Object ?

<b>Name:</b> <input type="text" value="SAL1"/>	<b>Description:</b> <input type="text"/>
<b>Frequency (seconds):</b> <input type="text" value="60"/> <small>(1-604800)</small>	<b>SLA Monitor ID*:</b> <input type="text" value="1"/>
<b>Threshold (milliseconds):</b> <input type="text" value="5000"/> <small>(0-60000)</small>	<b>Timeout (milliseconds):</b> <input type="text" value="5000"/> <small>(0-604800000)</small>
<b>Data Size (bytes):</b> <input type="text" value="28"/> <small>(0-16384)</small>	<b>ToS:</b> <input type="text" value="0"/>
<b>Number of Packets:</b> <input type="text" value="1"/>	<b>Monitor Address*:</b> <input type="text" value="10.115.117.1"/>
<b>Available Zones</b> <span>↻</span> <input type="text" value="Search"/> Backbone Backup new Outside VLAN2816	<b>Selected Zones/Interfaces</b> Outside <span>🗑️</span>

画像 2.SLA1モニタの設定ウィンドウ。

セカンダリデフォルトゲートウェイ(ISP2)のSLAモニタ。

## Edit SLA Monitor Object



Name:

Description:

Frequency (seconds):

(1-604800)

SLA Monitor ID\*:

Threshold (milliseconds):

(0-60000)

Timeout (milliseconds):

(0-604800000)

Data Size (bytes):

(0-16384)

ToS:

Number of Packets:

Monitor Address\*:

Available Zones

Backbone

Add

Selected Zones/Interfaces

Backup

Backup

new

Outside

VLAN2816

Cancel

Save

画像 3.SLA2モニタの設定ウィンドウ

ステップ 2 : ルートトラックを使用してスタティックルートを設定します。

FMCで、Device > Device Management > Edit the desired FTD > Routing > Static Routesに移動し、正しいSLAモニタを使用してスタティックルートを追加します。

SLAモニタは、デフォルトゲートウェイをモニタするモニタである必要があります。

プライマリデフォルトゲートウェイのスタティックルート :

### Edit Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network	+	Selected Network
<input type="text" value="Search"/>	<input type="button" value="Add"/>	any-ipv4 
10.10.10.1		
10.117.0.250		
10.34.24.91		
172.16.0.20		
172.20.20.13		
192.168.1.20		

Ensure that egress virtualrouter has route to that destination

Gateway  
10.115.117.1 +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
SAL1 +

図 4. Outside インターフェイスのスタティックルート設定ウィンドウ。

セカンダリデフォルトゲートウェイのスタティックルート。

**Edit Static Route Configuration**

Type:  IPv4  IPv6

Interface\*  
backup

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Selected Network

Search

10.10.10.1  
10.117.0.250  
10.34.24.91  
172.16.0.20  
172.20.20.13  
192.168.1.20

Add

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway  
172.20.20.13 +

Metric:  
254  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
SLA2 +

図 5. バックアップインターフェイスのスタティックルート設定ウィンドウ。

ステップ 3 : ポリシーベースルートを設定します。

をDevice > Device Management > Edit the desired FTD > Routing > Policy Based Routing, 追加するために移動し、入インターフェイスを選択します。

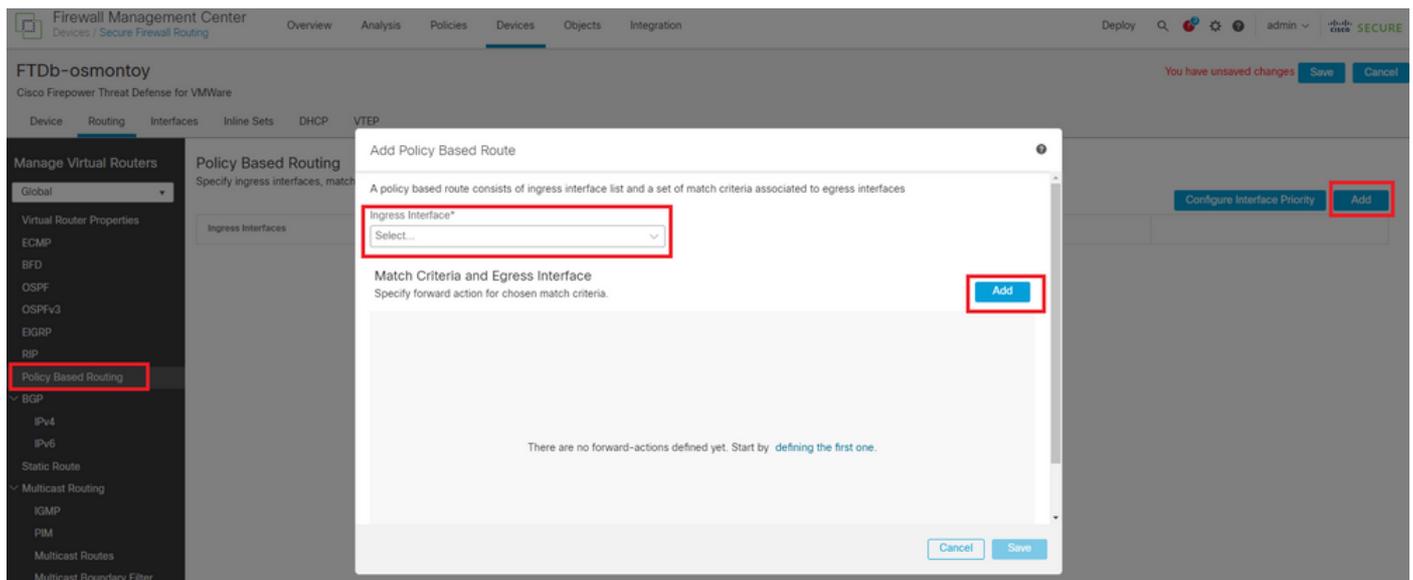


図 6.PBR設定ウィンドウを開きます。

転送アクションを設定します。

- 照合する新しいアクセスコントロールリストを選択または追加します。

IP Address

- Send toオプションから選択します。
- この例では、10.115.117.234がFTD外部IPアドレスです。

### Edit Forwarding Actions

Match ACL:\*  +

Send To:\*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

Default Interface

**IPv4 settings**    IPv6 settings

Recursive:

Default:

Peer Address

Verify Availability +

図 7. Forwarding Actions Configuration ウィンドウで確認できます。

下にスクロールして、ISP1のVerify Availability 値を追加します。

### Edit Forwarding Actions

Default Interface

**IPv4 settings**    IPv6 settings

Recursive:

Default:

Peer Address

Verify Availability +

IP Address:	Sequence:	Track:	
10.115.117.1	1	1	✎ 🗑

図 8. *Forwarding Actions Configuration* ウィンドウで確認できます。

バックアップインターフェイスに対して同じプロセスを繰り返します。ただし、別のアクセスコントロールリストオブジェクトを使用してください。

Edit Forwarding Actions

Match ACL:\* internal\_networks +

Send To:\* IP Address

IPv4 Addresses: 172.20.20.77

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: None

Default Interface

**IPv4 settings** IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel Save

図 9. *Forwarding Actions Configuration* ウィンドウ

設定についても同じプロセスを繰り返します。Verify Availabilityが、ここではISP2に対して繰り返します。

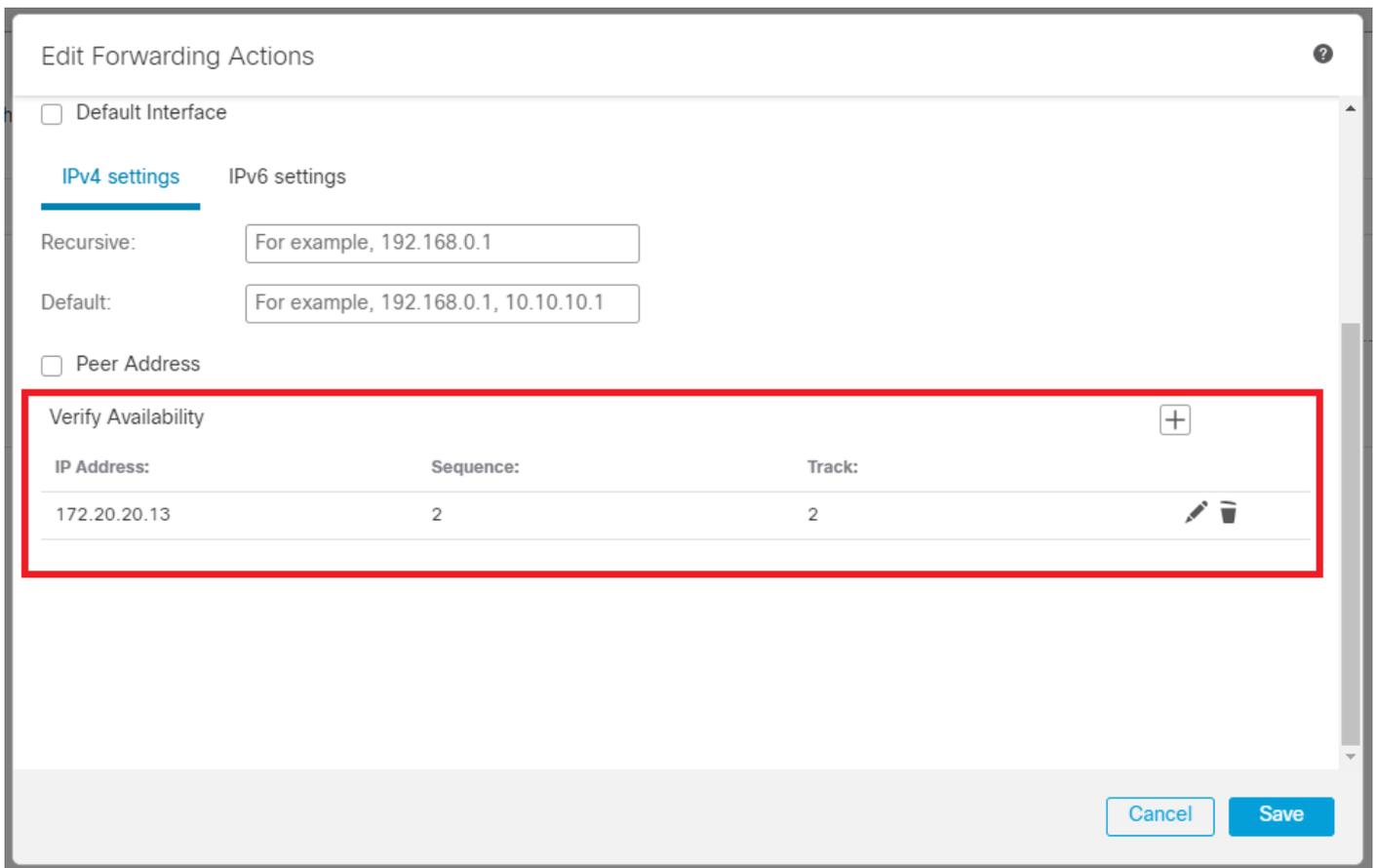


図10.アベイラビリティ設定の確認

設定を検証します。

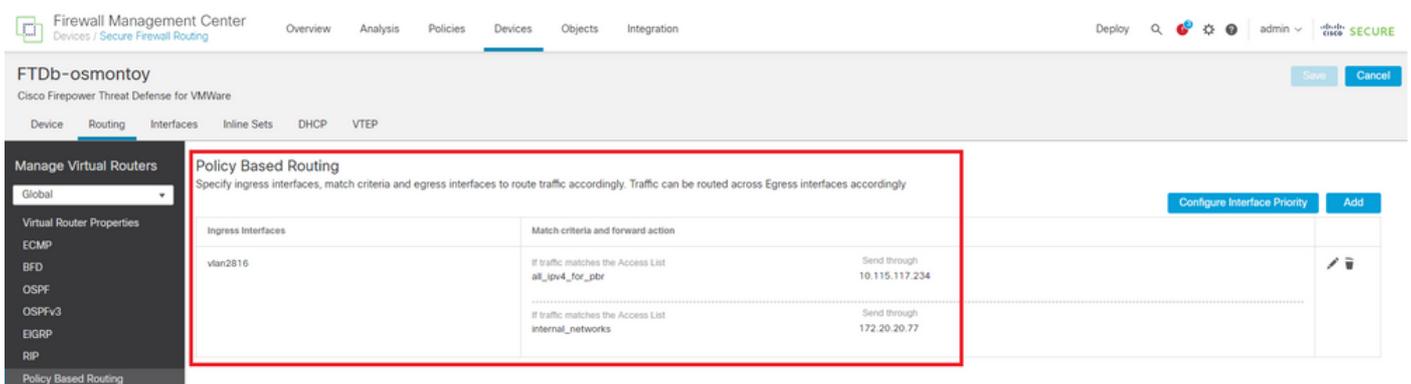


図 11.PBR設定。

確認

セキュアシェル(SSH)からFTDにアクセスし、system support disagnotsic-cliコマンドを使用して次のコマンドを実行します。

•

show route-map : このコマンドは、ルートマップ設定を表示します。

<#root>

firepower#

show route-map

route-map FMC\_GENERATED\_PBR\_1679065711925

, permit, sequence 5

Match clauses:

ip address (access-lists): internal\_networks

Set clauses:

ip next-hop verify-availability 10.115.117.1 1

track 1 [up]

ip next-hop 10.115.117.234

route-map FMC\_GENERATED\_PBR\_1679065711925, permit, sequence 10

Match clauses:

ip address (access-lists): all\_ipv4\_for\_pbr

Set clauses:

ip next-hop verify-availability 172.20.20.13 2

track 2 [up]

ip next-hop 172.20.20.77

firepower#

- show running-config sla monitor : このコマンドは、SLA設定を表示します。

<#root>

firepower#

```
show running-config sla monitor
```

```
sla monitor 1
```

```
type echo protocol ipIcmpEcho 10.115.117.1 interface outside  
sla monitor schedule 1 life forever start-time now
```

```
sla monitor 2
```

```
type echo protocol ipIcmpEcho 172.20.20.13 interface backup  
sla monitor schedule 2 life forever start-time now  
firepower#
```

- show sla monitor configuration : このコマンドは、SLA設定値を表示します。

<#root>

firepower#

show sla monitor configuration

SA Agent, Infrastructure Engine-II

Entry number:

1

Owner:

Tag:

Type of operation to perform: echo

Target address: 10.115.117.1

Interface: outside

Number of packets: 1

Request size (ARR data portion): 28

Operation timeout (milliseconds): 5000

Type Of Service parameters: 0x0

Verify data: No

Operation frequency (seconds): 60

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE  
Status of entry (SNMP RowStatus): Active  
Enhanced History:

Entry number:

2

Owner:  
Tag:  
Type of operation to perform: echo

Target address: 172.20.20.13

Interface: backup  
Number of packets: 1  
Request size (ARR data portion): 28  
Operation timeout (milliseconds): 5000  
Type Of Service parameters: 0x0  
Verify data: No  
Operation frequency (seconds): 60  
Next Scheduled Start Time: Start Time already passed  
Group Scheduled : FALSE  
Life (seconds): Forever  
Entry Ageout (seconds): never  
Recurring (Starting Everyday): FALSE  
Status of entry (SNMP RowStatus): Active  
Enhanced History:

- show sla monitor operational-state : このコマンドは、SLA動作の動作状態を表示します。

<#root>

firepower#

show sla monitor operational-state

Entry number: 1

Modification time: 15:48:04.332 UTC Fri Mar 17 2023  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 74  
Number of operations skipped: 0  
Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never  
Connection loss occurred: FALSE  
Timeout occurred: FALSE  
Over thresholds occurred: FALSE  
Latest RTT (milliseconds): 1  
Latest operation start time: 17:01:04.334 UTC Fri Mar 17 2023  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2

Modification time: 15:48:04.335 UTC Fri Mar 17 2023  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 74  
Number of operations skipped: 0

Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never  
Connection loss occurred: FALSE  
Timeout occurred: FALSE  
Over thresholds occurred: FALSE  
Latest RTT (milliseconds): 1  
Latest operation start time: 17:01:04.337 UTC Fri Mar 17 2023  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

- show track : このコマンドは、SLA追跡プロセスによって追跡されるオブジェクトに関する情報を表示します。

<#root>

firepower#

show track

Track 1

Response Time Reporter 1 reachability

Reachability is Up

4 changes, last change 00:53:42  
Latest operation return code: OK  
Latest RTT (milliseconds) 1  
Tracked by:  
ROUTE-MAP 0  
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 2 reachability

Reachability is Up

2 changes, last change 01:13:41  
Latest operation return code: OK  
Latest RTT (milliseconds) 1  
Tracked by:  
ROUTE-MAP 0  
STATIC-IP-ROUTING 0

- show running-config route : このコマンドは、現在のルート設定を表示します。

firepower#

show running-config route

route

outside

0.0.0.0 0.0.0.0 10.115.117.1 1

track 1

route

backup

0.0.0.0 0.0.0.0 172.20.20.13 254

track 2

route v1an2816 10.42.0.37 255.255.255.255 10.43.0.1 254  
firepower#

- show route : このコマンドは、データインターフェイスのルーティングテーブルを表示します。

<#root>

firepower#

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 10.115.117.1 to network 0.0.0.0

S\* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside

S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone  
C 10.88.243.0 255.255.255.0 is directly connected, backbone  
L 10.88.243.67 255.255.255.255 is directly connected, backbone  
C 10.115.117.0 255.255.255.0 is directly connected, outside  
L 10.115.117.234 255.255.255.255 is directly connected, outside  
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816  
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816  
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816  
C 172.20.20.0 255.255.255.0 is directly connected, backup  
L 172.20.20.77 255.255.255.255 is directly connected, backup

プライマリリンクに障害が発生した場合 :

- show route-map : このコマンドは、リンクに障害が発生したときにルートマップ設定を表示します。

<#root>

firepower#

```
show route-map FMC_GENERATED_PBR_1679065711925
```

```
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 5
```

```
Match clauses:
```

```
ip address (access-lists): internal_networks
```

```
Set clauses:
```

```
ip next-hop verify-availability 10.115.117.1 1
```

```
track 1 [down]
```

```
ip next-hop 10.115.117.234
```

```
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
```

```
Match clauses:
```

```
ip address (access-lists): all_ipv4_for_pbr
```

```
Set clauses:
```

```
ip next-hop verify-availability 172.20.20.13 2
```

```
track 2 [up]
```

```
ip next-hop 172.20.20.77
firepower#
```

- show route : このコマンドは、インターフェイスごとに新しいルーティングテーブルを表示します。

```
<#root>
```

```
firepower#
```

```
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 10.115.117.1 to network 0.0.0.0
```

```
s* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup
```

```
S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
```

C 172.20.20.0 255.255.255.0 is directly connected, backup  
L 172.20.20.77 255.255.255.255 is directly connected, backup

#### 関連情報

- [Cisco Secure Firewall Management Center アドミニストレーションガイド 7.3](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 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。