Configurar PBR com SLAs IP para ISP DUAL no FTD Gerenciado pelo FMC

Contents

Introduction

Este documento descreve como configurar o PBR junto com os SLAs IP em um FTD que é gerenciado pelo (FMC).

Contribuição de Daniel Perez Verti Vazquez, engenheiro do Cisco TAC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- configuração de PBR em **Cisco Adaptive Security Appliance (ASA)**
- FlexConfig ativado **Firepower**
- SLAs IP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco FTD versão 7.0.0 (Build 94)
- Cisco FMC versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar **Policy Based Routing (PBR)** juntamente com **Internet Protocol Service Level Agreement (IP SLA)** em um Cisco **Firepower Threat Defense (FTD)** que é gerenciado pelo Cisco **Firepower Management Center (FMC)**.

O roteamento tradicional toma decisões de encaminhamento com base apenas nos endereços IP de destino. O PBR é uma alternativa aos protocolos de roteamento e roteamento estático.

Ele fornece um controle mais granular sobre o roteamento, pois permite o uso de parâmetros como endereços IP de origem ou portas de origem e destino como critérios de roteamento além do endereço IP de destino.

Possíveis cenários para PBR incluem aplicativos sensíveis à origem ou tráfego em links dedicados.

Junto com o PBR, os SLAs IP podem ser implementados para garantir a disponibilidade do próximo salto. Um SLA IP é um mecanismo que monitora a conectividade de ponta a ponta através da troca de pacotes regulares.

No momento da publicação, o PBR não é diretamente suportado através do CVP **Graphical User Interface (GUI)** , a configuração do recurso requer o uso de políticas FlexConfig.

Por outro lado, só **Internet Control Message Protocol (ICMP)** Os SLAs são suportados pelo FTD.

Neste exemplo, o PBR é usado para rotear pacotes sobre um primário **Internet Service Provider (ISP)** circuito baseado no endereço IP de origem.

Enquanto isso, um SLA IP monitora a conectividade e força um recuo para o circuito de backup em caso de qualquer falha.

Configurar

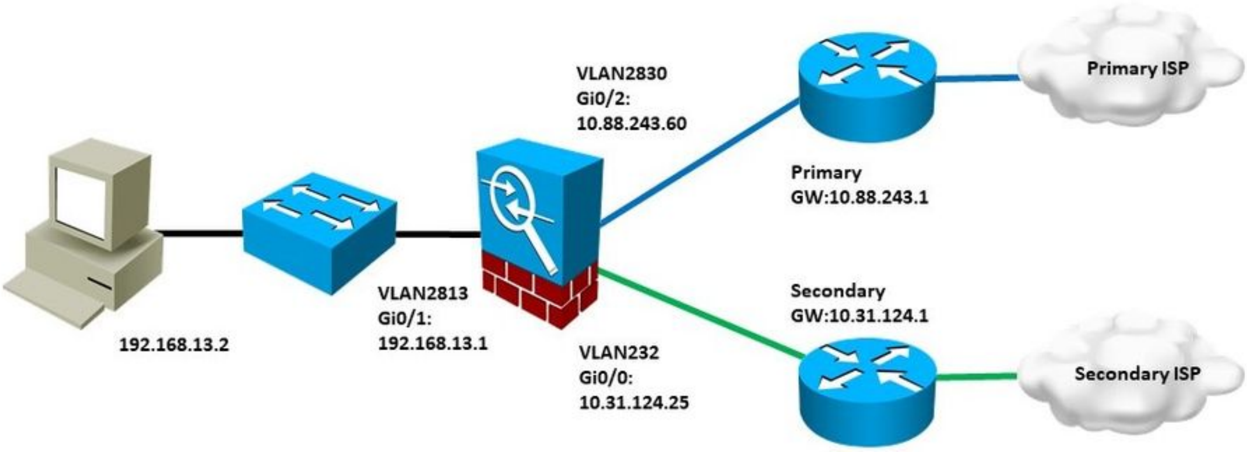
Diagrama de Rede

Neste exemplo, o Cisco FTD tem duas interfaces externas: VLAN230 e VLAN232. Cada um se conecta a um ISP diferente.

O tráfego da rede interna VLAN2813 é roteado através do ISP primário que usa PBR.

O mapa de rotas PBR toma decisões de encaminhamento com base apenas no endereço IP de origem (tudo o que é recebido da VLAN2813 deve ser roteado para 10.88.243.1 na VLAN230) e é aplicado na interface GigabitEthernet 0/1 de FTD.

Enquanto isso, o FTD usa SLAs IP para monitorar a conectividade com cada gateway do ISP. Em caso de qualquer falha na VLAN230, o FTD faz failovers para o circuito de backup na VLAN232.

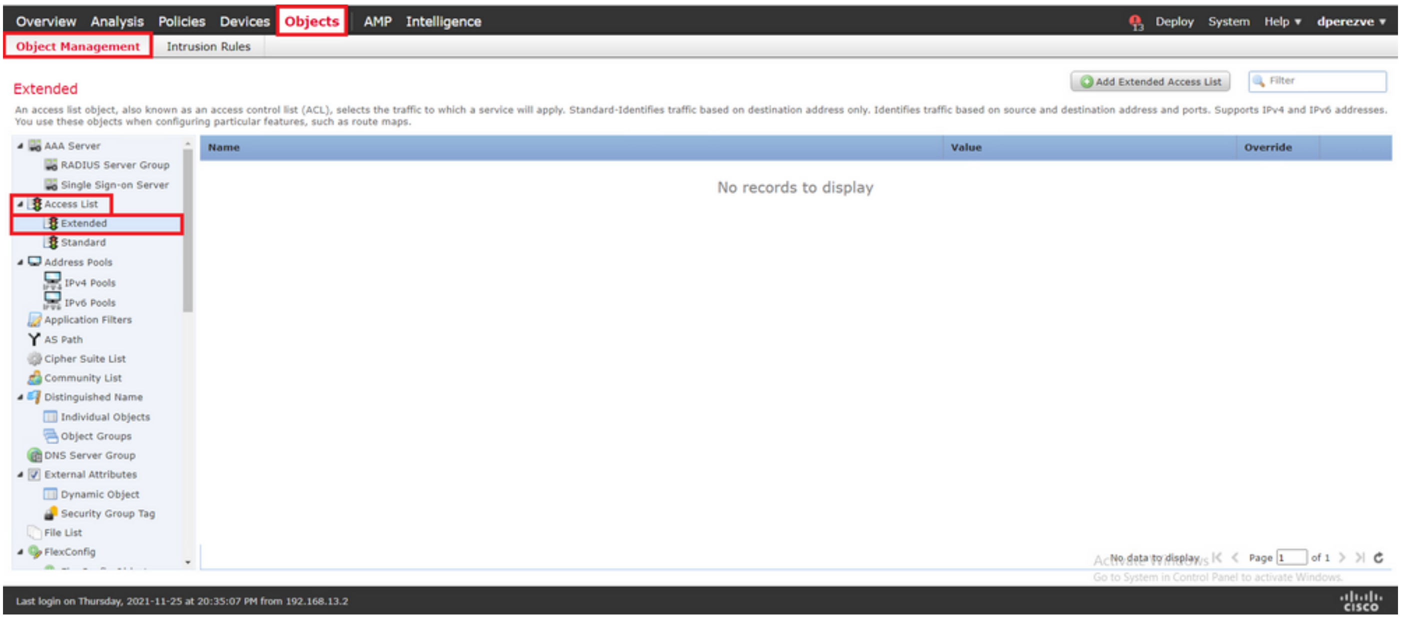


Configurações

Etapa 1. Configurar lista de acesso PBR

Na primeira etapa da configuração de PBR, defina quais pacotes devem ser sujeitos à política de roteamento. O PBR usa mapas de rotas e lista de acesso para identificar o tráfego.

Para definir uma lista de acesso para os critérios de correspondência, navegue até **Objects > Object Management** e selecione **Extended** sob o comando **Access List** categoria no sumário.



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

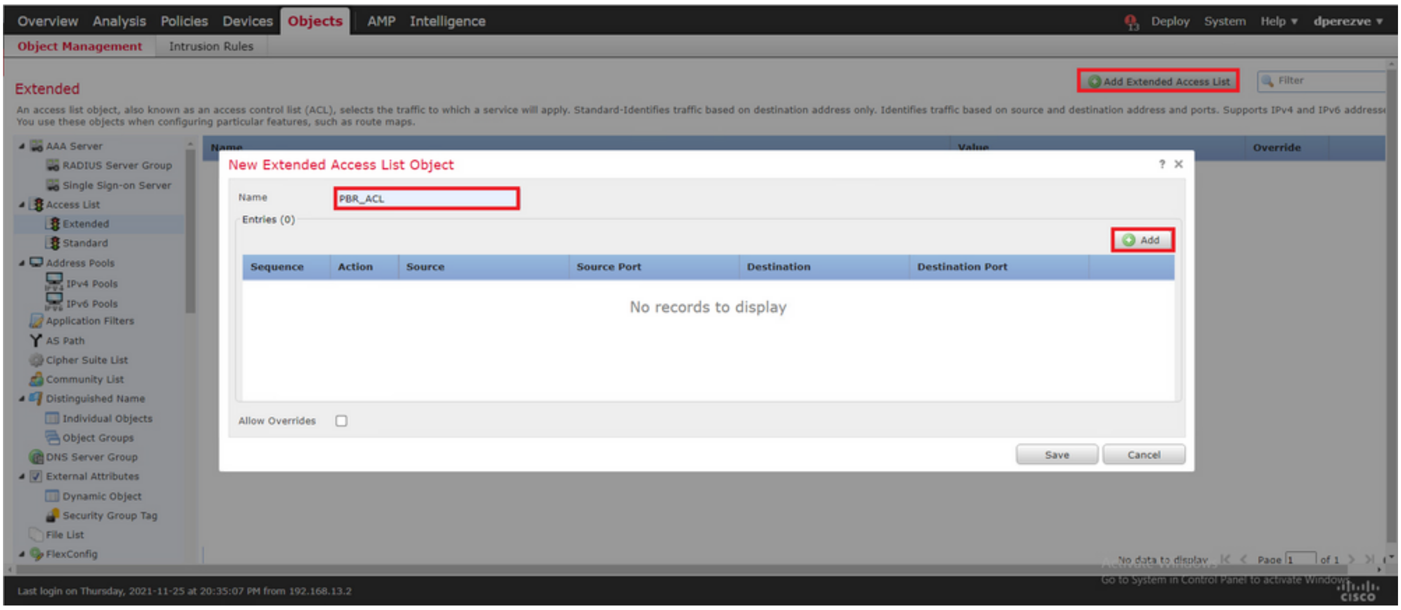
No records to display

No data to display

Activate Windows
Go to System in Control Panel to activate Windows.

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

Clique em **Add Extended Access List** . No **New Extended Access List Object** , atribua um nome para o objeto e selecione a **Add** para começar com a configuração da lista de acesso.



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.

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

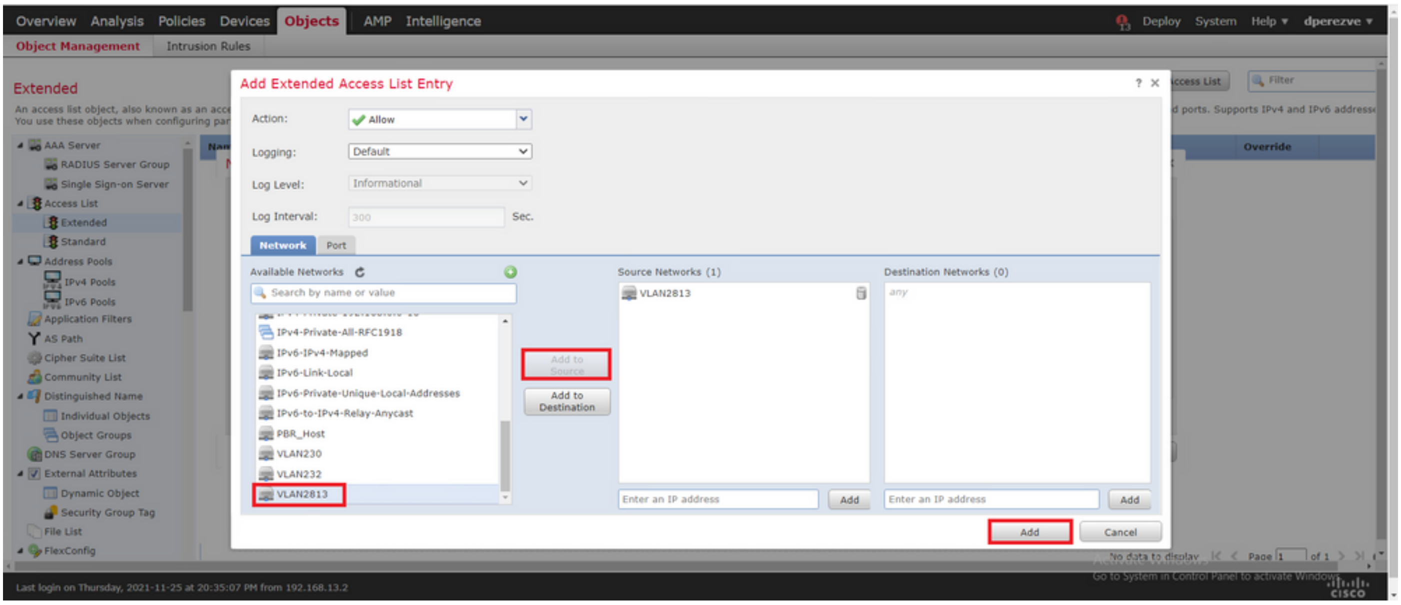
No data to display | Page 1 of 1

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

No **Add Extended Access List Entry** selecione o objeto que representa a rede interna, neste caso, VLAN2813.

Clique em **Add to Source** para defini-la como a origem da lista de acesso.

Clique em **Add** para criar a entrada.



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

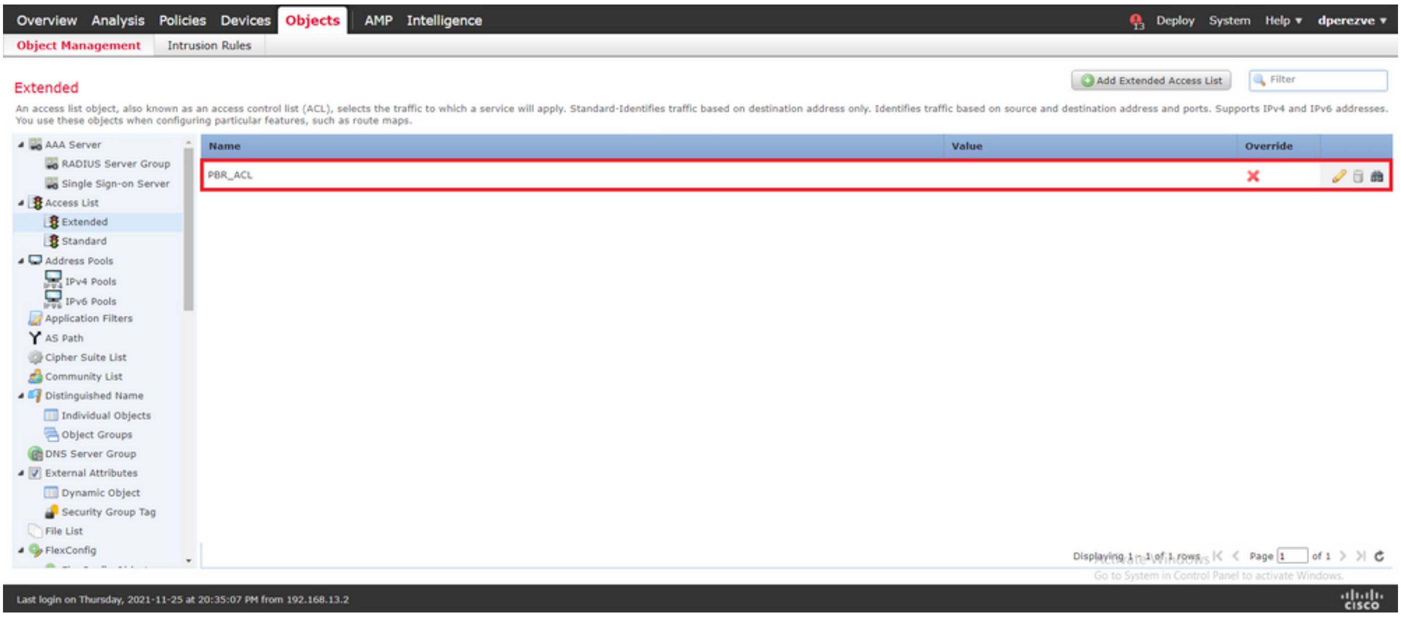
Enter an IP address | Add

Add | Cancel

No data to display | Page 1 of 1

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

Clique em **Save** . O objeto deve ser adicionado à lista de objetos.



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		✗

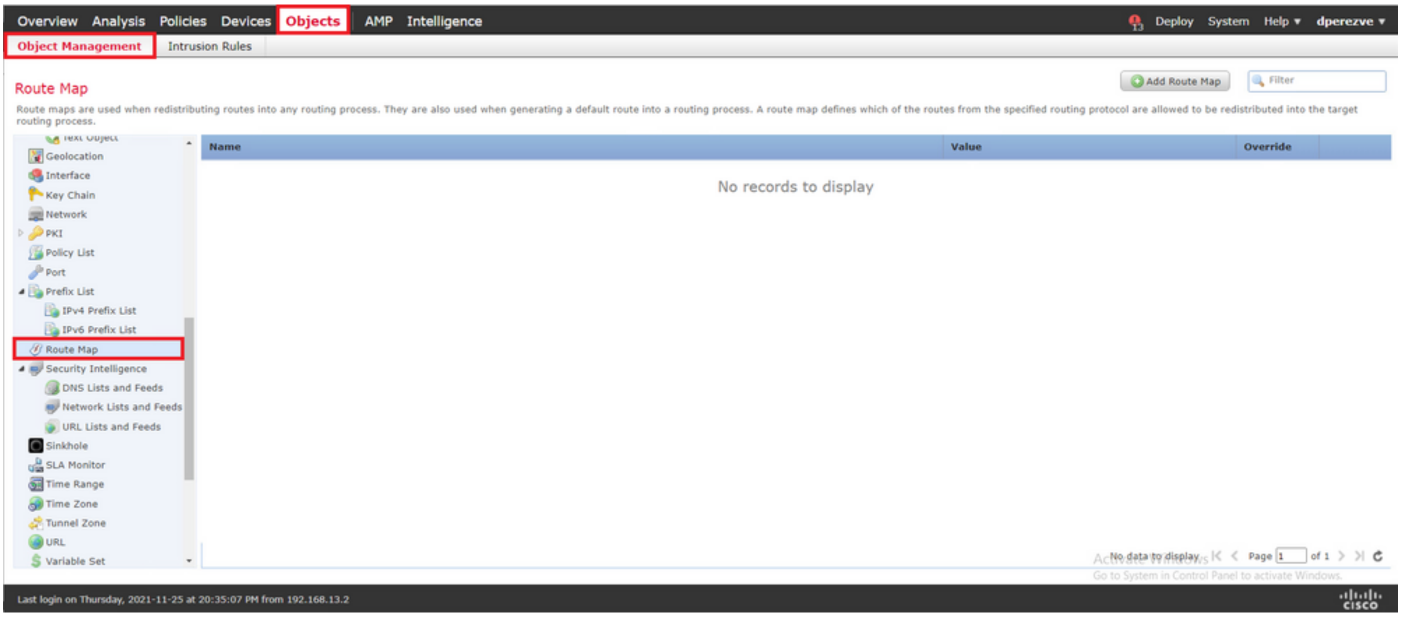
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

Etapa 2. Configurar o mapa de rota PBR

Depois que a lista de acesso PBR estiver configurada, atribua-a a um mapa de rotas. O mapa de rotas avalia o tráfego em relação às cláusulas de correspondência definidas na lista de acesso.

Após uma correspondência, o mapa de rotas executa as ações definidas na política de roteamento.

Para definir um mapa de rotas, navegue até **Objects > Object Management** e selecione **Route Map** no índice.



Route Map

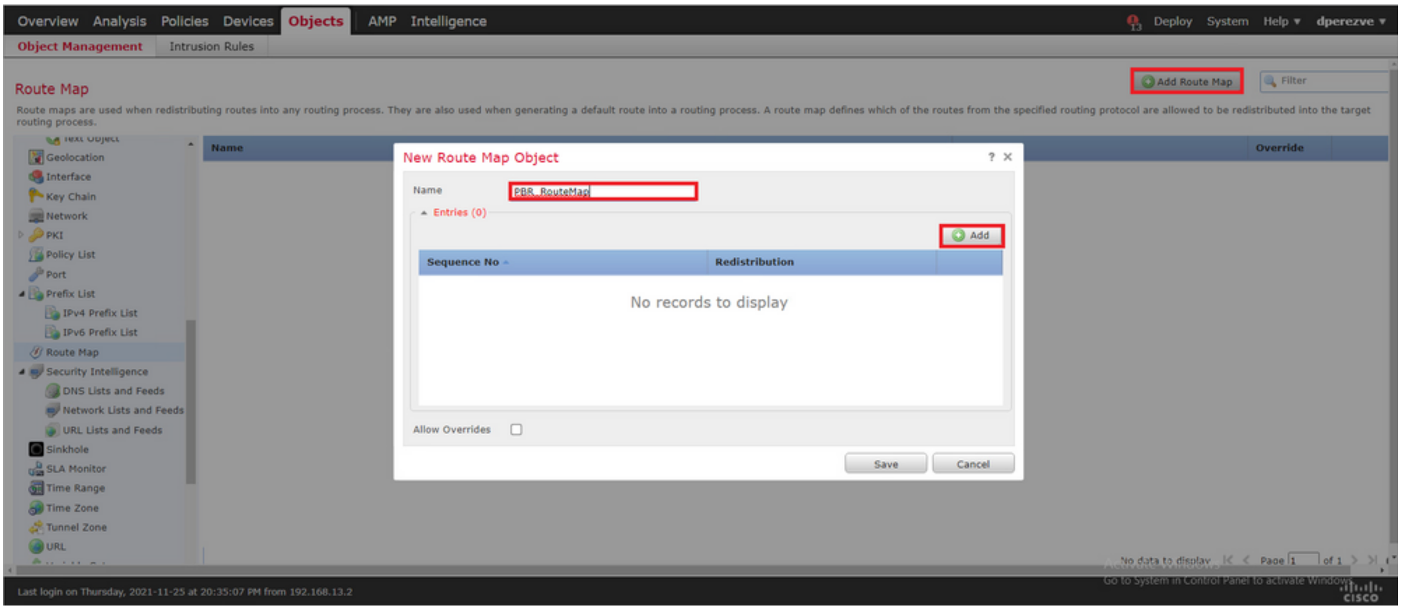
Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Name	Value	Override

No records to display

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

Clique em **Add Route Map** >. No **New Route Map Object** atribua um nome para o objeto e clique em **Add** para criar uma nova entrada do mapa de rotas.



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.

New Route Map Object

Name: PBR_RouteMap

No records to display

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

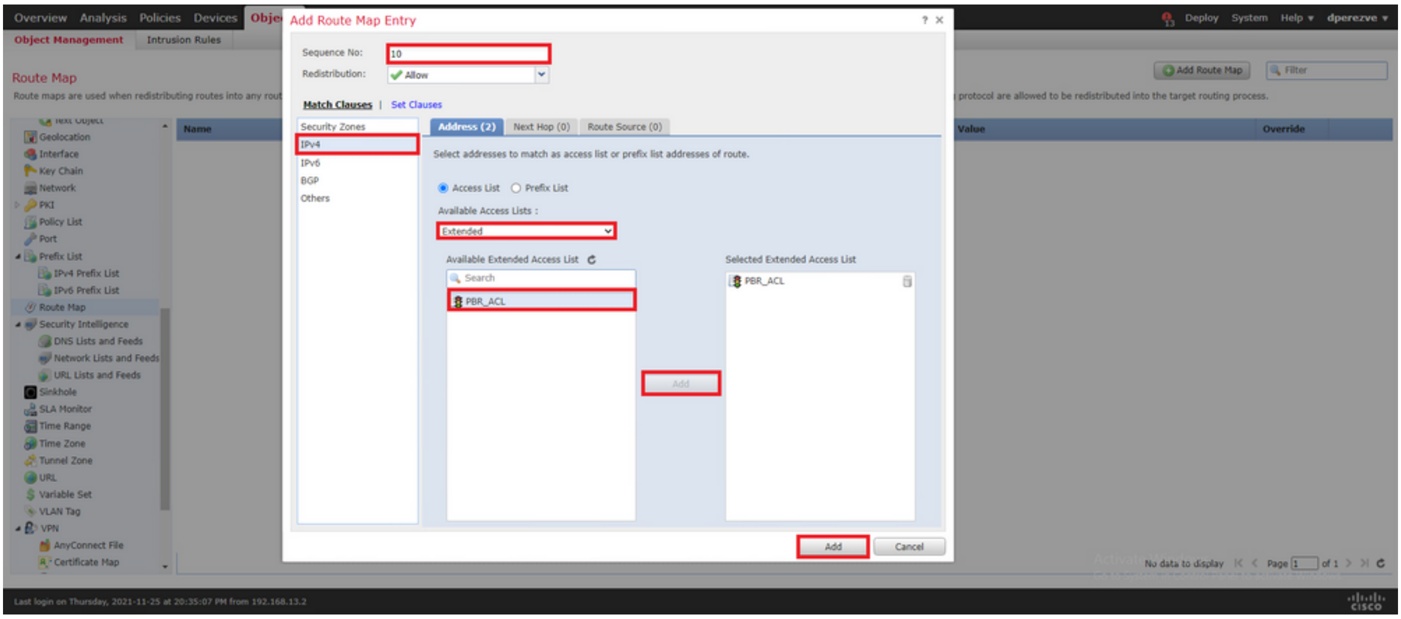
No **Add Route Map Entry** , defina um número de sequência para a posição da nova entrada.

Navegue até **IPv4 > Match Clauses** e selecione **Estendido** no **Available Access List** menu suspenso.

Selecione o objeto da lista de acesso criado na Etapa 1.

Clique em **Add** para criar a entrada.

> **Observação**: o FTD suporta até 65536 (de 0 a 65535) entradas diferentes. Quanto menor o número, maior a avaliação de prioridade.



Route Map

Add Route Map Entry

Sequence No: 10

Redistribution: Allow

Select addresses to match as access list or prefix list addresses of route.

Access List

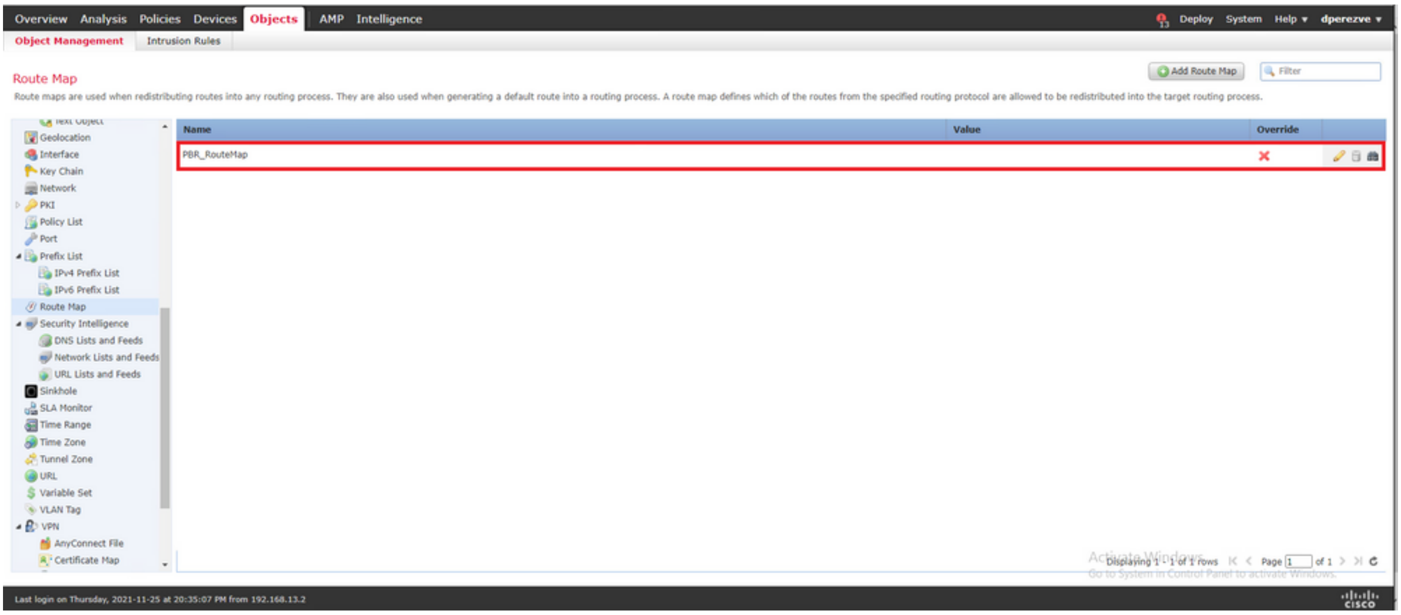
Available Access Lists : Extended

Available Extended Access List: PBR_ACL

Selected Extended Access List: PBR_ACL

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

Clique em **Save** . Adicione o objeto à lista de objetos.



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.

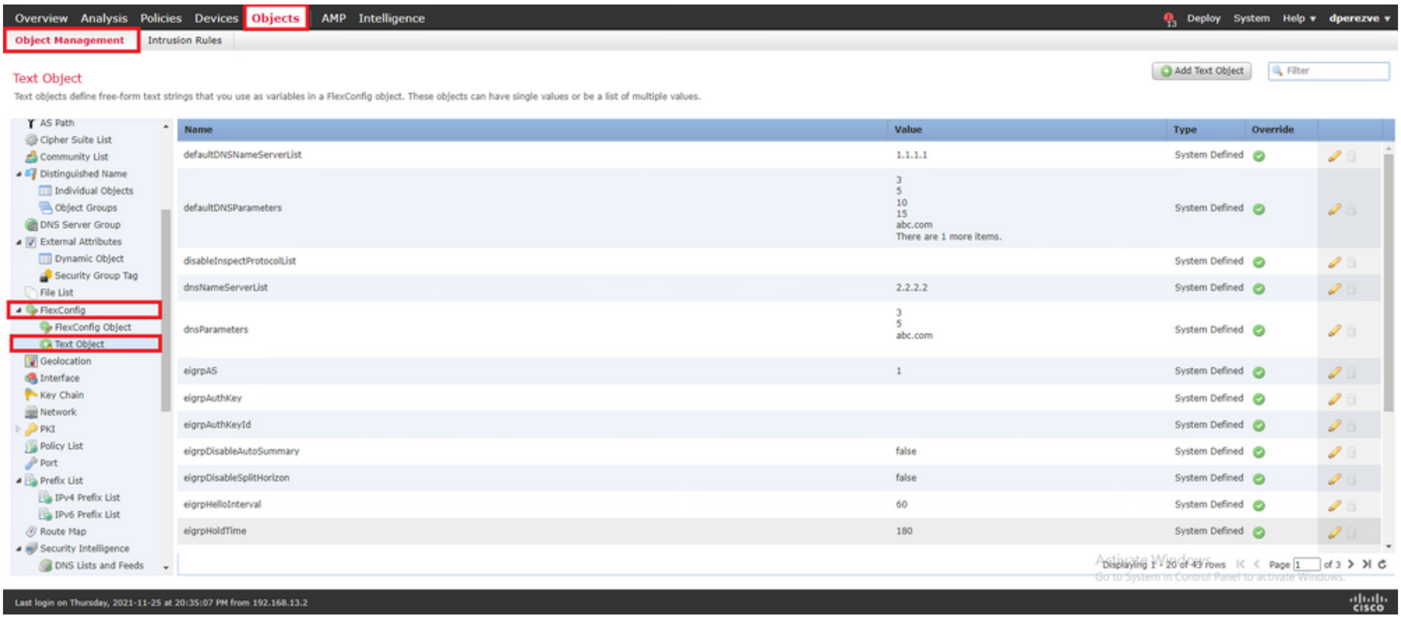
Name	Value	Override
PBR_RouteMap		✗

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

Etapa 3. Configurar objetos de texto FlexConfig

A próxima etapa envolve a definição de objetos de texto FlexConfig que representam Gateways padrão para cada circuito. Esses objetos de texto são usados posteriormente na configuração do objeto FlexConfig que associa o PBR aos SLAs.

Para definir um objeto de texto FlexConfig, navegue até **Objects > Object Management** e selecione **Text Object** sob o comando **FlexConfig** categoria no sumário.



Text Object

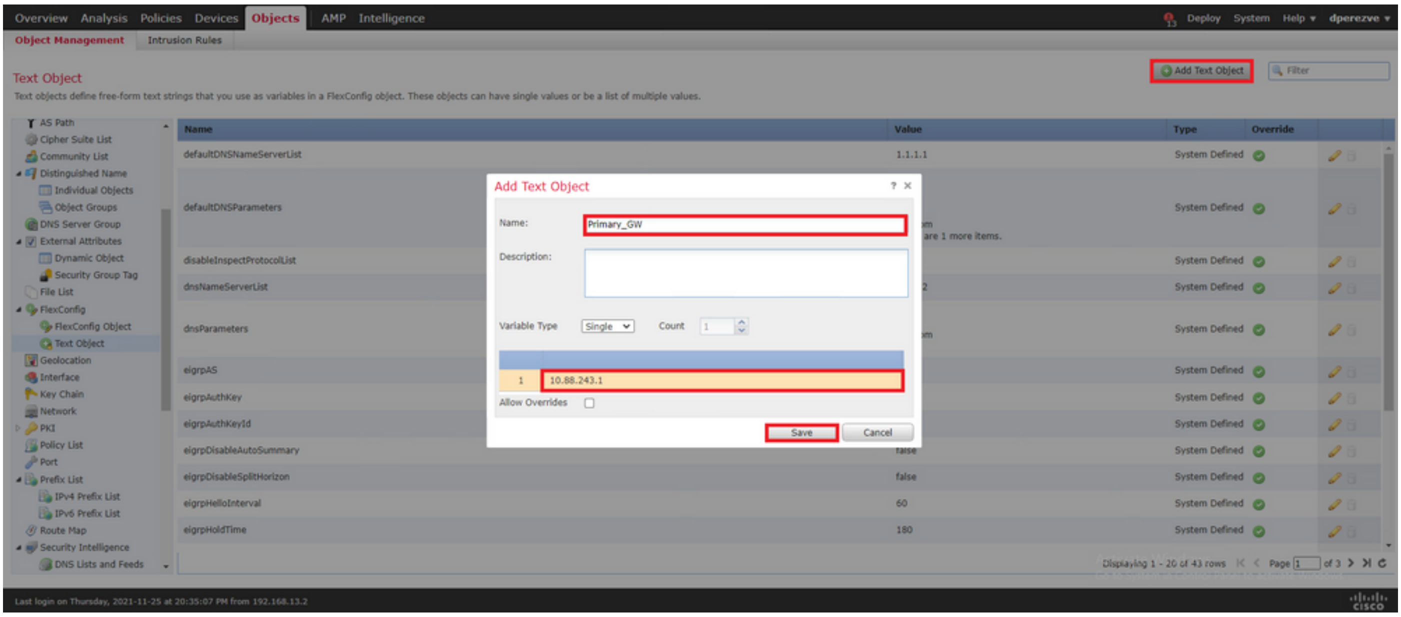
Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

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	✓

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

Clique em **Add Text Object** . No **Add Text Object** atribua um nome para o objeto que representa o Gateway principal e especifique o endereço IPv4 desse dispositivo.

Clique em **Save** para adicionar o novo objeto.



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	...m ...are 1 more items.	System Defined	✓
disableInspectProtocolList		System Defined	✓
dnsNameServerList	...2	System Defined	✓
dnsParameters	...m	System Defined	✓
eigrpAS		System Defined	✓
eigrpAuthKey		System Defined	✓
eigrpAuthKeyId		System Defined	✓
eigrpDisableAutoSummary	false	System Defined	✓
eigrpDisableSplitHorizon	false	System Defined	✓
eigrpHelloInterval	60	System Defined	✓
eigrpHoldTime	180	System Defined	✓

Add Text Object

Name: Primary_GW

Description:

Variable Type: Single   Count: 1

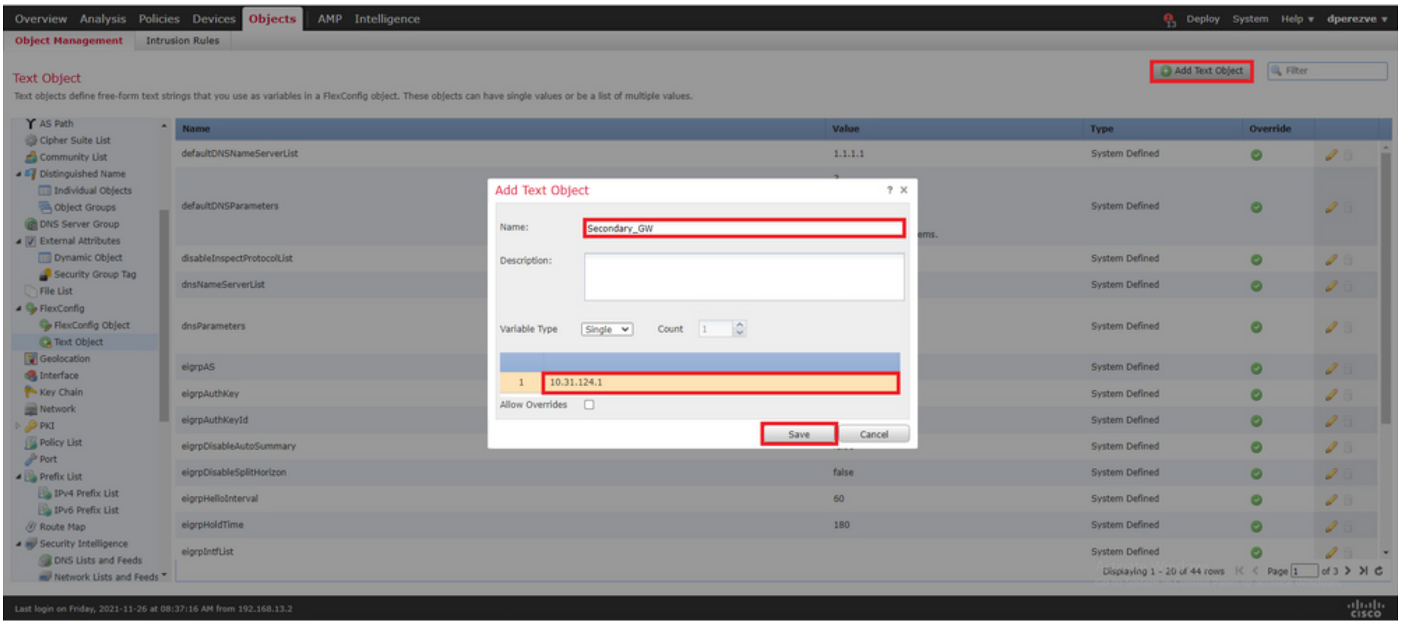
1   10.88.243.1

Allow Overrides □

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

Clique em **Add Text Object** novamente para criar um segundo objeto, desta vez para o Gateway no circuito de backup.

Preencha o novo objeto com o nome e endereço IP apropriados e clique em **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.

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	✓
defaultDNSParameters	...ems.	System Defined	✓
disableInspectProtocolList		System Defined	✓
dnsNameServerList		System Defined	✓
dnsParameters		System Defined	✓
eigrpAS		System Defined	✓
eigrpAuthKey		System Defined	✓
eigrpAuthKeyId		System Defined	✓
eigrpDisableAutoSummary		System Defined	✓
eigrpDisableSplitHorizon	false	System Defined	✓
eigrpHelloInterval	60	System Defined	✓
eigrpHoldTime	180	System Defined	✓
eigrpIntfList		System Defined	✓

Add Text Object

Name: Secondary_GW

Description:

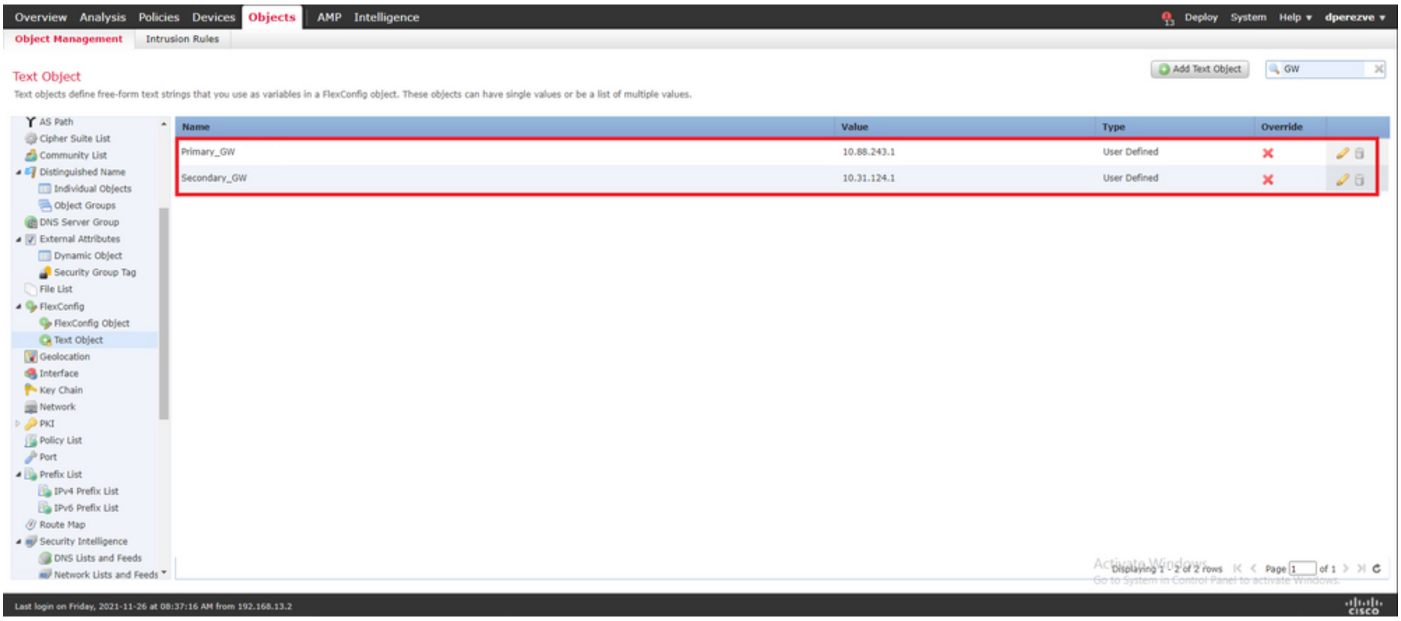
Variable Type: Single   Count: 1

1   10.31.124.1

Allow Overrides □

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

Os dois objetos devem ser adicionados à lista junto com os objetos padrão.



Text Object

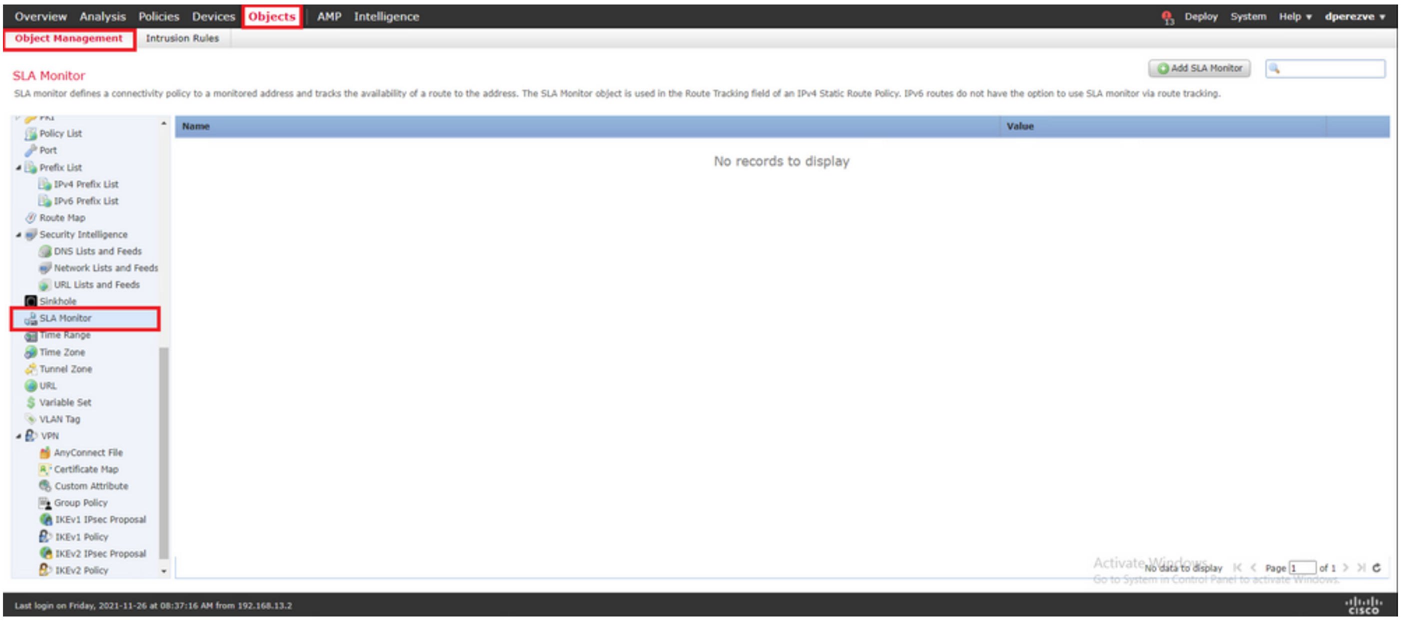
Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
Primary_GW	10.88.243.1	User Defined	✗
Secondary_GW	10.31.124.1	User Defined	✗

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

Etapa 4. Configurar monitor de SLA

Para definir os objetos de SLA usados para monitorar a conectividade com cada Gateway, navegue até **Objects > Object Management** e selecione **SLA Monitor** no índice.



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	

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

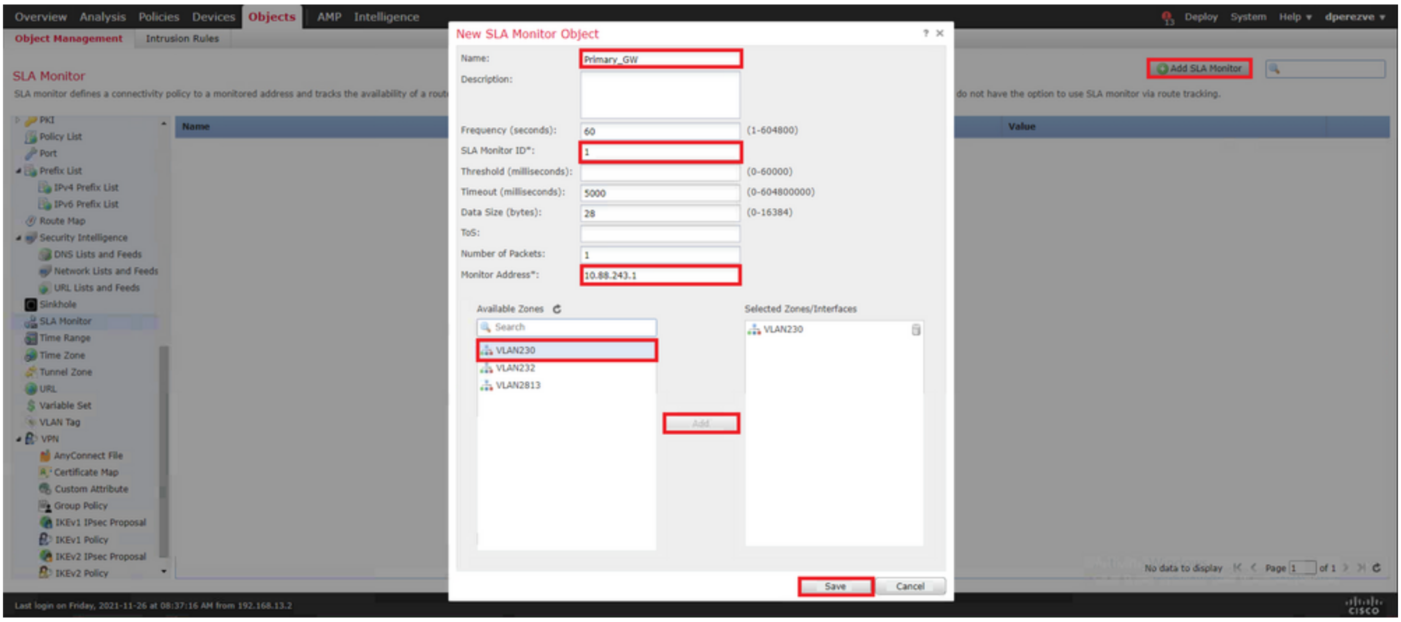
Selecione a opção **Add SLA Monitor** objeto.

No **New SLA Monitor** , defina um nome junto com um identificador para a operação do SLA, o endereço IP do dispositivo que deve ser monitorado (neste caso, o Gateway principal) e a interface ou zona pela qual o dispositivo pode ser alcançado.

Além disso, também é possível ajustar o tempo limite e o limite. Clique em **Save** .

> **Observação**: o FTD suporta até 2.000 operações de SLA. Os valores da ID do SLA variam de 1 a 2147483647.

> **Observação**: se os valores de timeout e limite não forem especificados, o FTD usará temporizadores padrão: 5000 milissegundos em cada caso.



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

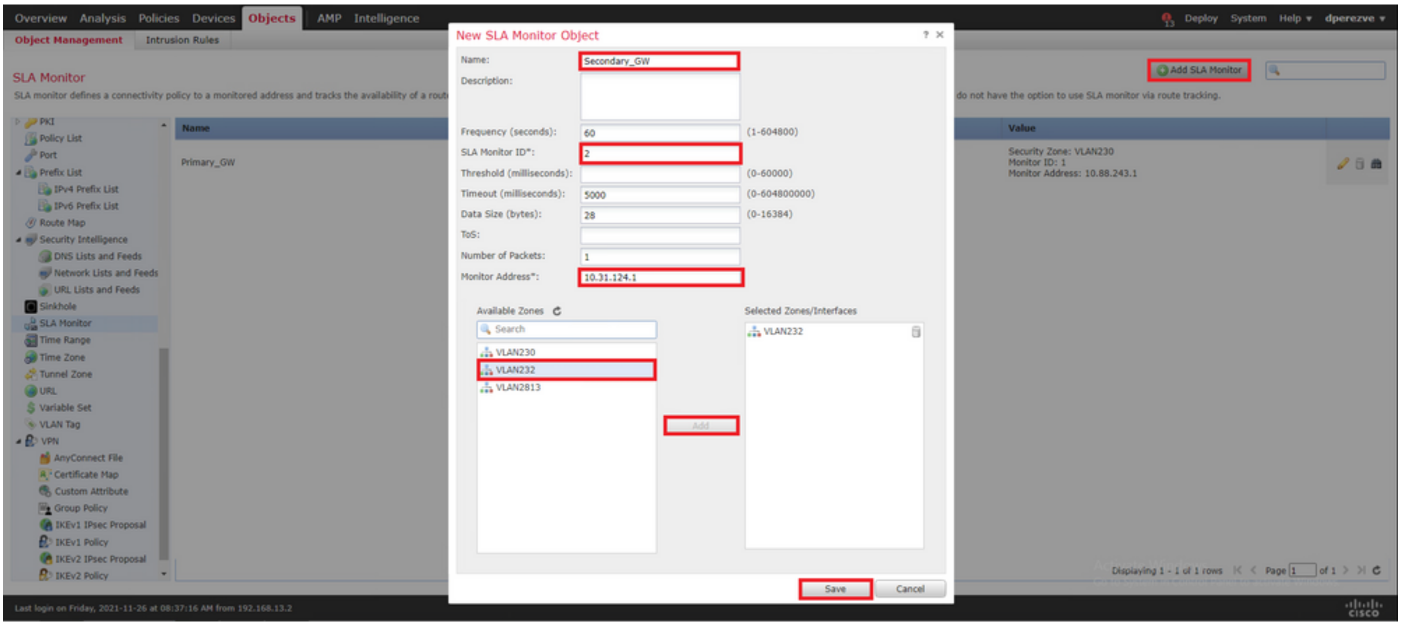
Name: Primary_GW
Description:
Frequency (seconds): 60 (1-604800)
SLA Monitor ID*: 1
Threshold (milliseconds): (0-60000)
Timeout (milliseconds): 5000 (0-604800000)
Data Size (bytes): 28 (0-16384)
ToS:
Number of Packets: 1
Monitor Address*: 10.88.243.1

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

Selecione a opção **Add SLA Monitor** novamente para criar um segundo objeto, desta vez para o Gateway no circuito de backup.

Preencha o novo objeto com as informações apropriadas, verifique se o ID do SLA é diferente daquele definido para o Gateway principal e salve as alterações.



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

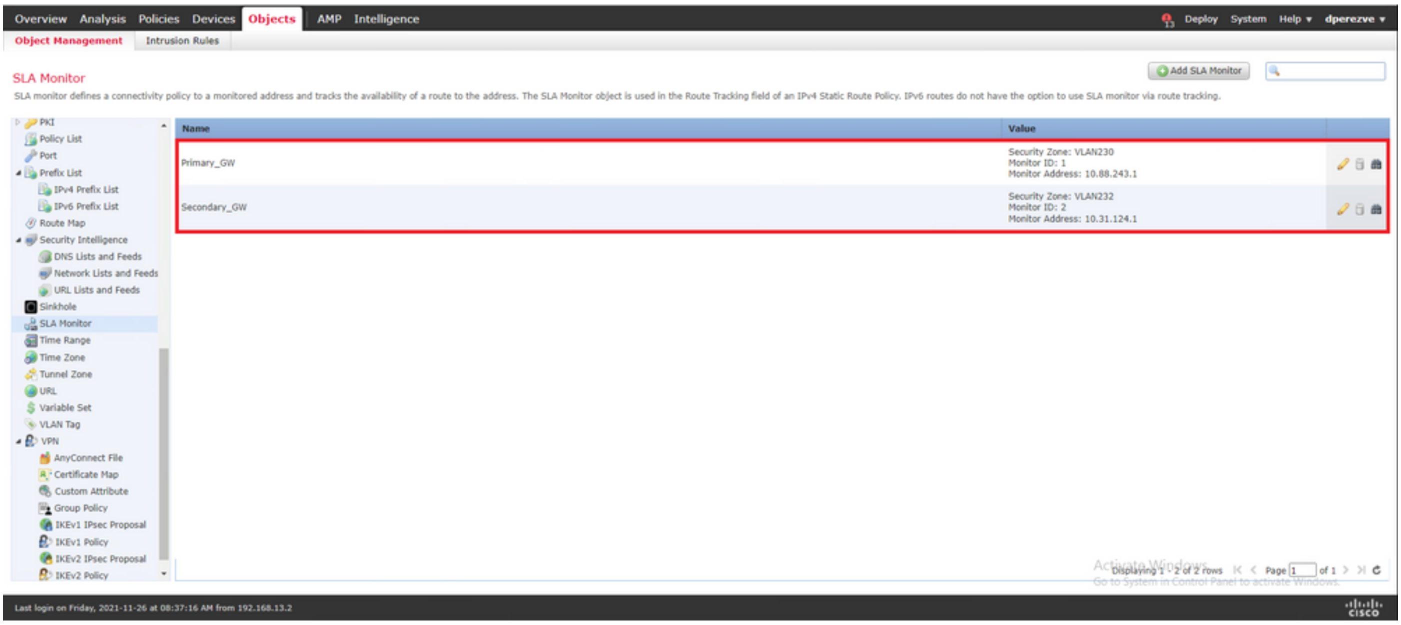
New SLA Monitor Object

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

Os dois objetos devem ser adicionados à lista.



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.

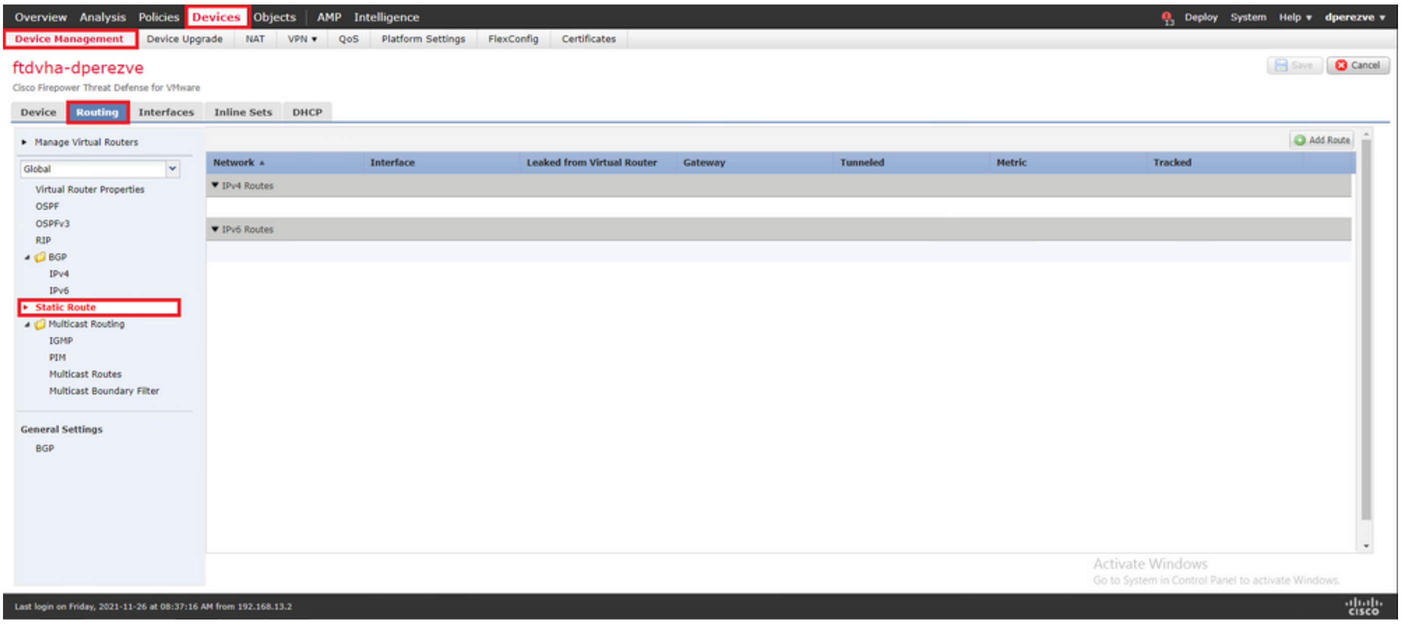
Name	Value
Primary_GW	Security Zone: VLAN230 Monitor ID: 1 Monitor Address: 10.88.243.1
Secondary_GW	Security Zone: VLAN232 Monitor ID: 2 Monitor Address: 10.31.124.1

Etapa 4. Configurar rotas estáticas com o Route Track

Depois que os objetos SLA IP forem criados, defina uma rota para cada Gateway e associe-os aos SLAs.

Na verdade, essas rotas não fornecem conectividade de dentro para fora (todo o roteamento é executado por PBR); em vez disso, elas são necessárias para rastrear a conectividade com os Gateways por meio de SLAs.

Para configurar rotas estáticas, navegue até **Devices > Device Management** , edite o FTD disponível e selecione **Static Route** no índice da **Routing** guia.



Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
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
Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2

ftdvha-dperezve

Cisco Firepower Threat Defense for VMware

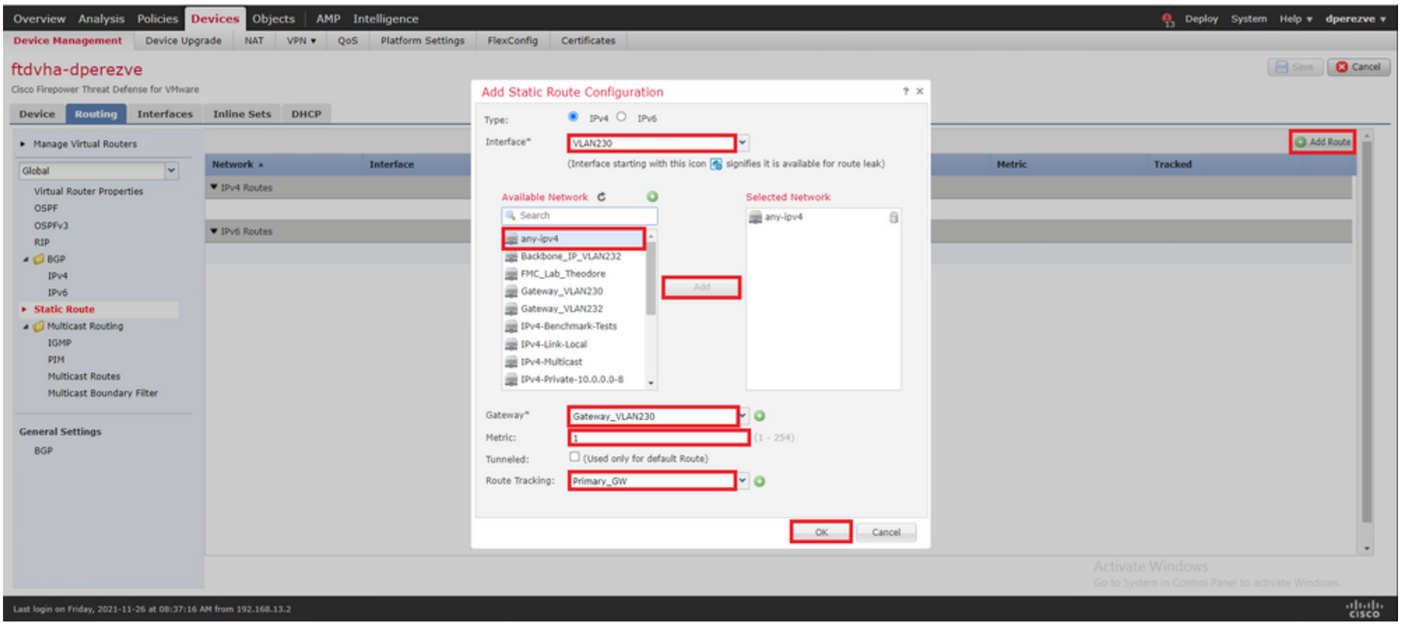
Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
▼ IPv6 Routes						

No **Add Static Route Configuration** , no menu suspenso **Interface**, especifique o nome da interface pela qual o Gateway principal deve estar acessível.

Em seguida, selecione a rede de destino e o Gateway principal no **Gateway** suspenso.

Especifique uma métrica para a rota e no **Route Track** e selecione o objeto SLA para o gateway principal criado na Etapa 3.

Clique em **OK** para adicionar a nova rota.


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
Network ▲ Interface Metric Tracked
▼ IPv4 Routes
▼ IPv6 Routes
Add Route
Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2

Add Static Route Configuration

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)

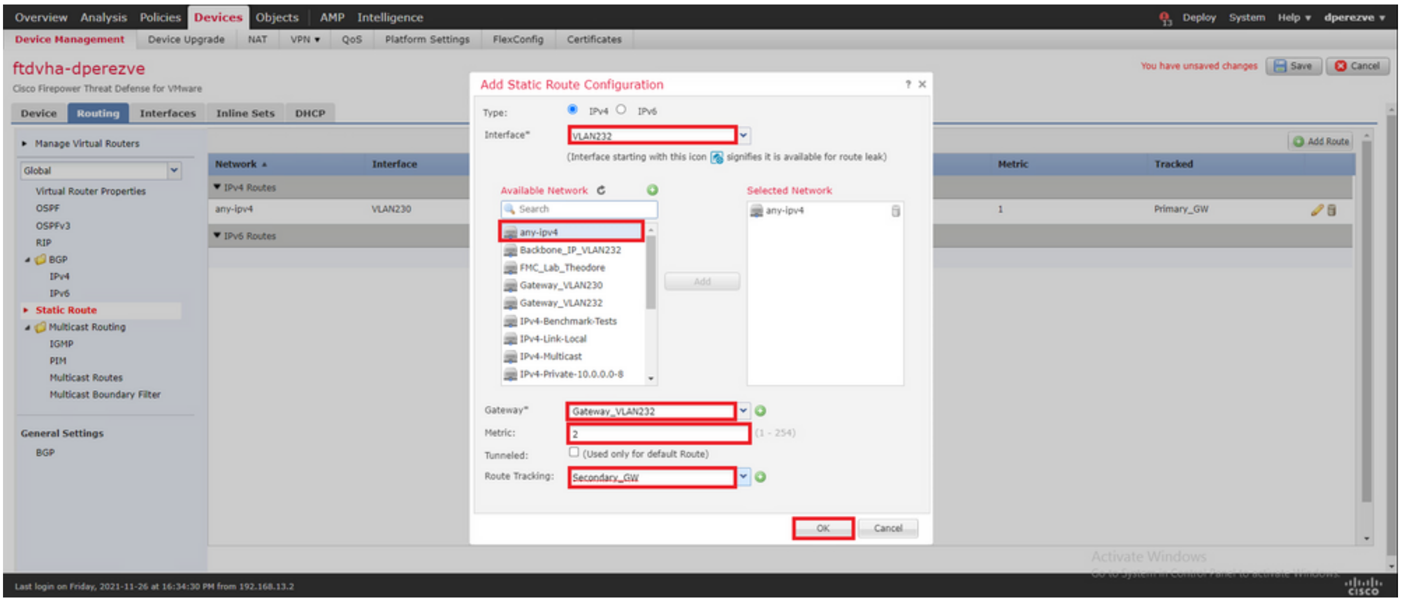
Route Tracking: Primary_GW

OK Cancel

Uma segunda rota estática deve ser configurada para o Gateway de backup.

Clique em **Add Route** para definir uma nova rota estática.

Preencha a **Add Static Route Configuration** com as informações do Gateway de backup e verifique se a métrica dessa rota é superior à configurada na primeira rota.


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
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			

Add Static Route Configuration

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

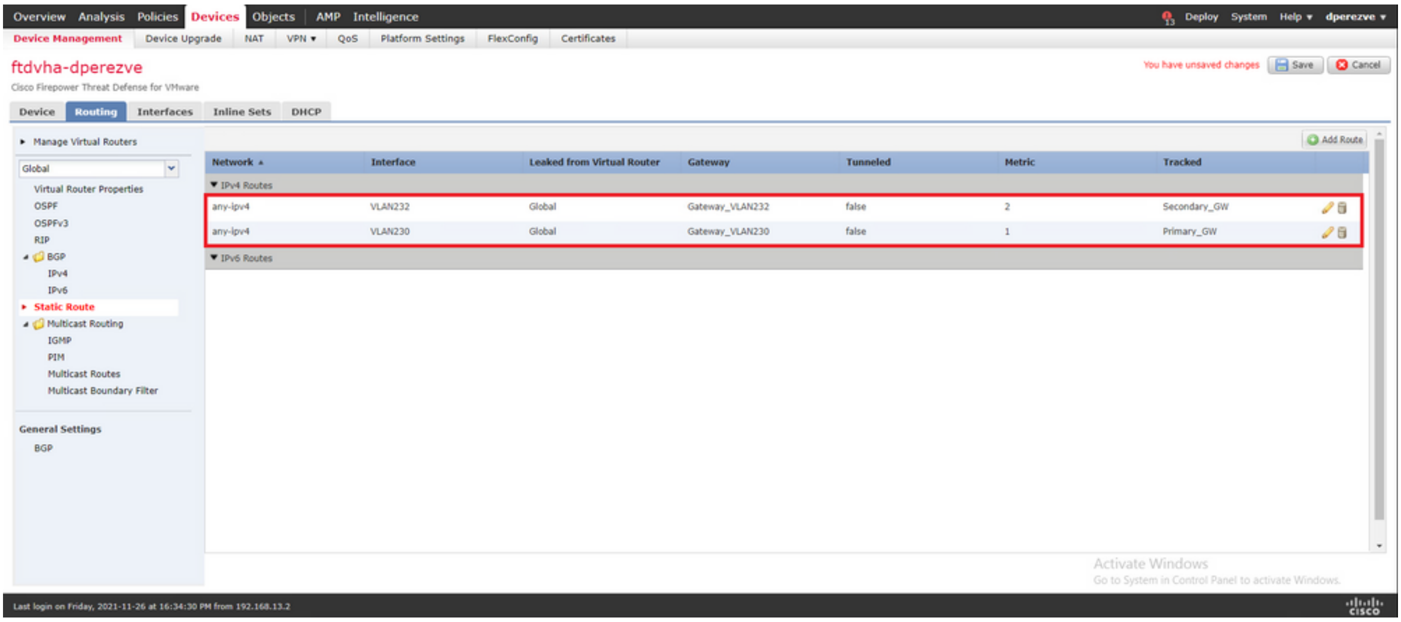
Metric: 2 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking: Secondary_GW

OK Cancel

As duas rotas devem ser adicionadas à lista.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
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
Activate Windows
Go to System in Control Panel to activate Windows.

ftdvha-dperezve

Cisco Firepower Threat Defense for VMware

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						

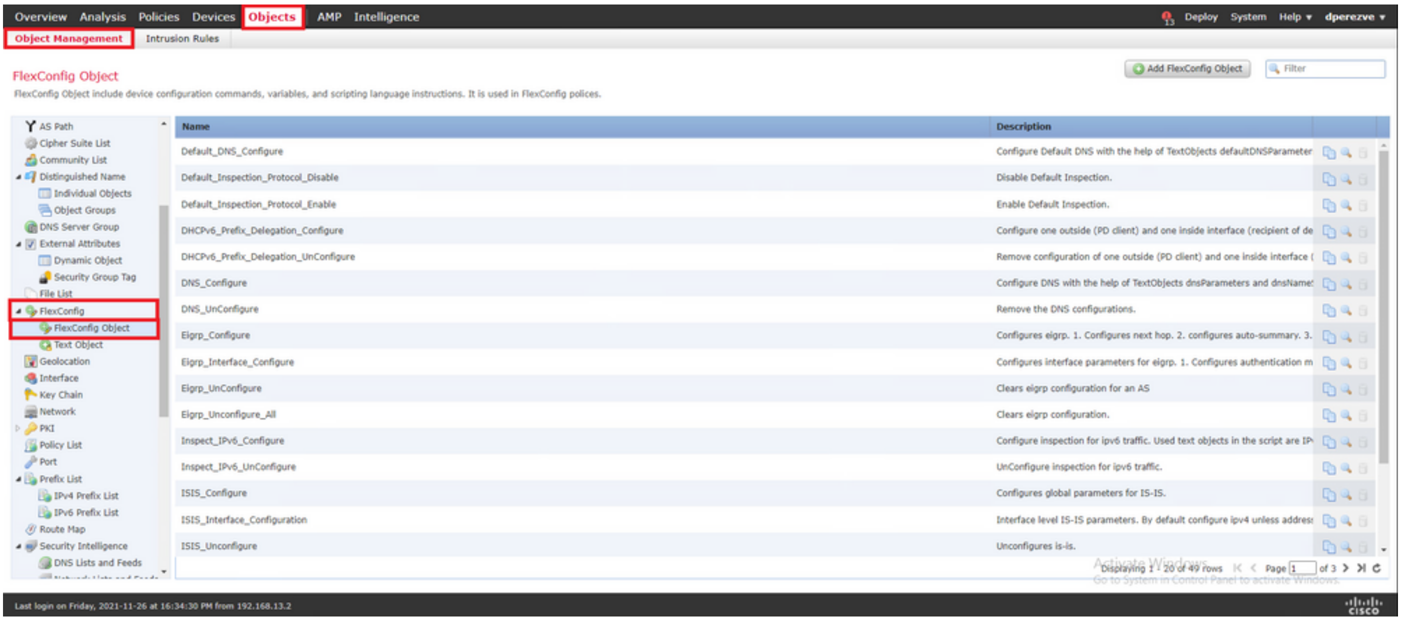
Last login on Friday, 2021-11-26 at 16:34:30 PM from 192.168.13.2

Etapa 5. Configurar objeto FlexConfig do PBR

Habilite os SLAs no mapa de rota usado para o PBR e aplique esse mapa de rota em uma interface do FTD.

Até agora, o mapa de rotas foi associado apenas à lista de acesso que define os critérios de correspondência. No entanto, os últimos ajustes não são suportados pela GUI do FMC, portanto um objeto FlexConfig é necessário.

Para definir o objeto PBR FlexConfig, navegue até **Objects > Object Management** e selecione **FlexConfig Object** sob o comando **FlexConfig** categoria no sumário.



FlexConfig Object

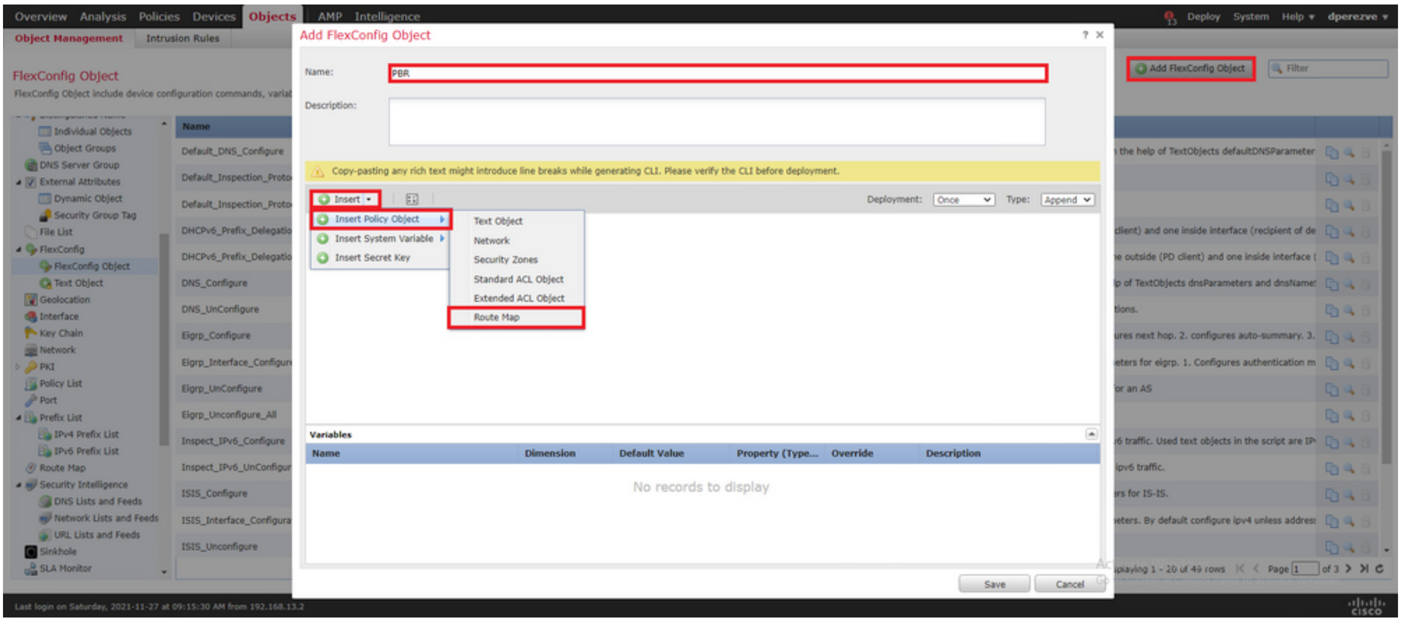
FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.

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.

Displaying 1 - 20 of 49 rows Page 1 of 3

Last login on Friday, 2021-11-26 at 16:34:30 PM from 192.168.13.2

Selecione a opção **Add FlexConfig Object** botão. No **Add FlexConfig Object** janela atribuir um nome e navegar até **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

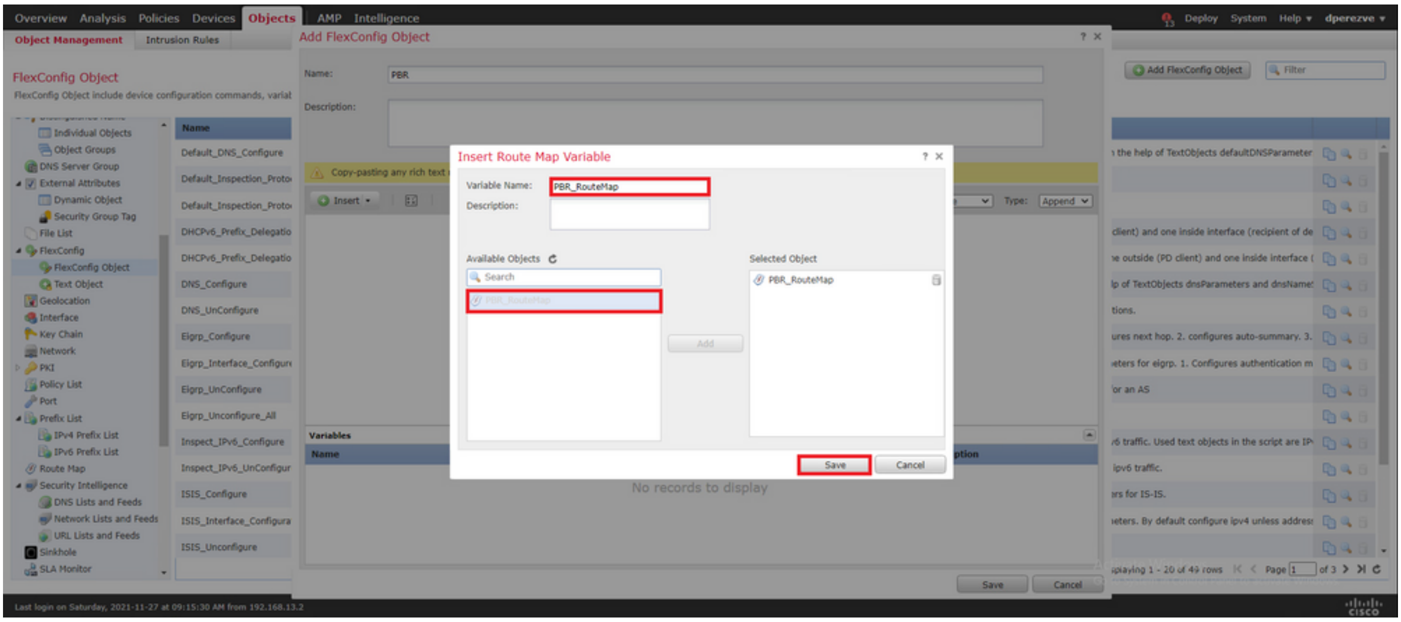
Variables

Name	Dimension	Default Value	Property (Type...	Override	Description

No records to display

No **Insert Route Map Variable** , atribua um nome para a variável e selecione o objeto PBR criado na Etapa 2.

Clique em **Save** para adicionar o mapa de rotas como parte do objeto FlexConfig.


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

Add FlexConfig Object

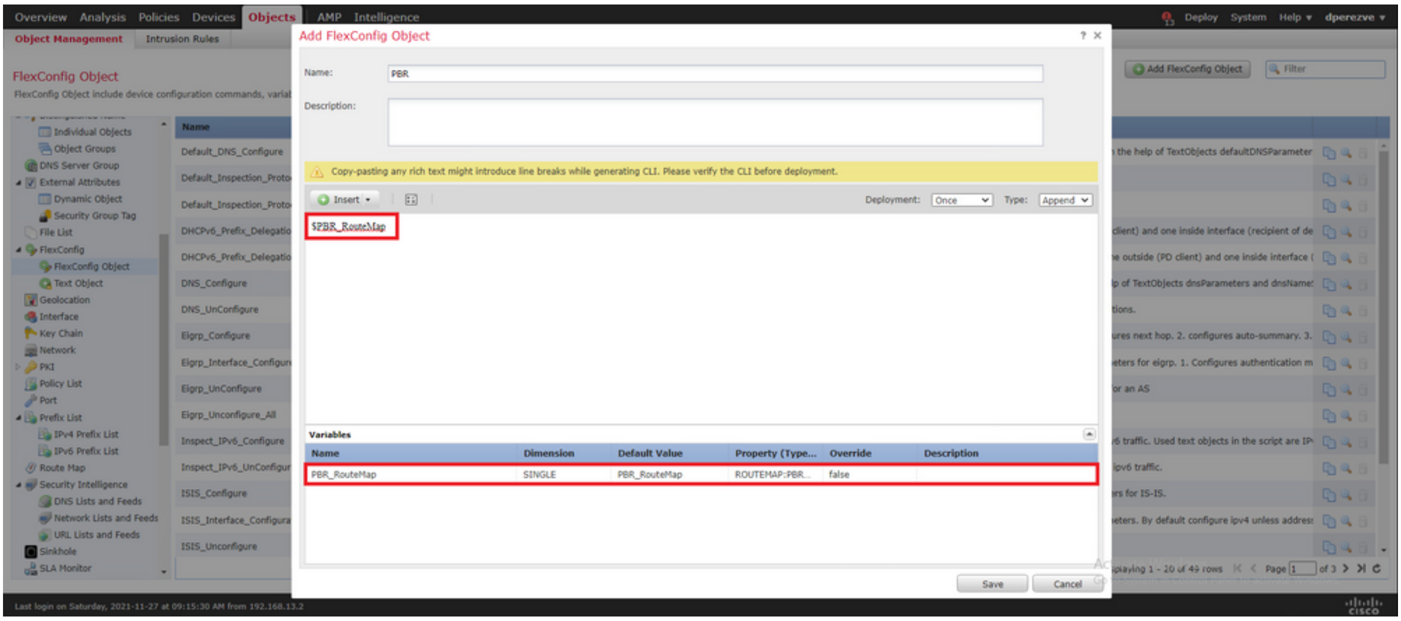
Name: PBR

Insert Route Map Variable

Variable Name: PBR_RouteMap

Description:

Selected Object: PBR_RouteMap



Add FlexConfig Object

Name: PBR

Description:

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

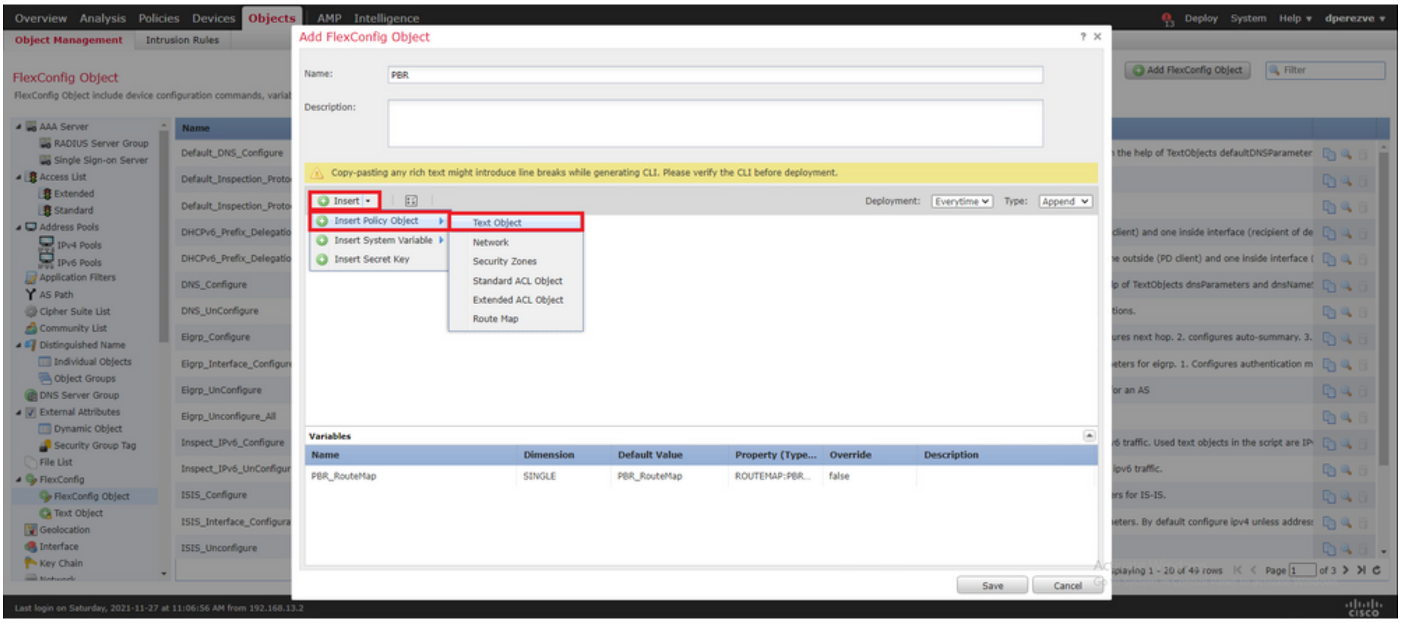
Deployment: Once Type: Append

```
$PBR_RouteMap
```

Variables

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

Além da variável de mapa de rotas, devemos adicionar os objetos de texto FlexConfig que representam cada Gateway (definido na Etapa 3). No **Add FlexConfig Object** janela navegar até **Insert > Insert Policy Object > Text Object .**



Add FlexConfig Object

Name: PBR

Description:

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

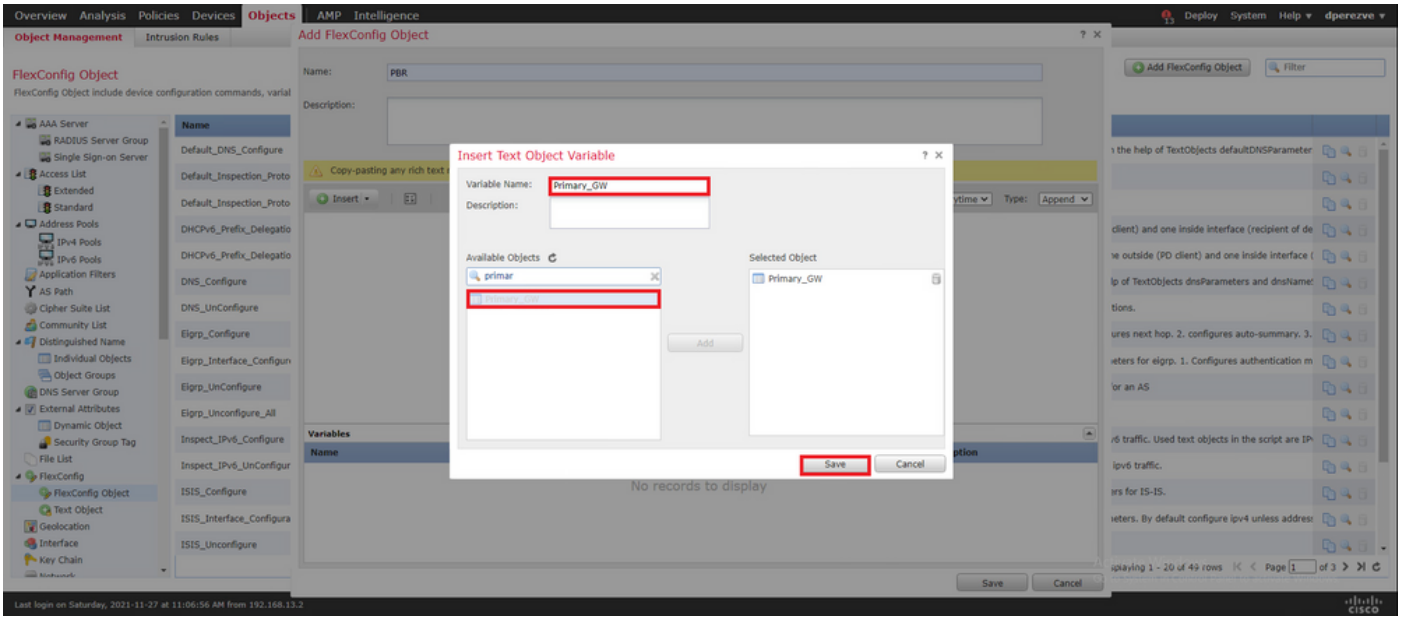
Deployment: Everytime Type: Append

Variables

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

No **Insert Text Object Variable** atribua um nome para a variável e selecione o objeto de texto que representa o Gateway primário definido na Etapa 3.

Clique em **Save** para adicioná-lo ao objeto FlexConfig.


Insert Text Object Variable

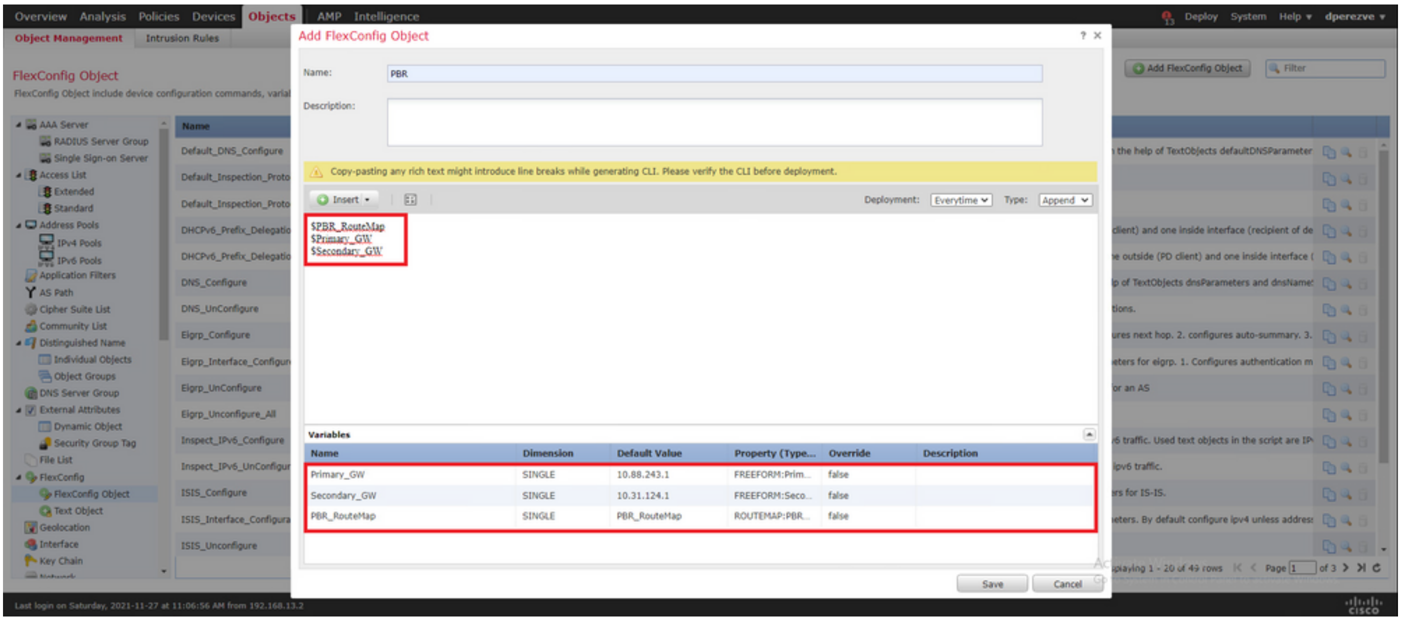
Variable Name: Primary_GW

Description:

Available Objects: primar

Selected Object: Primary_GW

Repita essas últimas etapas para o Gateway de backup. No final do processo, as duas variáveis devem ser acrescentadas ao objeto FlexConfig.


Add FlexConfig Object

Name: PBR

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

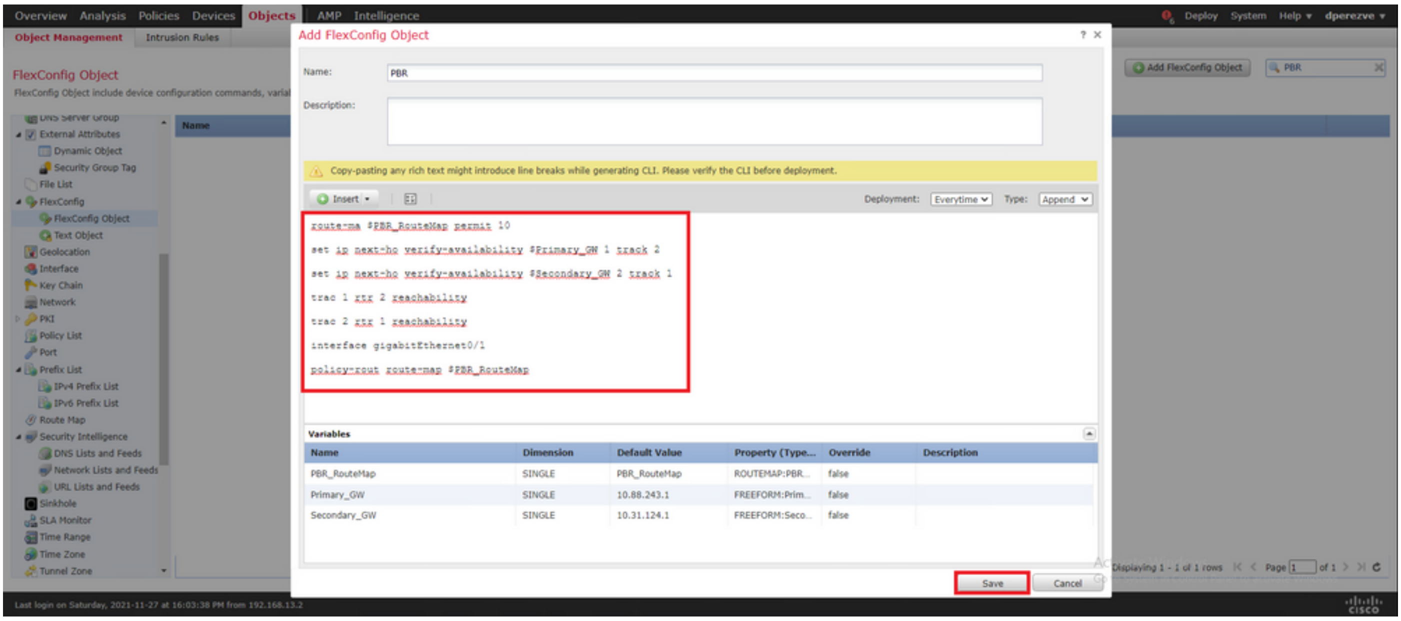
Name	Dimension	Default Value	Property (Type...	Override	Description
Primary_GW	SINGLE	10.88.243.1	FREEFORM:Prim...	false	
Secondary_GW	SINGLE	10.31.124.1	FREEFORM:Seco...	false	
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	

A sintaxe para a configuração do PBR deve ser a mesma do Cisco ASA. O número de sequência para o mapa de rotas deve corresponder ao configurado na Etapa 2 (10 neste caso), bem como as IDs de SLA.

Para configurar o PBR para verificar a disponibilidade do próximo salto, o comando **set ip next-hop verify-availability** deve ser usado.

O mapa de rotas deve ser aplicado à interface interna, neste caso, VLAN2813. Uso **policy-route route-map** na configuração da interface.

Clique em **Save** quando a configuração estiver concluída.



Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
FlexConfig Object
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.

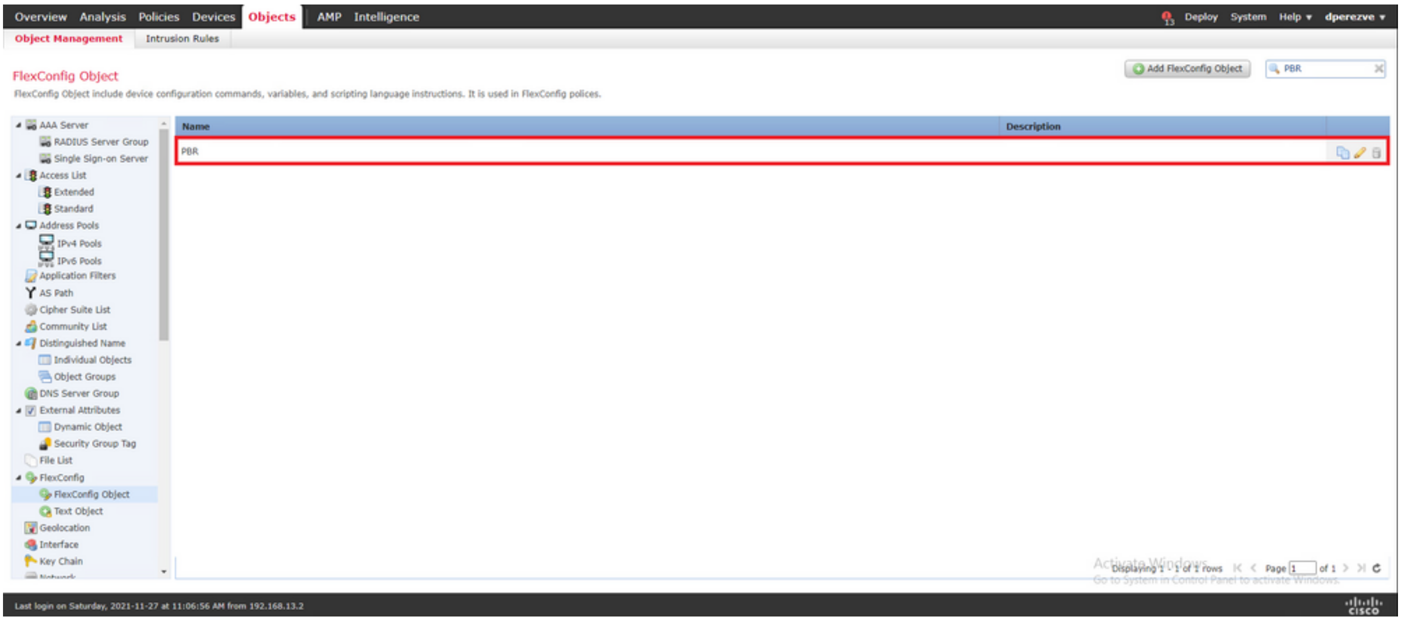
Deployment: Everytime Type: Append

```
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	

O objeto FlexConfig deve ser adicionado à lista.

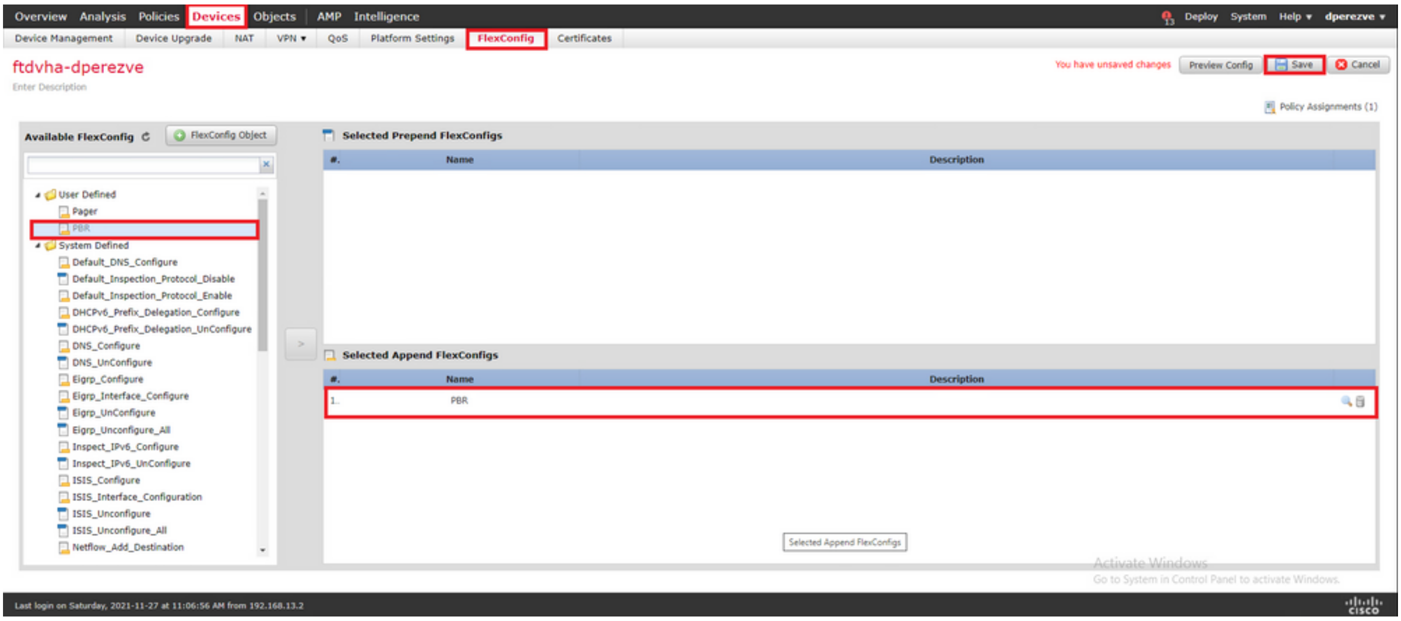


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
FlexConfig Object
FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.
Add FlexConfig Object
PBR
Name
Description
PBR
Displaying 1 - 1 of 1 rows
Last login on Saturday, 2021-11-27 at 11:06:56 AM from 192.168.13.2

Etapa 6. Atribuir objeto FlexConfig PBR à política FlexConfig

Navegue até **Devices > FlexConfig** e edite a política FlexConfig disponível.

Selecione o objeto PBR FlexConfig em **Available FlexConfig** sumário, salve as alterações e implante as alterações no FTD.



Verificar

Após o término da implantação, o FTD deve enviar solicitações de eco ICMP regulares aos dispositivos monitorados para garantir a acessibilidade. Enquanto isso, uma rota rastreada para o Gateway principal deve ser adicionada à tabela de roteamento.

```
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
```

Como a conectividade ao Gateway principal está ativa, o tráfego da sub-rede interna (VLAN2813) deve ser encaminhado através do circuito primário do ISP.

```
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
```

Se o FTD não receber uma resposta de eco do Gateway primário dentro do temporizador de limite especificado no objeto Monitor de SLA, o host será considerado inalcançável e marcado como inativo. A rota rastreada para o Gateway principal também é substituída pela rota rastreada para o peer de backup.

```
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
```

O 622001 de mensagens informativas é gerado sempre que o FTD adiciona ou remove uma rota rastreada da tabela de roteamento.

```
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
```

Agora, todo o tráfego de VLAN2813 deve ser encaminhado através do circuito ISP de backup.

```
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
```

Troubleshoot

Para validar qual entrada de PBR é aplicada em **interesting traffic** execute o comando **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
```