

FMCによって管理されるFTD上のデュアルISPに対するIP SLAによるPBRの設定

内容

[概要](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[ステップ 1 : PBRアクセスリストの設定](#)

[ステップ 2 : PBRルートマップの設定](#)

[ステップ 3 : FlexConfigテキストオブジェクトの設定](#)

[ステップ 4 : SLAモニタの設定](#)

[ステップ 4 : ルートトラックを使用したスタティックルートの設定](#)

[ステップ 5 : PBR FlexConfigオブジェクトの設定](#)

[手順 6 : FlexConfigポリシーへのPBR FlexConfigオブジェクトの割り当て](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、(FMC)で管理されるFTDでIP SLAとともにPBRを設定する方法について説明します。

著者 : Cisco TACエンジニア、Daniel Perez Vertti Vazquez

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。

- PBRの設定 Cisco Adaptive Security Appliance (ASA)
- FlexConfig on Firepower
- IP SLA

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。

- Cisco FTDバージョン7.0.0 (ビルド94)
- Cisco FMCバージョン7.0.0 (ビルド94)

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、初期（デフォルト）設定の状態から起動しています。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

このドキュメントでは、 Policy Based Routing (PBR) ~と共に Internet Protocol Service Level Agreement (IP SLA) Cisco Firepower Threat Defense (FTD) Cisco Firepower Management Center(FMC)で管理されます。

従来のルーティングでは、宛先IPアドレスのみに基づいて転送が決定されます。PBRは、ルーティングプロトコルとスタティックルーティングの代替手段です。

ルーティングの制御をより詳細に行えます。これは、宛先IPアドレスの他に、ルーティング基準として送信元IPアドレスや送信元ポートと宛先ポートなどのパラメータを使用できるためです。

PBRの考えられるシナリオには、発信元に依存するアプリケーションや、専用リンク上のトラフィックが含まれます。

PBRとともに、ネクストホップの可用性を確保するためにIP SLAを実装できます。IP SLAは、通常のパケットの交換を通じてエンドツーエンドの接続を監視するメカニズムです。

発行時点では、FMCを通じてPBRを直接サポートしていません Graphical User Interface (GUI) 機能を設定するには、FlexConfigポリシーを使用する必要があります。

一方で、 Internet Control Message Protocol (ICMP) SLAはFTDでサポートされます。

この例では、PBRを使用してプライマリ上でパケットをルーティングします Internet Service Provider (ISP) 送信元IPアドレスに基づく回線。

その間、IP SLAは接続を監視し、障害が発生した場合にバックアップ回線へのフォールバックを強制します。

設定

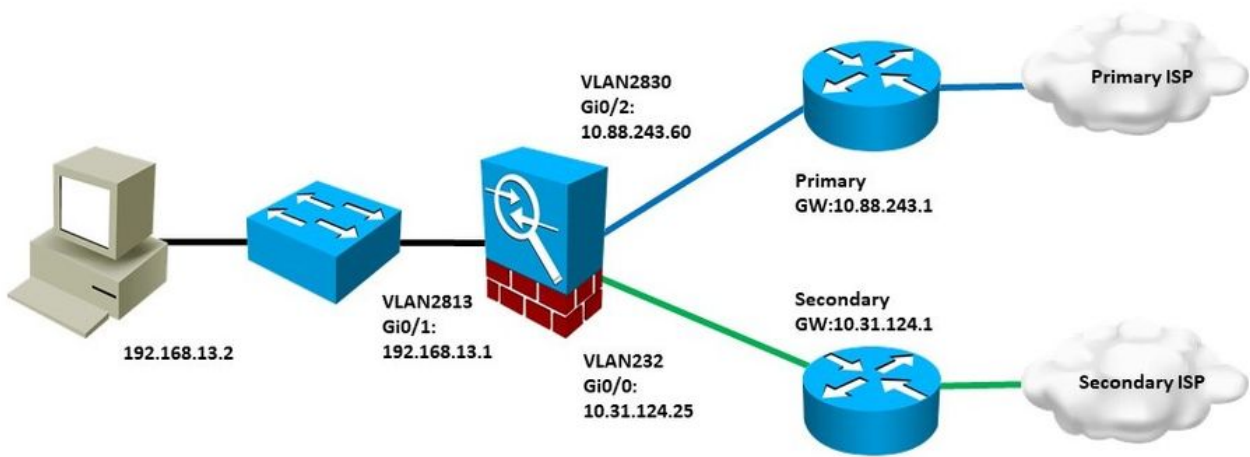
ネットワーク図

この例では、Cisco FTDにはVLAN230とVLAN232の2つの外部インターフェイスがあります。それぞれが異なるISPに接続します。

内部ネットワークVLAN2813からのトラフィックは、PBRを使用するプライマリISP経由でルーティングされます。

PBRルートマップは送信元IPアドレスのみに基づいて転送を決定し (VLAN2813から受信したものはすべてVLAN230の10.88.243.1にルーティングする必要があります)、FTDのインターフェイスGigabitEthernet 0/1に適用されます。

その間、FTDはIP SLAを使用して、各ISPゲートウェイへの接続を監視します。VLAN230で障害が発生した場合、FTDはVLAN232のバックアップ回線にフェールオーバーします。



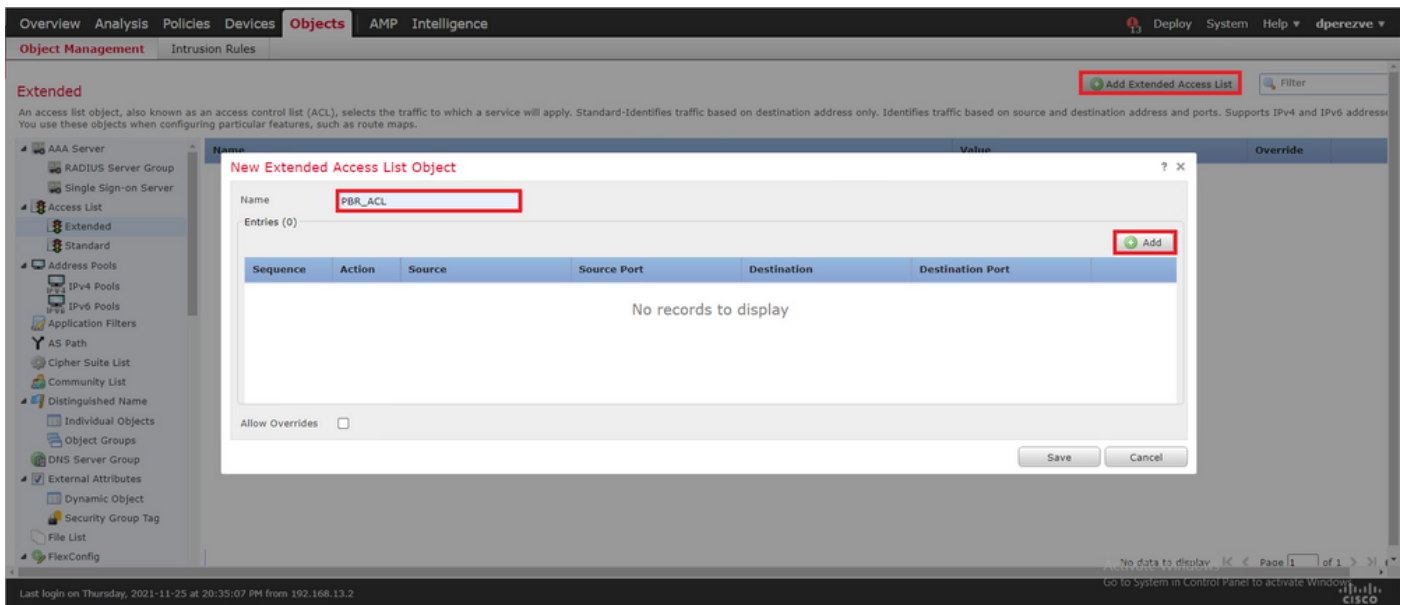
設定

ステップ 1 : PBRアクセスリストの設定

PBR設定の最初のステップで、ルーティングポリシーの対象にする必要があるパケットを定義します。PBRは、ルートマップとアクセスリストを使用してトラフィックを識別します。

一致基準のアクセスリストを定義するには、 **Objects > Object Management** を選択し、 **Extended** 下に **Access List** 目次のカテゴリ。

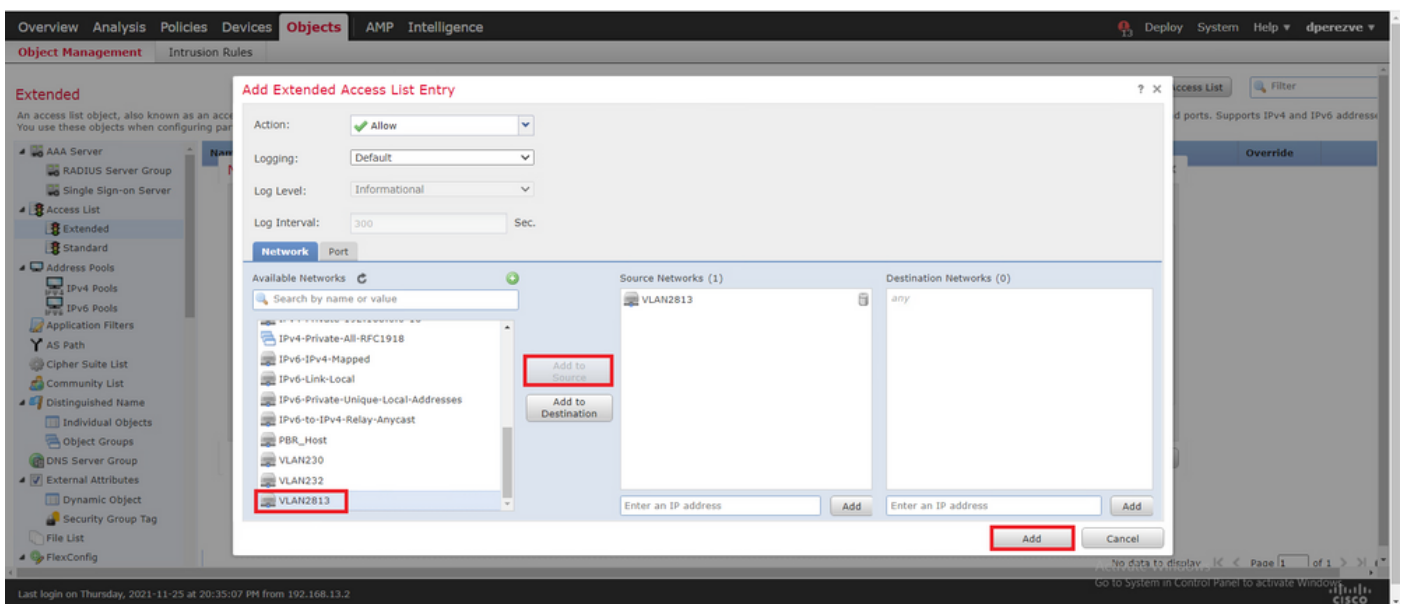
クリック **Add Extended Access List** .内 **New Extended Access List Object** ウィンドウで、オブジェクトに名前を割り当て、 **Add** ボタンをクリックします。



内 Add Extended Access List Entry ウィンドウで、内部ネットワークを表すオブジェクトを選択します。この場合はVLAN2813です。

クリック Add to Source アクセスリストの送信元として定義します。

クリック Add をクリックしてエントリを作成します。



クリック save .オブジェクトをオブジェクトリストに追加する必要があります。

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
PBR_ACL		X

Displaying 1 of 1 rows | Page 1 of 1

ステップ 2 : PBRルートマップの設定

PBRアクセスリストを設定したら、それをルートマップに割り当てます。ルートマップは、アクセスリストで定義されたmatch句に対してトラフィックを評価します。

一致が発生すると、ルートマップはルーティングポリシーで定義されたアクションを実行します。

ルートマップを定義するには、 **Objects > Object Management** を選択し、 **Route Map** 目次を参照してください。

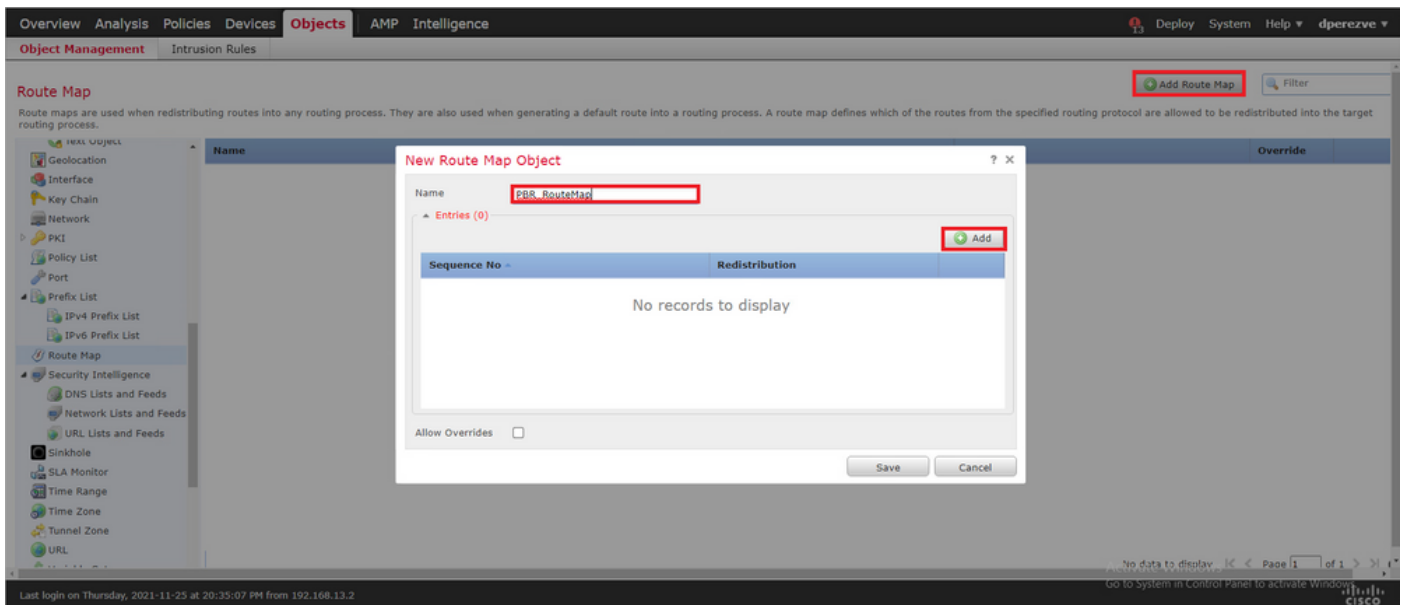
Route Map

Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Name	Value	Override
No records to display		

No data to display | Page 1 of 1

クリック **Add Route Map** > .内 **New Route Map Object** オブジェクトに名前を割り当て、 **Add** 新しいルートマップエントリを作成します。



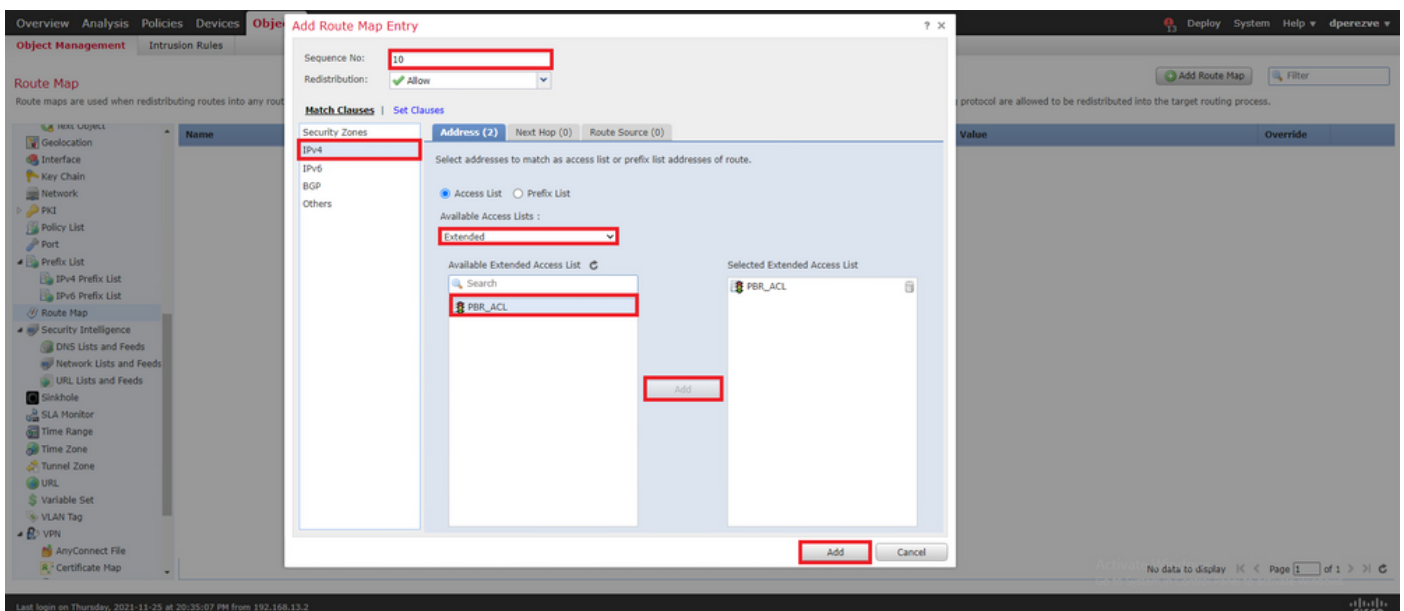
内 Add Route Map Entry ウィンドウで、新しいエントリの位置のシーケンス番号を定義します。

移動先 IPv4 > Match Clauses [Extended] を Available Access List ドロップダウンメニューをクリックします。

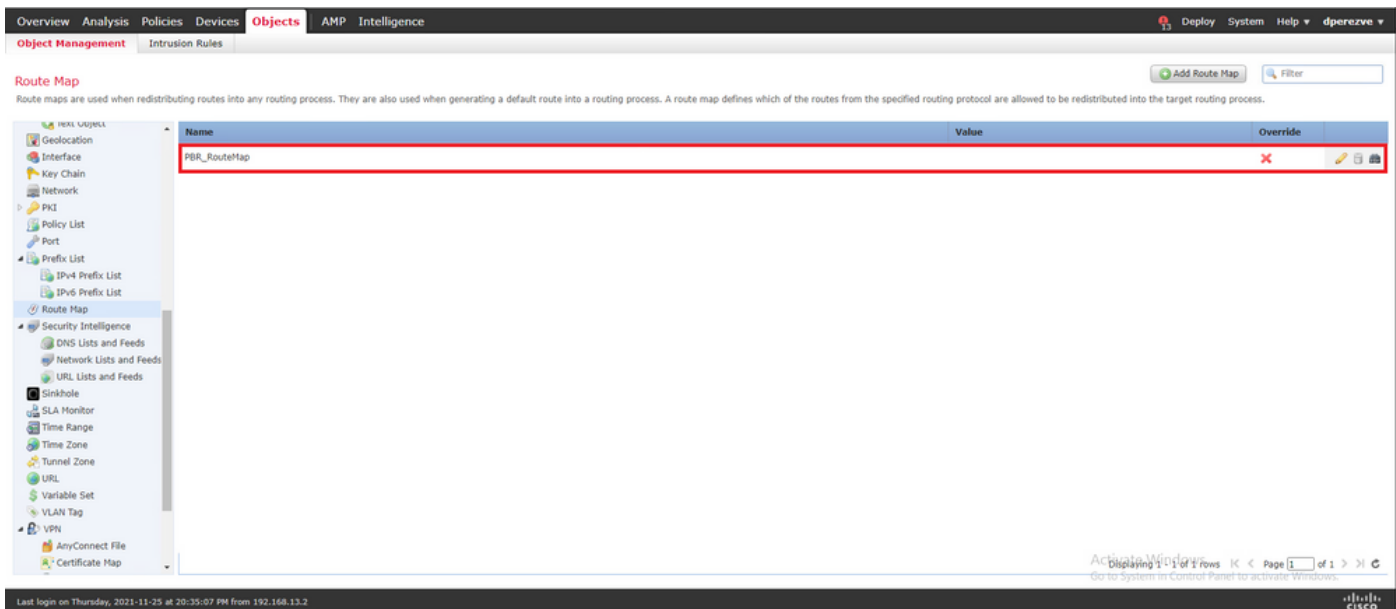
手順1で作成したアクセスリストオブジェクトを選択します。

クリック Add をクリックしてエントリを作成します。

注:FTDは最大65536(0 ~ 65535)の異なるエントリをサポートします。数値が小さいほど、プライオリティ評価が最も高くなります。



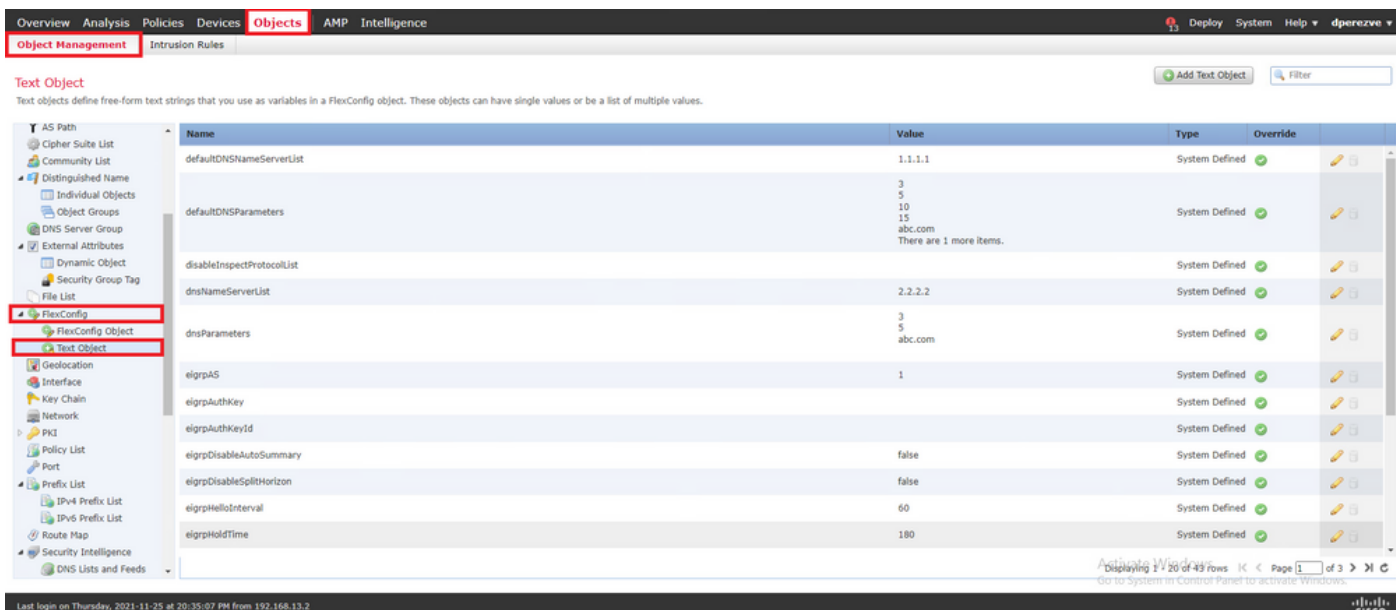
クリック Save. オブジェクトをオブジェクトリストに追加します。



ステップ 3 : FlexConfigテキストオブジェクトの設定

次の手順では、各回線のデフォルトゲートウェイを表すFlexConfigテキストオブジェクトを定義します。これらのテキストオブジェクトは、PBRとSLAを関連付けるFlexConfigオブジェクトの設定で後から使用されます。

FlexConfigテキストオブジェクトを定義するには、 **Objects > Object Management** を選択し、 **Text Object** 下に **FlexConfig** 目次のカテゴリ。



クリック **Add Text Object** .内 **Add Text Object** ウィンドウで、プライマリゲートウェイを表すオブジェクトの名前を割り当て、このデバイスのIPv4アドレスを指定します。

クリック **Save** 新しいオブジェクトを追加します。

Object Management | Intrusion Rules

Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Add Text Object

Name: Primary_GW

Description:

Variable Type: Single Count: 1

1 10.88.243.1

Allow Overrides:

Save Cancel

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	<input checked="" type="checkbox"/>
defaultDNSParameters		System Defined	<input checked="" type="checkbox"/>
disableInspectProtocolList		System Defined	<input checked="" type="checkbox"/>
dnsNameServerList		System Defined	<input checked="" type="checkbox"/>
dnsParameters		System Defined	<input checked="" type="checkbox"/>
eigrpAS		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKey		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKeyId		System Defined	<input checked="" type="checkbox"/>
eigrpDisableAutoSummary		System Defined	<input checked="" type="checkbox"/>
eigrpDisableSplitHorizon	false	System Defined	<input checked="" type="checkbox"/>
eigrpHelloInterval	60	System Defined	<input checked="" type="checkbox"/>
eigrpHoldTime	180	System Defined	<input checked="" type="checkbox"/>

Displaying 1 - 20 of 43 rows Page 1 of 3

Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

クリック **Add Text Object** 2番目のオブジェクトを再度作成するため、今回はバックアップ回線上のゲートウェイに対して作成します。

新しいオブジェクトに適切な名前とIPアドレスを入力し、 **Save** .

Object Management | Intrusion Rules

Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Add Text Object

Name: Secondary_GW

Description:

Variable Type: Single Count: 1

1 10.31.124.1

Allow Overrides:

Save Cancel

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	<input checked="" type="checkbox"/>
defaultDNSParameters		System Defined	<input checked="" type="checkbox"/>
disableInspectProtocolList		System Defined	<input checked="" type="checkbox"/>
dnsNameServerList		System Defined	<input checked="" type="checkbox"/>
dnsParameters		System Defined	<input checked="" type="checkbox"/>
eigrpAS		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKey		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKeyId		System Defined	<input checked="" type="checkbox"/>
eigrpDisableAutoSummary		System Defined	<input checked="" type="checkbox"/>
eigrpDisableSplitHorizon	false	System Defined	<input checked="" type="checkbox"/>
eigrpHelloInterval	60	System Defined	<input checked="" type="checkbox"/>
eigrpHoldTime	180	System Defined	<input checked="" type="checkbox"/>
eigrpIntfList		System Defined	<input checked="" type="checkbox"/>

Displaying 1 - 20 of 44 rows Page 1 of 3

Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2

2つのオブジェクトは、デフォルトオブジェクトとともにリストに追加する必要があります。

Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
Primary_GW	10.88.243.1	User Defined	<input checked="" type="checkbox"/>
Secondary_GW	10.31.124.1	User Defined	<input checked="" type="checkbox"/>

ステップ 4 : SLAモニタの設定

各ゲートウェイへの接続の監視に使用するSLAオブジェクトを定義するには、次のURLに移動します。 **Objects > Object Management** を選択し、 **SLA Monitor** 目次を参照してください。

SLA Monitor

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
No records to display	

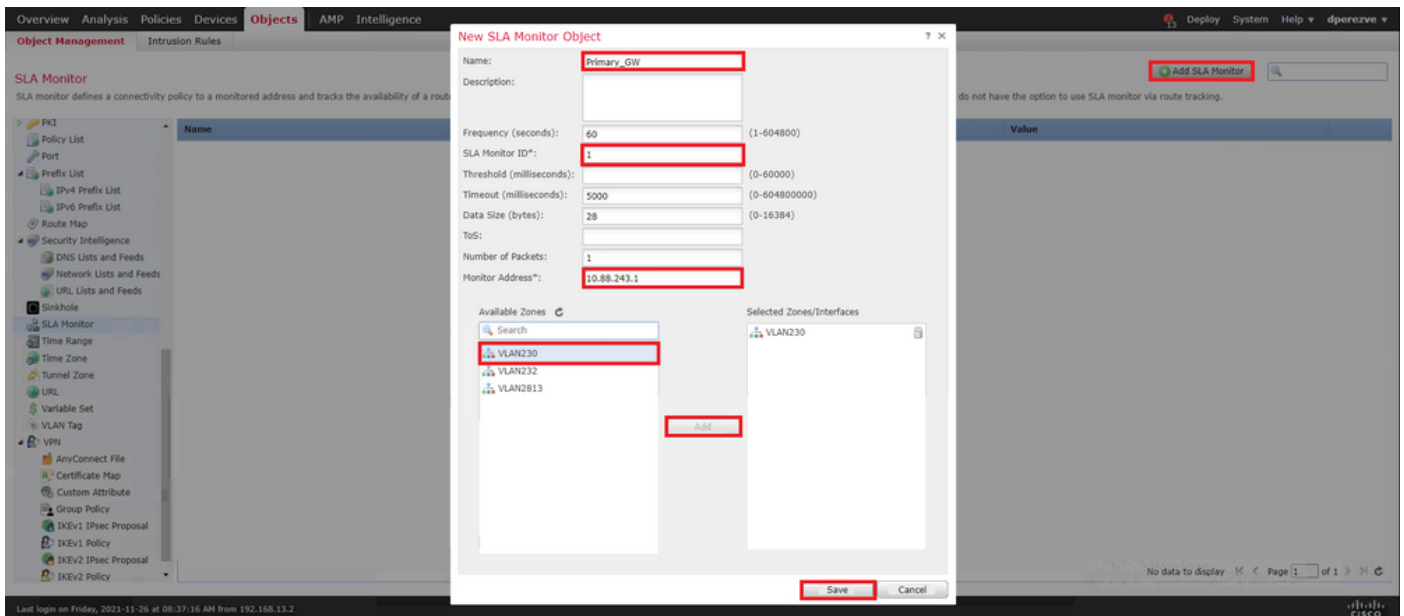
次のいずれかを選択します。 **Add SLA Monitor Object**.

内 **New SLA Monitor** ウィンドウで、SLAオペレーションのID、監視する必要があるデバイスのIPアドレス (この場合はプライマリゲートウェイ)、およびデバイスに到達できるインターフェイスまたはゾーンとともに名前を定義します。

また、タイムアウトとしきい値を調整することもできます。クリック **Save** .

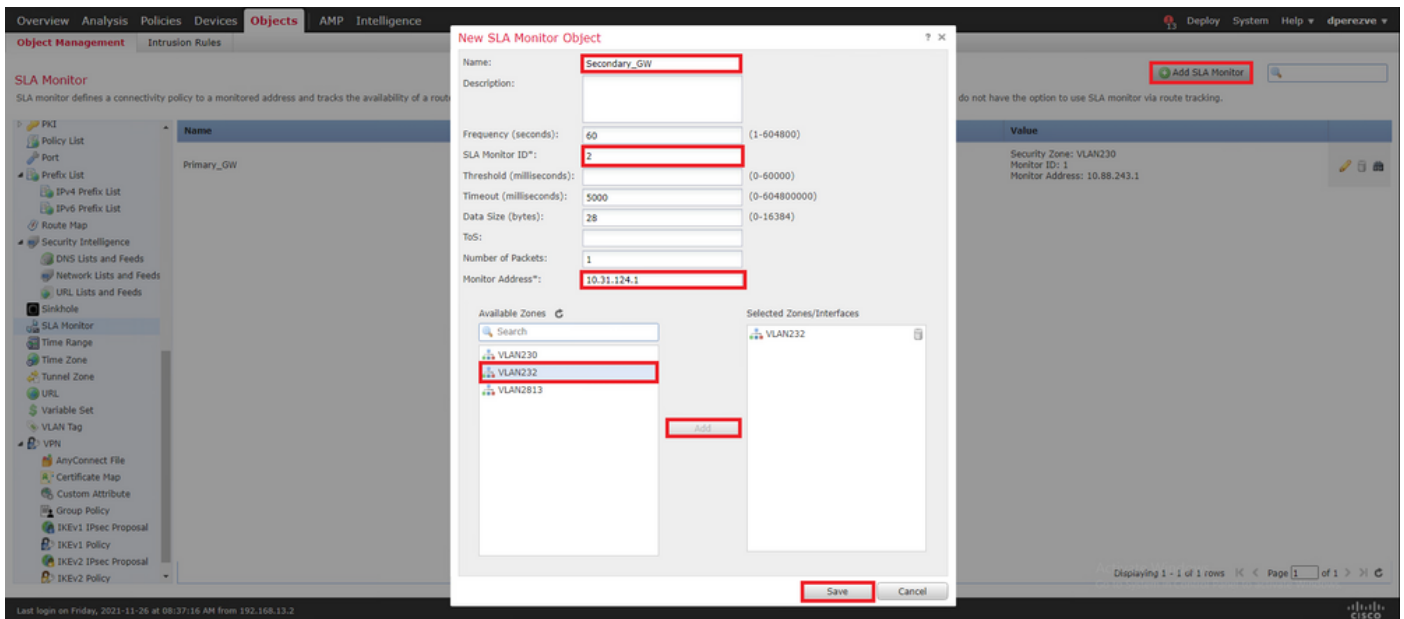
注:FTDは最大2000のSLA動作をサポートします。SLA IDの値の範囲は1 ~ 2147483647です。

注 : タイムアウト値としきい値が指定されていない場合、FTDはデフォルトのタイマーを使用します (それぞれの場合は5000ミリ秒)。

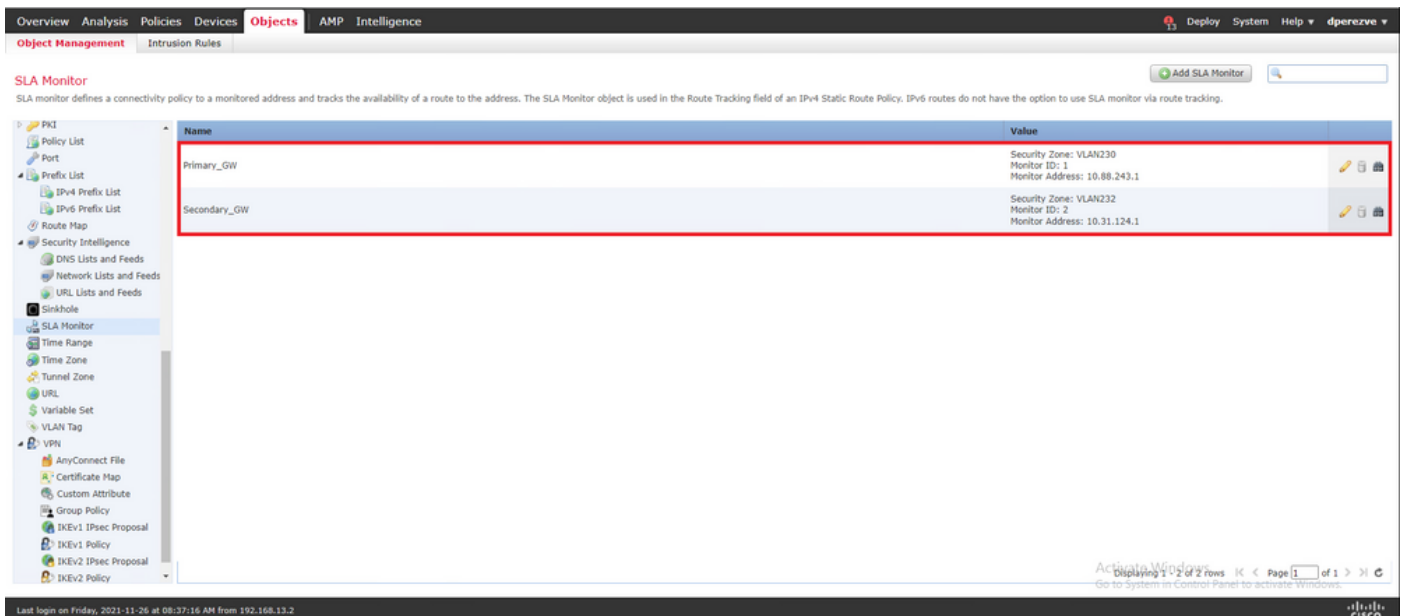


次のいずれかを選択します。Add SLA Monitor ボタンをもう一度押して2番目のオブジェクトを作成します。今度はバックアップ回線のゲートウェイ用です。

新しいオブジェクトに適切な情報を入力し、SLA IDがプライマリゲートウェイに定義されたものと異なることを確認して、変更を保存します。



2つのオブジェクトをリストに追加する必要があります。

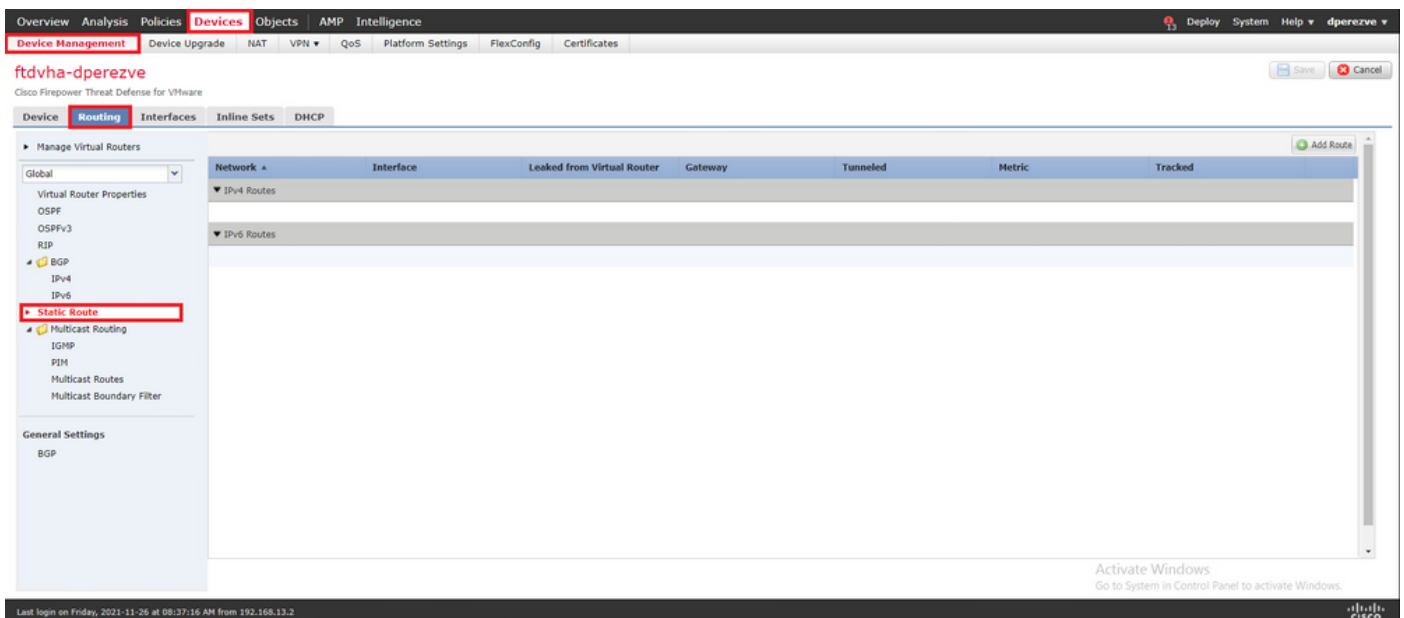


ステップ 4 : ルートトラックを使用したスタティックルートの設定

IP SLAオブジェクトが作成されたら、各ゲートウェイのルートを定義し、SLAに関連付けます。

これらのルートは、実際には内部から外部への接続を提供しません（すべてのルーティングはPBRを介して実行されます）。代わりに、SLAを介したゲートウェイへの接続を追跡するために必要です。

スタティックルートを設定するには、**Devices > Device Management** で手元のFTDを編集し、**Static Route** 目次の中の **Routing** tab.

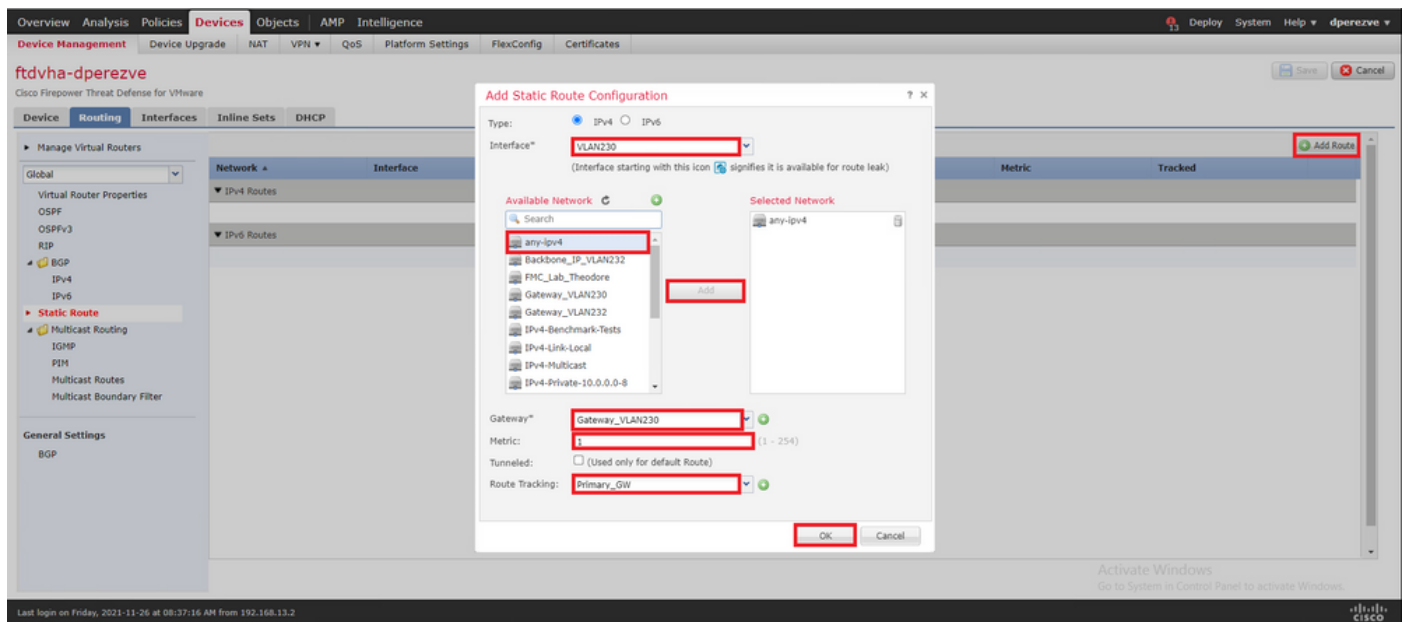


内 **Add Static Route Configuration** ウィンドウの[Interface] ドロップダウンで、プライマリゲートウェイに到達できる必要があるインターフェイスの名前を指定します。

次に、宛先ネットワークとプライマリゲートウェイを **Gateway** をクリックします。

ルートのメトリックを指定し、**Route Track** ドロップダウンをクリックし、手順3で作成したプライマリゲートウェイのSLAオブジェクトを選択します。

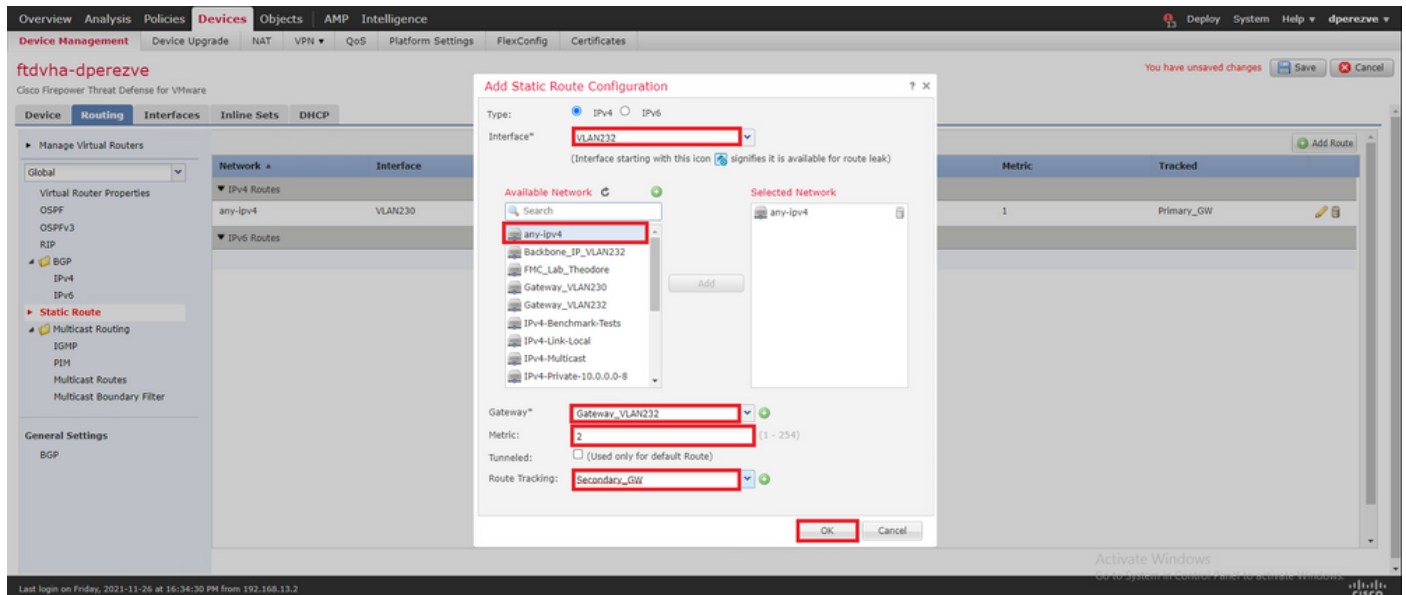
OKをクリックして、新しいルートを追加します。



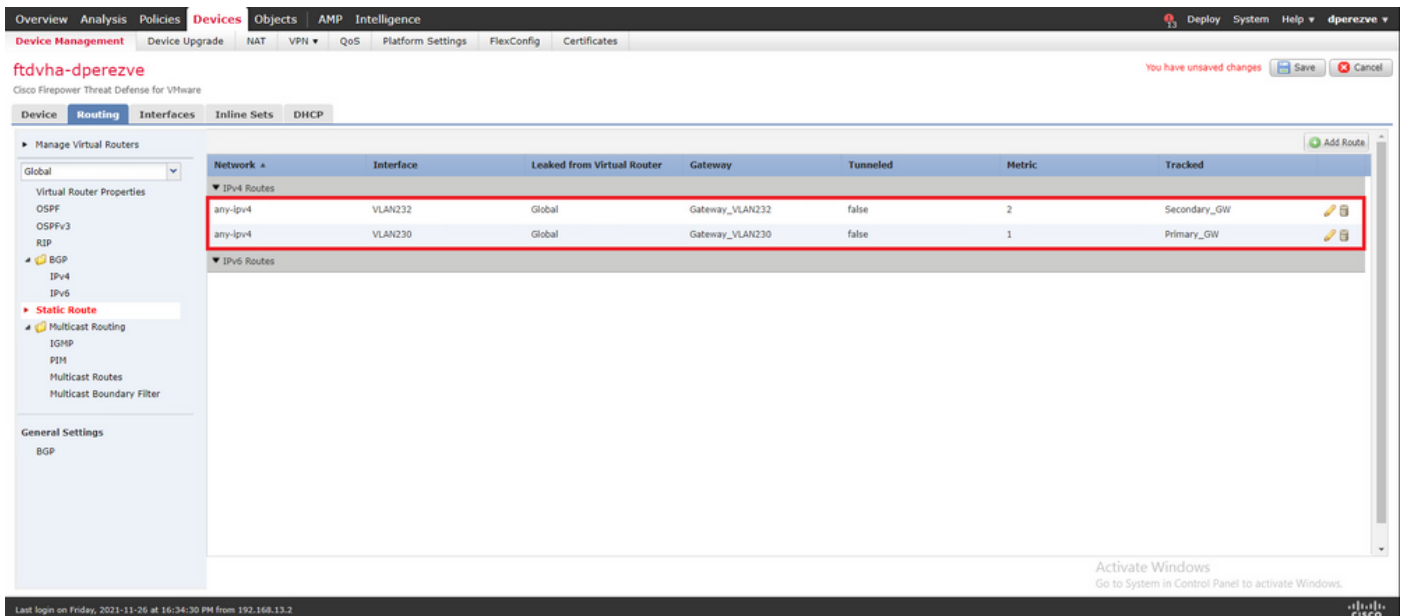
バックアップゲートウェイ用に2番目のスタティックルートを設定する必要があります。

クリック **Add Route** 新しいスタティックルートを定義します。

次の項目を入力します **Add Static Route Configuration** バックアップゲートウェイに関する情報を含め、このルートのメトリックが最初のルートで設定されたメトリックよりも高いことを確認します。



2つのルートをリストに追加する必要があります。

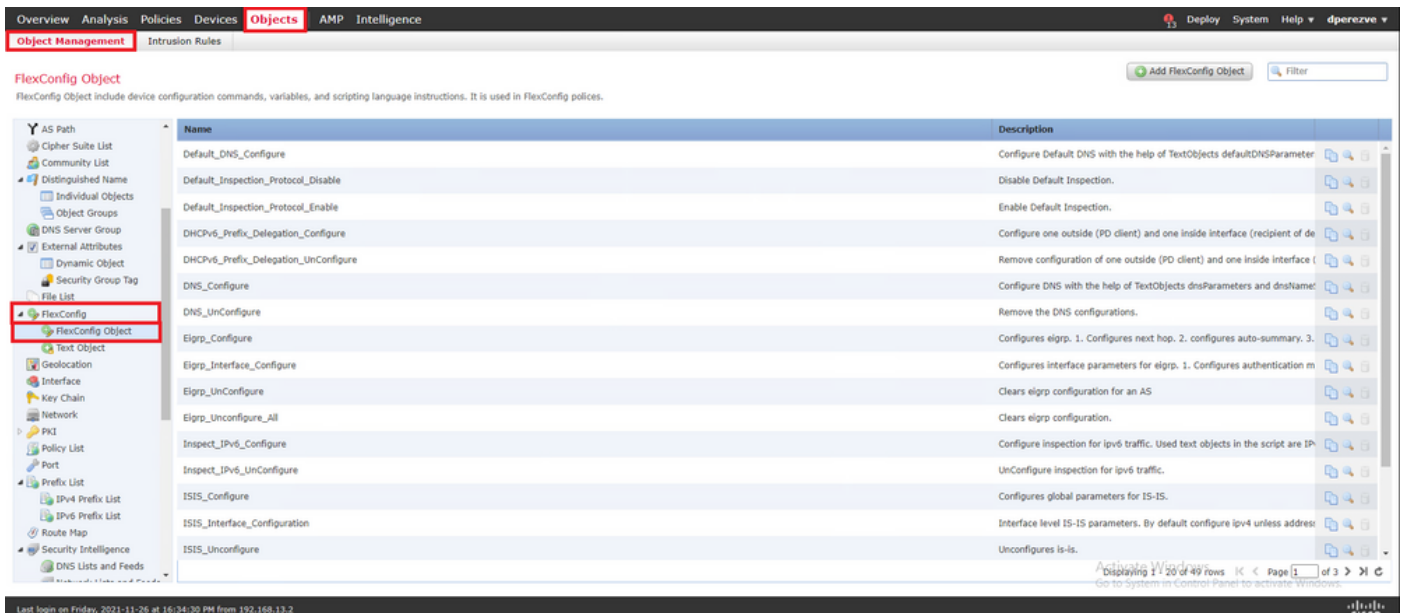


ステップ 5 : PBR FlexConfigオブジェクトの設定

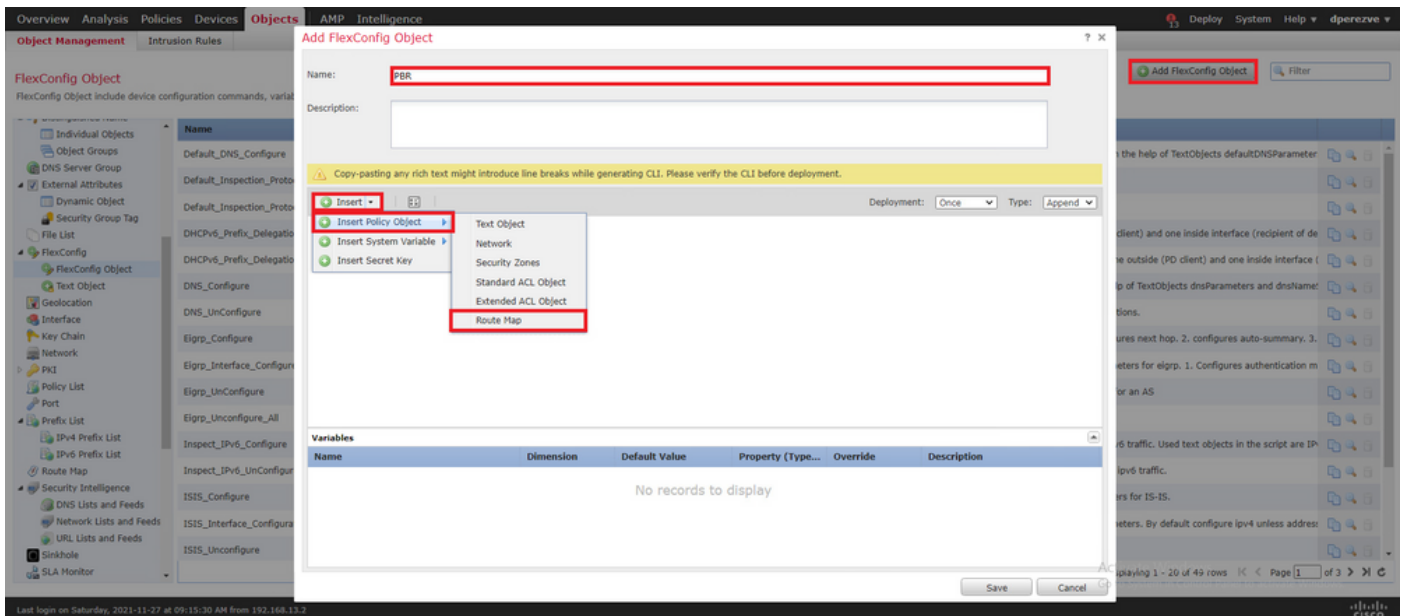
PBRに使用されるルートマップでSLAを有効にし、このルートマップをFTDのインターフェイスに適用します。

これまでのところ、ルートマップは、一致基準を定義するアクセスリストにのみ関連付けられています。ただし、最後の調整はFMC GUIではサポートされていないため、FlexConfigオブジェクトが必要です。

PBR FlexConfigオブジェクトを定義するには、**Objects > Object Management** を選択し、**FlexConfig Object** 下に **FlexConfig** 目次のカテゴリ。

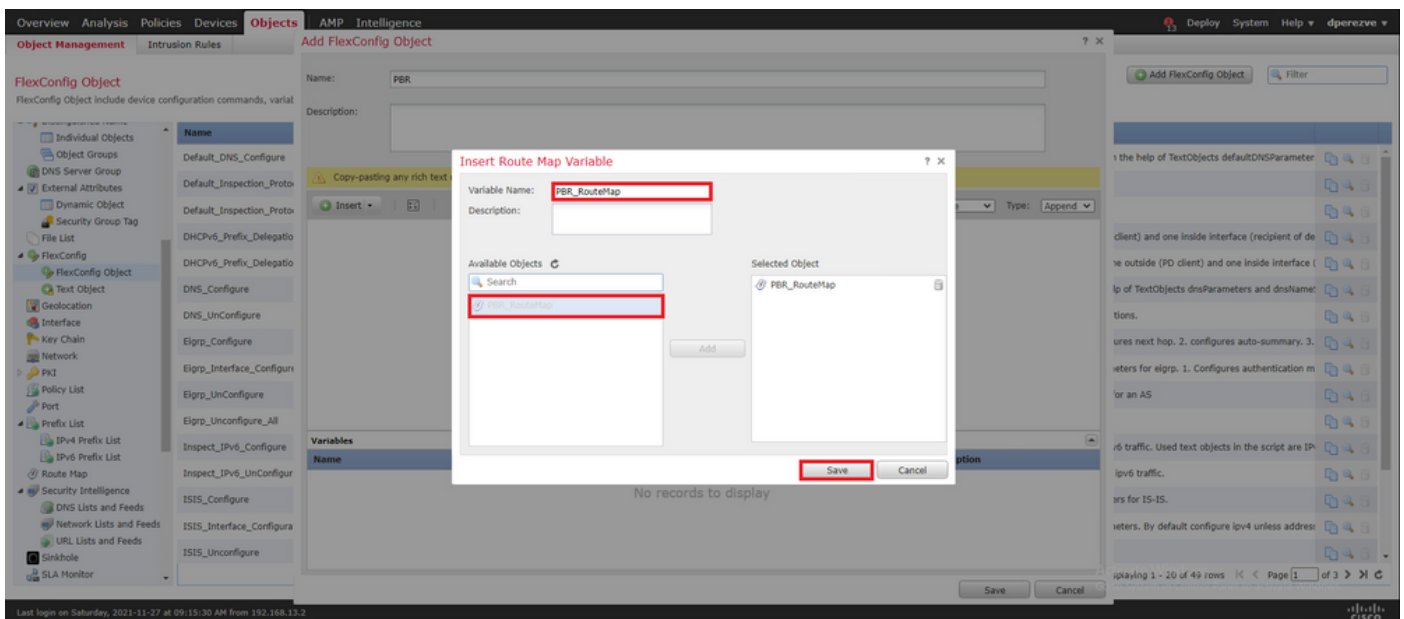


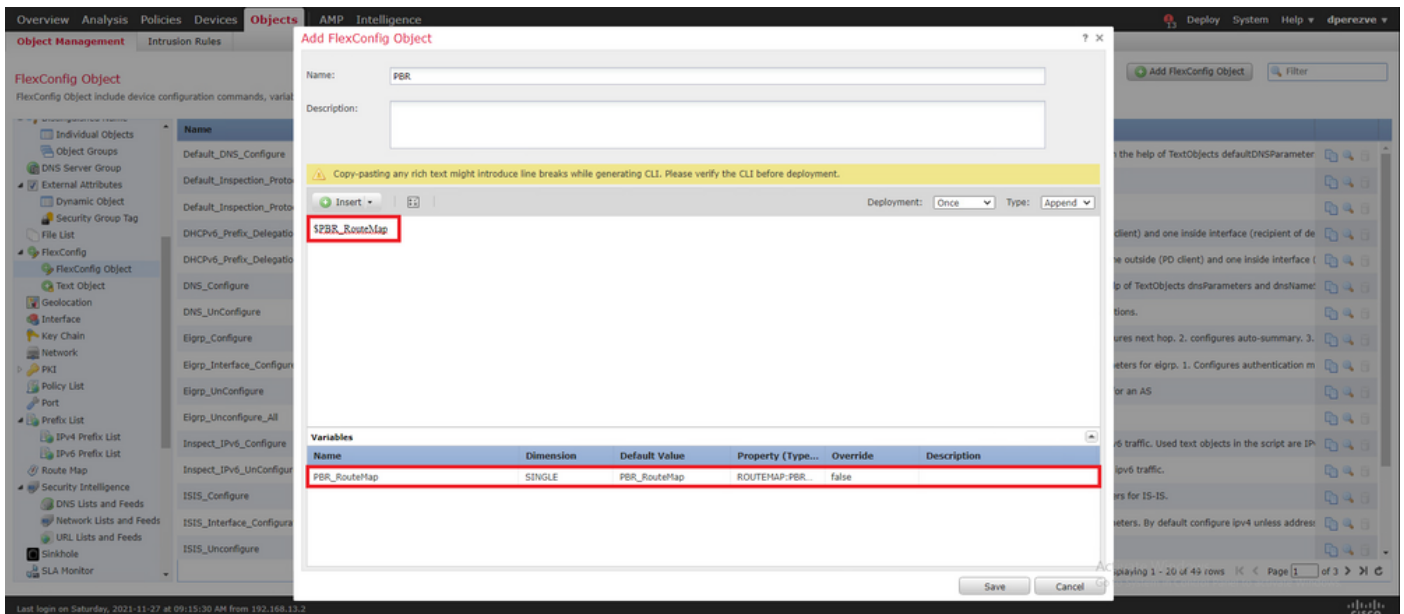
次のいずれかを選択します。 **Add FlexConfig Object** をクリックして、クエリーを実行します。内 **Add FlexConfig Object** ウィンドウに名前を割り当て、 **Insert > Insert Policy Object > Route Map** .



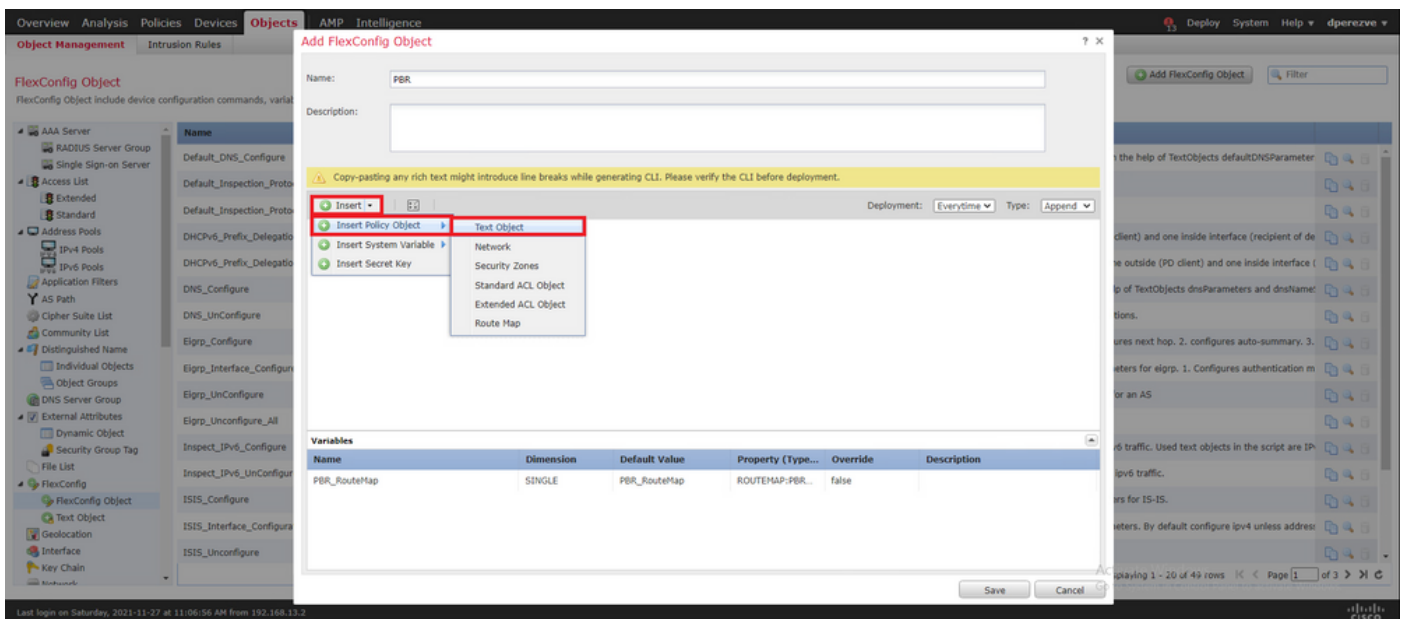
内 Insert Route Map Variable ウィンドウで、変数に名前を割り当て、手順2で作成したPBRオブジェクトを選択します。

クリック save FlexConfigオブジェクトの一部としてルートマップを追加します。



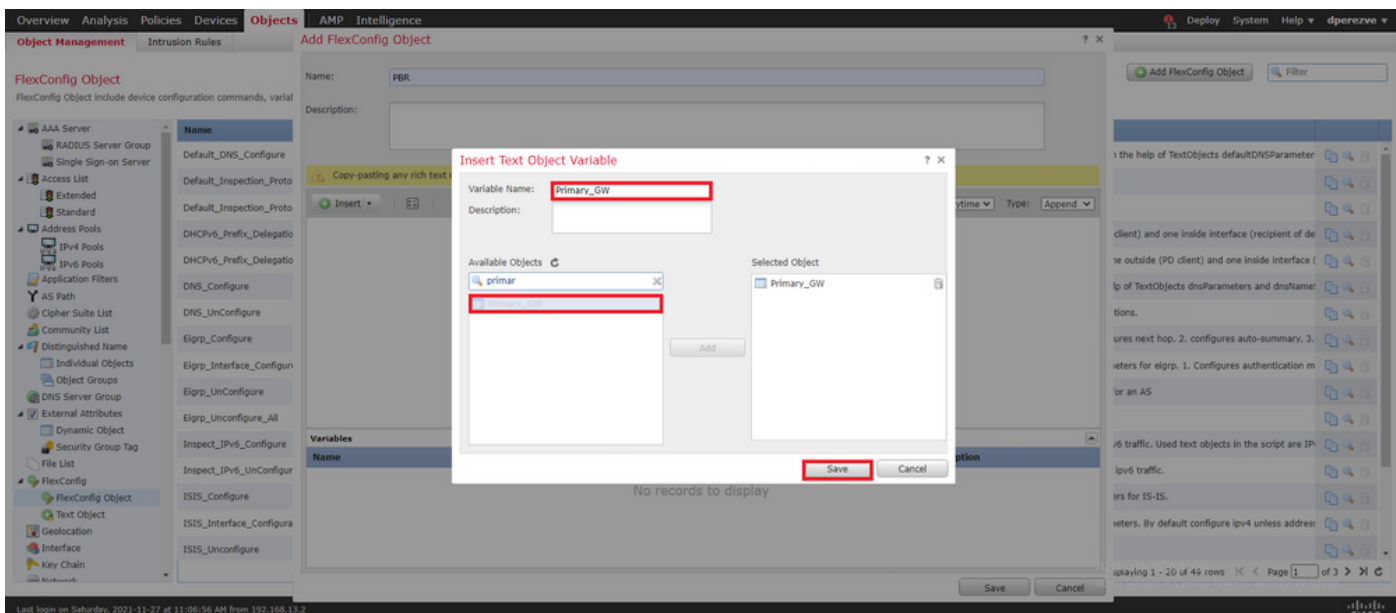


ルートマップ変数の他に、各ゲートウェイ（ステップ3で定義）を表すFlexConfigテキストオブジェクトを追加する必要があります。内 Add FlexConfig Object ウィンドウの移動 Insert > Insert Policy Object > Text Object .

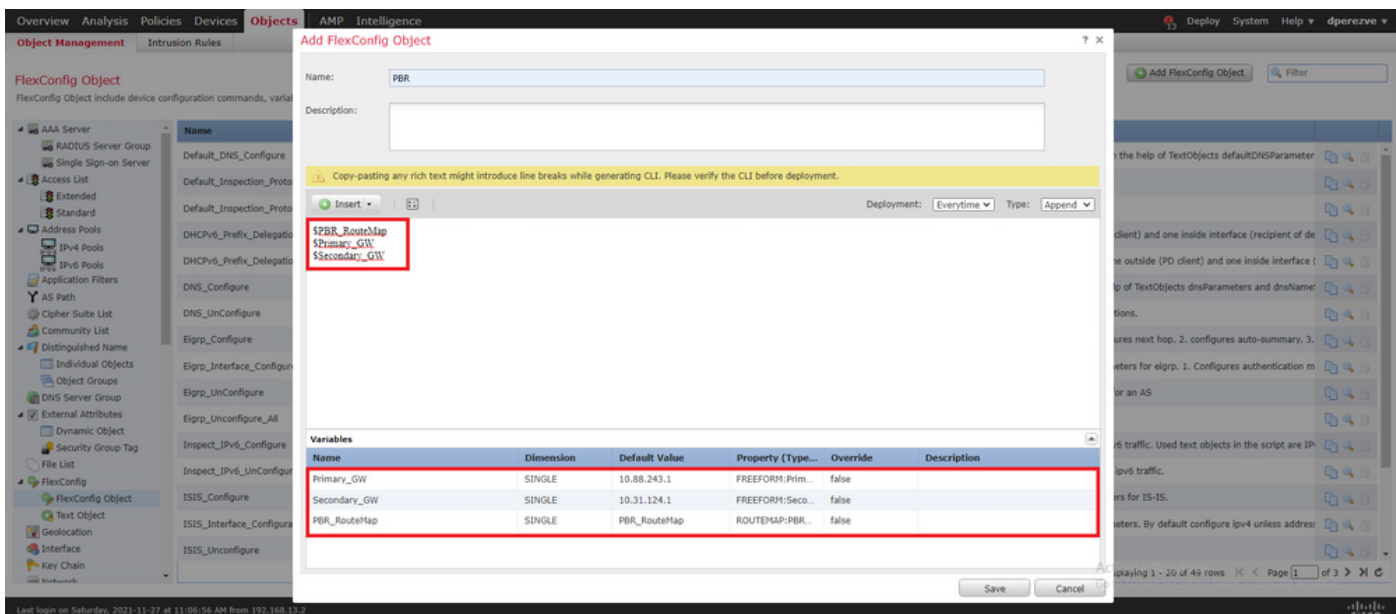


内 Insert Text Object Variable window変数に名前を割り当て、ステップ3で定義したプライマリゲートウェイを表すテキストオブジェクトを選択します。

クリック Save ボタンをクリックします。



バックアップゲートウェイに対して、これらの最後の手順を繰り返します。プロセスの最後に、2つの変数をFlexConfigオブジェクトに追加する必要があります。

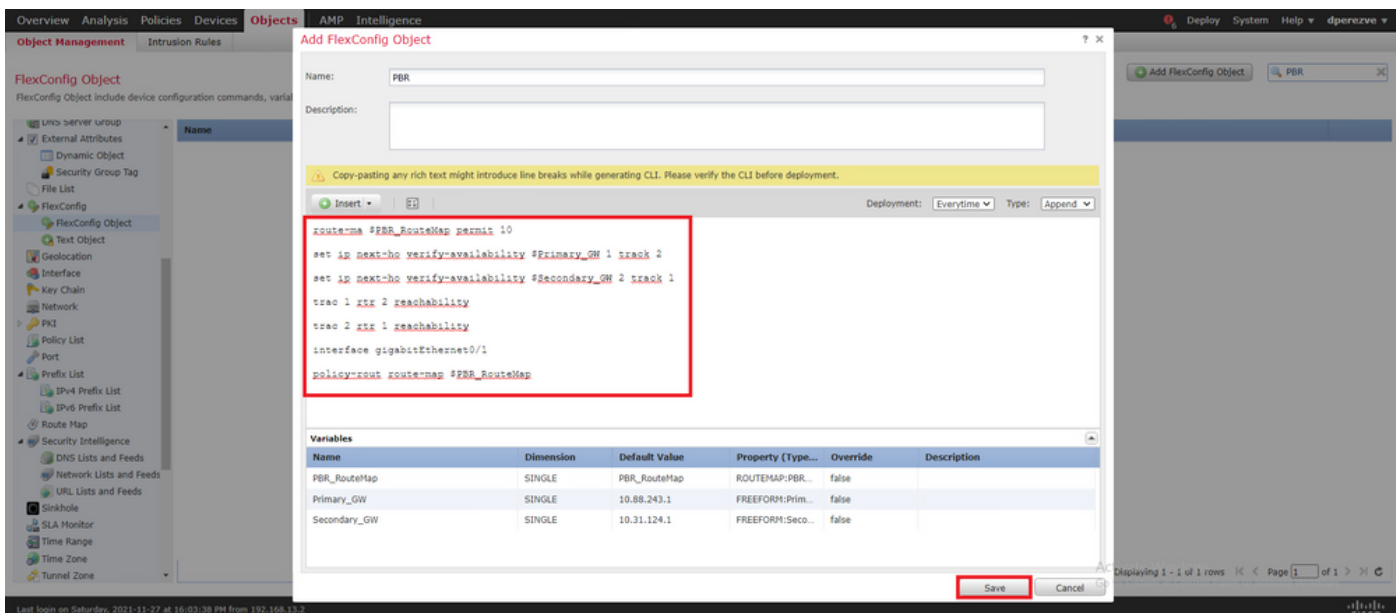


PBR設定の構文は、Cisco ASAと同じである必要があります。ルートマップのシーケンス番号は、ステップ2 (この場合は10) で設定したシーケンス番号とSLA IDと一致する必要があります。

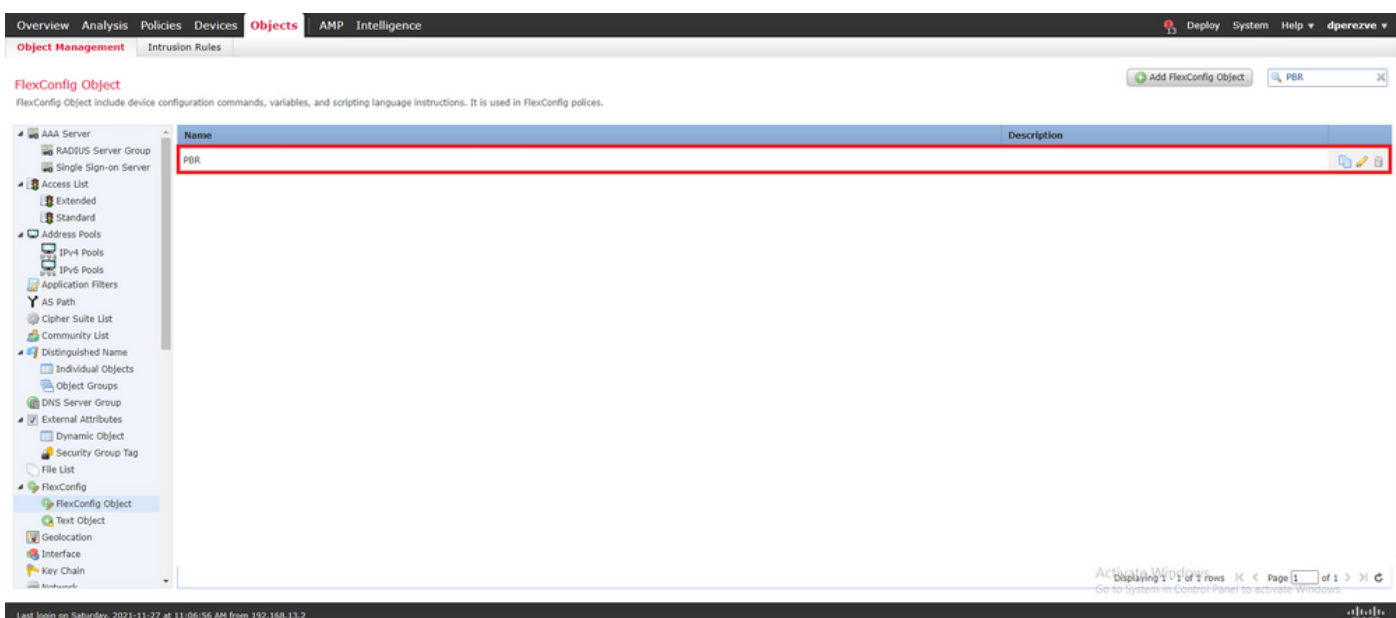
ネクストホップの可用性を確認するようにPBRを設定するには、`set ip next-hop verify-availability` コマンドを使用する必要があります。

内部インターフェイス (この場合はVLAN2813) にルートマップを適用する必要があります。利用 `policy-route route-map` コマンドを発行します。

クリック **Save** 設定が完了したら、



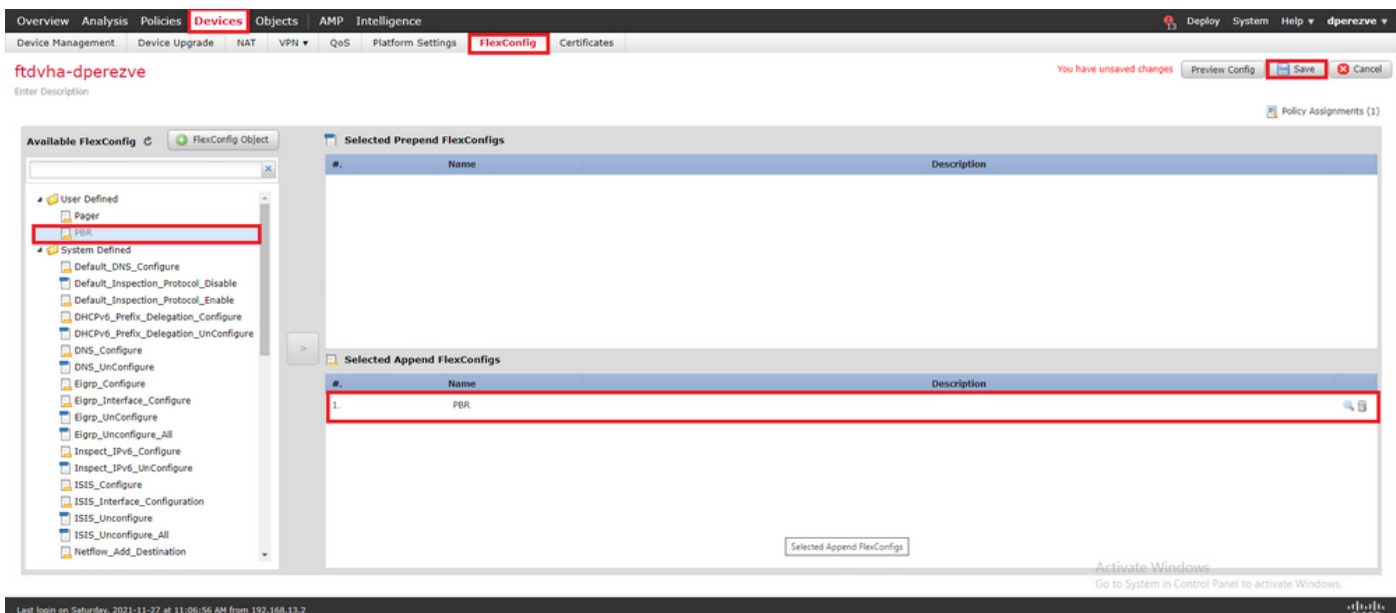
FlexConfigオブジェクトをリストに追加する必要があります。



手順 6 : FlexConfigポリシーへのPBR FlexConfigオブジェクトの割り当て

移動先 **Devices > FlexConfig FlexConfigポリシー**を編集します。

PBR FlexConfigオブジェクトを選択します。 Available FlexConfig 目次、変更の保存、およびFTDへの変更の展開を行います。



確認

導入が完了すると、FTDは到達可能性を確保するために、監視対象デバイスに定期的なICMPエコー要求を送信する必要があります。その間、プライマリゲートウェイへのトラッキング対象ルートをルーティングテーブルに追加する必要があります。

```
firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address
(access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2 [up]
ip next-hop verify-availability 10.31.124.1 2 track 1 [up]
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
Gateway of last resort is 10.88.243.1 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [1/0] via 10.88.243.1,
VLAN230 C 10.31.124.0 255.255.255.0 is directly connected,
VLAN232 L 10.31.124.25 255.255.255.255 is directly connected,
VLAN232 C 10.88.243.0 255.255.255.0 is directly connected,
VLAN230 L 10.88.243.60 255.255.255.255 is directly connected,
VLAN230 C 192.168.13.0 255.255.255.0 is directly connected,
VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected,
VLAN2813
```

プライマリゲートウェイへの接続がアップしているため、内部サブネット(VLAN2813)からのトラフィックはプライマリISP回線を経由して転送する必要があります。

```
firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed
Phase: 1 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop verify-availability 10.31.124.1 2 track 1
Additional Information: Matched route-map PBR_RouteMap, sequence 10, permit Found next-hop 10.88.243.1 using egress ifc VLAN230
Phase: 2 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic
Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any
Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection
```

advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176701, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,

port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,

```
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN230(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=176711, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=anyError: not enough buffer space to print ASP rule Result: input-interface: VLAN2813(vrfid:0) input-status: up input-line-status: up output-interface: VLAN230(vrfid:0) output-status: up output-line-status: up Action: allow
```

FTDがSLAモニタオブジェクトで指定されたしきい値タイマー内にプライマリゲートウェイからエコー応答を受信しない場合、ホストは到達不能と見なされ、ダウンとしてマークされます。プライマリゲートウェイへのトラッキング対象ルートも、バックアップピアへのトラッキング対象ルートに置き換えられます。

```
firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address (access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2 [down] ip next-hop verify-availability 10.31.124.1 2 track 1 [up] 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 Gateway of last resort is 10.31.124.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [2/0] via 10.31.124.1, VLAN232 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25 255.255.255.255 is directly connected, VLAN232 C 192.168.13.0 255.255.255.0 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813
```

情報メッセージ622001は、FTDがルーティングテーブルにトラッキング対象ルートを追加または削除するたびに生成されます。

```
firepower# show logg | i 622001 %FTD-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.31.124.1, distance 2, table default, on interface VLAN232%FTD-6-305012: Teardown dynamic UDP translation from VLAN2813:192.168.13.5/49641 to VLAN230:10.88.243.60/49641 duration 0:02:10
```

これで、VLAN2813からのすべてのトラフィックは、バックアップISP回線を介して転送される必要があります。

```
firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed Phase: 1 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop verify-availability 10.31.124.1 2 track 1 Additional Information: Matched route-map PBR_RouteMap, sequence 10, permit Found next-hop 10.31.124.1 using egress ifc VLAN232 Phase: 2 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
```

deny=false hits=177180, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic

VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),

```
output_ifc=VLAN232(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177190, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Result: input-interface:
VLAN2813(vrfid:0) input-status: up input-line-status: up output-interface: VLAN232(vrfid:0)
output-status: up output-line-status: up Action: allow
```

トラブルシューティング

どのPBRエントリが適用されているかを検証するため、**interesting traffic debug policy-route**コマンドを実行します。

```
firepower# debug policy-route debug policy-route enabled at level 1 firepower# pbr: policy based
route lookup called for 192.168.13.5/45951 to 208.67.220.220/53 proto 17 sub_proto 0 received on
interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule from ACL(2) pbr: route map
PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr: evaluating verified next-hop
10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230 : next_hop = 10.88.243.1
pbr: policy based route lookup called for 192.168.13.5/56099 to 208.67.220.220/53 proto 17
sub_proto 0 received on interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule from
ACL(2) pbr: route map PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr:
evaluating verified next-hop 10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230
: next_hop = 10.88.243.1 pbr: policy based route lookup called for 192.168.13.2/24 to 8.8.8.8/0
proto 1 sub_proto 8 received on interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule
from ACL(2) pbr: route map PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr:
evaluating verified next-hop 10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230
: next_hop = 10.88.243.1 pbr: policy based route lookup called for 192.168.13.5/40669 to
208.67.220.220/53 proto 17 sub_proto 0 received on interface VLAN2813, NSGs, nsg_id=none
```


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。