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

Table des matières

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)** ainsi que **Internet Protocol Service Level Agreement (IP SLA)** sur un routeur 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.

D'un autre côté, seulement **Internet Control Message Protocol (ICMP)** Les SLA sont pris en charge par FTD.

Dans cet exemple, PBR est utilisé pour acheminer des paquets sur un **Internet Service Provider (ISP)** basé sur 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

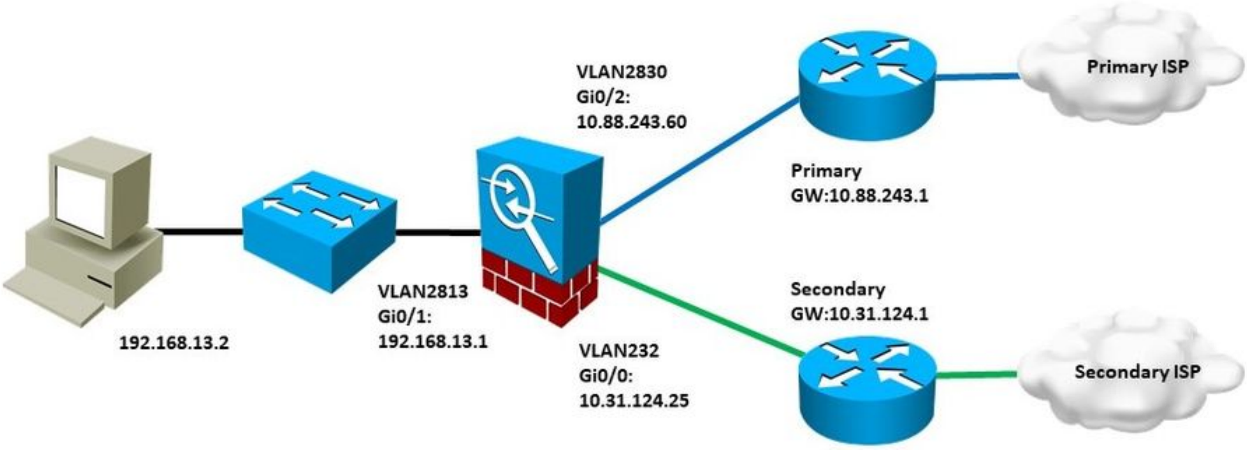
Diagramme du réseau

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.

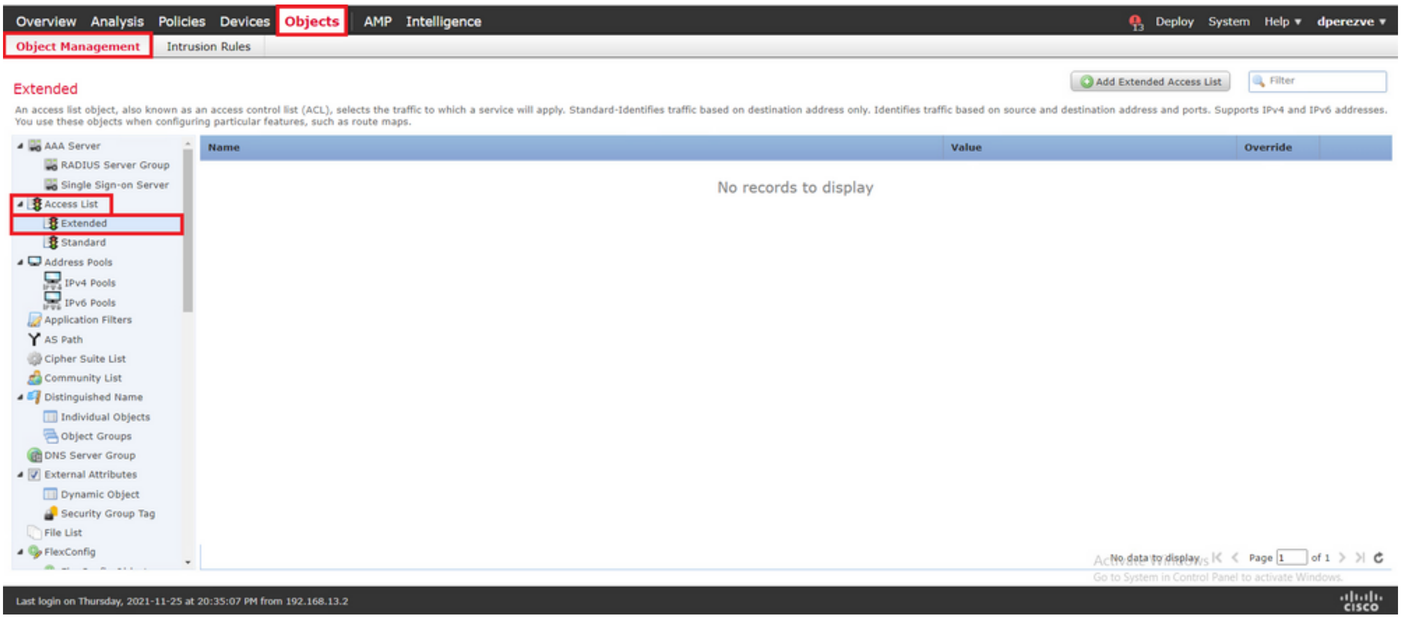


Configurations

Étape 1. Configurer la liste d'accès PBR

Àla 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.

Pour définir une liste d'accès pour les critères correspondants, accédez à **Objects > Object Management** et sélectionnez **Extended** sous la **Access List** dans la table des matières.



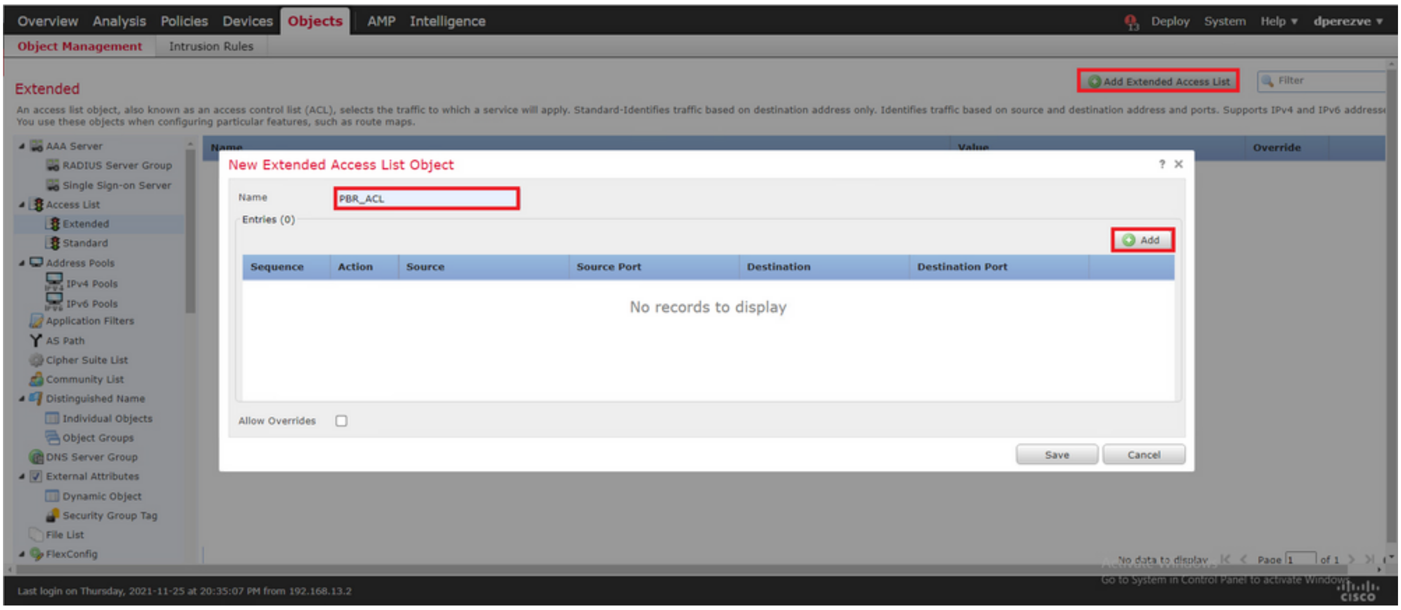
An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects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

No records to display

No data to display

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

Cliquer **Add Extended Access List .** Dans la **New Extended Access List Object** , attribuez un nom à l'objet, puis sélectionnez la **Add** afin de commencer avec la configuration de la liste d'accès.



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.

New Extended Access List Object

Name: PBR_ACL

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port

No records to display

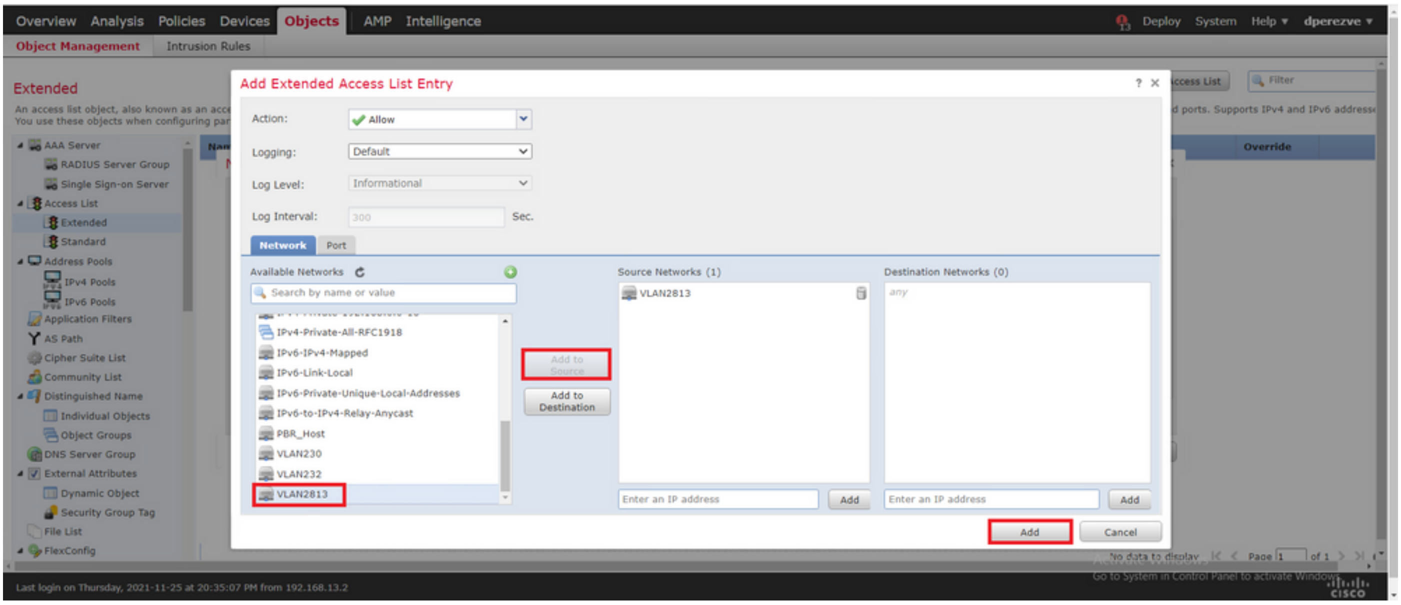
Allow Overrides □

Save Cancel

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

Cliquer **Add to Source** pour la définir comme source de la liste d’accès.

Cliquer **Add** pour créer l'entrée.



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network | Port

Available Networks

Search by name or value

IPv4-Private-All-RFC1918
IPv6-IPv4-Mapped
IPv6-Link-Local
IPv6-Private-Unique-Local-Addresses
IPv6-to-IPv4-Relay-Anycast
PBR_Host
VLAN230
VLAN232
VLAN2813

Add to Source

Add to Destination

Source Networks (1)

VLAN2813

Destination Networks (0)

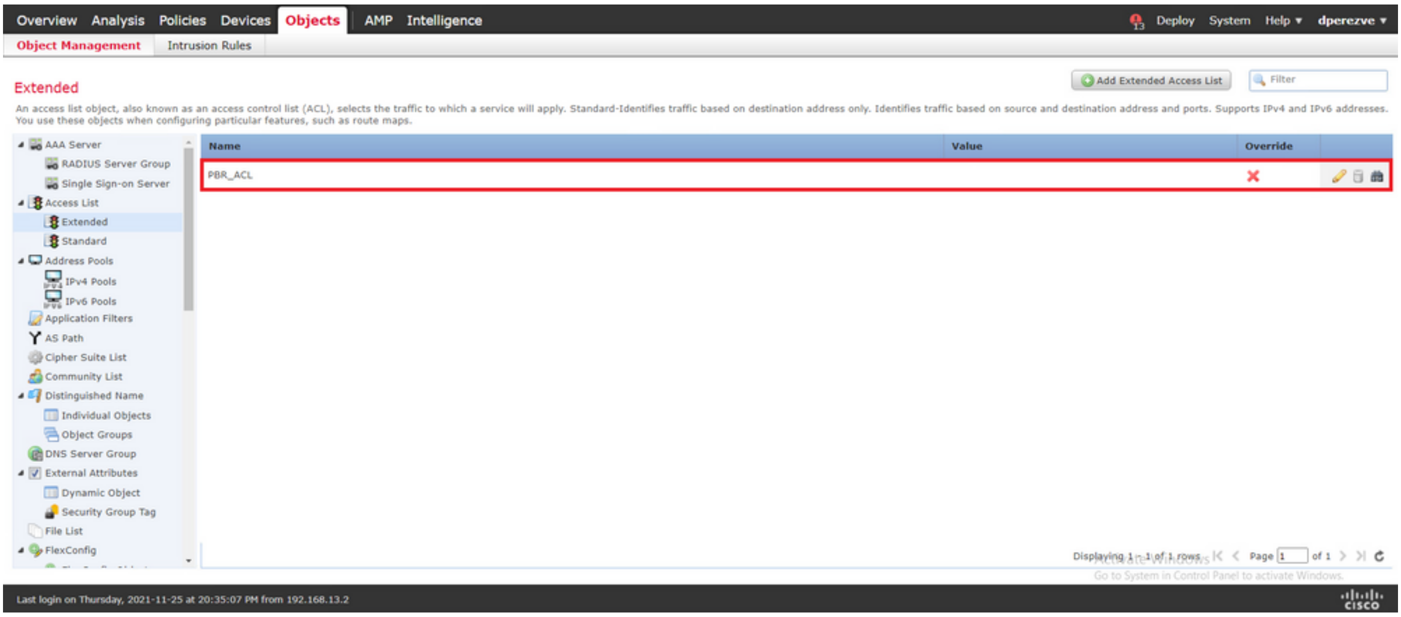
any

Enter an IP address Add

Enter an IP address Add

Add Cancel

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



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		✗

Displaying 1 - 1 of 1 rows

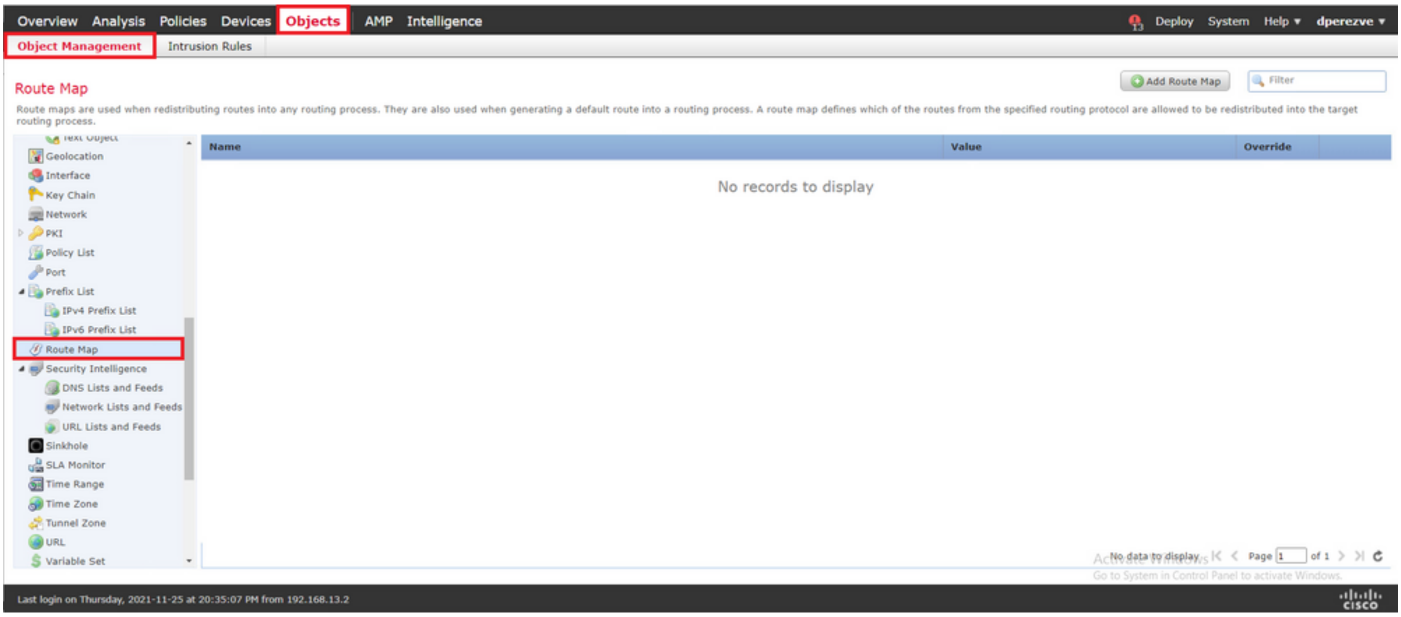
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

Étape 2. Configurer 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 la feuille de route, accédez à **Objects > Object Management** et sélectionnez **Route Map** dans la table des matières.



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.

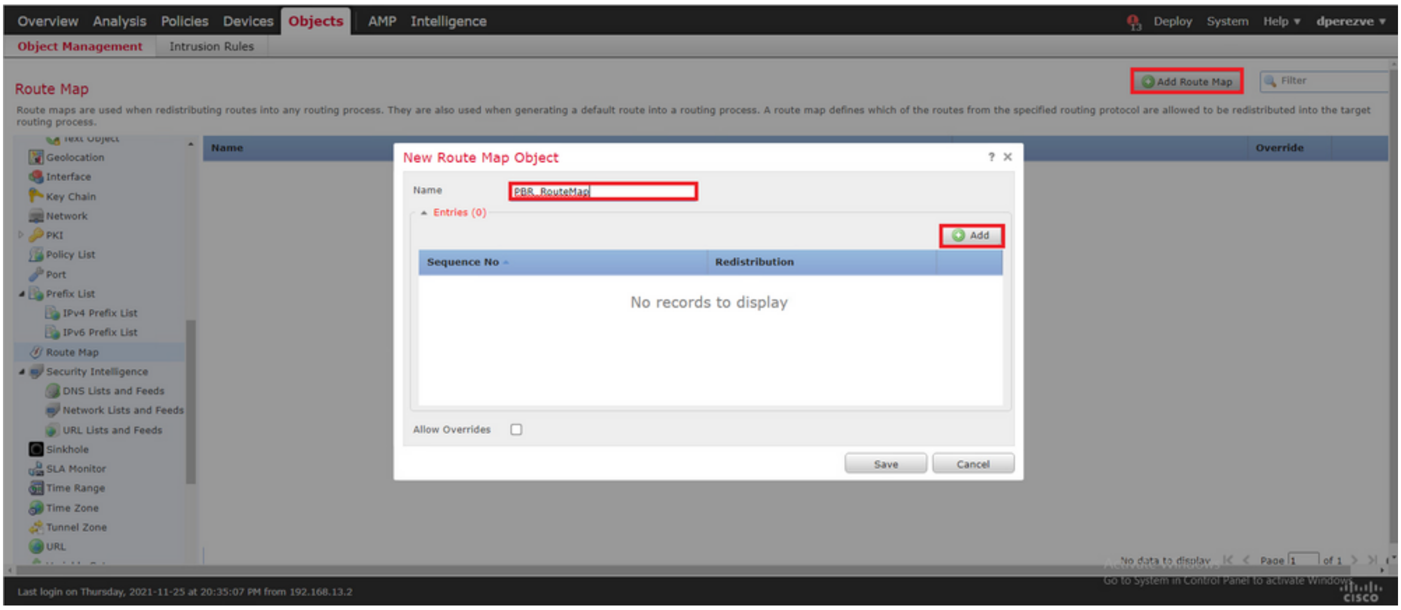
Name	Value	Override

No records to display

No data to display

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

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



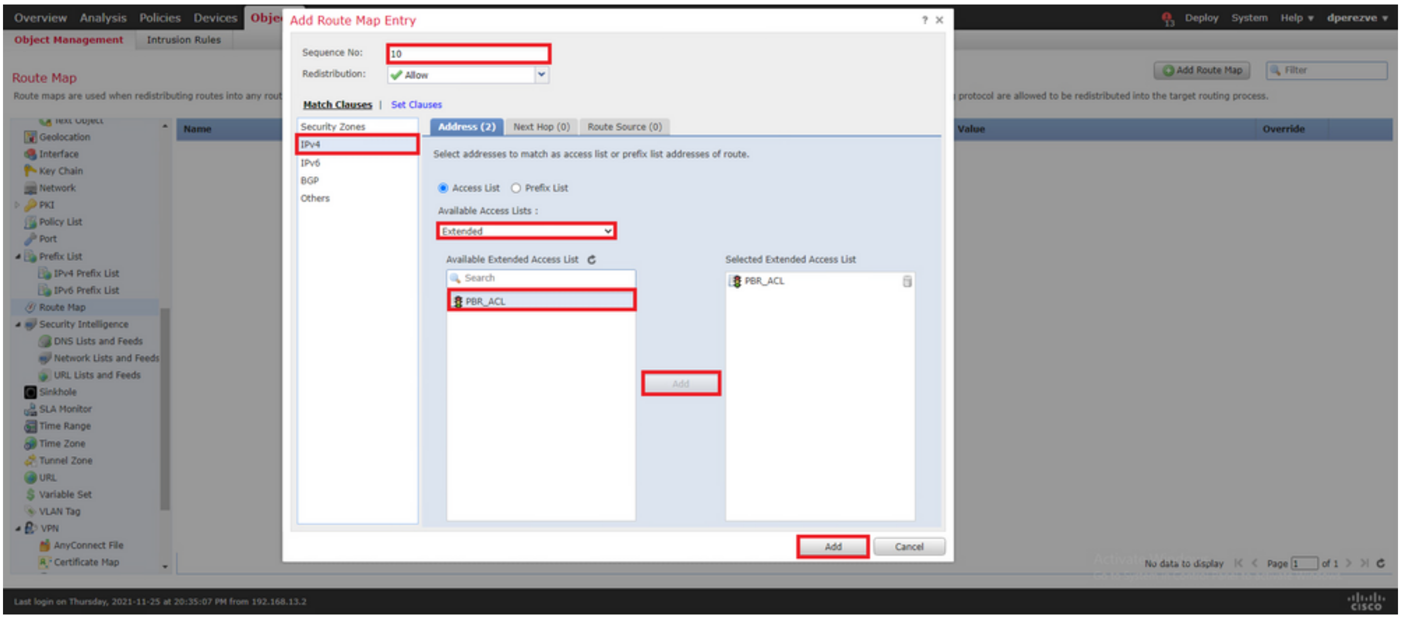
Dans la **Add Route Map Entry** , définissez un numéro d'ordre pour la position de la nouvelle entrée.

Naviguez jusqu'à **IPv4 > Match Clauses** et sélectionnez **Étendu** dans la liste **Available Access List** s'affiche**.**

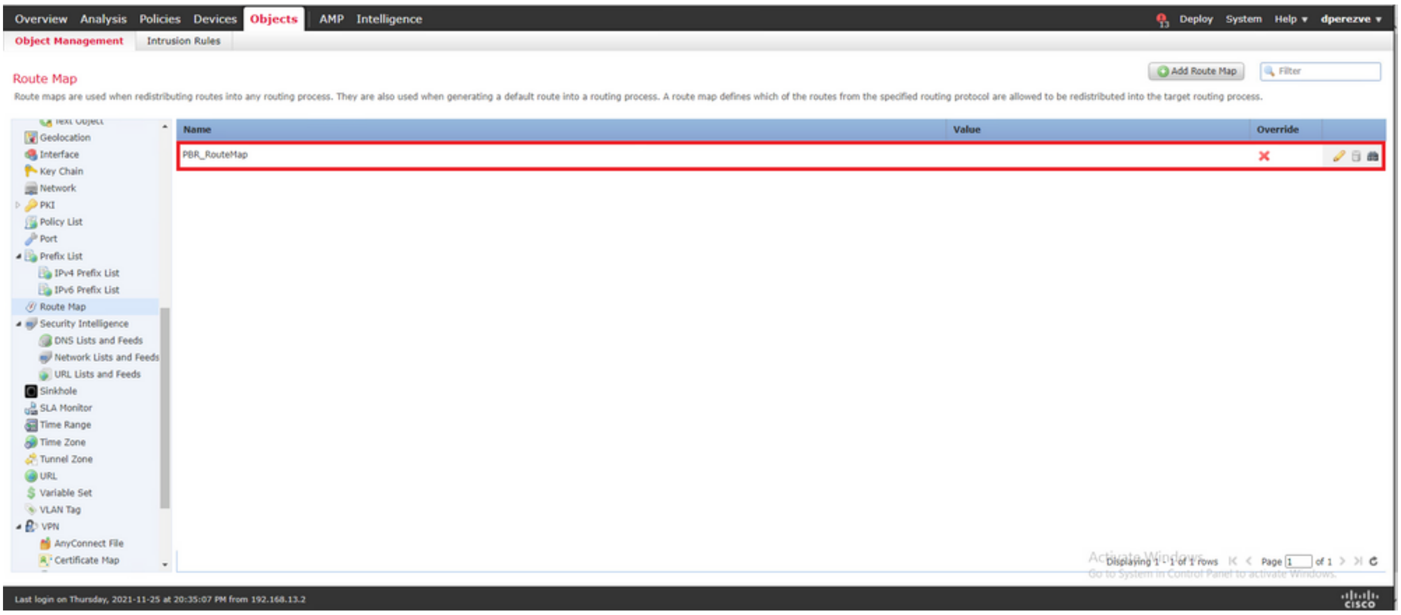
Sélectionnez l'objet de liste d'accès créé à l'étape 1.

Cliquer **Add** pour créer l'entrée.

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


Add Route Map Entry
Sequence No: 10
Redistribution: Allow
Match Clauses | Set Clauses
Security Zones
IPv4
IPv6
BGP
Others
Address (2) Next Hop (0) Route Source (0)
Select addresses to match as access list or prefix list addresses of route.
Access List Prefix List
Available Access Lists : Extended
Available Extended Access List
Search
PBR_ACL
Selected Extended Access List
PBR_ACL
Add
Add
Cancel

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



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
PBR_RouteMap		✗

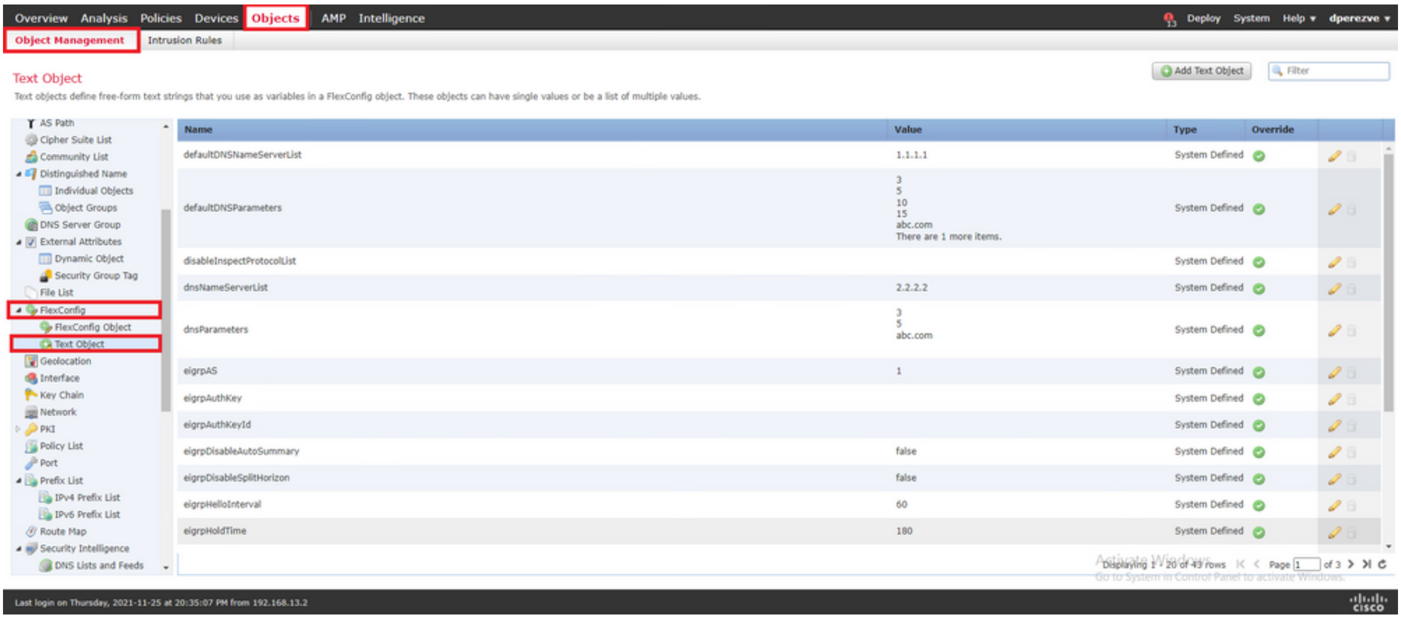
Displaying 1 - 1 of 1 rows Page 1 of 1

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

Étape 3. Configurer 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.

Pour définir un objet texte FlexConfig, accédez à **Objects > Object Management** et sélectionnez **Text Object** sous la **FlexConfig** dans la table des matières.



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.

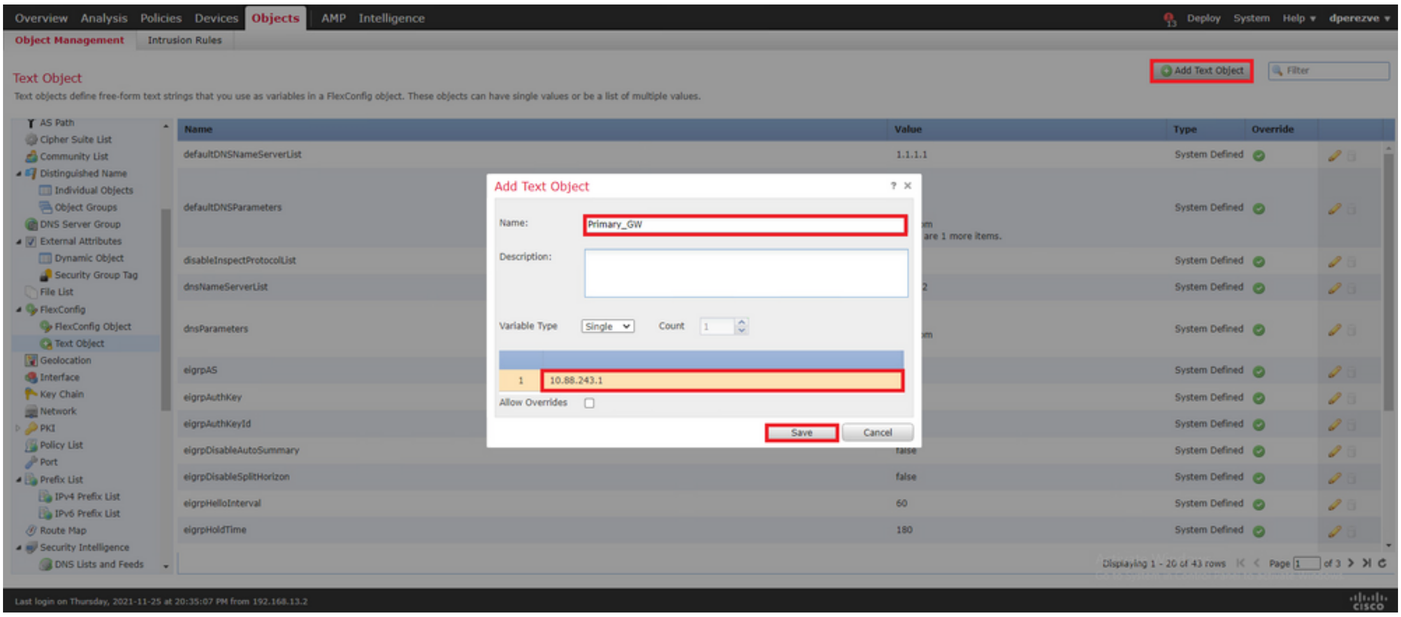
Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	✓
defaultDNSParameters	3 5 10 15 abc.com There are 1 more items.	System Defined	✓
disableInspectProtocolList		System Defined	✓
dnsNameServerList	2.2.2.2	System Defined	✓
dnsParameters	3 5 abc.com	System Defined	✓
eigrpAS	1	System Defined	✓
eigrpAuthKey		System Defined	✓
eigrpAuthKeyId		System Defined	✓
eigrpDisableAutoSummary	false	System Defined	✓
eigrpDisableSplitHorizon	false	System Defined	✓
eigrpHelloInterval	60	System Defined	✓
eigrpHoldTime	180	System Defined	✓

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

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

Cliquer **Save** pour ajouter le nouvel objet.



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 □

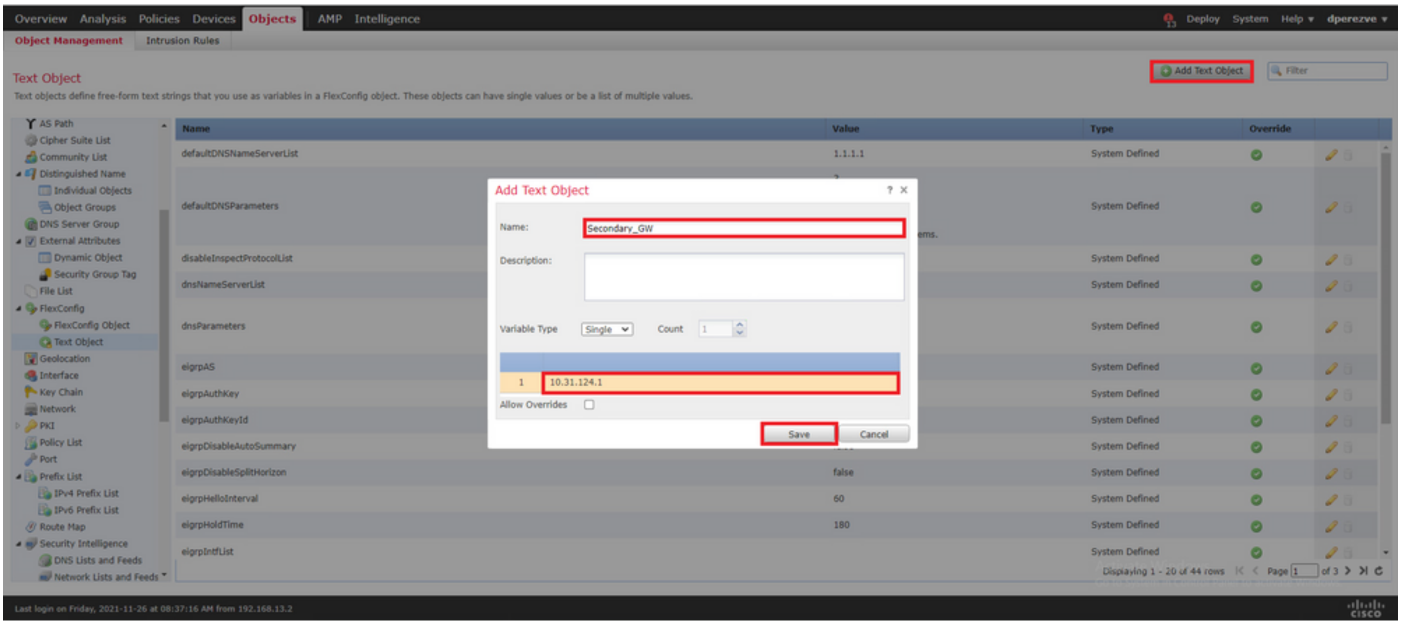
Save   Cancel

Displaying 1 - 20 of 43 rows

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

Cliquer **Add Text Object** à nouveau pour créer un deuxième objet, cette fois pour le modem routeur sur le circuit de sauvegarde.

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



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

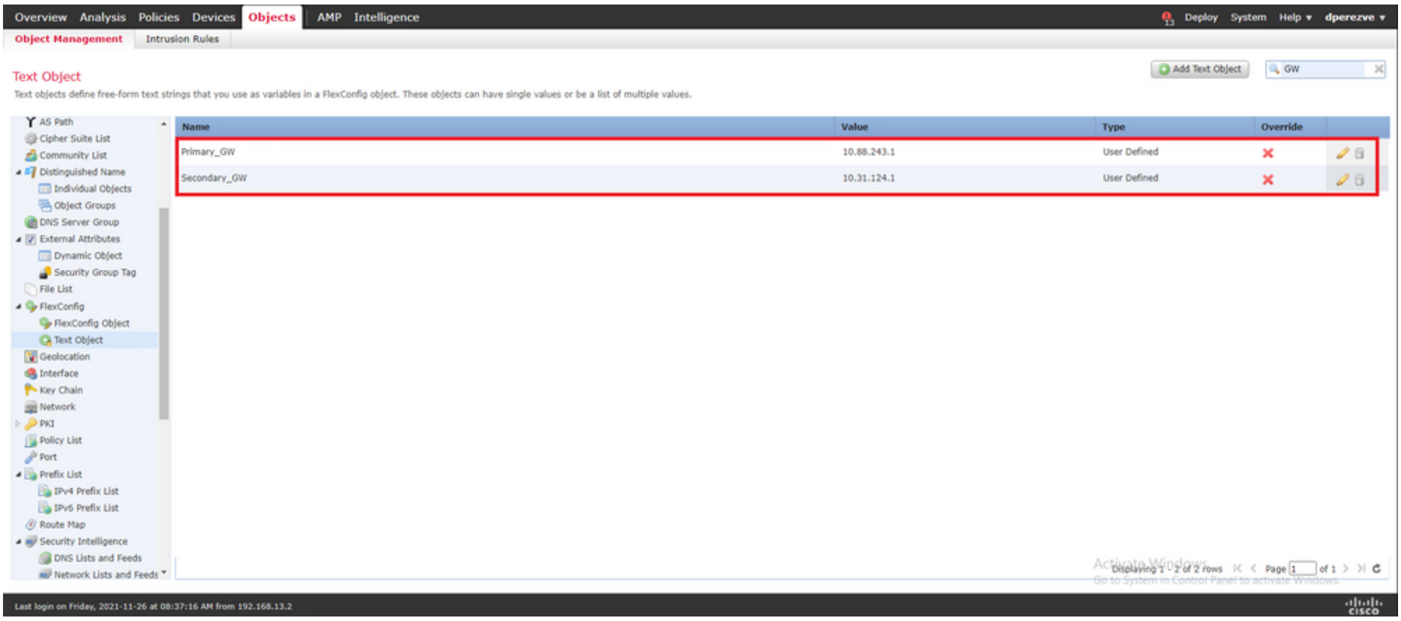
Allow Overrides □

Save   Cancel

Displaying 1 - 20 of 44 rows

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

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



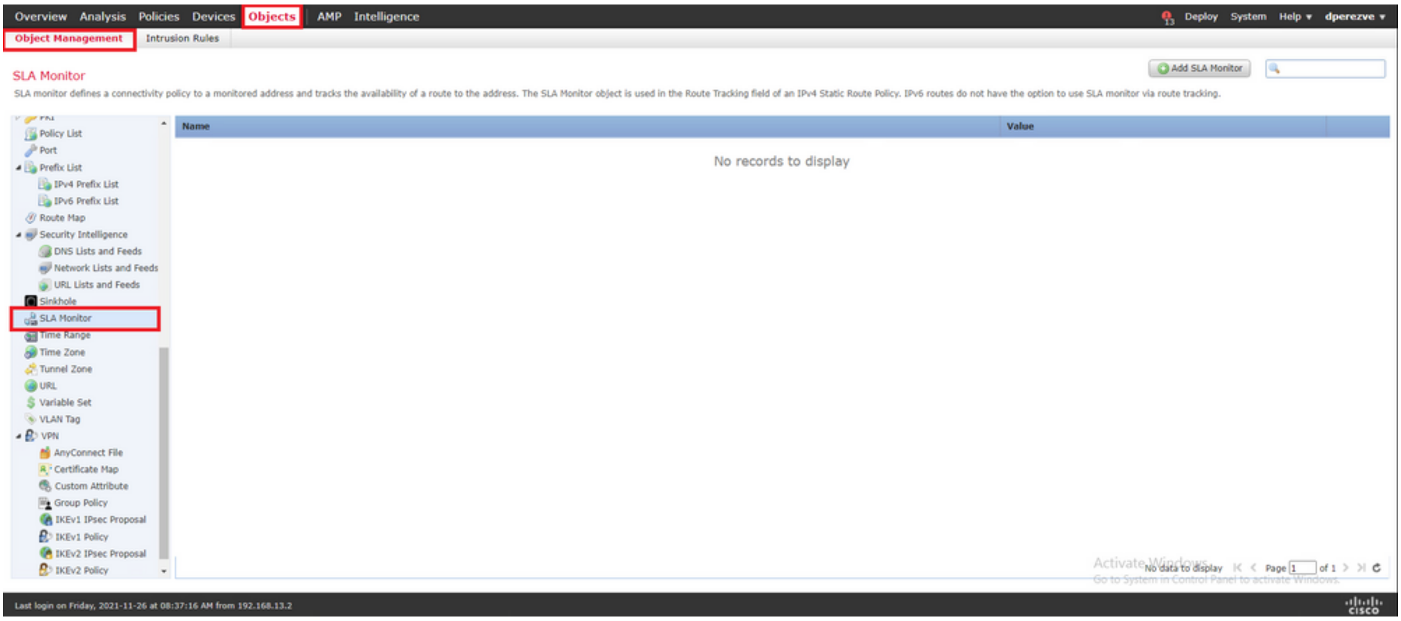
Text Object

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	✗
Secondary_GW	10.31.124.1	User Defined	✗

Étape 4. Configurer le Moniteur SLA

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



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	

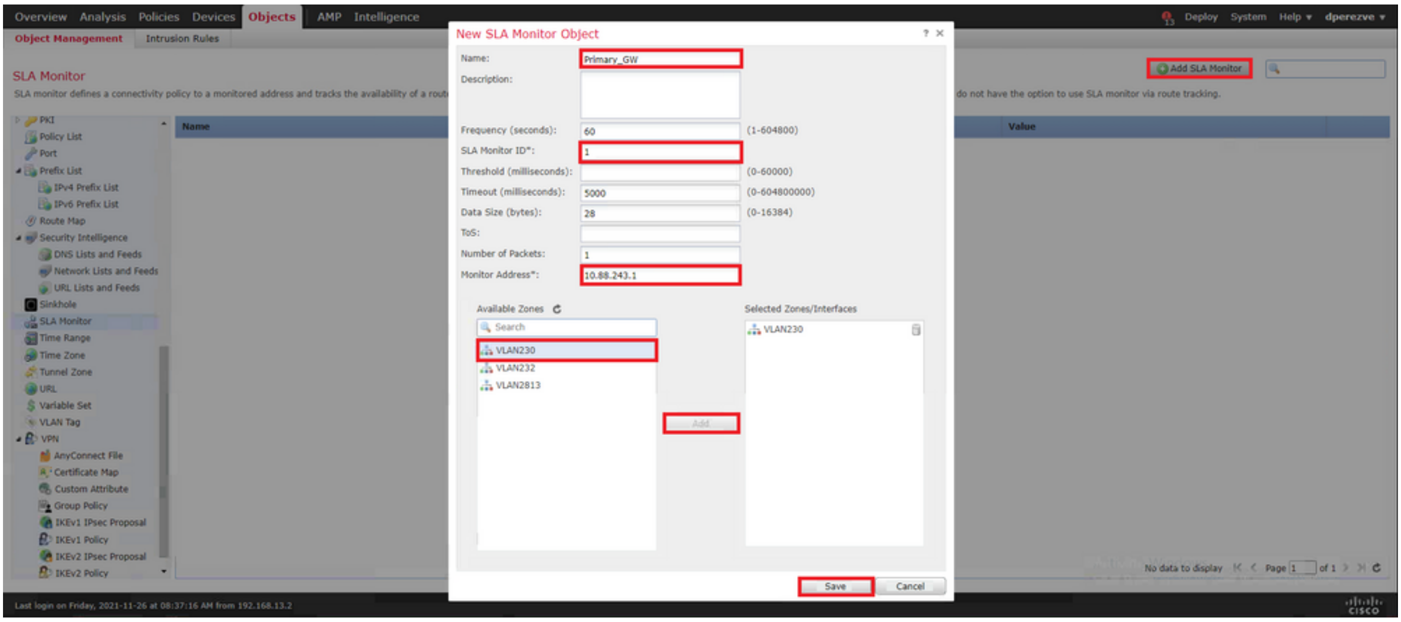
Sélectionnez le **Add SLA Monitor** objet.

Dans la **New SLA Monitor** , définissez un nom ainsi qu'un identifiant pour l'opération SLA, l'adresse IP du périphérique qui doit être surveillé (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. Cliquer **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 d'attente et de seuil ne sont pas spécifiées, FTD utilise des compteurs par défaut : 5 000 milisecondes dans chaque cas.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
Add SLA Monitor
Name
Value
No data to display Page 1 of 1

SLA Monitor

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rout … do not have the option to use SLA monitor via route tracking.

New SLA Monitor Object

Name:	Primary_GW	
Description:		
Frequency (seconds):	60	(1-604800)
SLA Monitor ID*:	1	
Threshold (milliseconds):		(0-60000)
Timeout (milliseconds):	5000	(0-604800000)
Data Size (bytes):	28	(0-16384)
ToS:		
Number of Packets:	1	
Monitor Address*:	10.88.243.1	

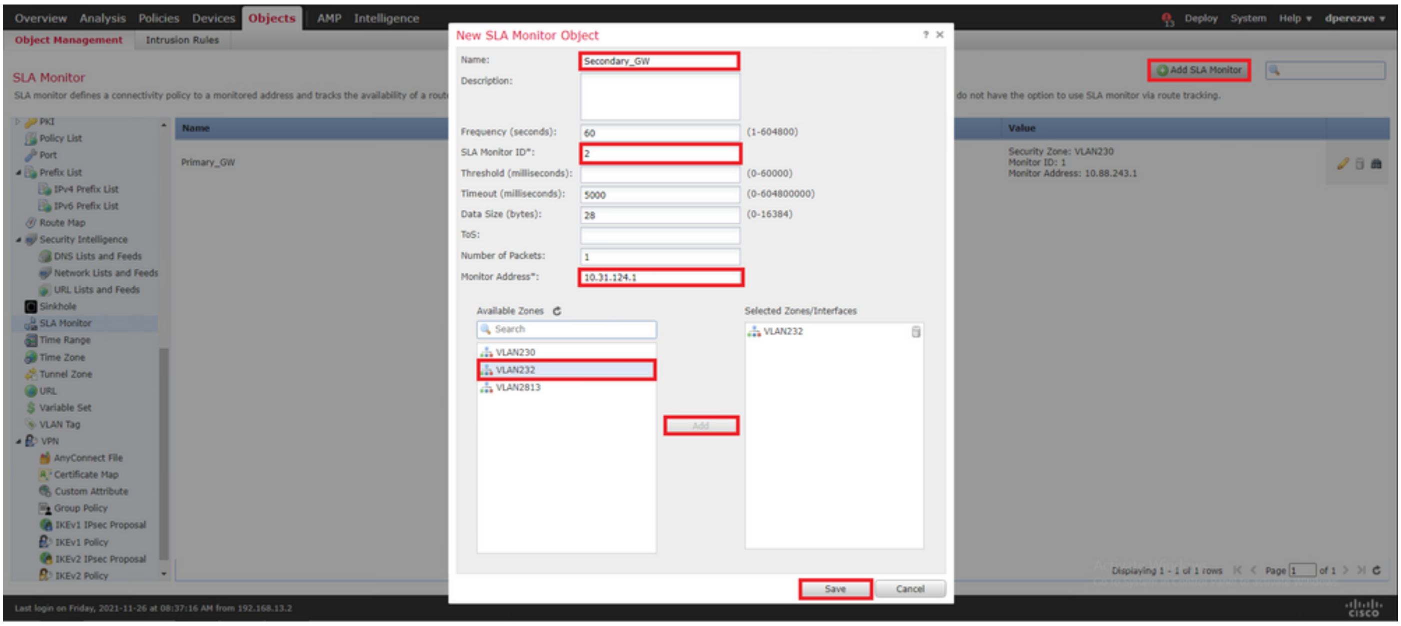
Available Zones: VLAN230, VLAN232, VLAN2813

Selected Zones/Interfaces: VLAN230

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

Sélectionnez le **Add SLA Monitor** afin de 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.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
Add SLA Monitor
Name
Value
Displaying 1 - 1 of 1 rows Page 1 of 1

SLA Monitor

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rout … do not have the option to use SLA monitor via route tracking.

Primary_GW — Security Zone: VLAN230
Monitor ID: 1
Monitor Address: 10.88.243.1

New SLA Monitor Object

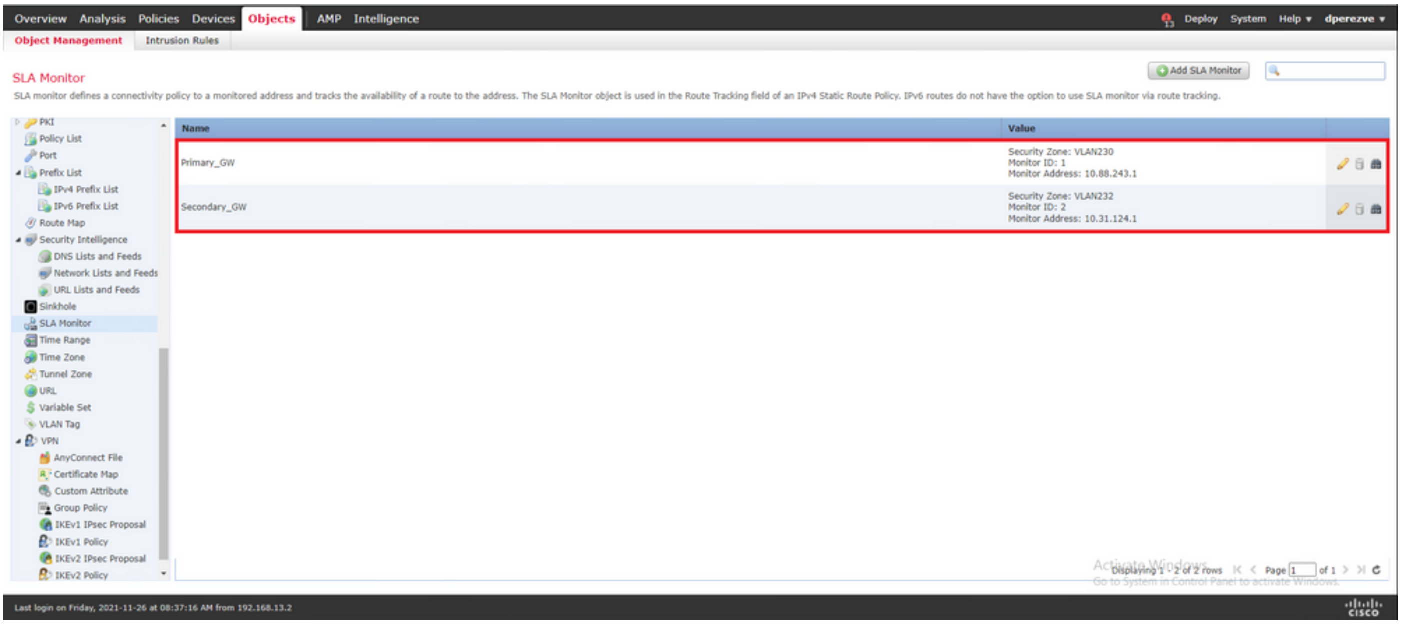
Name:	Secondary_GW	
Description:		
Frequency (seconds):	60	(1-604800)
SLA Monitor ID*:	2	
Threshold (milliseconds):		(0-60000)
Timeout (milliseconds):	5000	(0-604800000)
Data Size (bytes):	28	(0-16384)
ToS:		
Number of Packets:	1	
Monitor Address*:	10.31.124.1	

Available Zones: VLAN230, VLAN232, VLAN2813

Selected Zones/Interfaces: VLAN232

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

Les deux objets doivent être ajoutés à la liste.



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.

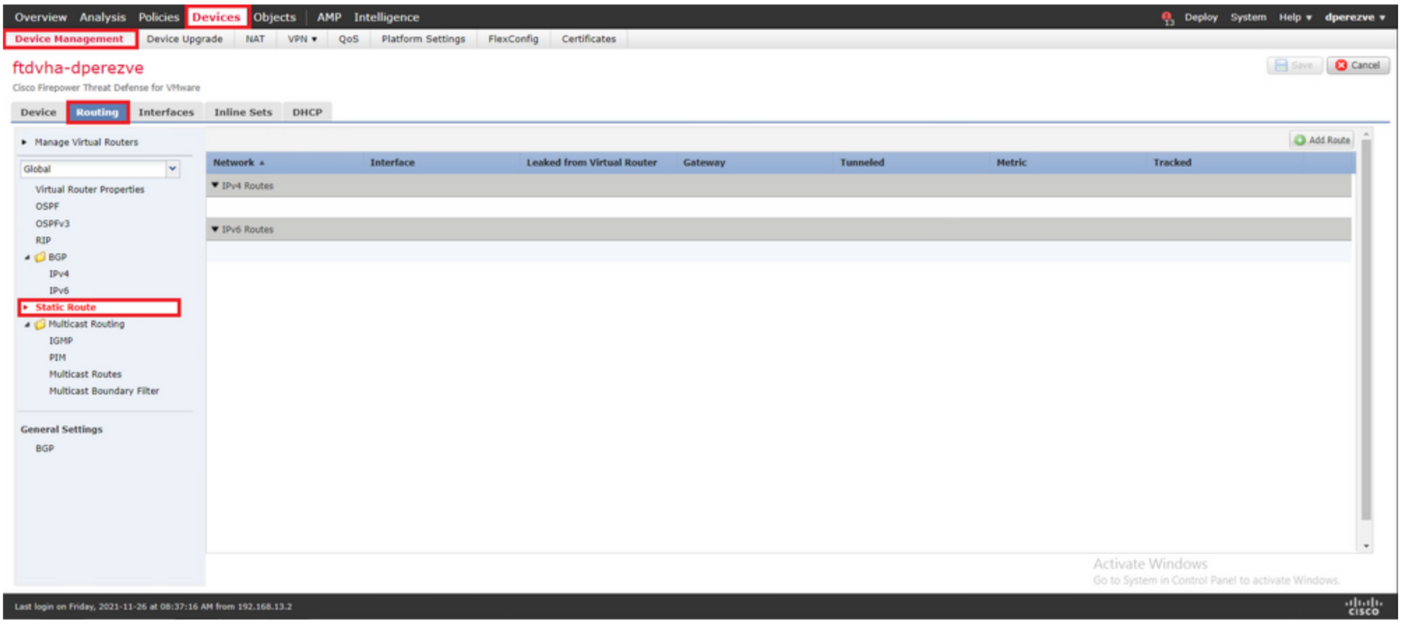
Name	Value
Primary_GW	Security Zone: VLAN230 Monitor ID: 1 Monitor Address: 10.88.243.1
Secondary_GW	Security Zone: VLAN232 Monitor ID: 2 Monitor Address: 10.31.124.1

Étape 4. Configuration de routes statiques avec route track

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, accédez à **Devices > Device Management** , modifiez le FTD disponible et sélectionnez **Static Route** dans la table des matières de l' **Routing** s'affiche.

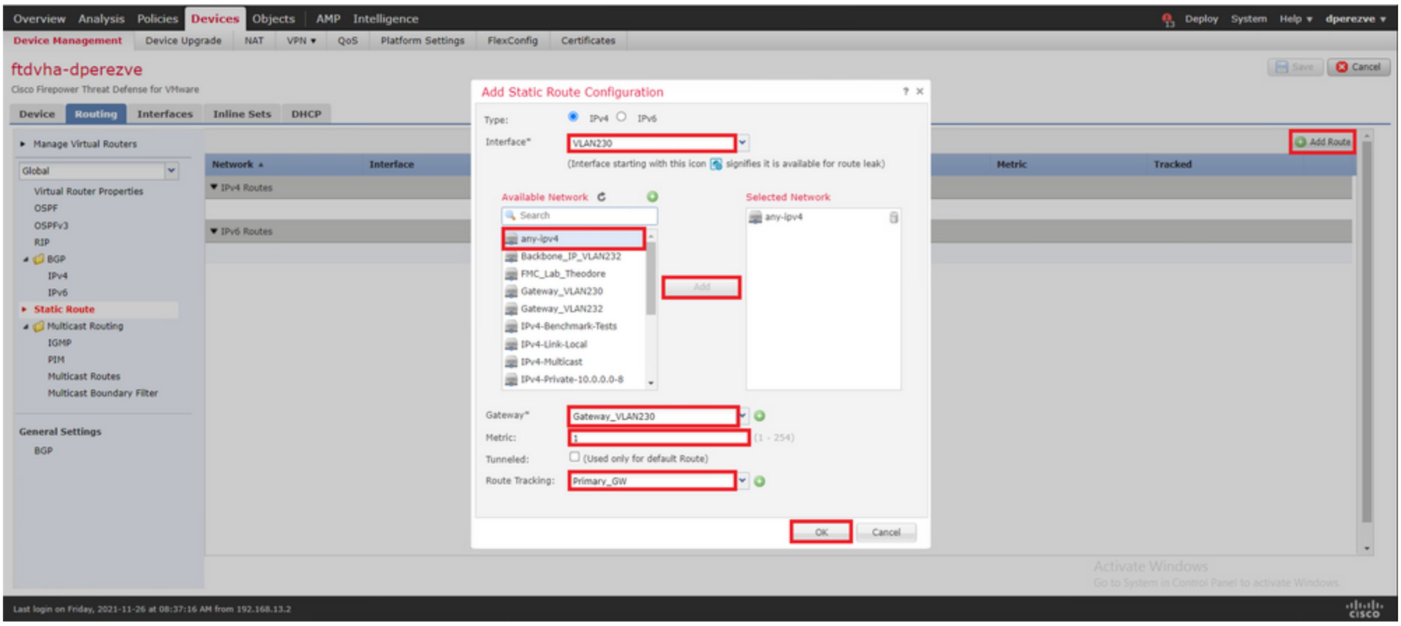


Dans la **Add Static Route Configuration** , dans la liste déroulante **Interface**, spécifiez le nom de l'interface par laquelle le modem routeur principal doit être accessible.

Sélectionnez ensuite le réseau de destination et le modem routeur principal dans le champ **Gateway** dans la liste déroulante.

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

Cliquez sur **OK** pour ajouter la nouvelle route.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
ftdvha-dperezve
Cisco Firepower Threat Defense for VMware
Save Cancel
Device Routing Interfaces Inline Sets DHCP
Manage Virtual Routers
Global
Virtual Router Properties
OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter
General Settings
BGP
Add Route
Network ▲ Interface Metric Tracked
▼ IPv4 Routes
▼ IPv6 Routes
Add Static Route Configuration
Available Network
Search
Add
Selected Network
OK Cancel
Activate Windows
Go to System in Control Panel to activate Windows.
Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2

Type: ● IPv4 ○ IPv6

Interface*: VLAN230

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

Available Network: any-ipv4, Backbone_IP_VLAN232, FMC_Lab_Theodore, Gateway_VLAN230, Gateway_VLAN232, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8

Selected Network: any-ipv4

Gateway*: Gateway_VLAN230

Metric: 1 (1 - 254)

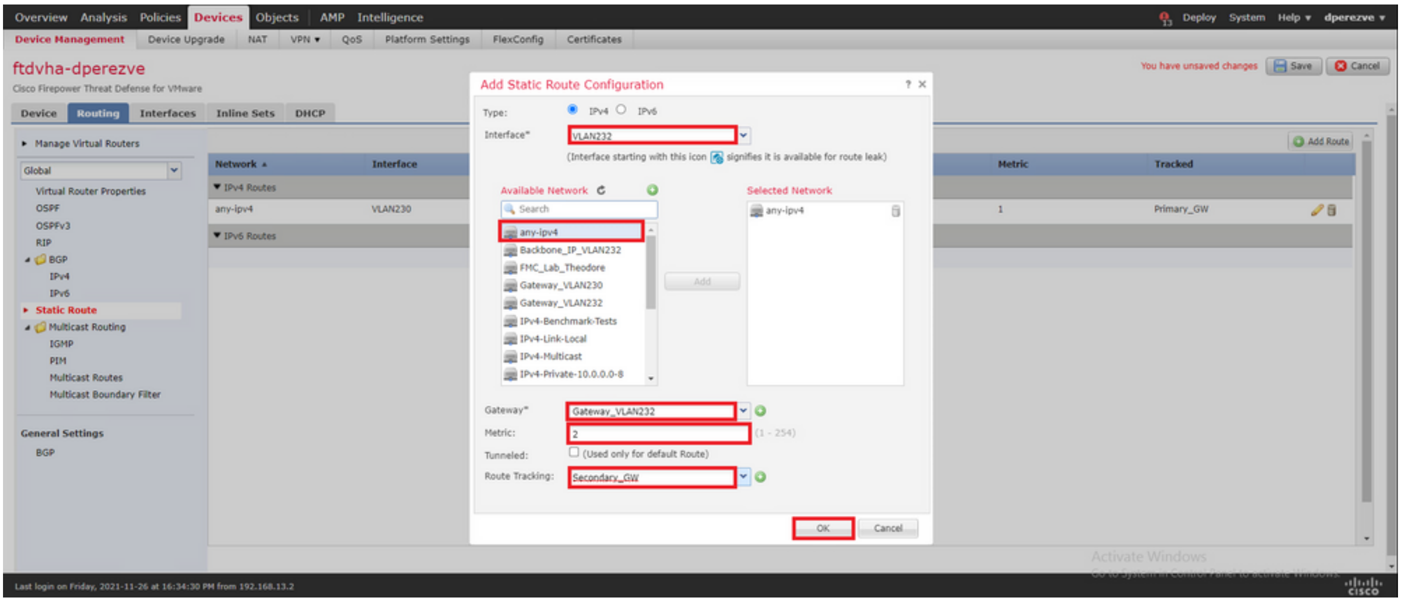
Tunneled: □ (Used only for default Route)

Route Tracking: Primary_GW

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

Cliquer **Add Route** pour définir une nouvelle route statique.

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


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
ftdvha-dperezve
Cisco Firepower Threat Defense for VMware
You have unsaved changes Save Cancel
Device Routing Interfaces Inline Sets DHCP
Manage Virtual Routers
Global
Virtual Router Properties
OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter
General Settings
BGP
Add Route
Add Static Route Configuration
Available Network
Search
Add
Selected Network
OK Cancel
Activate Windows
Go to System in Control Panel to activate Windows.
Last login on Friday, 2021-11-26 at 16:34:30 PM from 192.168.13.2

Network ▲	Interface	Metric	Tracked
▼ IPv4 Routes			
any-ipv4	VLAN230	1	Primary_GW
▼ IPv6 Routes			

Type: ● IPv4 ○ IPv6

Interface*: VLAN232

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

Available Network: any-ipv4, Backbone_IP_VLAN232, FMC_Lab_Theodore, Gateway_VLAN230, Gateway_VLAN232, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8

Selected Network: any-ipv4

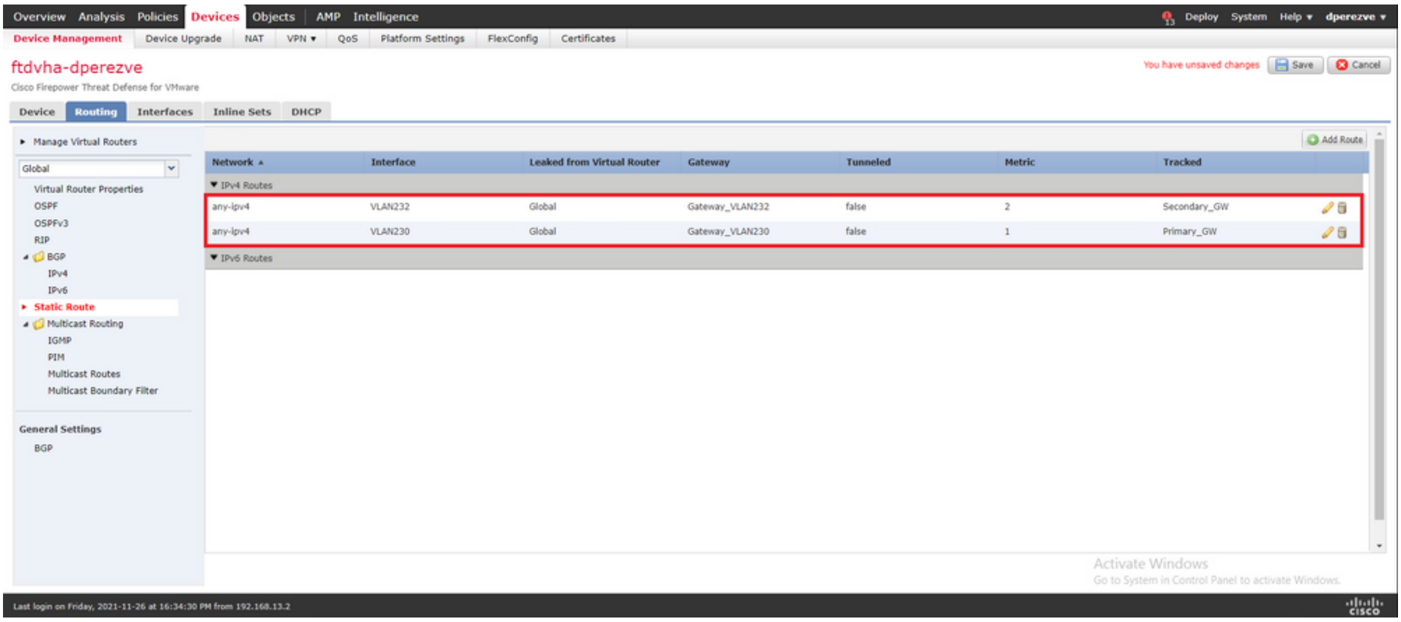
Gateway*: Gateway_VLAN232

Metric: 2 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking: Secondary_GW

Les deux routes doivent être ajoutées à la liste.



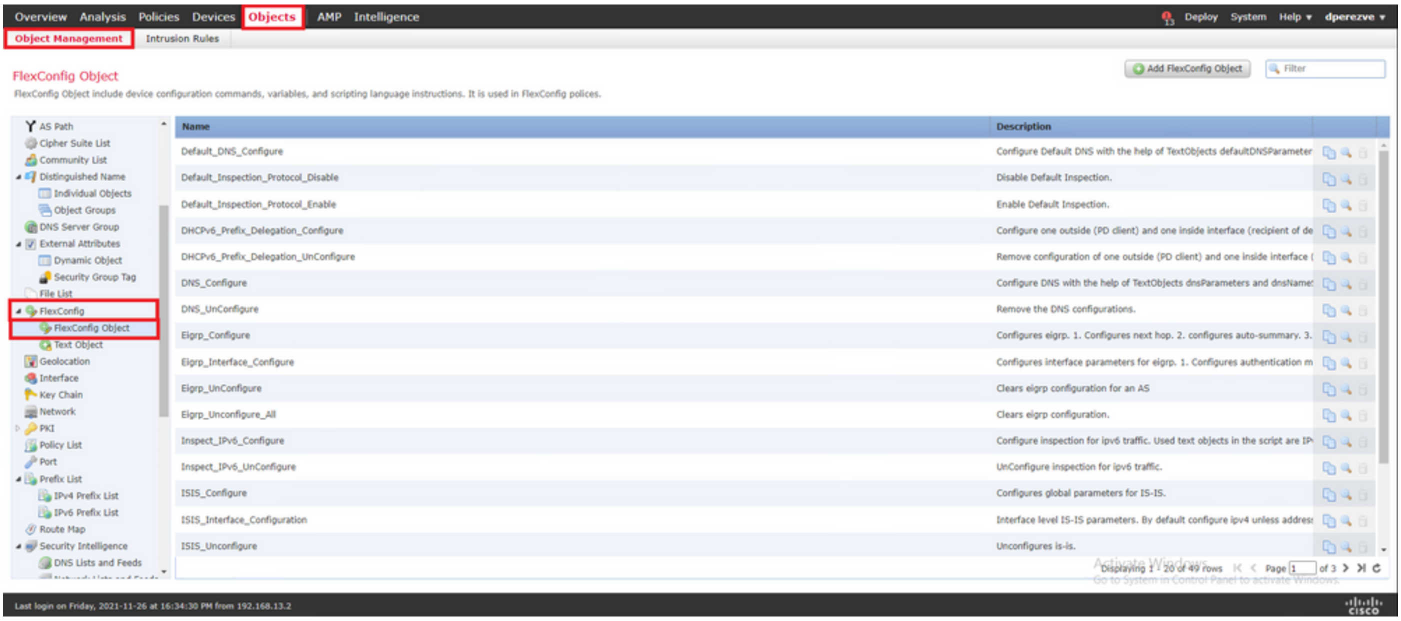
Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	VLAN232	Global	Gateway_VLAN232	false	2	Secondary_GW
any-ipv4	VLAN230	Global	Gateway_VLAN230	false	1	Primary_GW
▼ IPv6 Routes						

Étape 5. Configurer 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, accédez à **Objects > Object Management** et sélectionnez **FlexConfig Object** sous la **FlexConfig** dans la table des matières.

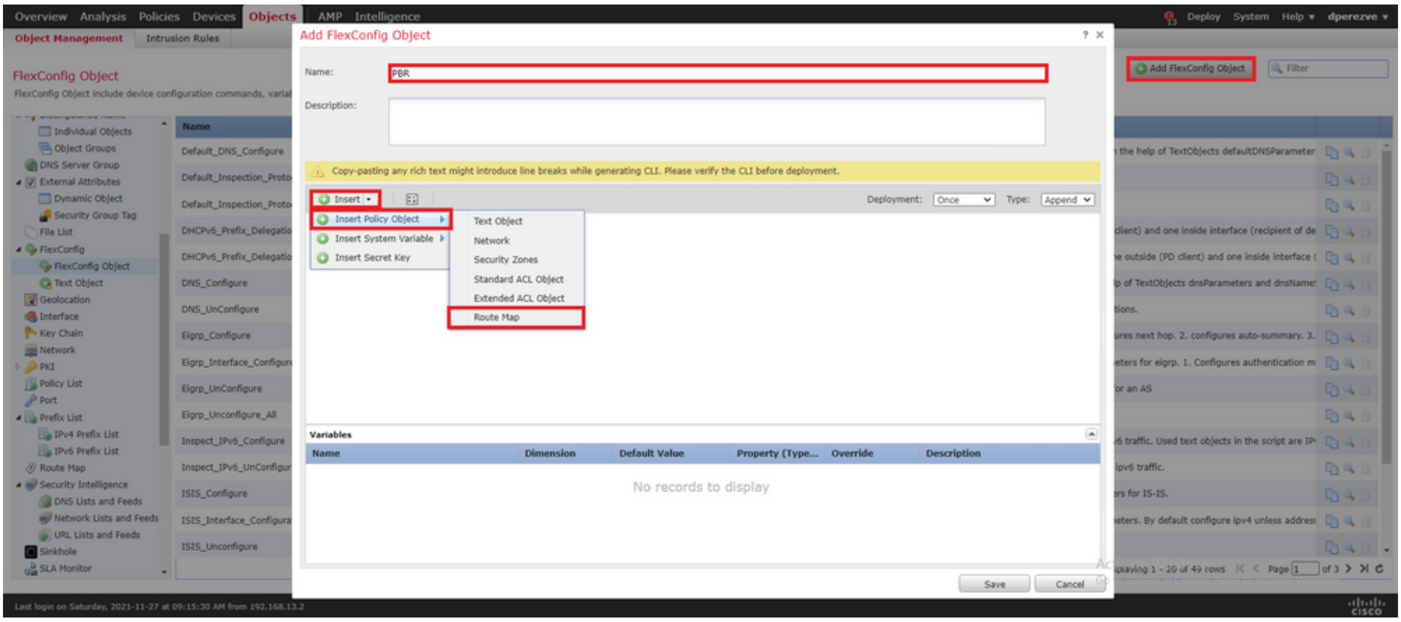


FlexConfig Object

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.

Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNSParameter
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (
DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName:
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP\
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless addres:
ISIS_Unconfigure	Unconfigures is-is.

Sélectionnez le **Add FlexConfig Object** s'affiche. Dans la **Add FlexConfig Object** attribuer un nom et accéder à **Insert > Insert Policy Object > Route Map** .



Add FlexConfig Object

Name: PBR

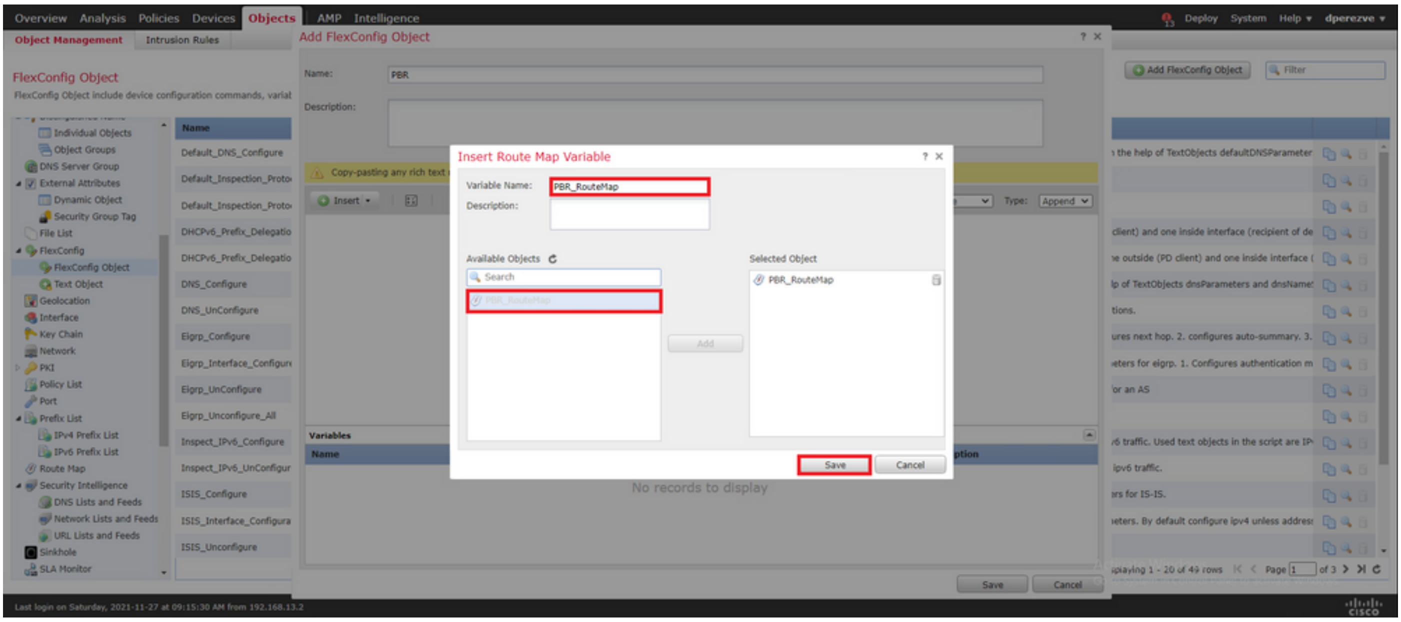
Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once Type: Append

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

Cliquer **Save** pour ajouter le mappage de route dans le cadre de l'objet FlexConfig.

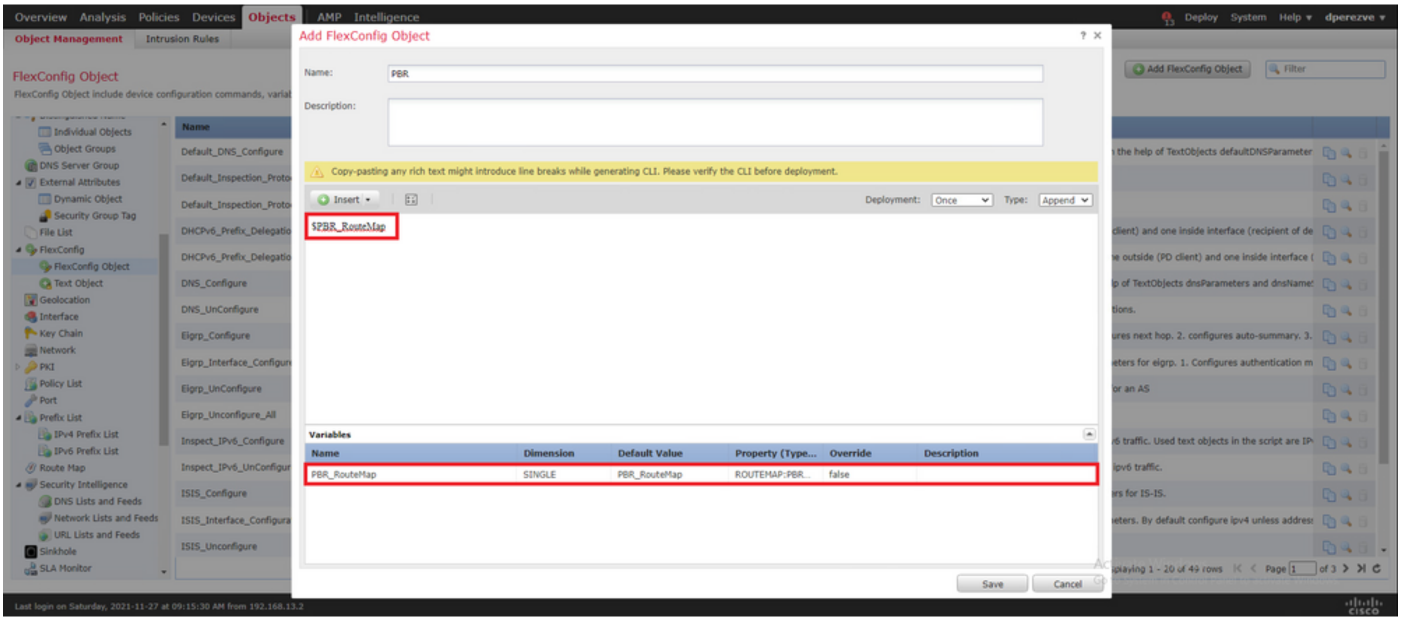

Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
FlexConfig Object
Add FlexConfig Object
Insert Route Map Variable
Available Objects
Search
Add
Selected Object
Save Cancel

Insert Route Map Variable

Variable Name: PBR_RouteMap

Description:

Selected Object: PBR_RouteMap



Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
Add FlexConfig Object
Insert
Save
Cancel

Name: PBR

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

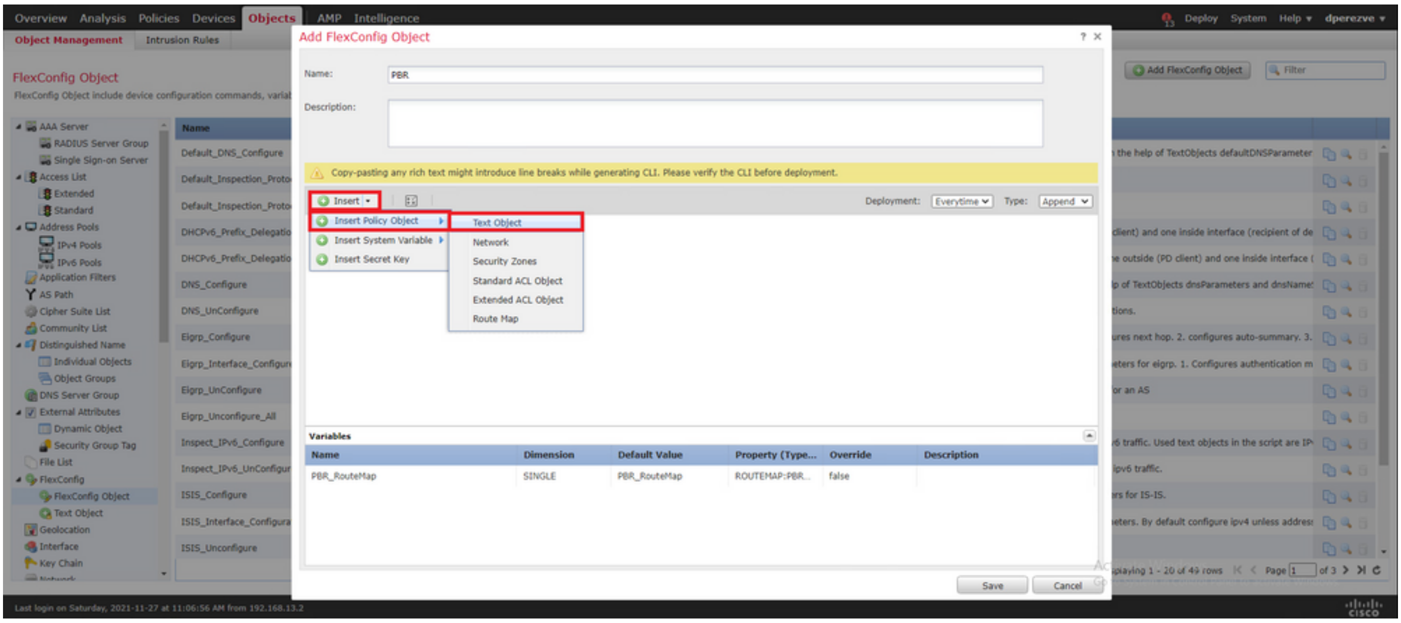
Deployment: Once Type: Append

```
$PBR_RouteMap
```

Variables

Name	Dimension	Default Value	Property (Type...	Override	Description
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	

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 **Add FlexConfig Object** fenêtre accéder à **Insert > Insert Policy Object > Text Object .**



Name: PBR

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

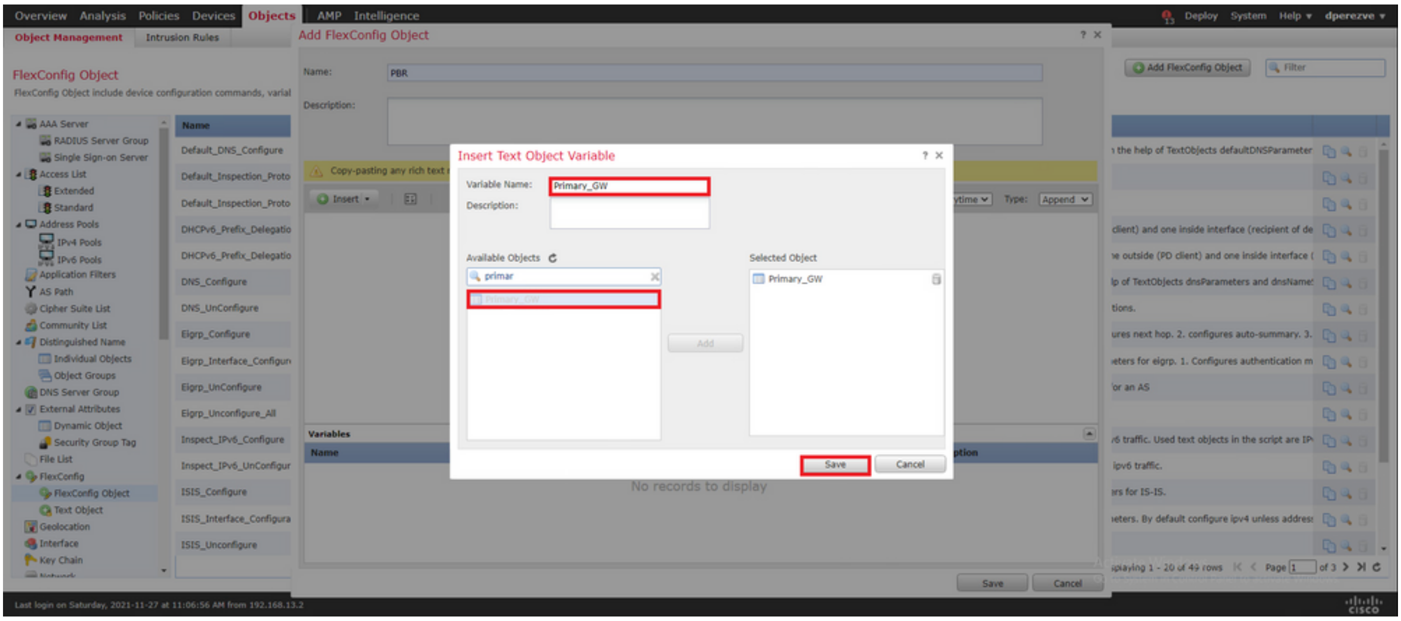
Deployment: Everytime Type: Append

Variables

Name	Dimension	Default Value	Property (Type...	Override	Description
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	

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

Cliquer **Save** afin de l'ajouter à l'objet FlexConfig.



Name: PBR

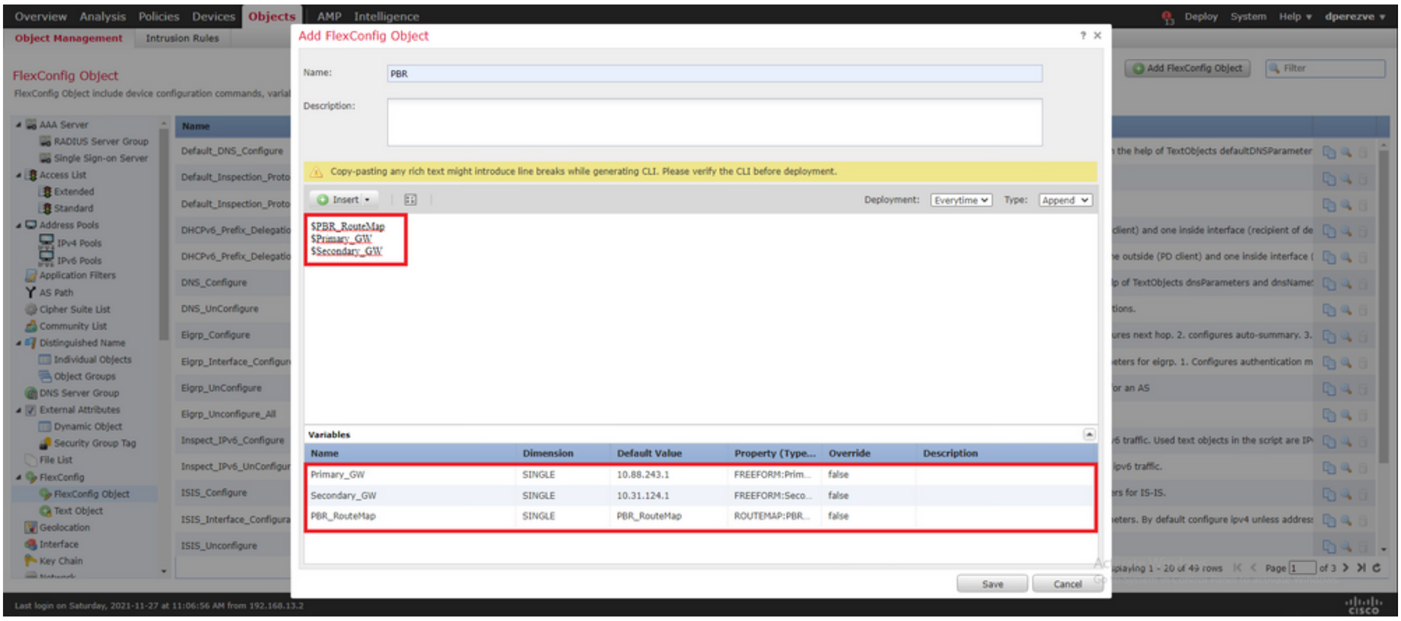
Variable Name: Primary_GW

Description:

Available Objects: primar — Primary_GW

Selected Object: Primary_GW

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



Name: PBR

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Everytime Type: Append

```
$PBR_RouteMap
$Primary_GW
$Secondary_GW
```

Variables

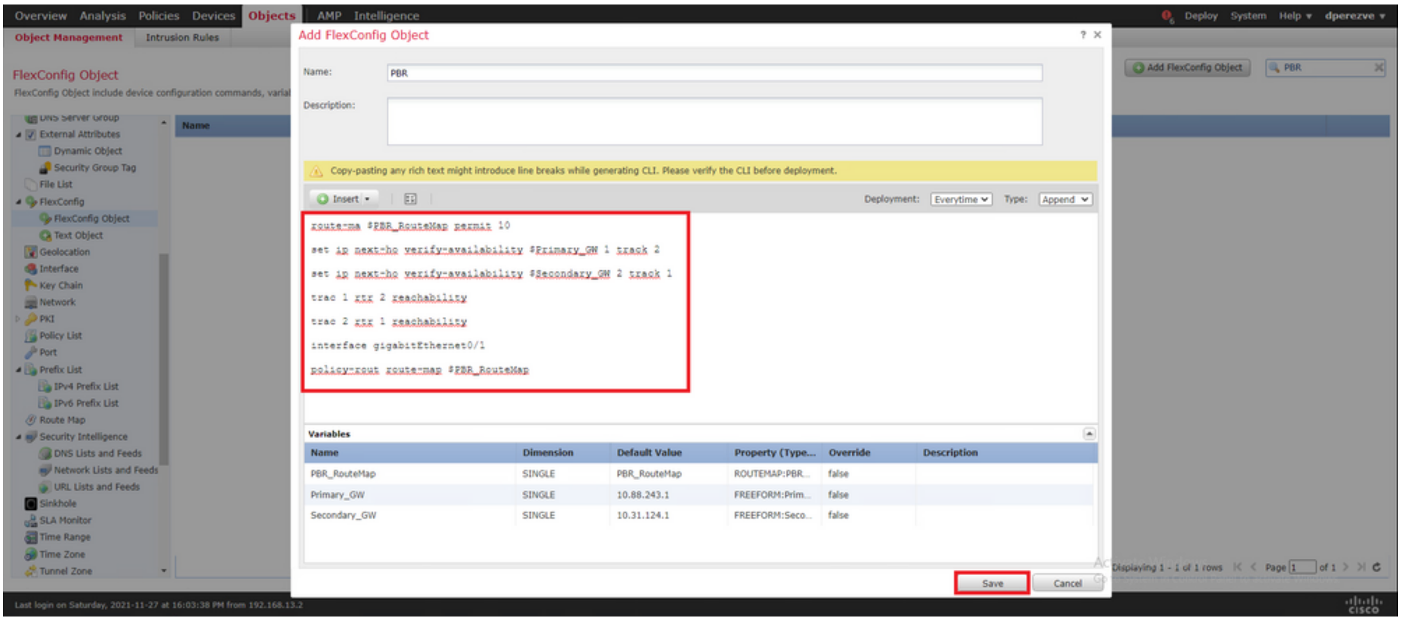
Name	Dimension	Default Value	Property (Type...	Override	Description
Primary_GW	SINGLE	10.88.243.1	FREEFORM:Prim...	false	
Secondary_GW	SINGLE	10.31.124.1	FREEFORM:Seco...	false	
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	

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, le **set ip next-hop verify-availability** doit être utilisée.

Le mappage de route doit être appliqué à l'interface interne, dans ce cas VLAN2813. Utilisation **policy-route route-map** sous la configuration d'interface.

Cliquer **Save** lorsque la configuration est terminée.



Add FlexConfig Object

Name: PBR

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

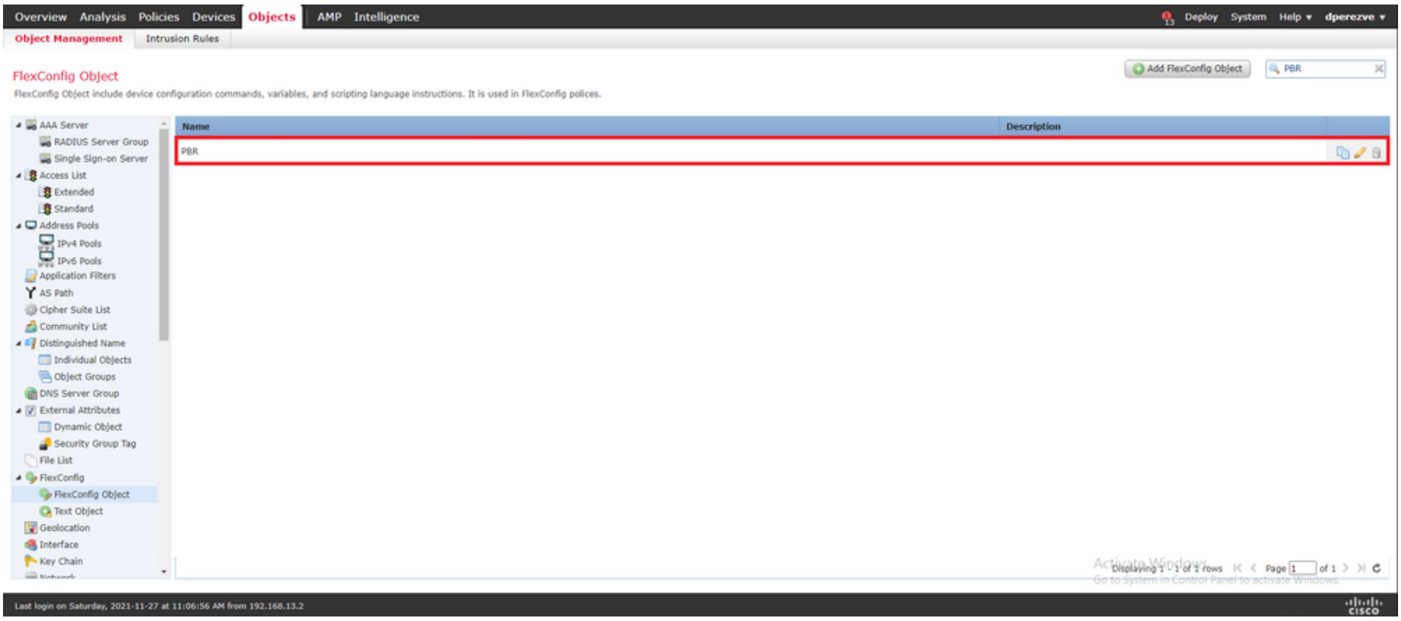
Deployment: Everytime Type: Append

```
route-ma $PBR_RouteMap permit 10
set ip next-ho verify-availability $Primary_GW 1 track 2
set ip next-ho verify-availability $Secondary_GW 2 track 1
trac 1 rtr 2 reachability
trac 2 rtr 1 reachability
interface gigabitEthernet0/1
policy-rout route-map $PBR_RouteMap
```

Variables

Name	Dimension	Default Value	Property (Type...	Override	Description
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	
Primary_GW	SINGLE	10.88.243.1	FREEFORM:Prim...	false	
Secondary_GW	SINGLE	10.31.124.1	FREEFORM:Seco...	false	

L'objet FlexConfig doit être ajouté à la liste.



FlexConfig Object

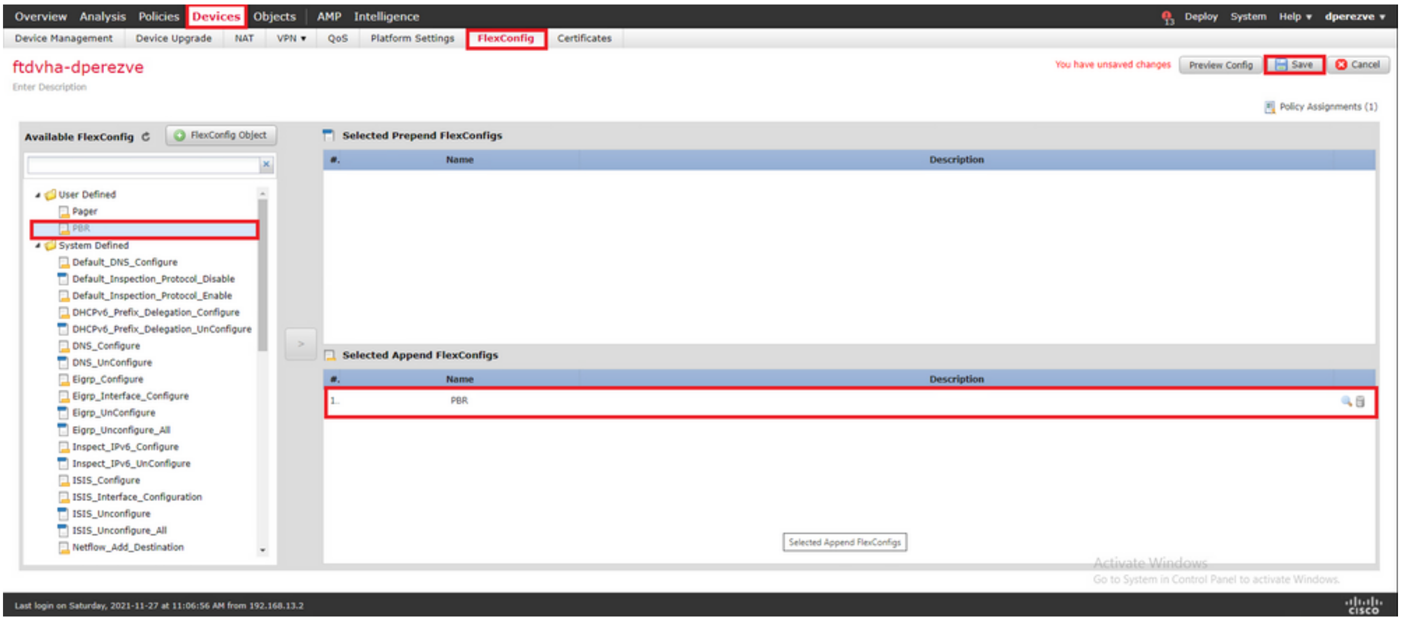
FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.

Name	Description
PBR	

Étape 6. Attribuer l'objet FlexConfig PBR à la politique FlexConfig

Naviguez jusqu'à **Devices** > **FlexConfig** et modifiez la stratégie FlexConfig disponible.

Sélectionnez l'objet PBR FlexConfig dans **Available FlexConfig** table des matières, enregistrer les modifications et déployer 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 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
```

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 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
```

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 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
```

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 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
```

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.