Configuration de PBR avec des SLA IP pour DOUBLE FAI sur FTD géré par FMC

Table des matières

- Introduction
  - Exigences
  - Composants utilisés
  - Informations générales
- Configurer
  - Diagramme du réseau
  - Configurations
    - Étape 1 : configuration de la liste d'accès PBR
    - Étape 2 : configuration de la carte de routage PBR
    - Étape 3 : configuration des objets texte FlexConfig
    - Étape 4 : configuration du SLA Monitor
    - Étape 4 : configuration des routes statiques avec la piste de routage
    - Étape 5. Configuration de l'objet PBR FlexConfig
    - Étape 6. Attribution de l'objet FlexConfig PBR à la stratégie FlexConfig
- Vérifier
- Dépannage

Introduction

Ce document décrit comment configurer PBR avec les IP SLA sur un FTD qui est géré par (FMC).

Contribution de Daniel Perez Verti Vazquez, ingénieur du centre d'assistance technique de Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration PBR activée **Cisco Adaptive Security Appliance (ASA)**
- FlexConfig activé **Firepower**
- SLA IP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD version 7.0.0 (build 94)

- Cisco FMC version 7.0.0 (build 94)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment configurer **Policy Based Routing (PBR)** avec **Internet Protocol Service Level Agreement (IP SLA)** sur un Cisco **Firepower Threat Defense (FTD)** qui est géré par Cisco Firepower Management Center (FMC).

Le routage traditionnel prend des décisions de transmission en fonction des adresses IP de destination uniquement. PBR est une alternative aux protocoles de routage et au routage statique.

Il offre un contrôle plus granulaire sur le routage, car il permet d'utiliser des paramètres tels que les adresses IP source ou les ports source et de destination comme critères de routage en plus de l'adresse IP de destination.

Les scénarios possibles pour PBR incluent des applications sensibles à la source ou le trafic sur des liaisons dédiées.

Parallèlement au PBR, les IP SLA peuvent être mis en oeuvre afin de garantir la disponibilité du tronçon suivant. Un IP SLA est un mécanisme qui surveille la connectivité de bout en bout par l'échange de paquets réguliers.

Au moment de la publication, PBR n'est pas directement pris en charge par FMC **Graphical User Interface (GUI)** , la configuration de la fonctionnalité nécessite l'utilisation de stratégies FlexConfig.

En revanche, seuls les contrats de niveau de service (**Internet Control Message Protocol (ICMP)** SLA) sont pris en charge par FTD.

Dans cet exemple, PBR est utilisé pour acheminer des paquets sur un **Internet Service Provider (ISP)** circuit principal en fonction de l'adresse IP source.

Entre-temps, un IP SLA surveille la connectivité et force un retour sur le circuit de secours en cas de défaillance.

Configurer

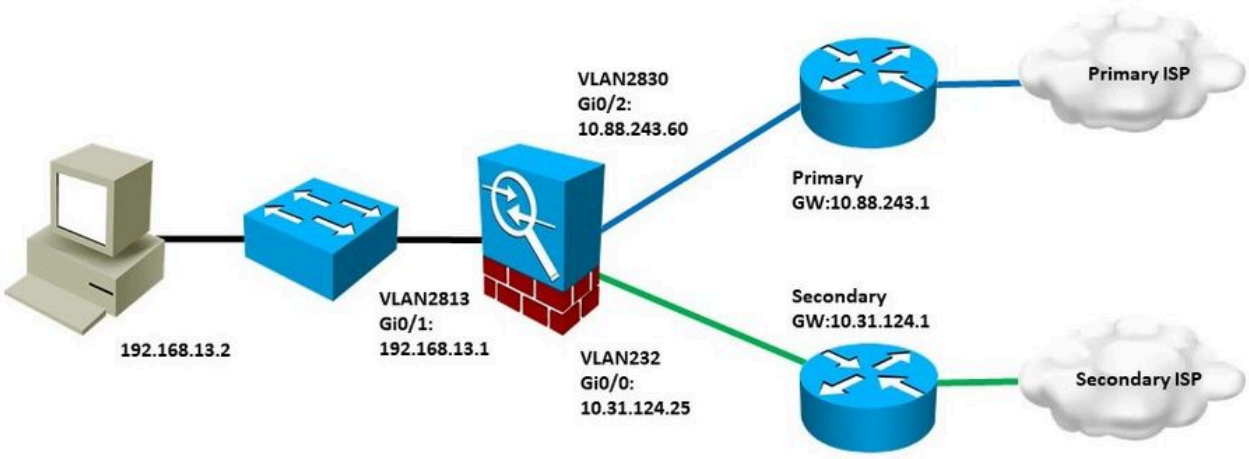
Diagramme du réseau

Dans cet exemple, Cisco FTD possède deux interfaces externes : VLAN230 et VLAN232. Chacun se connecte à un FAI différent.

Le trafic provenant du réseau interne VLAN2813 est acheminé via le FAI principal qui utilise PBR.

Le mappage de route PBR prend des décisions de transfert en fonction de l'adresse IP source uniquement (tout ce qui est reçu du VLAN2813 doit être routé vers 10.88.243.1 dans le VLAN230) et il est appliqué dans l'interface GigabitEthernet 0/1 de FTD.

En attendant, FTD utilise des SLA IP afin de surveiller la connectivité à chaque passerelle ISP. En cas de panne dans VLAN230, le FTD bascule vers le circuit de secours sur VLAN232.

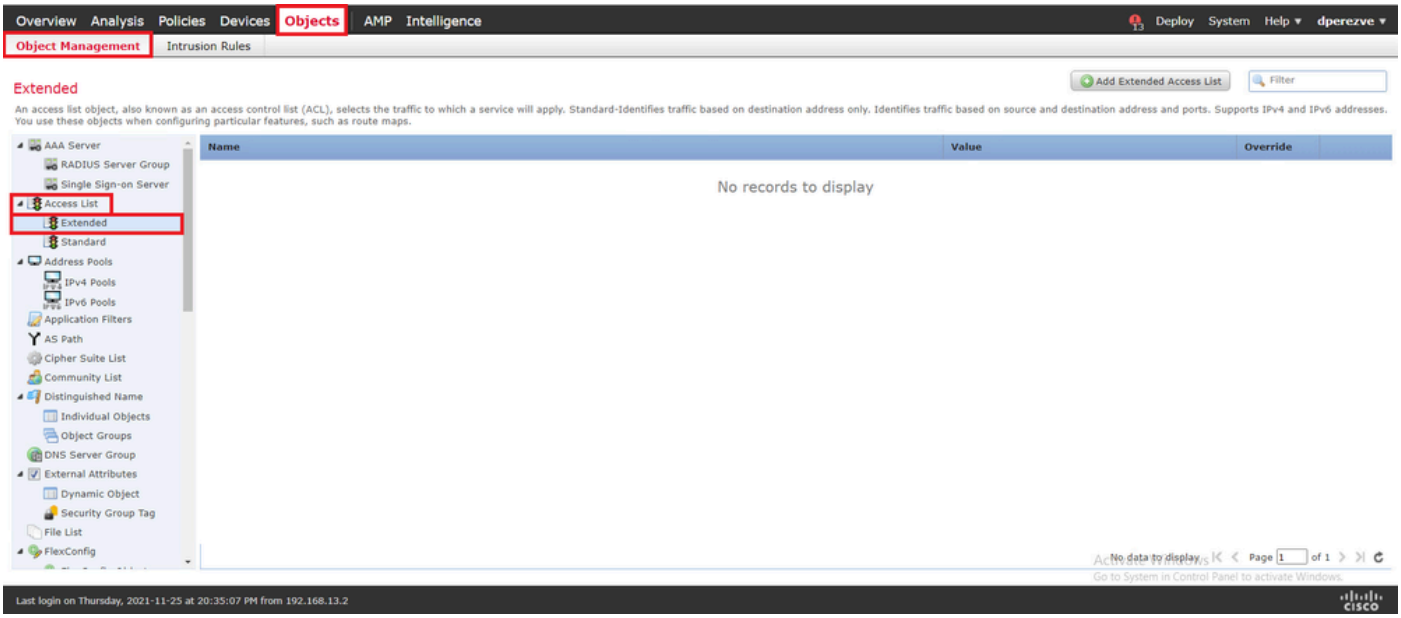


Configurations

Étape 1 : configuration de la liste d'accès PBR

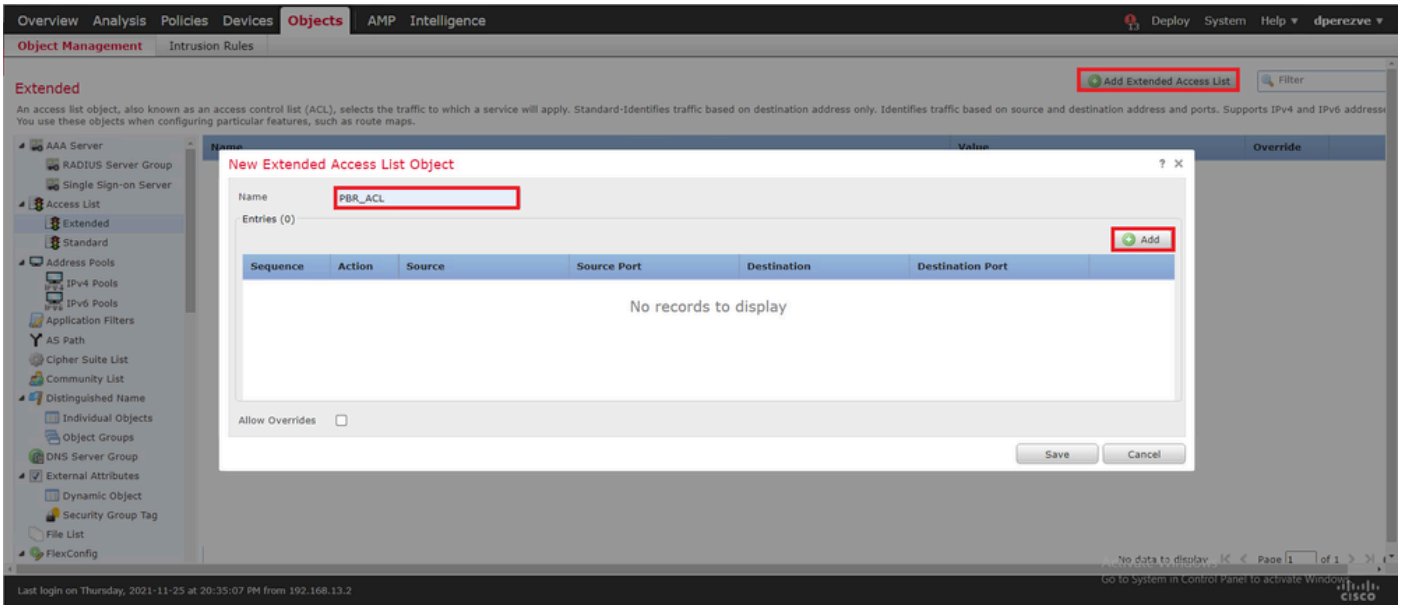
À la première étape de la configuration PBR, définissez quels paquets doivent faire l'objet de la politique de routage. PBR utilise des cartes de routage et des listes d'accès pour identifier le trafic.

Afin de définir une liste d'accès pour les critères correspondants naviguez jusqu'à **Objects** > **Object Management** et sélectionnez **Extended** sous la **Access List** catégorie dans la table des matières.



Cliquez sur **Add Extended Access List** . Dans la **New Extended Access List Object** fenêtre, attribuez un nom à

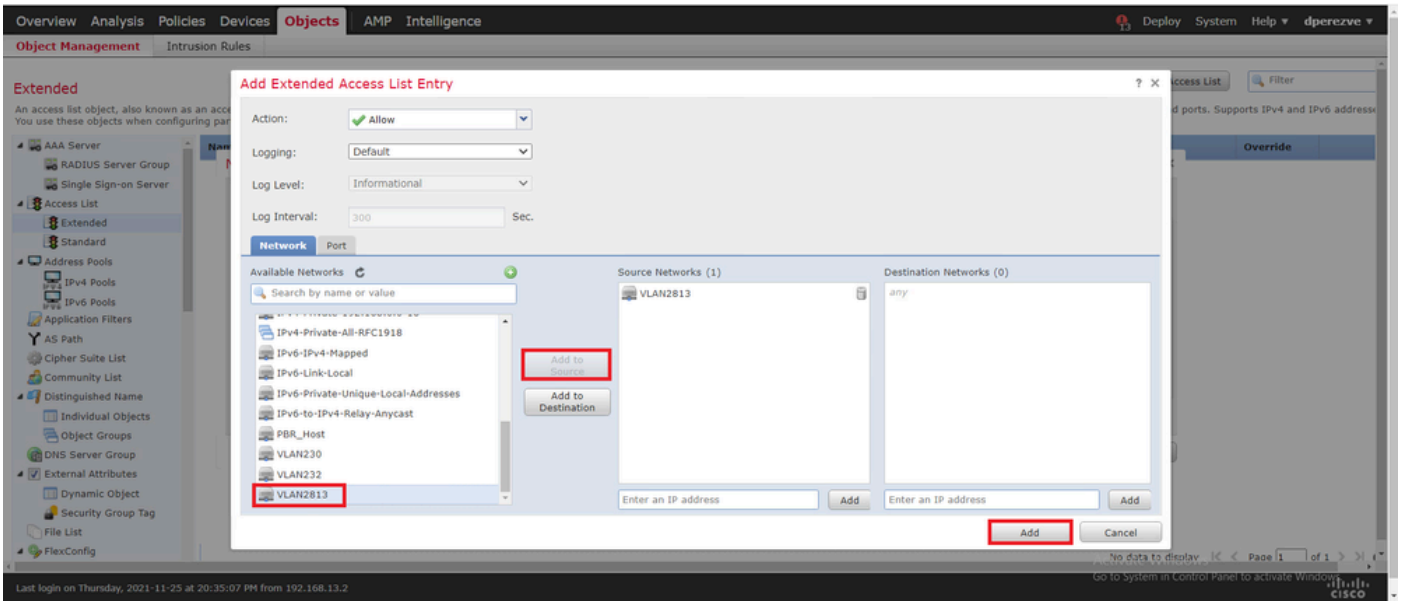
l'objet, puis sélectionnez le **Add** bouton afin de commencer avec la configuration de la liste d'accès.



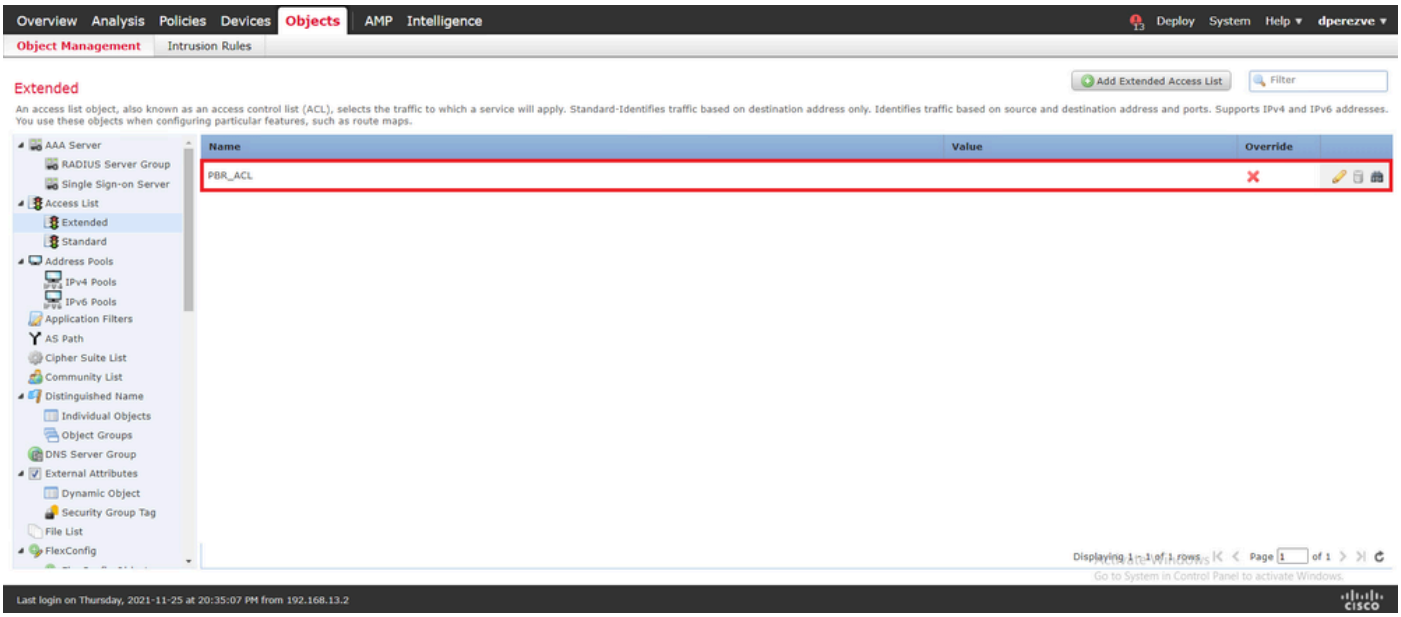
Dans la **Add Extended Access List Entry** fenêtre, sélectionnez l'objet qui représente le réseau interne, en l'occurrence VLAN2813.

Cliquez **Add to Source** sur cette option pour la définir comme source de la liste d'accès.

Cliquez sur **Add** pour créer l'entrée.



Cliquez sur **Save** . L'objet doit être ajouté à la liste d'objets.

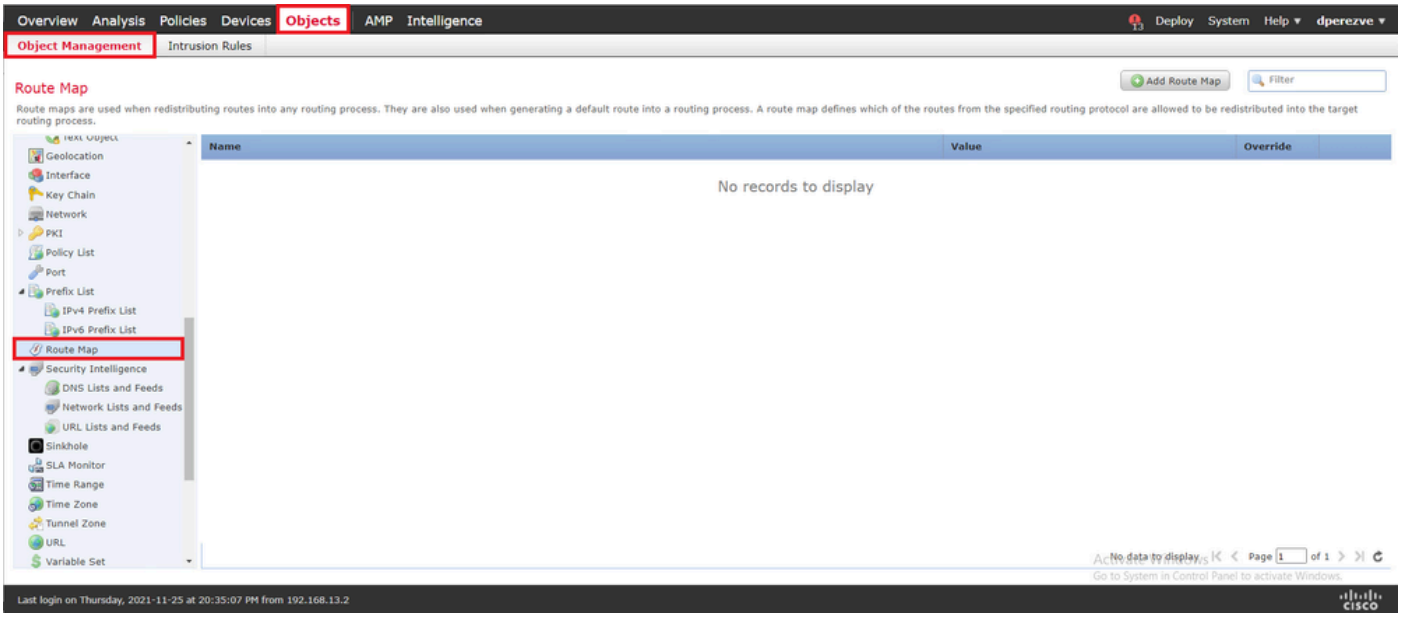


Étape 2 : configuration de la carte de routage PBR

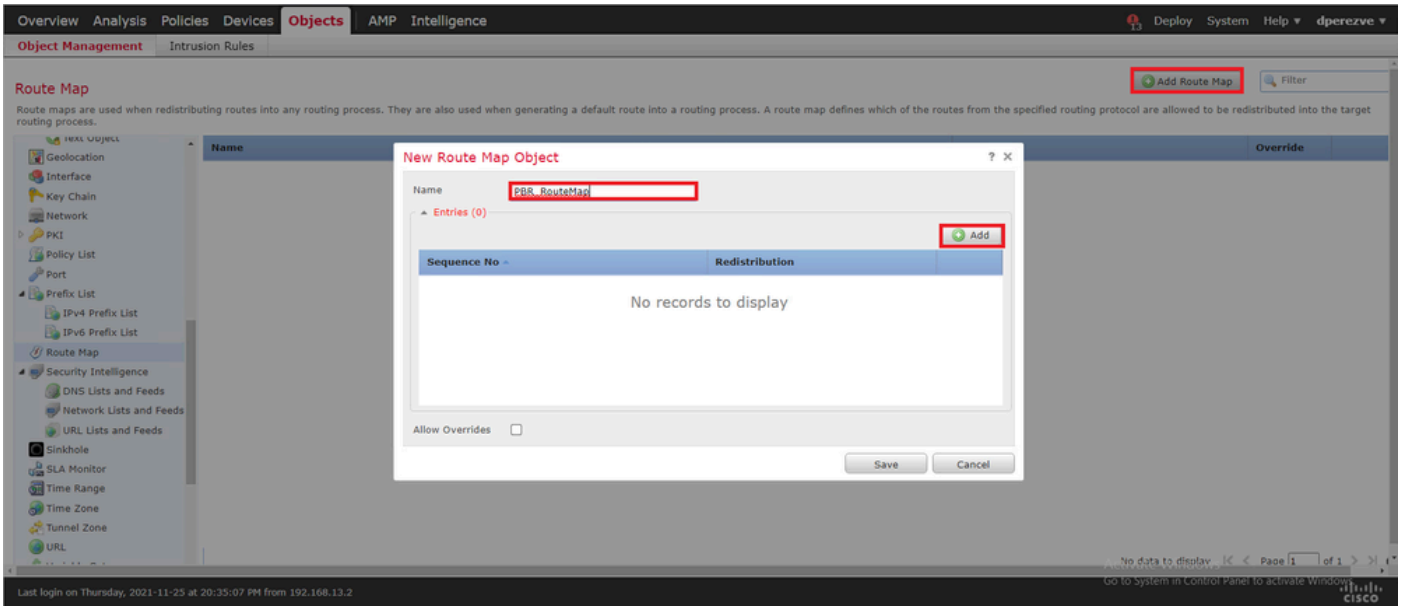
Une fois la liste d'accès PBR configurée, attribuez-la à une carte de routage. La carte de routage évalue le trafic par rapport aux clauses de correspondance définies dans la liste de contrôle d'accès.

Une fois la correspondance établie, le mappage de route exécute les actions définies dans la stratégie de routage.

Pour définir une feuille de route, accédez à **Objects** > **Object Management** et sélectionnez **Route Map** dans la table des matières.



Cliquez sur **Add Route Map** >. Dans la **New Route Map Object** , attribuez un nom à l'objet, puis cliquez sur **Add** pour créer une entrée de feuille de route.



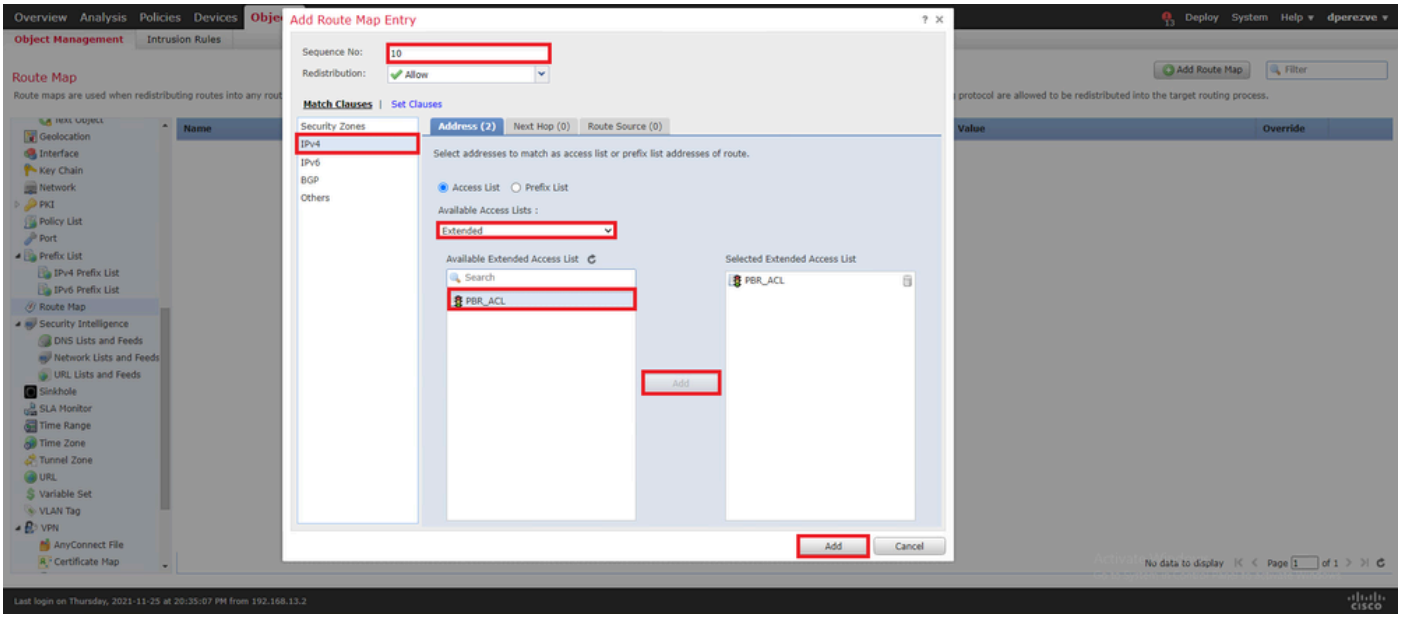
Dans la **Add Route Map Entry** fenêtre, définissez un numéro d'ordre pour la position de la nouvelle entrée.

Accédez à IPv4 > **Match Clauses** et sélectionnez Extended dans le menu **Available Access List** déroulant.

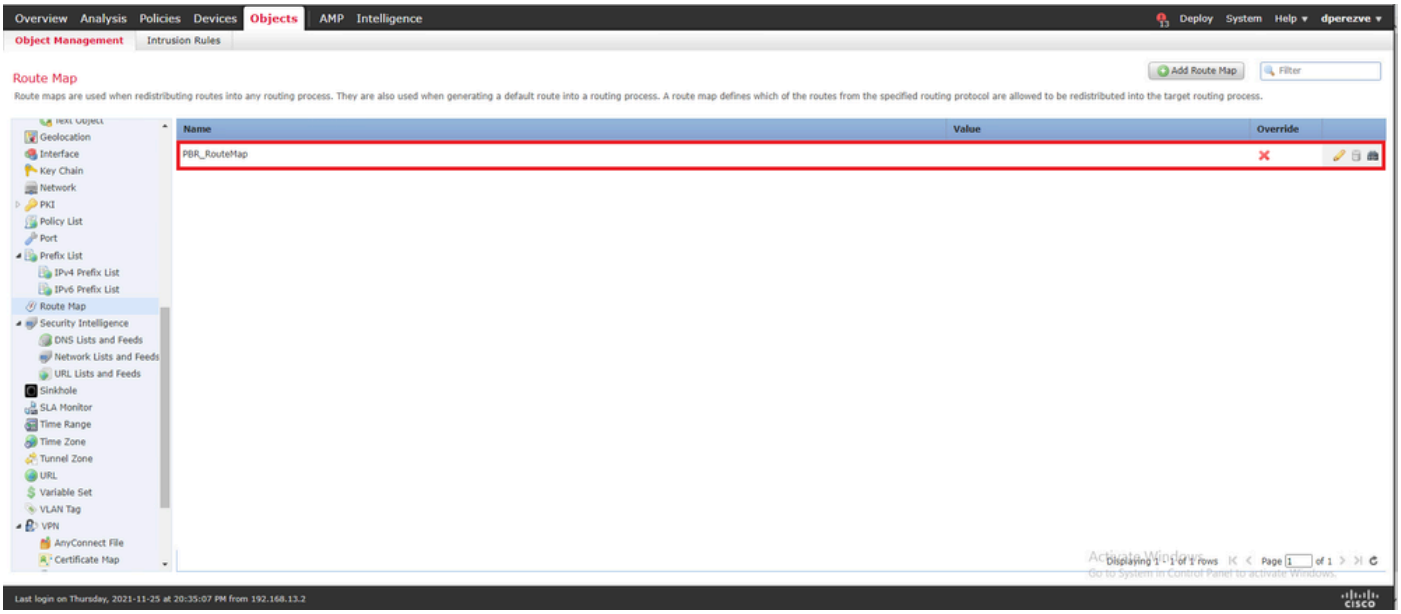
Sélectionnez l'objet de liste d'accès créé à l'étape 1.

Cliquez sur **Add** pour créer l'entrée.

Remarque : FTD prend en charge jusqu'à 65536 entrées différentes (de 0 à 65535). Plus le nombre est faible, plus l'évaluation prioritaire est élevée.



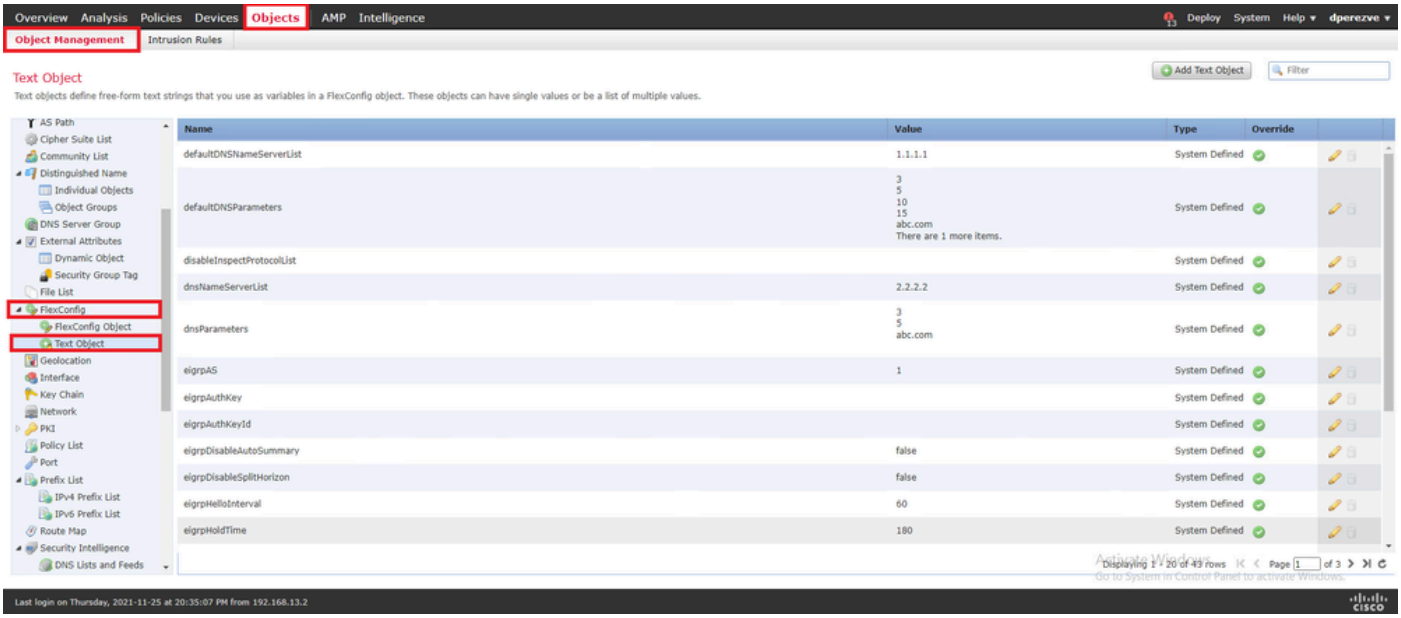
Cliquez sur **Save** . Ajoutez l'objet à la liste d'objets.



Étape 3 : configuration des objets texte FlexConfig

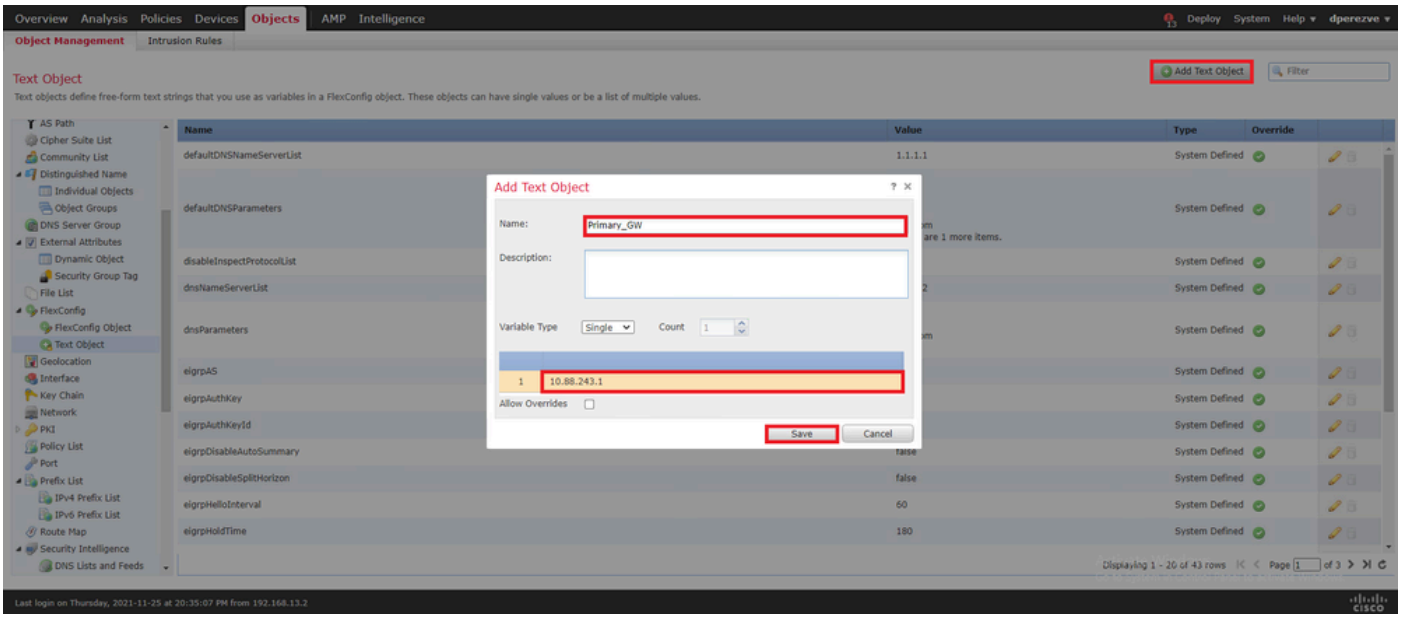
L'étape suivante consiste à définir des objets texte FlexConfig qui représentent les passerelles par défaut de chaque circuit. Ces objets texte sont utilisés ultérieurement dans la configuration de l'objet FlexConfig qui associe PBR aux SLA.

Afin de définir un objet texte FlexConfig naviguez jusqu'à **Objects** > **Object Management** et sélectionnez **Text Object** sous la **FlexConfig** catégorie dans la table des matières.



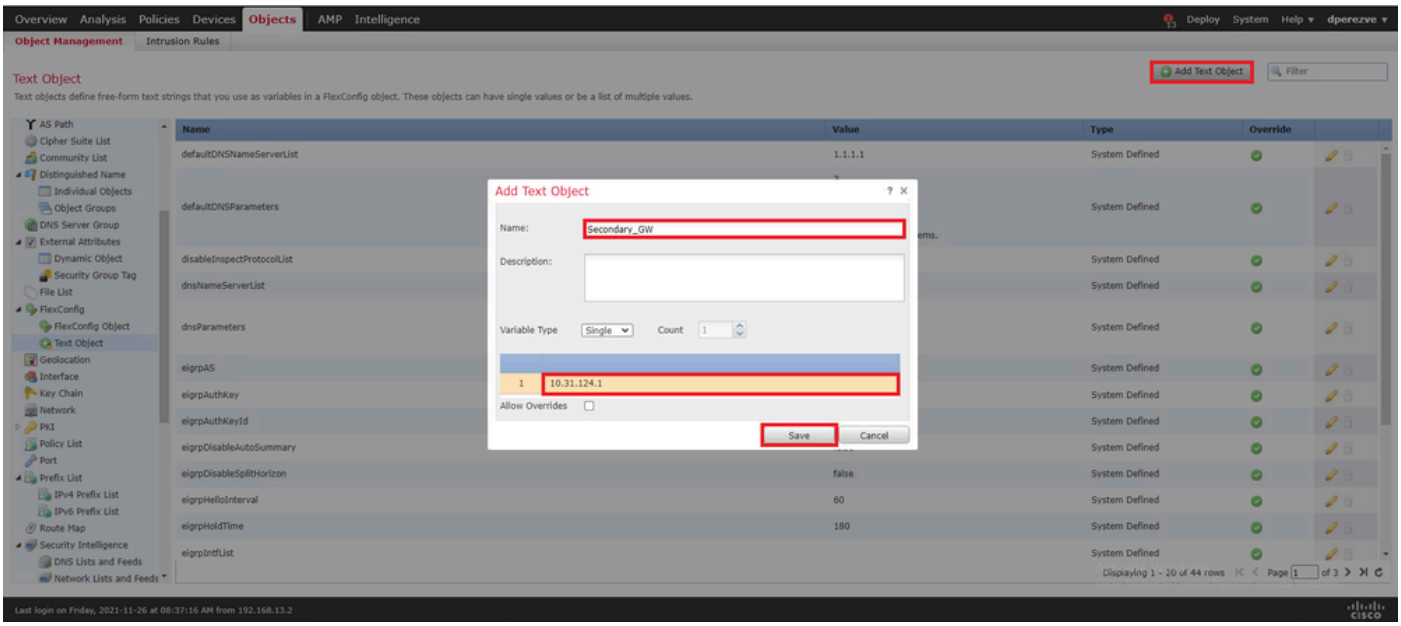
Cliquez sur **Add Text Object** . Dans la **Add Text Object** fenêtre, attribuez un nom à l'objet qui représente la passerelle principale et spécifiez l'adresse IPv4 de ce périphérique.

Cliquez sur **Save** pour ajouter le nouvel objet.

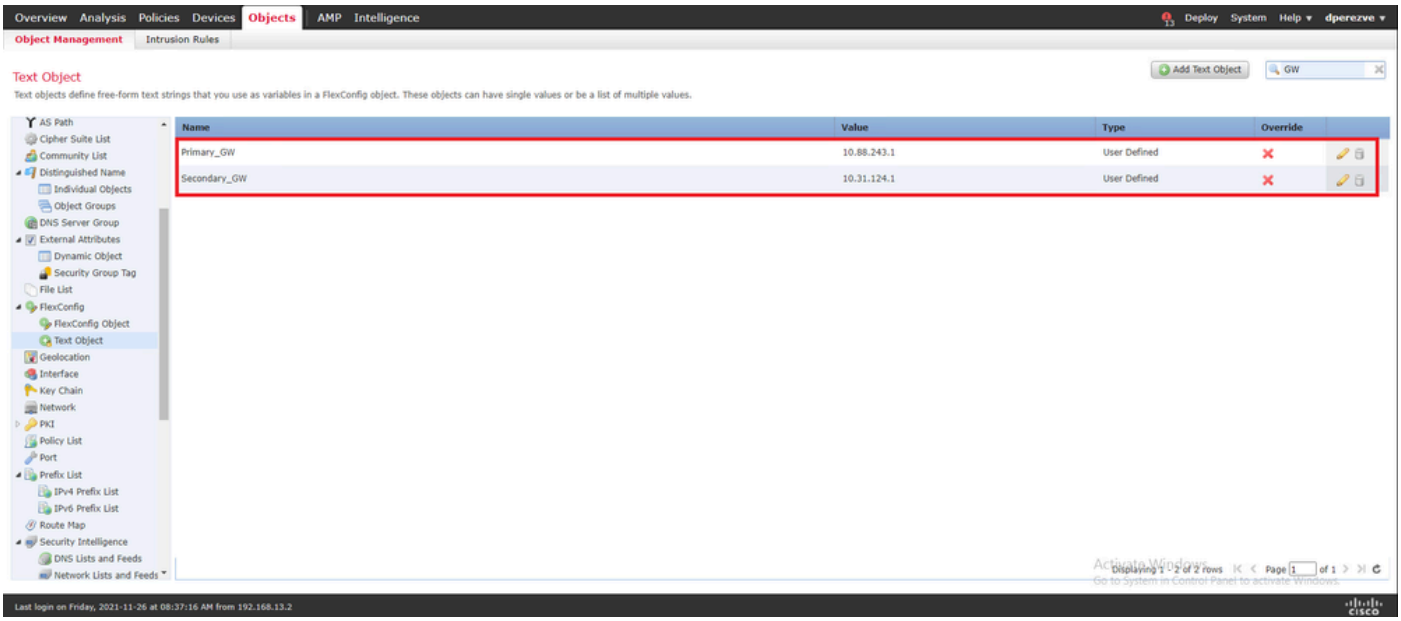


Cliquez **Add Text Object** à nouveau pour créer un deuxième objet, cette fois pour la passerelle sur le circuit de sauvegarde.

Remplissez le nouvel objet avec le nom et l'adresse IP appropriés, puis cliquez sur **Save** .

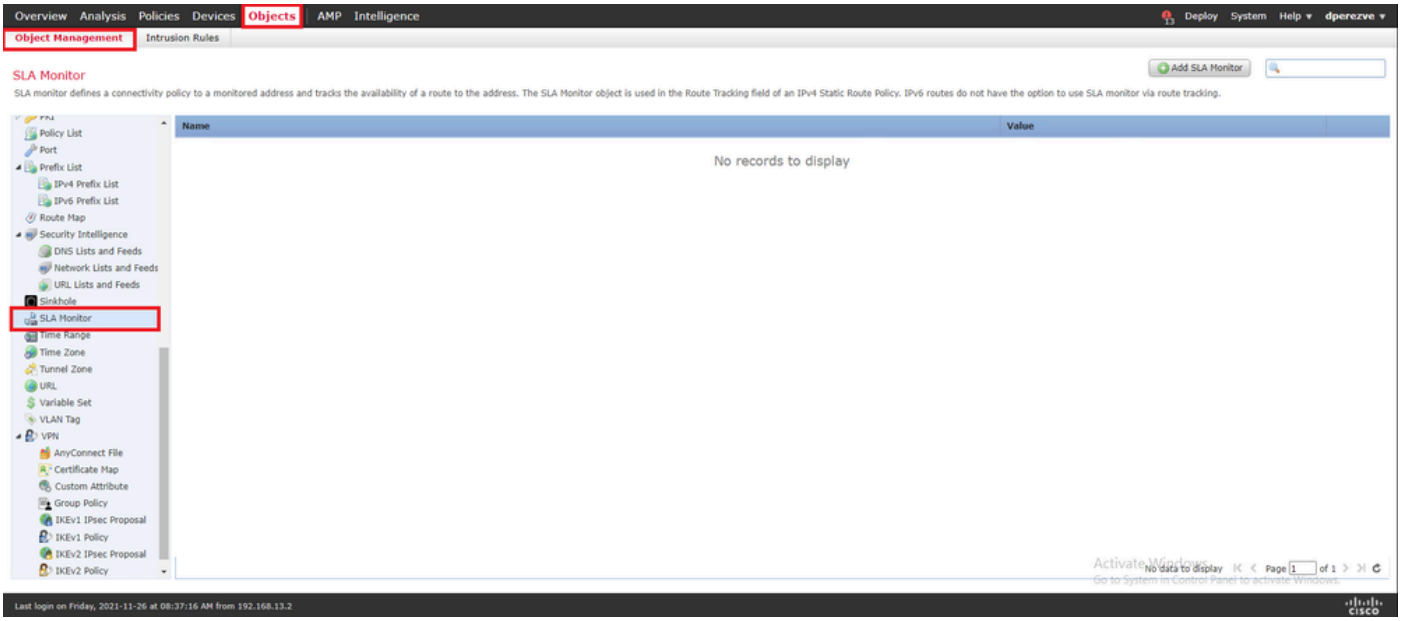


Les deux objets doivent être ajoutés à la liste avec les objets par défaut.



Étape 4 : configuration du SLA Monitor

Pour définir les objets SLA utilisés pour surveiller la connectivité à chaque modem routeur, accédez à **Objects** > **Object Management** et sélectionnez **SLA Monitor** dans la table des matières.



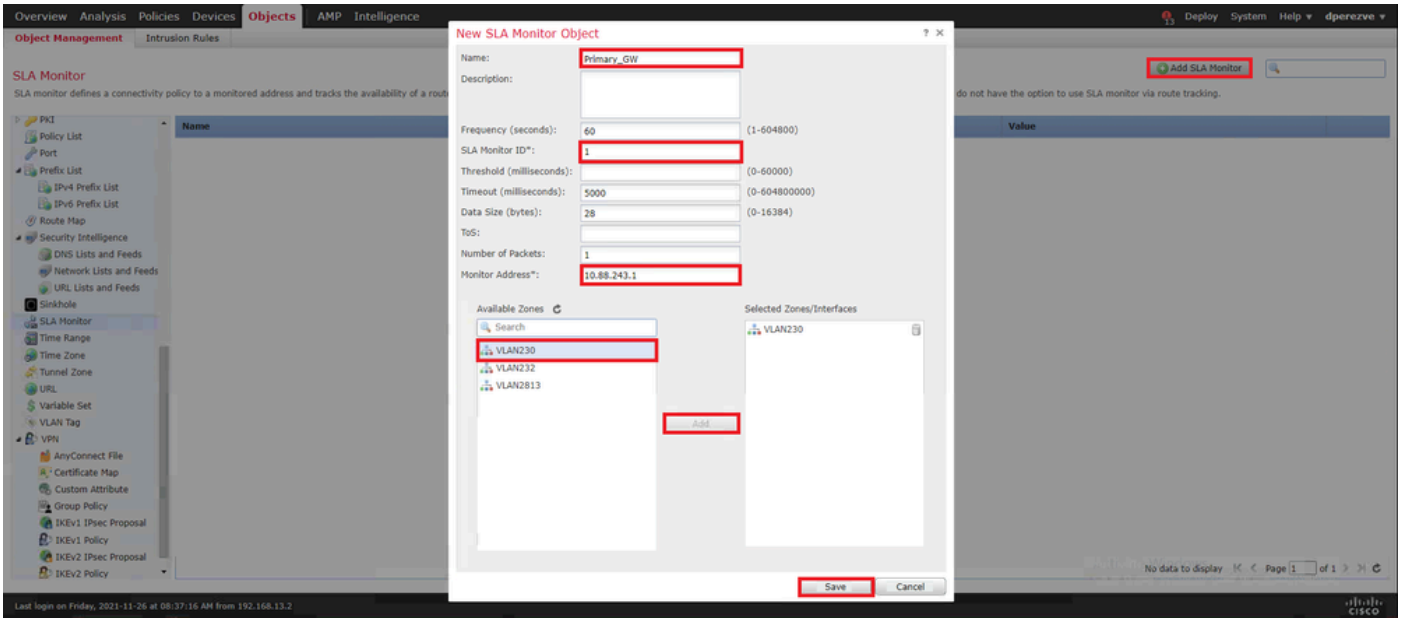
Sélectionnez l' **Add SLA Monitor** objet.

Dans cette **New SLA Monitor** fenêtre, définissez un nom ainsi qu'un identificateur pour l'opération SLA, l'adresse IP du périphérique à surveiller (dans ce cas, la passerelle principale) et l'interface ou la zone par laquelle le périphérique est accessible.

En outre, il est également possible d'ajuster le délai d'attente et le seuil. Cliquez sur **Save** .

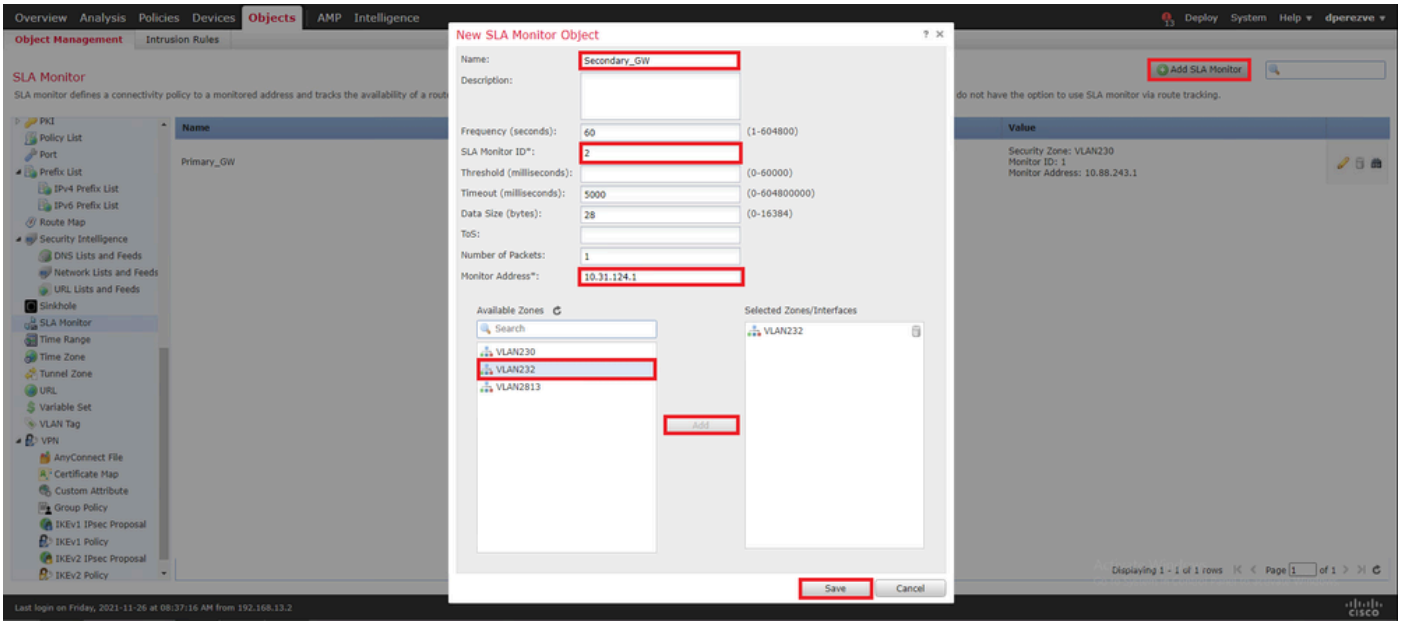
Remarque : FTD prend en charge jusqu'à 2 000 opérations SLA. Les valeurs de l'ID SLA sont comprises entre 1 et 2147483647.

Remarque : Si les valeurs de délai et de seuil ne sont pas spécifiées, FTD utilise des minuteurs par défaut : 5000 millisecondes dans chaque cas.

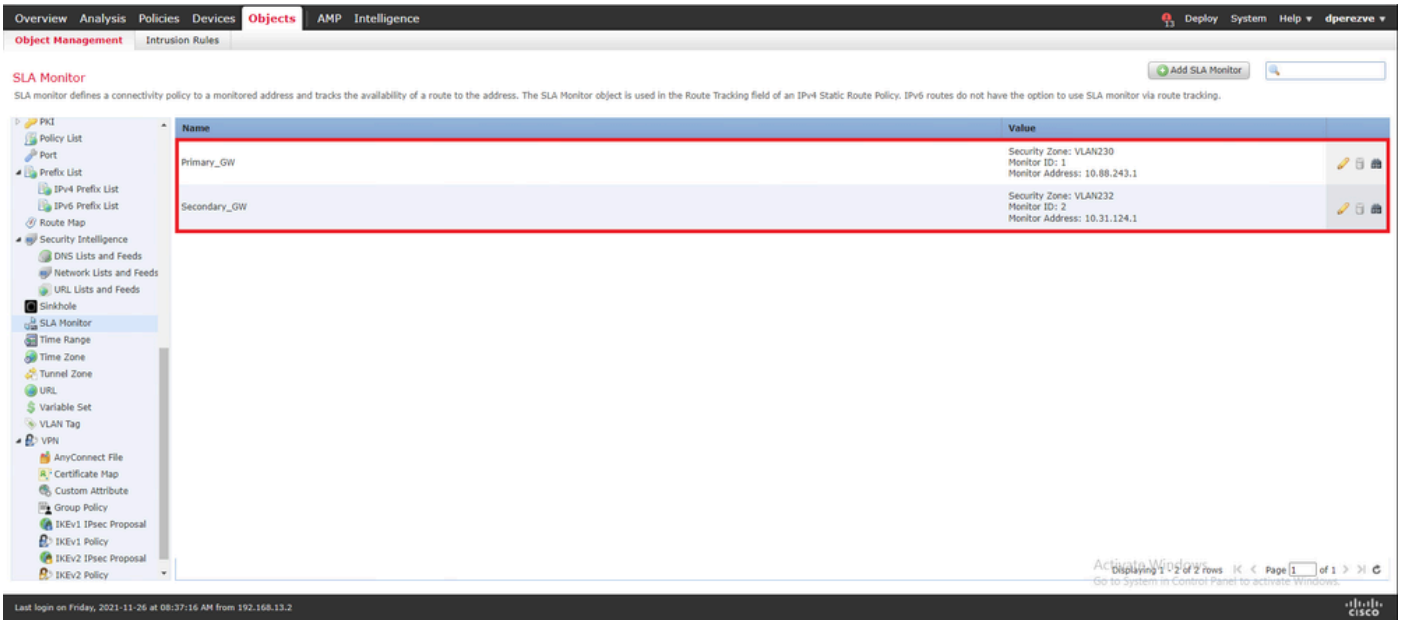


Cliquez de nouveau sur le **Add SLA Monitor** bouton pour créer un deuxième objet, cette fois pour le modem routeur sur le circuit de sauvegarde.

Remplissez le nouvel objet avec les informations appropriées, assurez-vous que l'ID SLA est différent de celui défini pour la passerelle principale et enregistrez les modifications.



Les deux objets doivent être ajoutés à la liste.

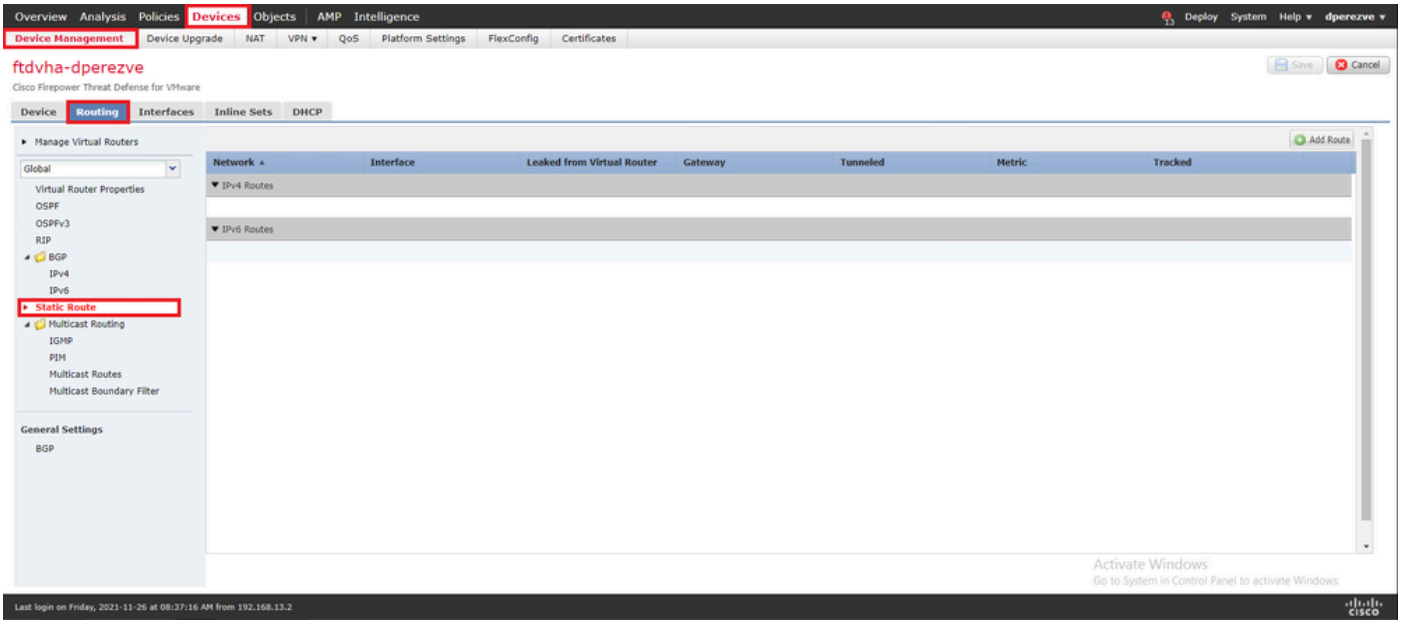


Étape 4 : configuration des routes statiques avec la piste de routage

Une fois les objets IP SLA créés, définissez une route pour chaque passerelle et associez-les aux SLA.

Ces routes ne fournissent pas réellement la connectivité de l'intérieur vers l'extérieur (tout le routage est effectué via PBR), mais elles sont nécessaires pour suivre la connectivité aux passerelles via les SLA.

Afin de configurer des routes statiques, naviguez jusqu'à **Devices** > **Device Management** , modifiez le FTD à portée de main et sélectionnez **Static Route** dans la table des matières dans l' **Routing** onglet.



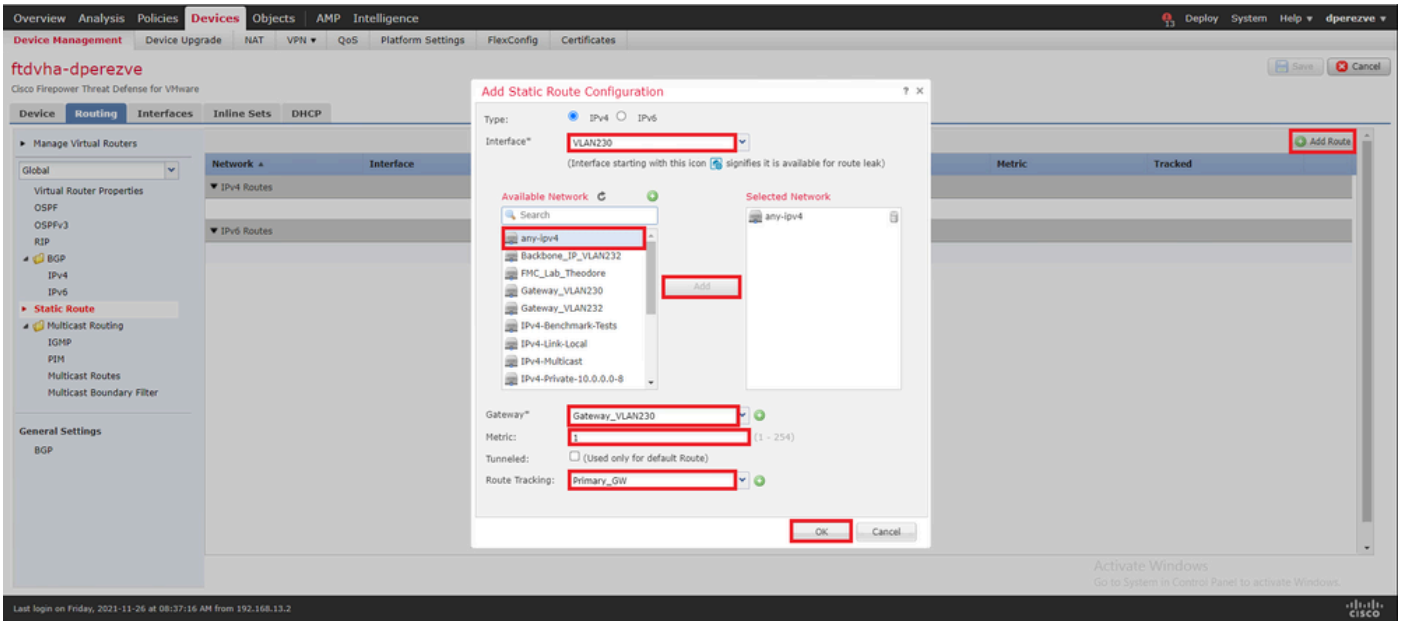
Dans la fenêtre **Add Static Route Configuration** , dans la liste déroulante Interface, spécifiez le nom de l'interface par laquelle la passerelle principale doit être accessible.

Sélectionnez ensuite le réseau de destination et la passerelle principale dans la **Gateway** liste

déroulante.

Spécifiez une mesure pour la route et dans **Route Track** la liste déroulante, puis sélectionnez l'objet SLA pour la passerelle principale créée à l'étape 3.

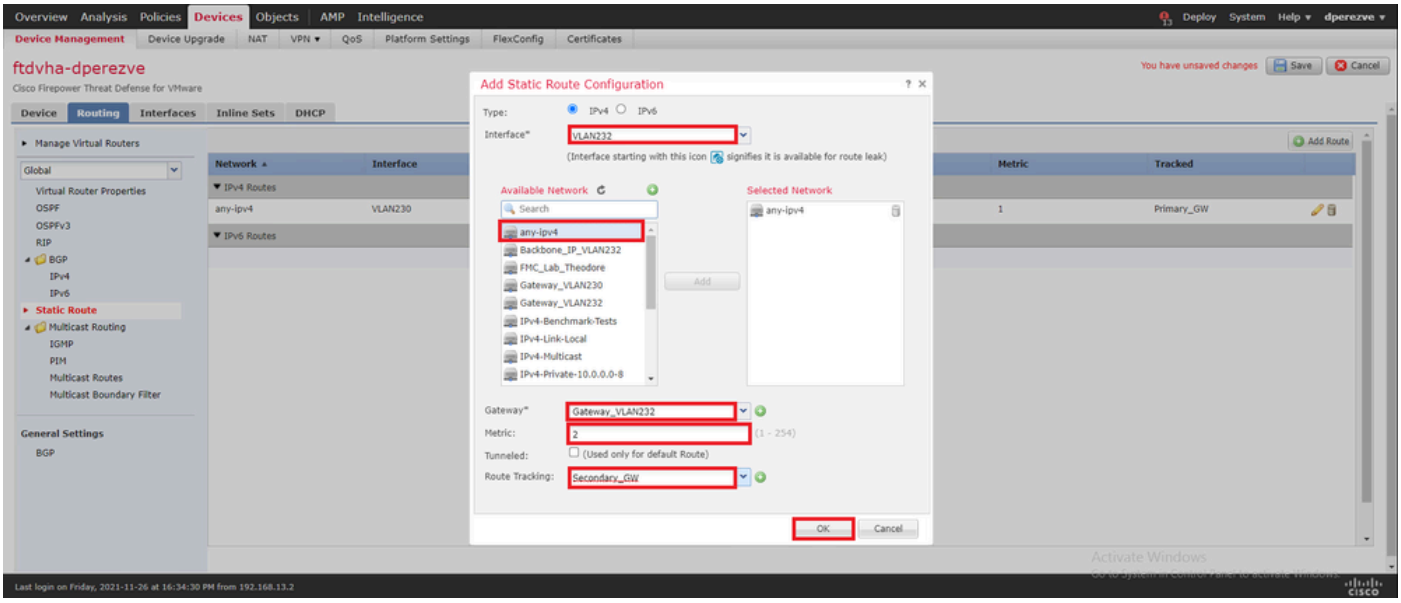
Cliquez sur OK pour ajouter la nouvelle route.



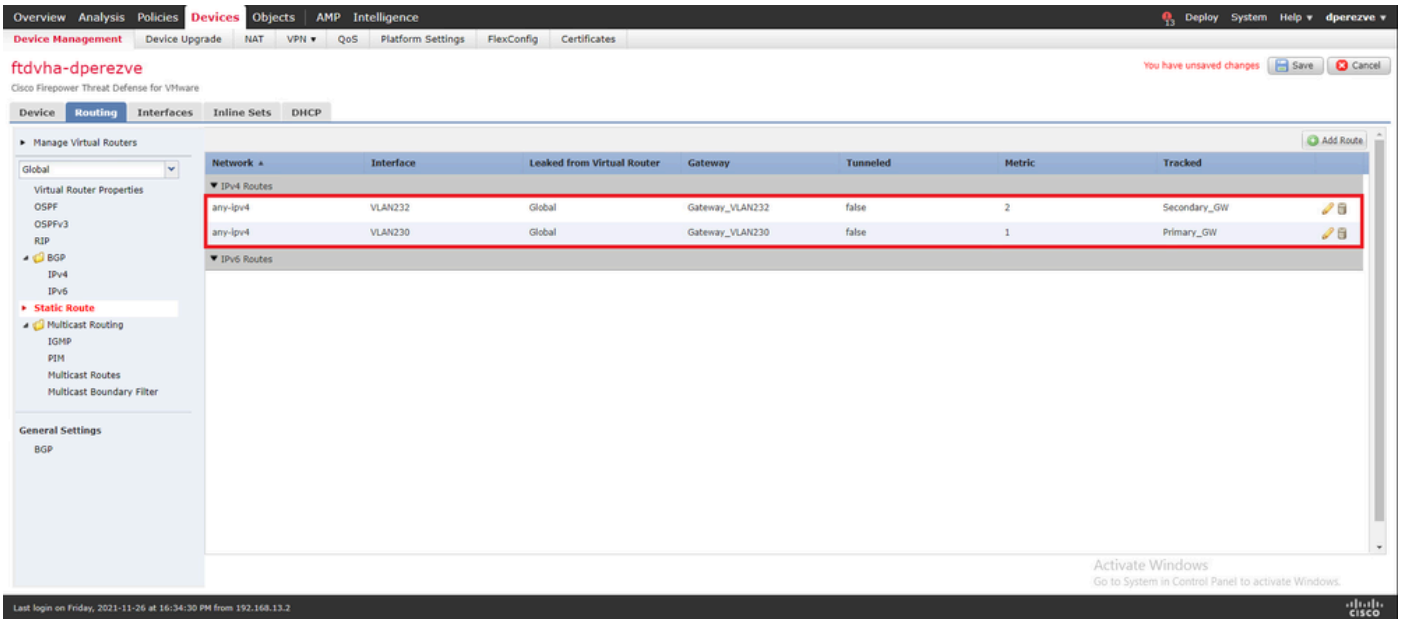
Une deuxième route statique doit être configurée pour la passerelle de secours.

Cliquez **Add Route** sur pour définir une nouvelle route statique.

Remplissez la **Add Static Route Configuration** avec les informations relatives à la passerelle de secours et assurez-vous que la métrique de cette route est supérieure à celle configurée dans la première route.



Les deux routes doivent être ajoutées à la liste.

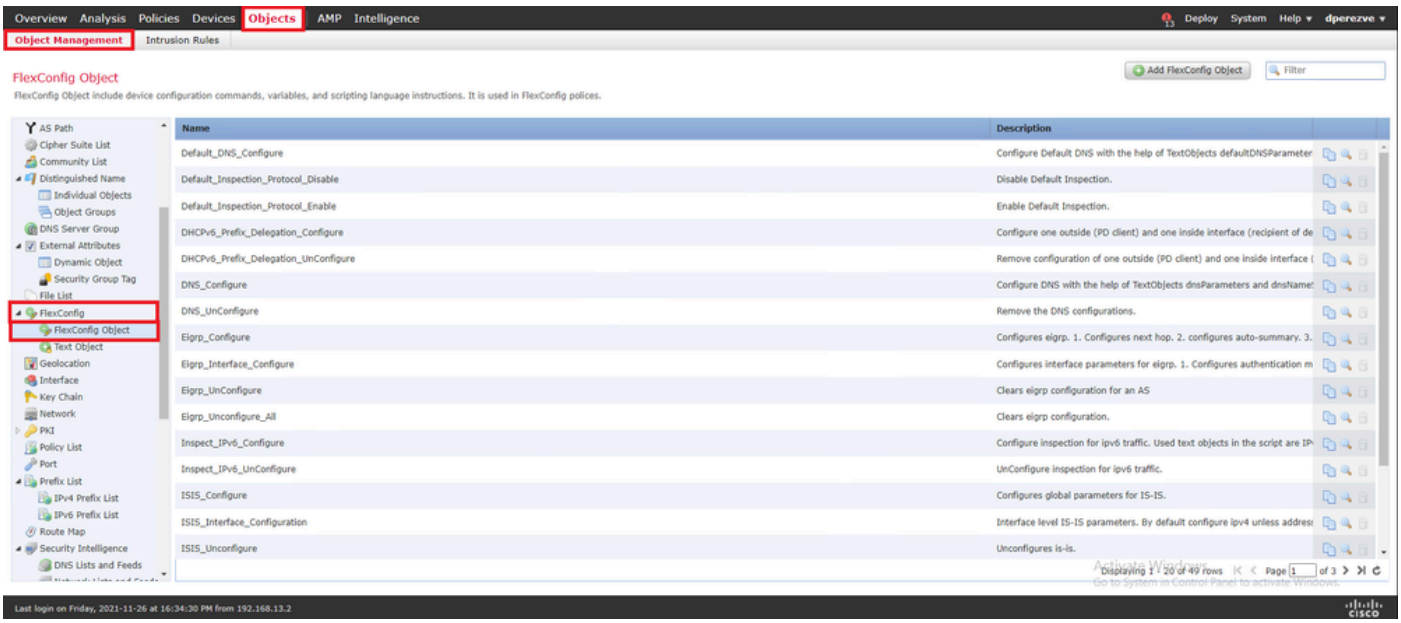


Étape 5. Configuration de l'objet PBR FlexConfig

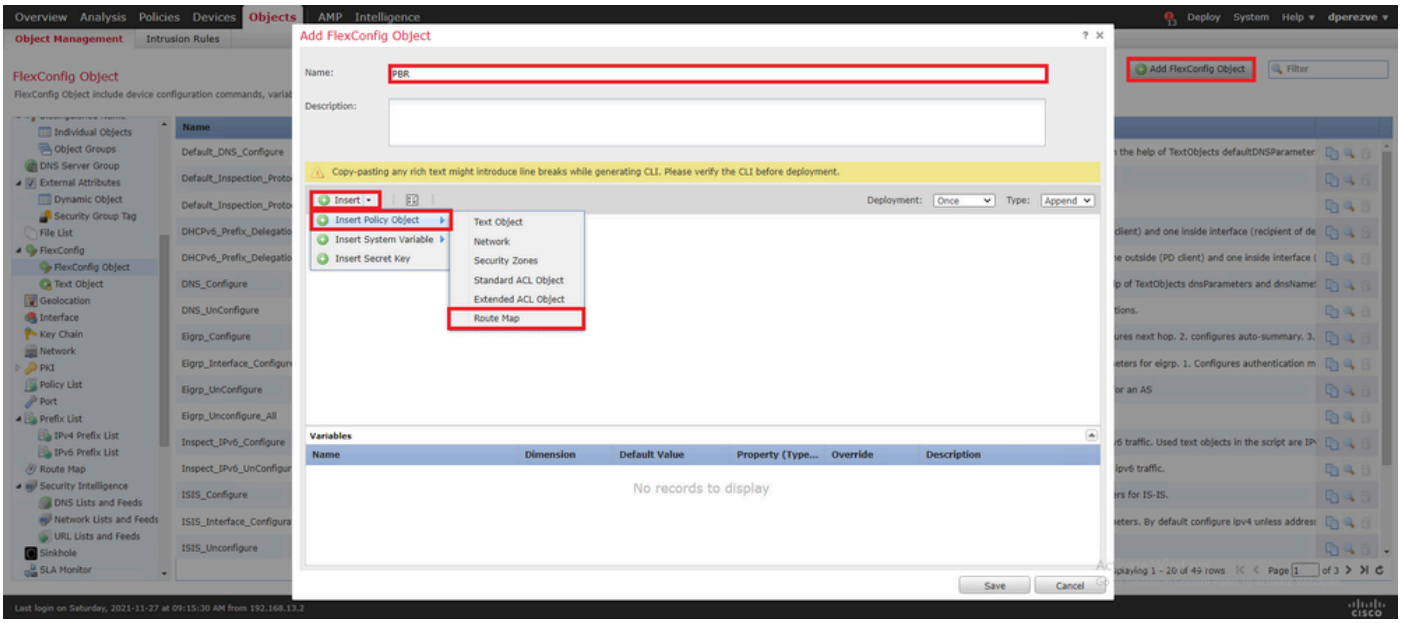
Activez les SLA sous la carte de routage utilisée pour PBR et appliquez cette carte de routage dans une interface du FTD.

Jusqu'à présent, la carte de routage n'a été associée qu'à la liste d'accès qui définit les critères de correspondance. Cependant, les derniers réglages ne sont pas pris en charge par l'interface utilisateur graphique de FMC, donc un objet FlexConfig est nécessaire.

Pour définir l'objet PBR FlexConfig, naviguez **Objects** > **Object Management** jusqu'à et sélectionnez **FlexConfig Object** sous la **FlexConfig** catégorie dans la table des matières.

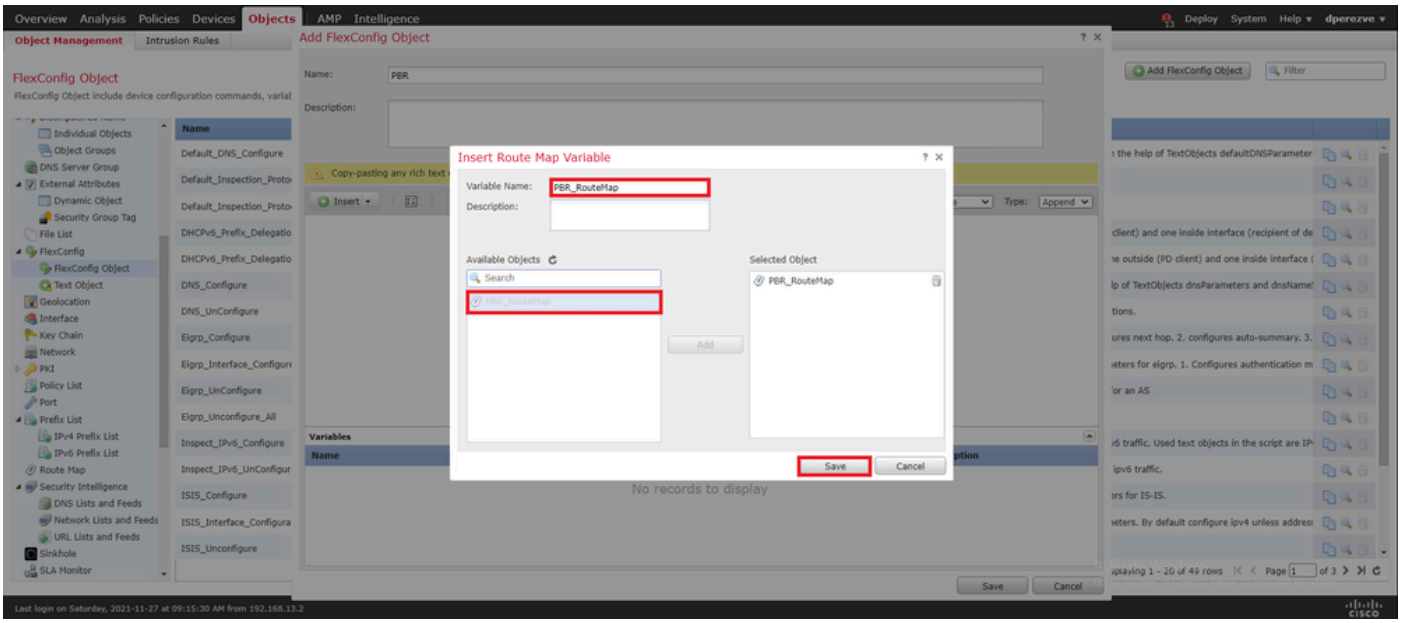


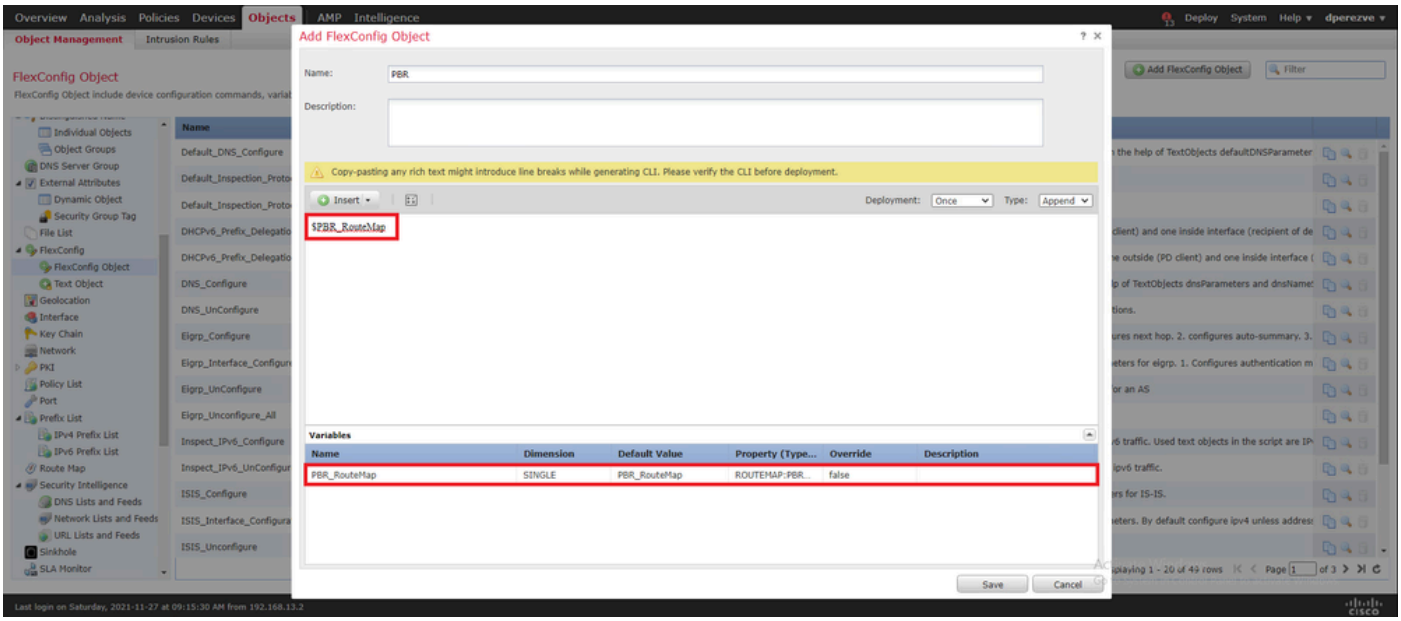
Sélectionnez le **Add FlexConfig Object** bouton. Dans la **Add FlexConfig Object** fenêtre, attribuez un nom et accédez à **Insert** > **Insert Policy Object** > **Route Map** .



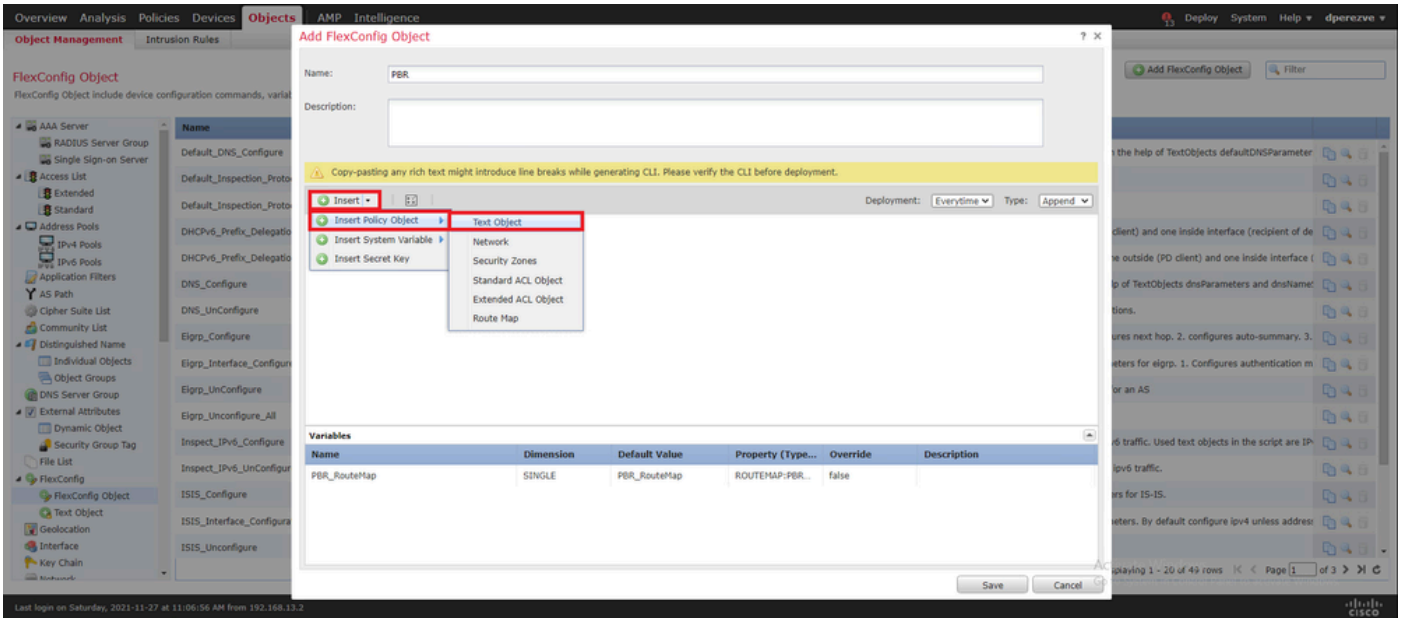
Dans la **Insert Route Map Variable** fenêtre, attribuez un nom à la variable et sélectionnez l'objet PBR créé à l'étape 2.

Cliquez sur cette option **Save** pour ajouter la carte de routage dans le cadre de l'objet FlexConfig.



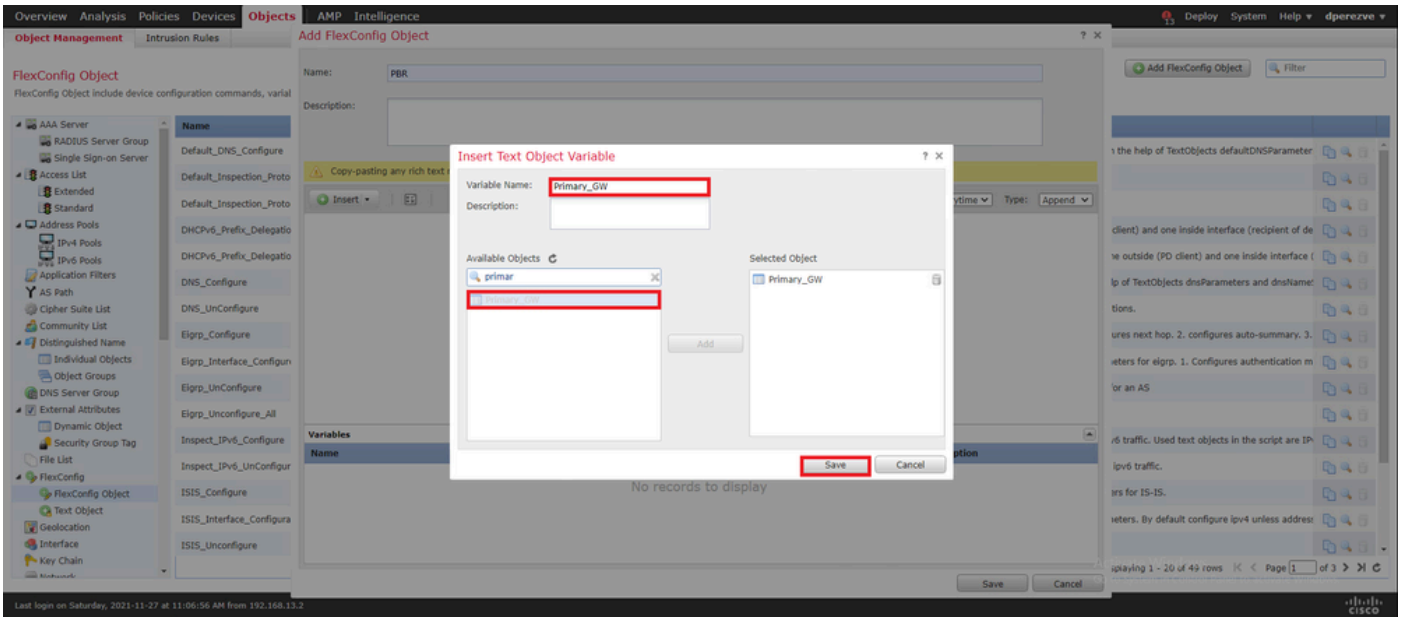


Outre la variable de mappage de route, nous devons ajouter les objets texte FlexConfig qui représentent chaque passerelle (définie à l'étape 3). Dans la fenêtre, **Add FlexConfig Object** accédez à **Insert > Insert Policy Object > Text Object .**

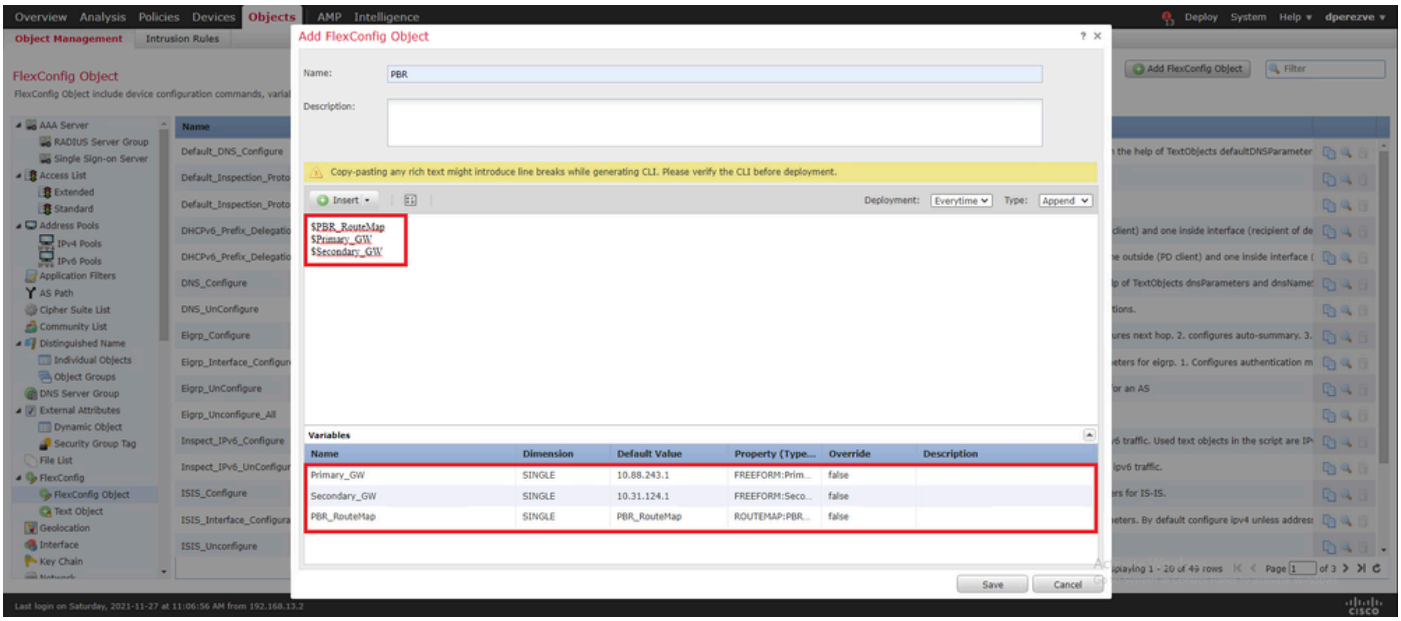


Dans la **Insert Text Object Variable** fenêtre, attribuez un nom à la variable et sélectionnez l'objet texte qui représente la passerelle principale définie à l'étape 3.

Cliquez **Save** sur ce bouton afin de l'ajouter à l'objet FlexConfig.



Répétez ces dernières étapes pour la passerelle de sauvegarde. À la fin du processus, les deux variables doivent être ajoutées à l'objet FlexConfig.

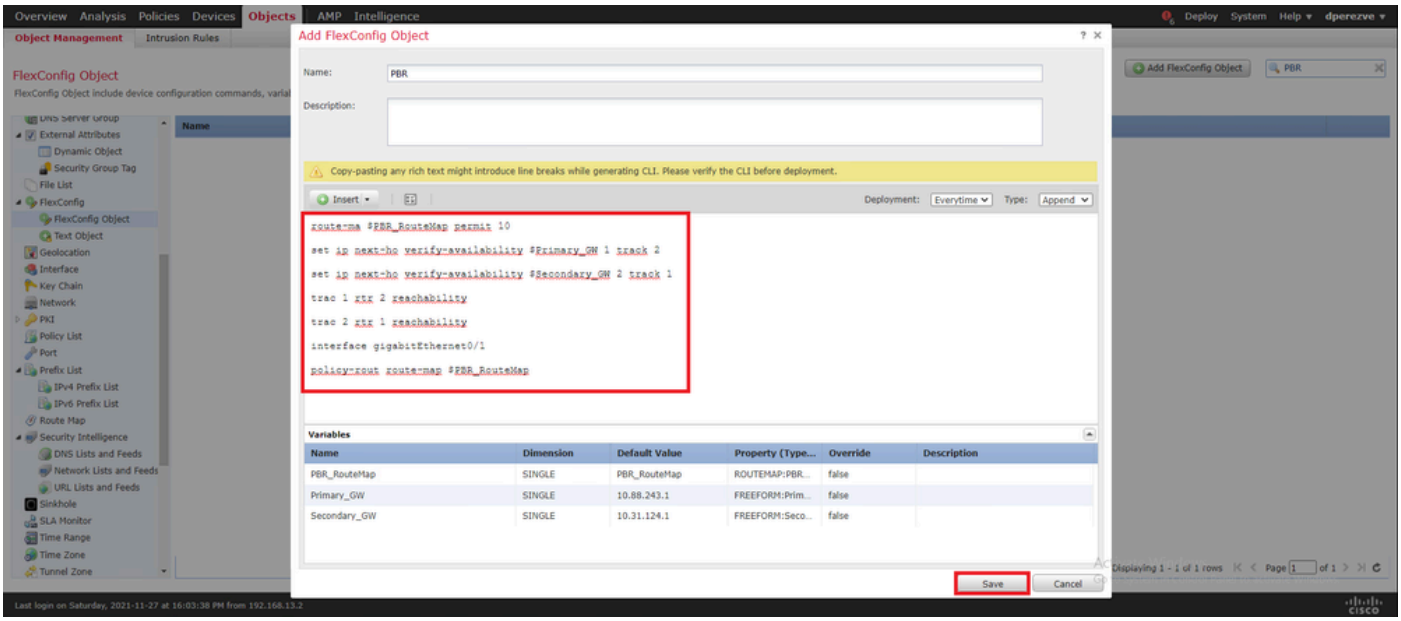


La syntaxe de la configuration PBR doit être identique à celle de Cisco ASA. Le numéro d'ordre de la carte de routage doit correspondre à celui configuré à l'étape 2 (10 dans ce cas) ainsi qu'aux ID SLA.

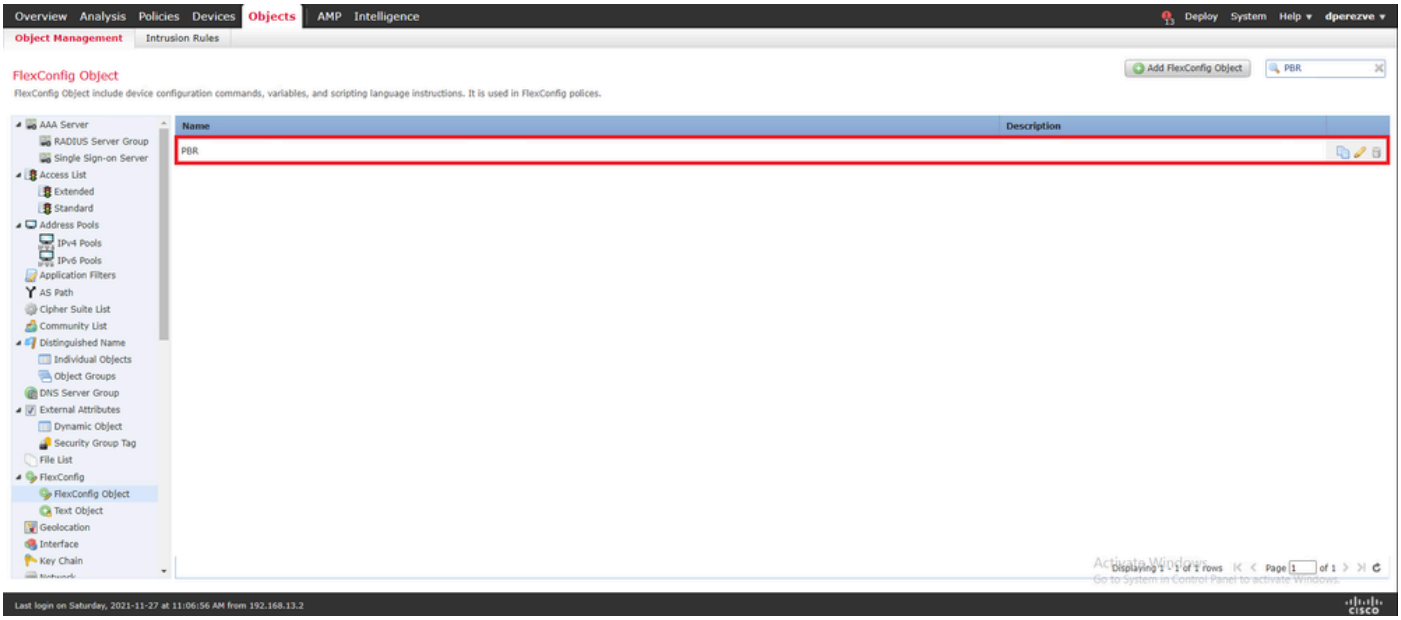
Pour configurer PBR afin de vérifier la disponibilité pour le tronçon suivant, la **set ip next-hop verify-availability** commande doit être utilisée.

La carte de routage doit être appliquée à l'interface interne, dans ce cas VLAN2813. Utilisez la **policy-route route-map** commande sous la configuration d'interface.

Cliquez **Save** sur lorsque la configuration est terminée.



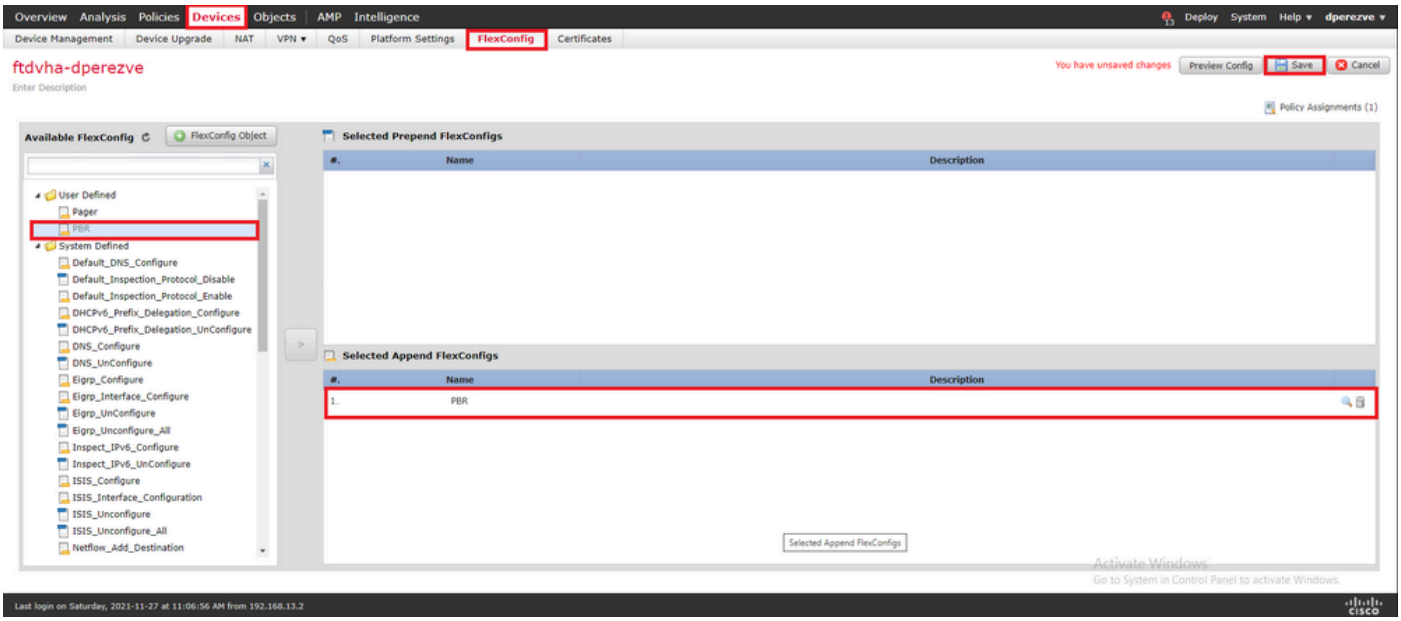
L'objet FlexConfig doit être ajouté à la liste.



Étape 6. Attribution de l'objet FlexConfig PBR à la stratégie FlexConfig

Accédez à la stratégie FlexConfig disponible **Devices > FlexConfig** et modifiez-la.

Sélectionnez l'objet PBR FlexConfig dans **Available FlexConfig** la table des matières, enregistrez les modifications et déployez les modifications dans FTD.



Vérifier

Une fois le déploiement terminé, FTD doit envoyer une requête d'écho ICMP régulière aux périphériques surveillés afin de garantir l'accessibilité. Entre-temps, une route suivie vers la passerelle principale doit être ajoutée à la table de routage.

```
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
```

Comme la connectivité à la passerelle principale est active, le trafic provenant du sous-réseau interne (VLAN2813) doit être transféré via le circuit ISP principal.

```
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
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
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
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
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
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 rul


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
```

Si le FTD ne reçoit pas de réponse d'écho de la passerelle principale dans le délai spécifié dans l'objet SLA Monitor, l'hôte est considéré comme inaccessible et marqué comme étant hors service. La route suivie vers la passerelle principale est également remplacée par la route suivie vers l'homologue de secours.

```
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
```

Le message d'information 622001 est généré chaque fois que FTD ajoute ou supprime une route suivie de la table de routage.

```
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 interfa
```

Maintenant, tout le trafic provenant du VLAN2813 doit être transféré via le circuit ISP de secours.

```
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
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
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
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
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
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
```

Dépannage

Afin de valider quelle entrée PBR est appliquée dans **interesting traffic** , exécutez la commande debug policy-route.

```
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 s
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
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
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.