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および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、FTDは、プライマリ専用回線が使用不能になった場合にセカンダリISPへの接続を使用できます。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、定義したモニタリングターゲットに関連付けます。SSLA操作では、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。

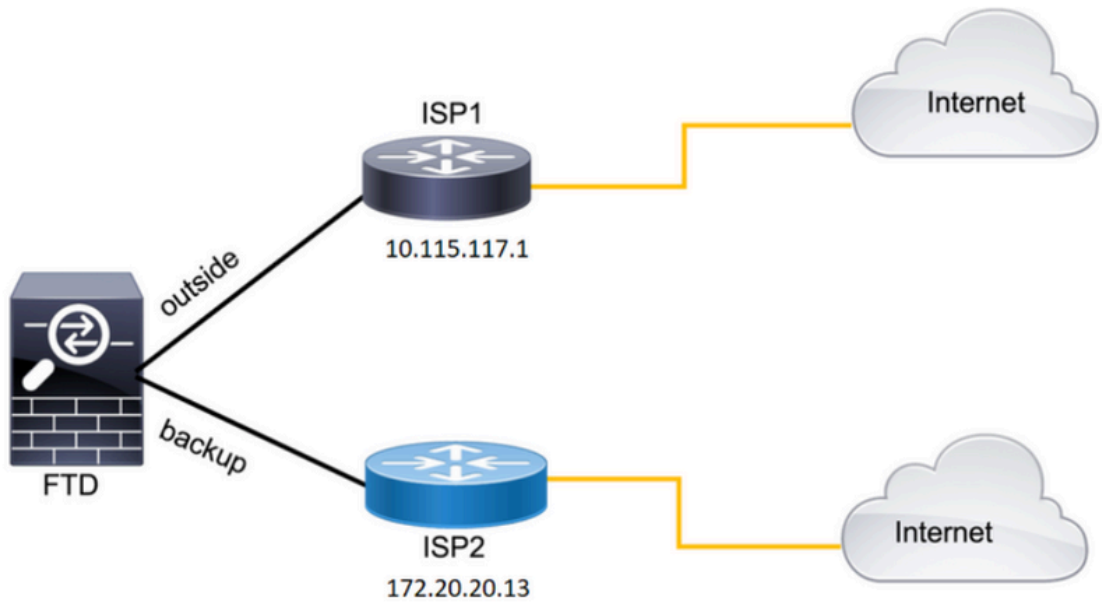
複数のネクストホップとポリシーベースのルーティング転送アクションを同時に設定できるようになりました。トラフィックがルートの基準に一致すると、システムは成功するまで、指定した順序でトラフィックをIPアドレスに転送しようとします。

この機能は、バージョン7.1以降が稼働し、FMCバージョン7.3以降で管理されているFTDデバイスで使用できます。

設定

ネットワーク図

次の図は、ネットワークダイアグラムの例を示しています。



画像 1.図の例。

ISP1 = 10.115.117.1

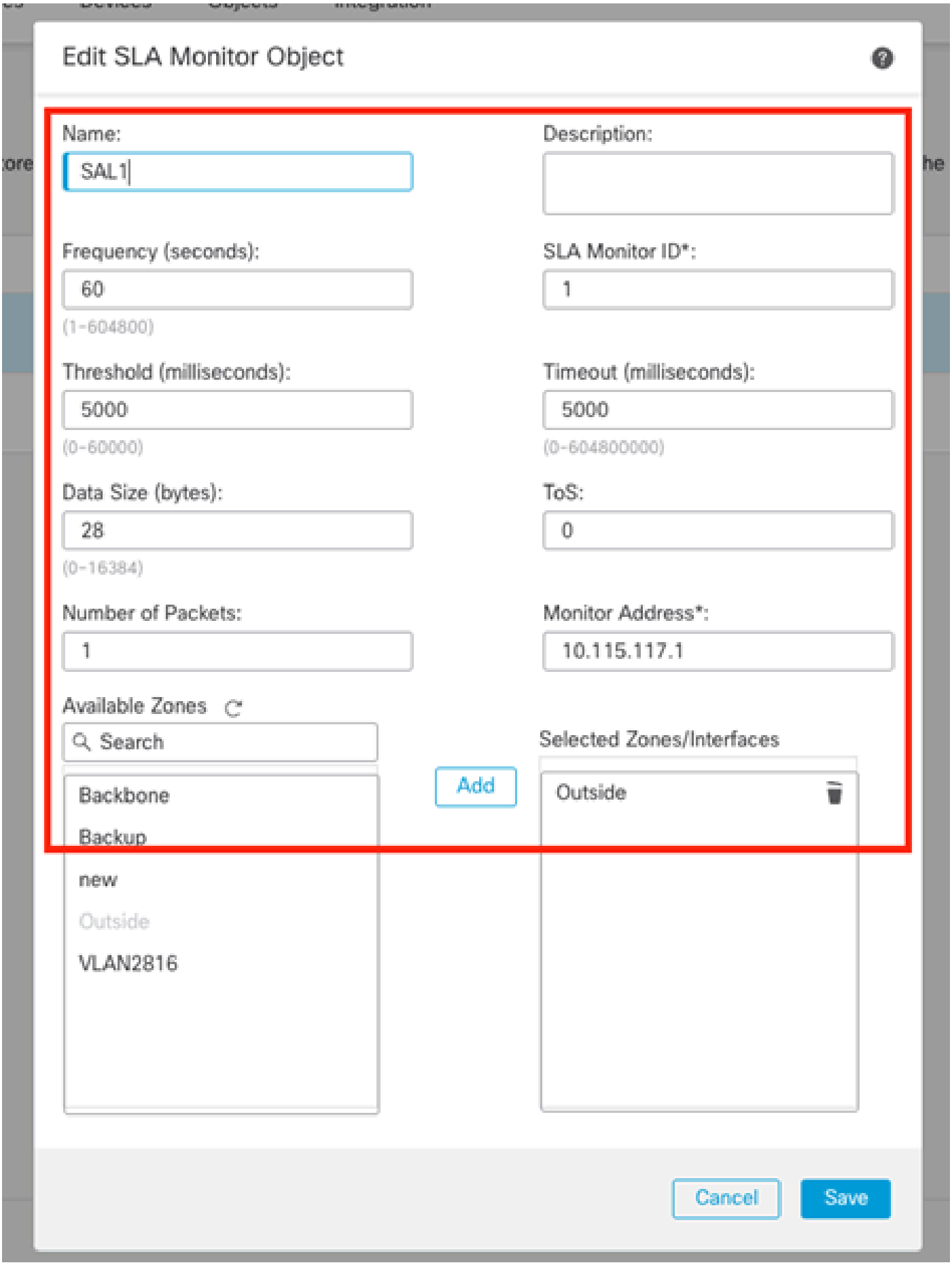
ISP2 = 172.20.20.13

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。

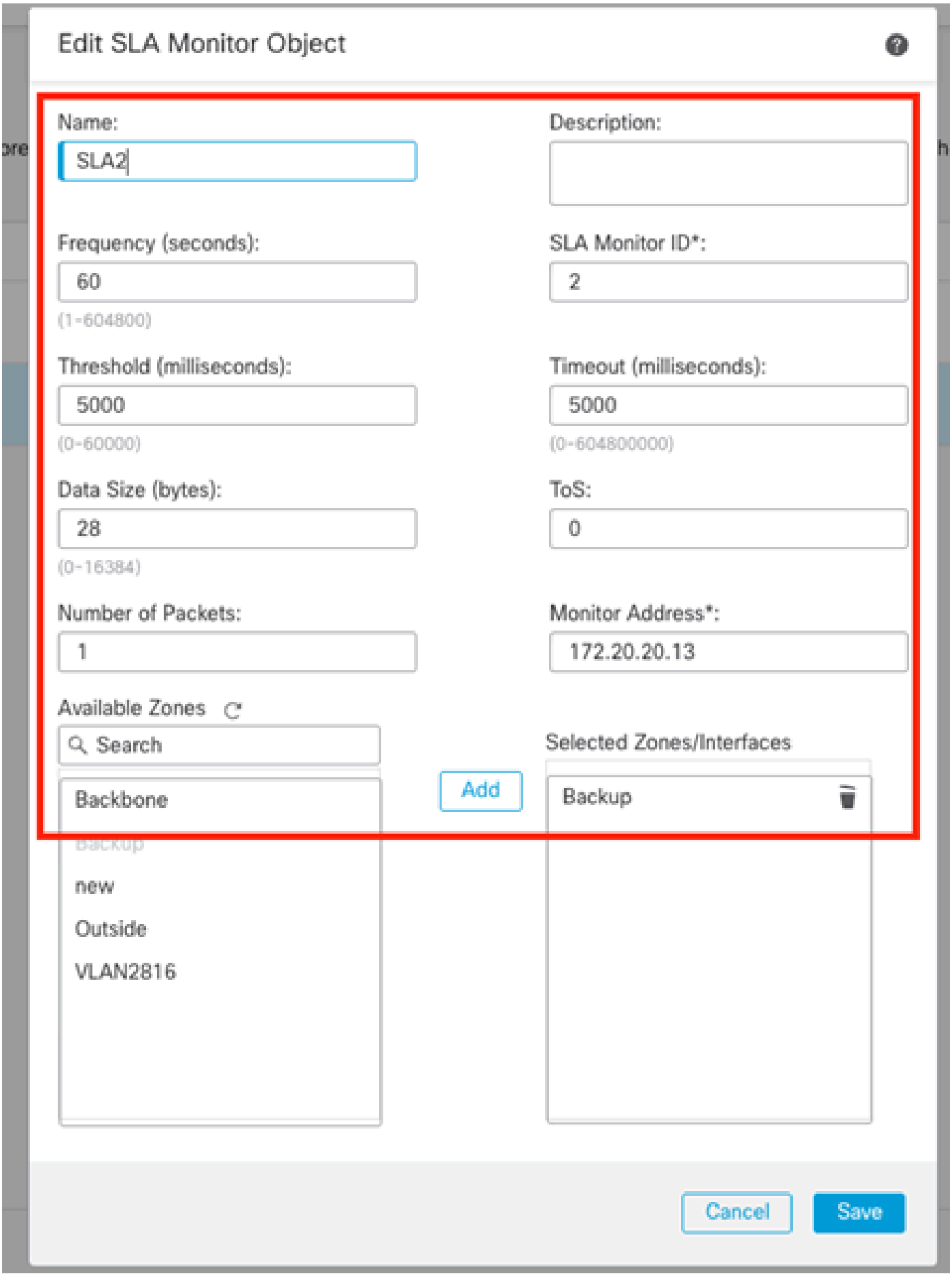
FMCで、Object > Object Management > SLA Monitor > Add SLA Monitorの順に移動し、ISPのIPアドレスのSLA Monitorオブジェクトを追加します。

プライマリデフォルトゲートウェイ(ISP1)のSLAモニタ。



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。



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の順に移動し、正しいSLAモニタで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ものでなければなりません。

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：

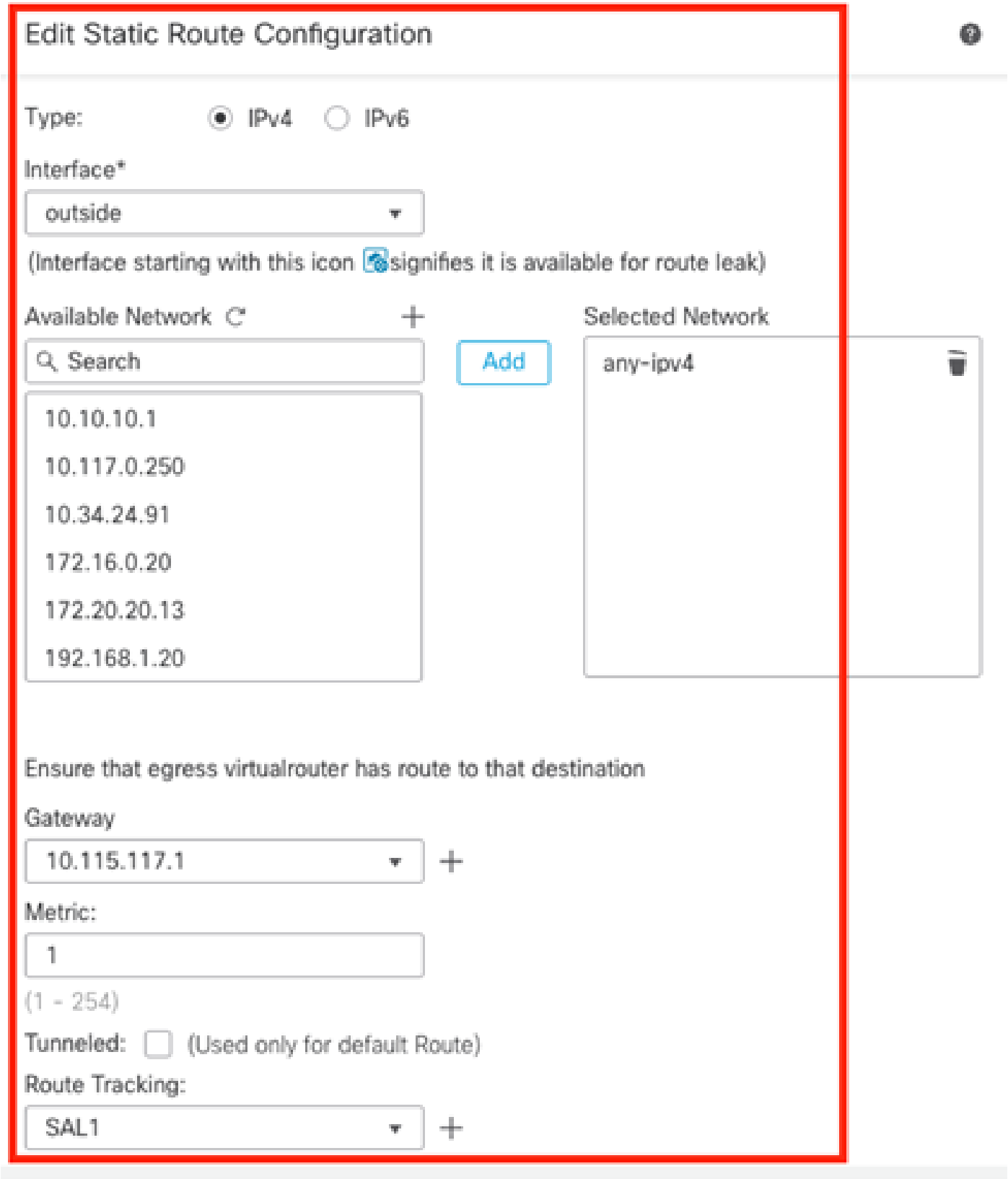


図 4.Outsideインターフェイスのスタティックルート設定ウィンドウ。

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。

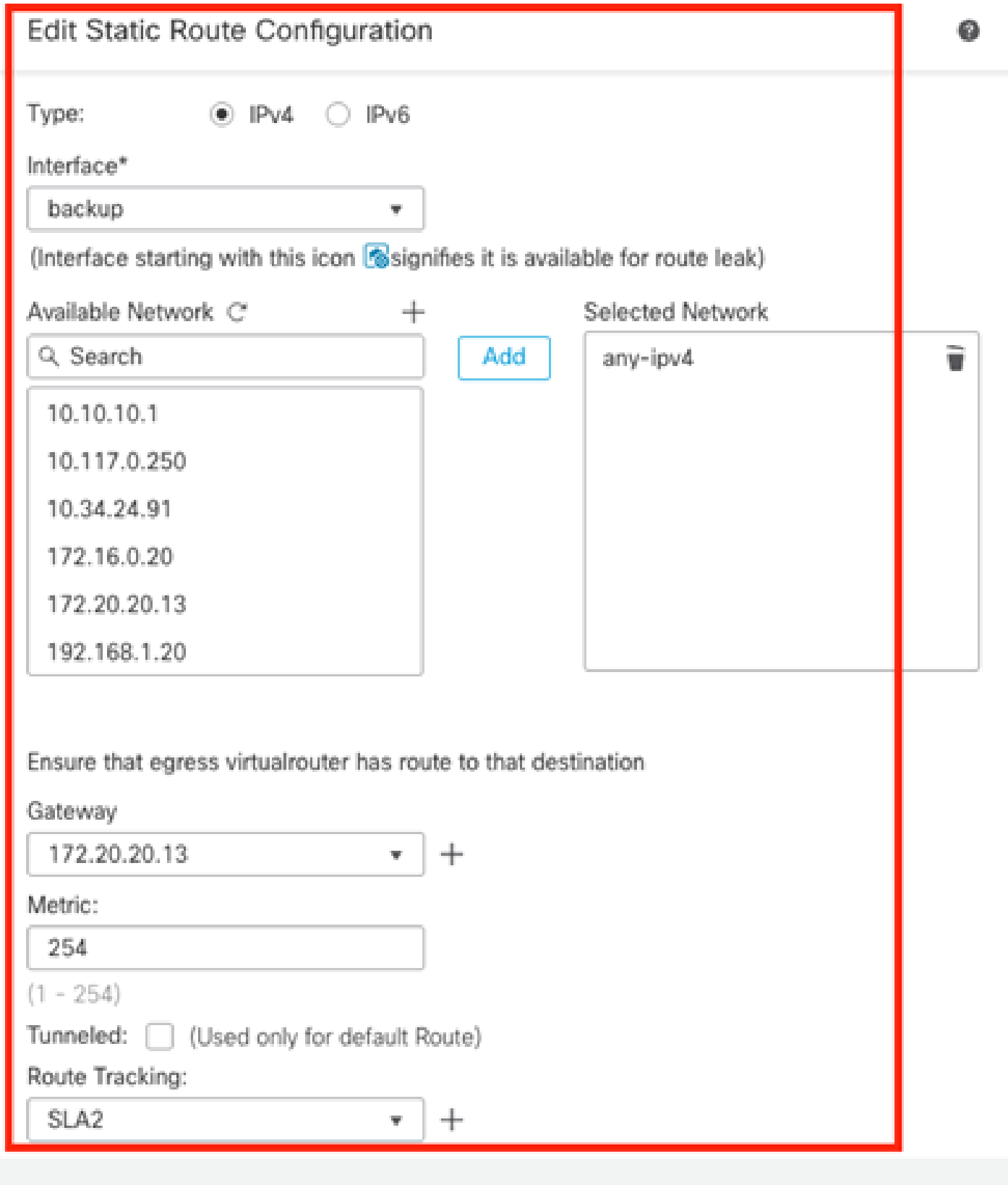


図 5.バックアップインターフェイスのスタティックルート設定ウィンドウ。

ステップ 3：ポリシーベースルートを設定します。

Device > Device Management > Edit the desired FTD > Routing > Policy Based Routingの順に移動し、PBRを追加して、入力インターフェイスを選択します。

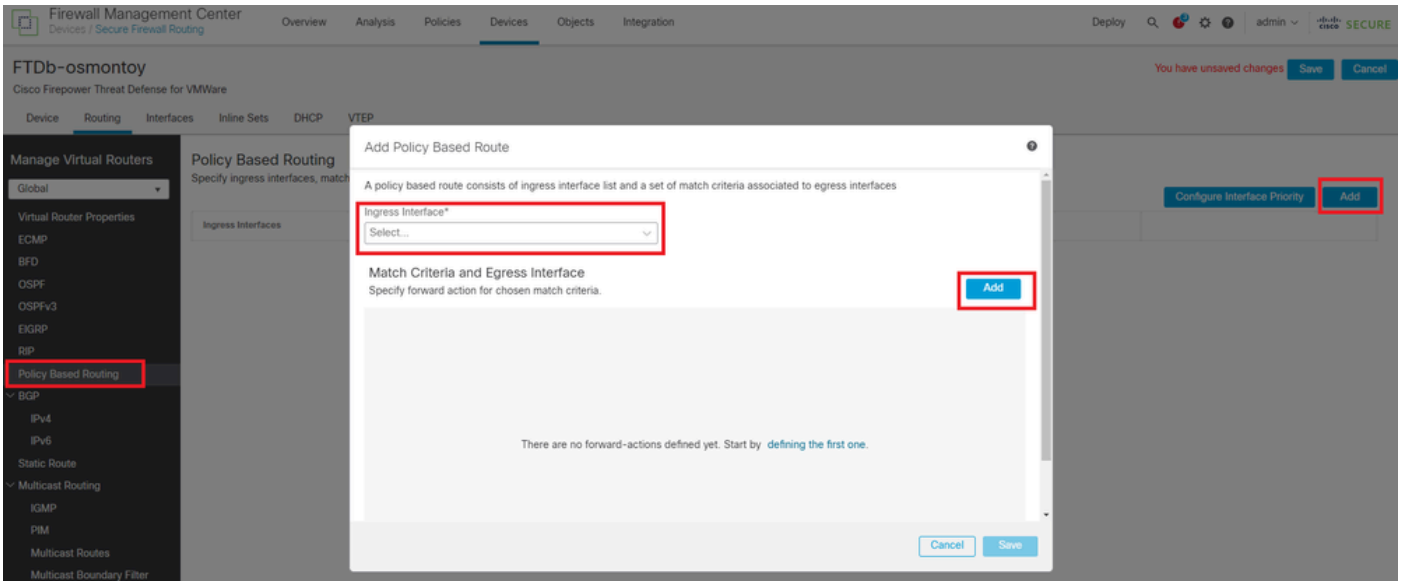


図 6.PBR設定ウィンドウで確認できます。

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

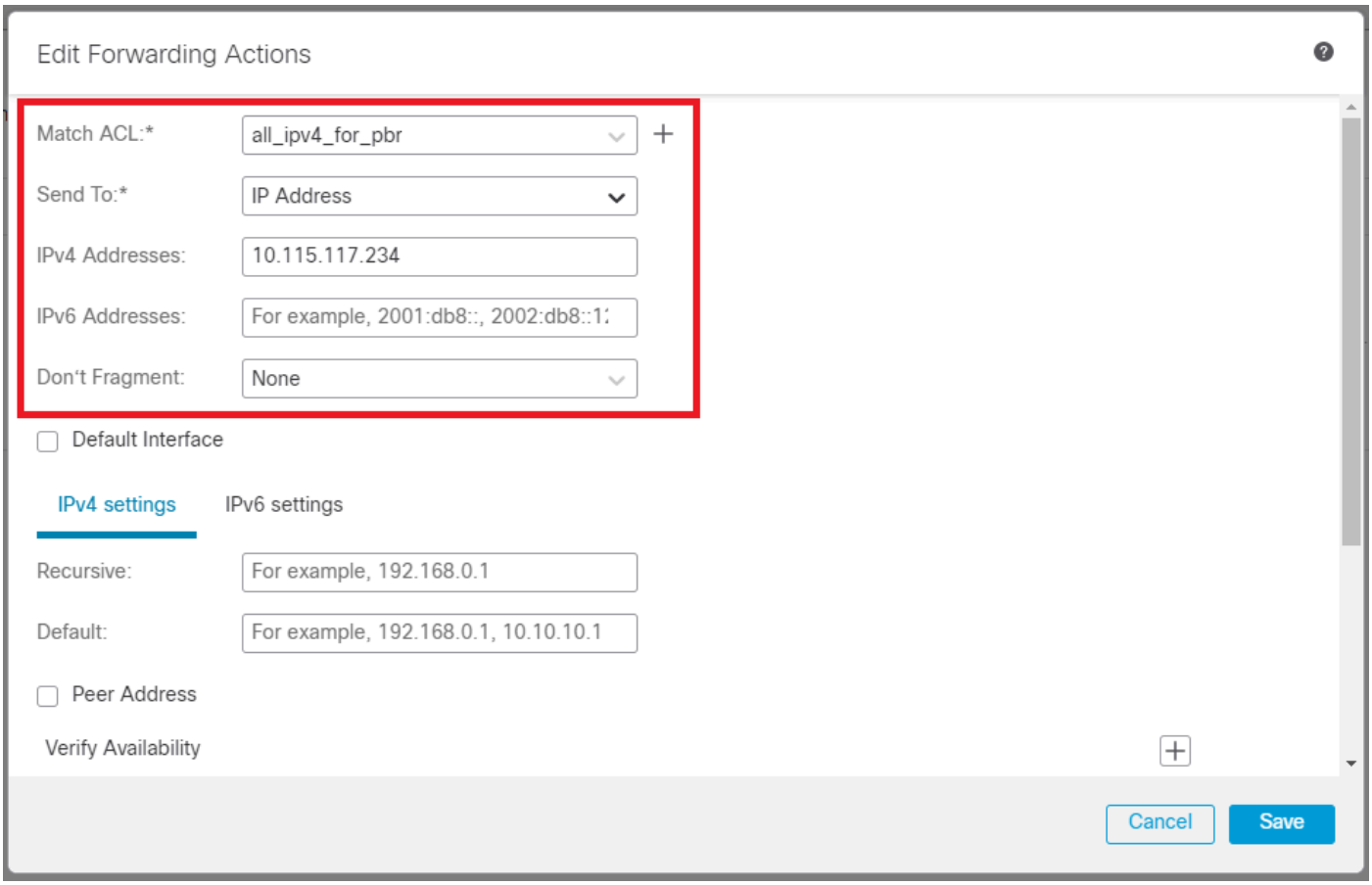


図 7.Forwarding Actions Configurationウィンドウで確認できます。

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

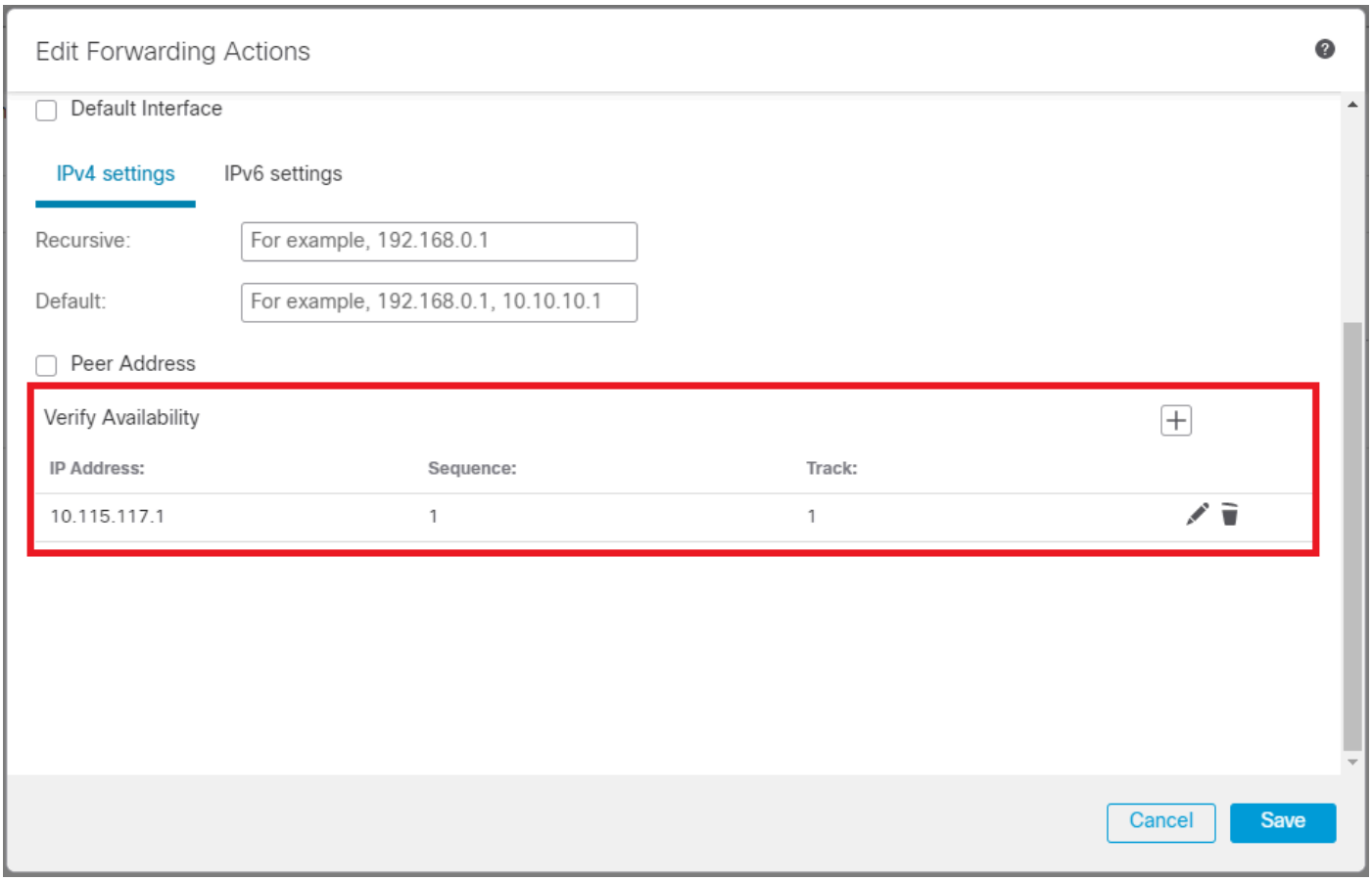


図 8.Forwarding Actions Configurationウィンドウで確認できます。

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、必ず別のアクセスコントロールリスト(ACL)オブジェクトを使用してください。

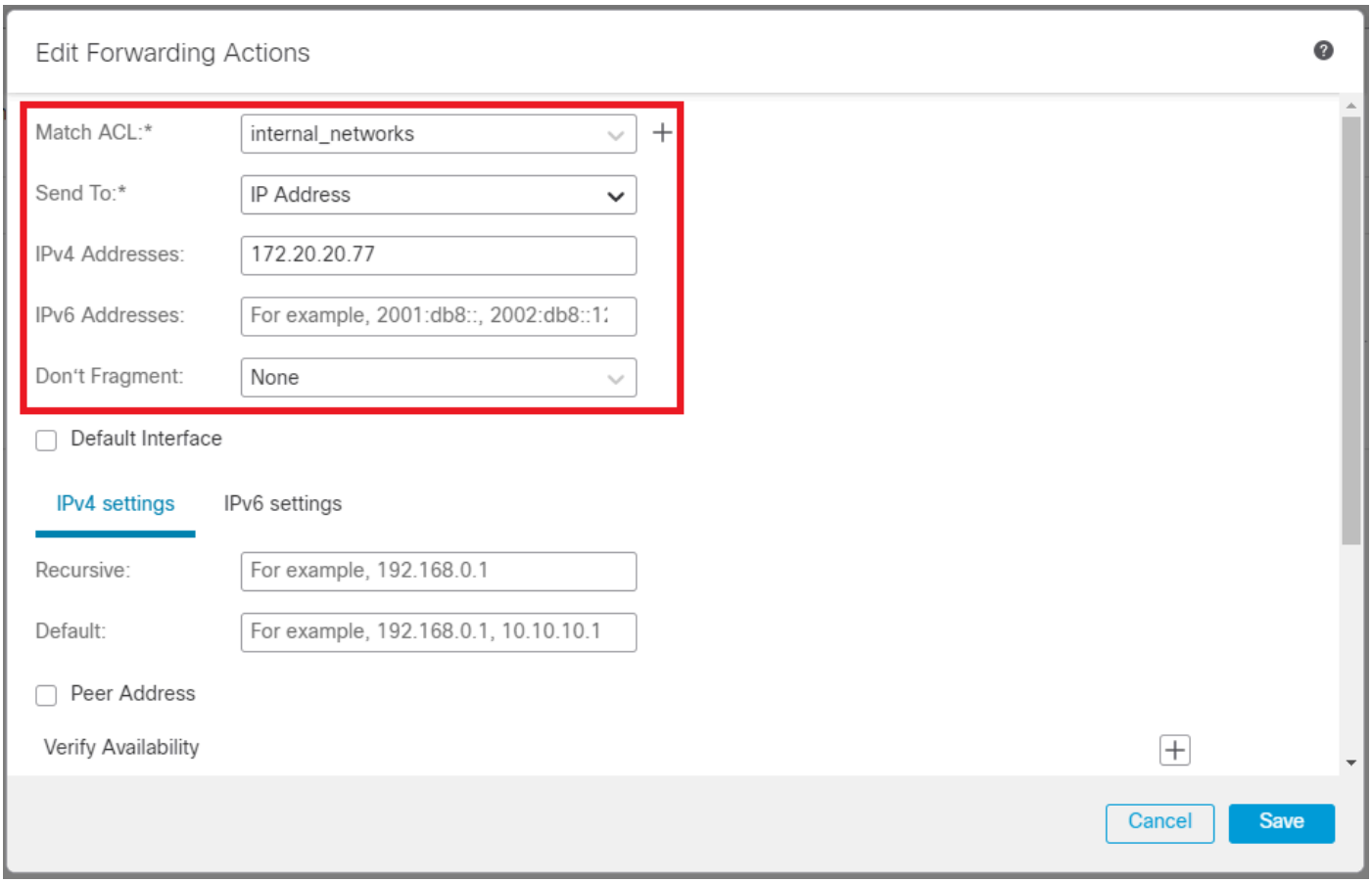


図 9.Forwarding Actions Configurationウィンドウ

Verify Availabilityconfigurationについても同じプロセスを繰り返しますが、ここではISP2について繰り返します。

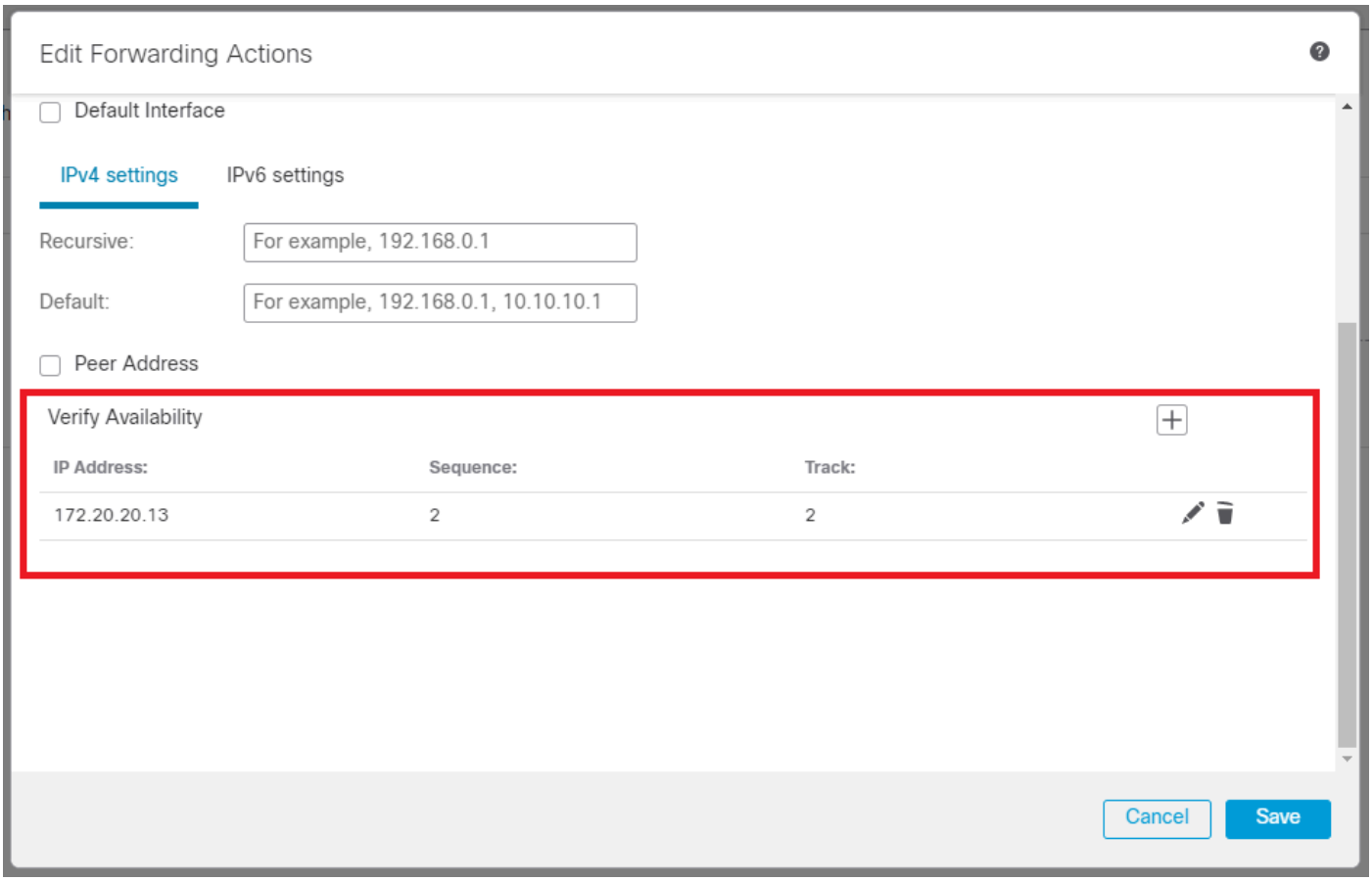


図10.アベイラビリティ設定の確認

設定を検証します。

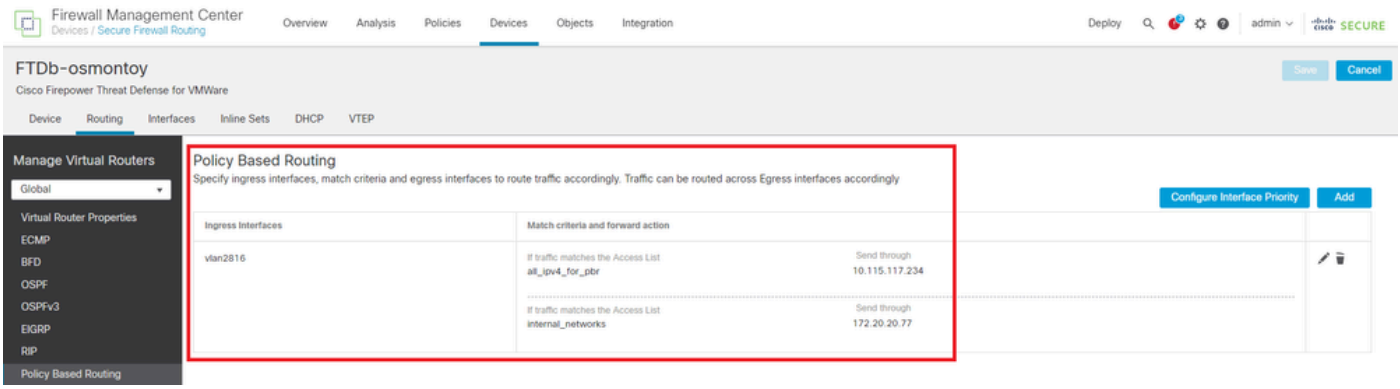


図 11.PBRの設定

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 (millisecs) 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 (millisecs) 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。

<#root>

```
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 vlan2816 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。