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

## Contents

Introduction **Requirements Componentes Utilizados** Informações de Apoio Configurar Diagrama de Rede Configurações Etapa 1. Configurar lista de acesso PBR Etapa 2. Configurar o mapa de rota PBR Etapa 3. Configurar objetos de texto FlexConfig Etapa 4. Configurar monitor de SLA Etapa 4. Configurar rotas estáticas com o Route Track Etapa 5. Configurar objeto FlexConfig do PBR Etapa 6. Atribuir objeto FlexConfig PBR à política FlexConfig Verificar Troubleshoot

# 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.



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.

Overview Analysis Policies Devices Ot	jects AM	P Intelligence				🧛 Deploy Sys	tem Help 🔻	dperezve v
Object Management Intrusion Rules								
Extended An access list object, also known as an access control list You use these objects when configuring particular feature	ACL), selects th , such as route r	e traffic to which a service will appl naps.	y. Standard-Identifies traffic based	f on destination address only. Iden	tifies traffic based on source and de	Add Extended Access List	supports IPv4 ar	d IPv6 addresse
AAA Server	ed Access L	ist Object			Value	? ×	Override	
Access List  Entries (0)	PBR_ACL							
Standard	Action	Source	Source Port	Destination	Destination Port	Add		
Pv4 Pools Pv6 Pools P			No records to	display				
Individual Objects Allow Overrid	is 🗌					_		
DNS Server Group					Save	Cancel		
Dynamic Object     Security Group Tag     File List								
4 Sp FlexConfig						No data to display	< < Page 1	lof1>>
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192	168.13.2					Go to System in Control I	Panel to activate	Vindows illiilii cisco

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.

Overview Analysis Policies De	objects	AMP Intelligence							Help 🔻 d	perezve 🔻
Object Management Intrusion Rules										
Extended	Add Extended /	Access List Entry					? ×	ccess List	Filter	
An access list object, also known as an acce You use these objects when configuring par	Action:	🛹 Allow	~					d ports. Supp	orts IPv4 and I	Pv6 address(
AAA Server	Logging:	Default	~					-	Override	
Single Sign-on Server	Log Level:	Informational	~							
Access List	Log Interval:		Sec.							
Standard	Network Por	t								
Address Pools	Available Networks	c	0	Source Networks (1)		Destination Networks (0)				
IPv4 Pools	Search by nam	ne or value		💭 VLAN2813	6	any				
Application Filters										
Y AS Path	Prv4-Private-	All-RFC1918								
Cipher Suite List	IPv6-Link-Loo	cal	Add to Source							
Distinguished Name	IPv6-Private-	Unique-Local-Addresses	Add to							
Individual Objects	IPv6-to-IPv4-	Relay-Anycast	Destination							
B Object Groups	PBR_Host									
BNS Server Group	VLAN230									
4 📝 External Attributes	VLAN232									
Dynamic Object	WLAN2813		*	Enter an IP address	Add	Enter an IP address	Add			
Security Group Tag										
File List						Add	Cancel			
4 🎭 FlexConfig							No data to	display K <	Page 1	of 1 > >  (*
1.							Go to System	In Control Parcel	CORDENSION OF	Mows .
Last login on Thursday, 2021-11-25 at 20:35:0										illulu.

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



#### 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.



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.

Overview Analysis Policies Devices Objects AM	IP Intelligence			👫 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules				
Route Map				Add Route Map
Route maps are used when redistributing routes into any routing process.	They are also used when generating a default ro	ute into a routing process. A route map defines which of the	e routes from the specified routing	protocol are allowed to be redistributed into the target
Geolocation Name	New Route Map Object		? ×	Override
Sinterface	Name PBR_RouteMap			
Network	Entries (0)			
P PKI Policy List	Sequence No -	Redistribution	Add	
Port	bequence no -	Real Articular		
IPv4 Prefix List		No records to display		
🕞 IPv6 Prefix List Ø Route Map				
Security Intelligence				
DNS Lists and Feeds      Network Lists and Feeds				
URL Lists and Feeds	Allow Overrides		_	
g SLA Monitor		Save	Cancel	
📆 Time Range				
and Tunnel Zone				
URL CONTRACTOR				A No data to display K < Page 1 of 1 > > , "
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2				Go to System in Control Panel to activate Windows cisco

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.

Overview Analysis Policies Devices Obje	Add Route Map Entry			? ×	鵫 Deploy System Help 🕷 dperezve 🕷
Object Management Intrusion Rules					
	Sequence No: 10				
Route Map	Redistribution: 🖋 Allow	~			Add Koute Map
Route maps are used when redistributing routes into any rout	Match Clauses   Set Clauses				protocol are allowed to be redistributed into the target routing process.
	Security Zones Addree IPv4 IPv6 BGP Others Availab	ess (2) Next Hop (0) Route Source (0) addresses to match as access list or prefix list ad cess List O Prefix List be Access List :	sresses of route.		Value Override
Policy List Prote Prefix List Prefix List	Extern	ded 🗸	Selected Extended Access List		
Ibv6 Prefix List     Route Hap     Scutity Instillence     DNS Lists and Freds     Network: Lists and Freds     URL Lists and Freds     Skukole     SLA Monitor     Time Prane	Ē	PBR_ACL	(\$ FRE,ACL ()		
Ga Time Kange Time Zone Time Zone URL Variable Set VLAN Top B VPN					
AnyConnect File			Add Can	cel	ACTIVAL No data to display K < Page 1 of 1 > > C.
Last Joein on Thursday. 2021-11-25 at 20:35-07 PM from 102.16	8.13.2				որոր

Clique em save. Adicione o objeto à lista de objetos.



#### 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.

Overview Analysis Polici	es Devices Objects AMP Intelligence		🆺 Deploy System Help 🛛 dperezve	e v
Object Management Intro	usion Rules			
Text Object Text objects define free-form text s	trings 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	
Y AS Path	Name	Value	Type Override	
Community List	defaultDNSNameServerList	1.1.1.1	System Defined 🥥 🥔 🥘	^
Distinguished Name     Individual Objects     Object Groups     DNS Server Group     External Attributes	defaultDNSParameters	3 5 10 15 abc.com There are 1 more items.	System Defined 🥥 🥔 🖓	
Dynamic Object	disableInspectProtocolList		System Defined 🥥 🥔 📋	1
Security Group Tag	dnsNameServerList	2.2.2.2	System Defined 🥥 🥔 🥥	1
FlexConfig     FlexConfig Object     Text Object	dnsParameters	3 5 abc.com	System Defined 🥥 🥒 🖯	l
Geolocation	elgrpAS	1	System Defined 🥥 🥔 🦪	
🏲 Key Chain	eigrpAuthKey		System Defined 🥥 🥔 📋	1
Network     PKI	eigrpAuthKey1d		System Defined 🥥 🥔 🥥	ſ
Policy List	eigrpDisableAutoSummary	false	System Defined 🥥 🥔 📑	
a 🗓 Prefix List	eigrpDisableSplitHorizon	false	System Defined 🥥 🥔 🕘	
IPv4 Prefix List	eigrpHelloEnterval	60	System Defined 🥥 🥔 🖯	
Ø Route Map	eigrpHoldTime	180	System Defined 🥥 🥔 🧳	
Security Intelligence     DNS Lists and Feeds			Apitality 10 20 07 19 70ws K < Page 1 of 3 > > Go to System in Control Panel to activate Windows.	c
Last login on Thursday, 2021-11-25 a	t 20:35:07 PM from 192.168.13.2		1111	

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.

Overview Analysis Polici	ies Devices Objects AMP Intelligence	2		P3 Deploy System Help	# dperezve #
Object Management Intr	usion Rules				
Text Object Text objects define free-form text s	trings that you use as variables in a FlexConfig object. The	se objects can have single values or be a list of multiple values.		Add Text Object	
Y AS Path	Name		Value	Type Override	
Community List	defaultDNSNameServerList		1.1.1.1	System Defined 🥥	08 ÷
Distinguished Name     Individual Objects     Object Groups     DNS Server Group	defaultDNSParameters	Add Text Object Name: Primary_GW	7 × m are 1 more items.	System Defined 🥥	18
Dynamic Object	disableInspectProtocolList	Description:		System Defined 🕥	18
File List	dnsNameServerList		2	System Defined 📀	08
GexConfig     GexConfig Object     GexConfig Object	dnsParameters	Variable Type Single  Count 1	ol	System Defined 🥥	18
Geolocation	eigrpAS	1 10.88.243.1		System Defined 🕑	08
Key Chain	eigrpAuthKey	Allow Overrides		System Defined 🥥	18
D PKI	eigrpAuthKeyId		Save	System Defined 🥥	08
Policy List	eigrpDisableAutoSummary		Taise	System Defined 🥥	18
A B Prefix List	eigrpDisableSplitHorizon		false	System Defined 🥥	08
IPv4 Prefix List	eigrpHelloInterval		60	System Defined 🥥	08
@ Route Map	eigrpHoldTime		180	System Defined 🥥	08
Security Intelligence     DNS Lists and Feeds				Displaying 1 - 20 of 43 rows K < Page 1	_d3 > X C
Last login on Thursday, 2021-11-25 a	at 20:35:07 PM from 192.168.13.2				alute

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 .

Overview Analysis Policie	es Devices Objects AMP Intelligence			🧛 Deplo	y System Help	r dperezve v
Object Management Intru	sion Rules					
Text Object Text objects define free-form text st	rings that you use as variables in a FlexConfig object. These objects car	have single values or be a list of multiple values.		Add Text	Object 🔍 Filter	
Y AS Path	Name		Value	Туре	Override	
Cipher Suite List	defaultDNSNameServerList		1.1.1.1	System Defined	0	/8 Ê
Distinguished Name     Individual Objects     Object Groups     DNS Server Group      External Attributes	defaultDNSParameters	Add Text Object Name: Secondary_GW	? ×	System Defined	٥	16
Dynamic Object	disableInspectProtocolList	Description:		System Defined	0	18
Security Group Tag	dnsNameServerList			System Defined	0	08
Gy FlexConfig     Gy FlexConfig Object     Gy Text Object	dnsParameters	Variable Type Single V Count 1		System Defined	0	18
Geolocation	eigrpAS			System Defined	0	08
Key Chain	eigrpAuthKey	1 10.31.124.1		System Defined	0	18
Network PKI	elgrpAuthKeyId		the second	System Defined	0	08
Policy List	eigrpDisableAutoSummary		Save Cancel	System Defined	0	18
Prefix List	eigrpDisableSplitHorizon		false	System Defined	0	08
IPv4 Prefix List	elgrpHelloInterval		60	System Defined	0	18
@ Route Map	elgrpHoldTime		180	System Defined	0	08
Security Intelligence     DNS Lists and Feeds     Network Lists and Feeds	eigepIntflüst			System Defined Displaying 1 - 20 of 44 ro	ws IC < Page 1	/ ] от з > > > К с
Last login on Friday, 2021-11-26 at 08	1:37:16 AM from 192.168.13.2					altalta cisco

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



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.



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.

Overview Analysis Policies Devices Objects AMP Intelligence				P Deploy System Help v dperezve v
Object Management Intrusion Rules	New SLA Monitor Ob	ject	7 ×	
SLA Monitor SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rou	Name: Description:	Primary_GW	]	Add SLA Monitor
Norm	Frequency (seconds): SLA Monitor ID*: Threshold (milliseconds): Timeout (milliseconds): Data Size (bytes): ToS: Number of Packets: Monitor Address*:	60 1 5000 28 1 1 0.08.243.1	(1-604800) (0-60000) (0-604800000) (0-16384)	Value
URL Lids and Feeds  URL Lids and Feeds  URL Lids and Feeds  URL Sone  URL Sone  URL  Value  Constitution  Constit	Available Zones C Search Su VLAV230 Su VLAV232 Sa VLAV2813		Selected Zones/Interfaces	
B IKEV2 Policy			Save Cancel	No data to display K < Page 1 of 1 9 P C
Last Jonin on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2			Cancer	altalte

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.

Overview Analysis Policie	es Devices Objects AMP Intelligence					👫 Deploy System Help 🔻	lperezve +
Object Management Intru	usion Rules	New SLA Monitor Ob	ject		? ×		
SLA Monitor SLA monitor defines a connectivity p	policy to a monitored address and tracks the availability of a rout	Name: Description:	Secondary_GW			do not have the option to use SLA monitor via route tracking.	
Policy List	Name	Frequency (seconds):	60	(1-604800)		Value	
Port  Port  profix List  profix List  Profix List  Profix List  Profix List  Distance Nap  DIS Lists and Feeds  DIS Lists and Feeds	Primary_GW	SLA Monitor ID": Threshold (milliseconds): Timeout (milliseconds): Data Size (bytes): ToS: Number of Packets:	2 5000 28 1	(0-60000) (0-604800000) (0-16384)		Security Zone: VLAR230 Menitor ID: 1 Monitor Address: 10.88.243.1	/ () <b>m</b>
Network Lists and Feeds     U.R. Lists and Feeds     Stat Monitor     Stat Monitor     Time Zone     Time Zone     Time Zone     URL     Variable Set     VLAN Tag     Certificate Mag     Concop Policy     KEV1 Place Proposal     KEV1 Place Place		Monitor Address*: Available Zones C Search As VLAN230 S VLAN232 As VLAN2813	20.33.124.1	Selected Zones/Interfaces		Displaying 1 - 1 of 1 rows K < Page 1 of	1 > > €
				Save Cance	4	Go to system in control variet to activitie windo	
Last login on Friday, 2021-11-26 at 08							-iliulu

Os dois objetos devem ser adicionados à lista.

Overview Analysis Polic	ies Devices Objects AMP Intelligence	💁 Deploy System Help 🕶 dperezve 🕶
Object Management Intr	rusion Rules	
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 ha	Add SLA Monitor
Þ 🥜 PKI	Name	Value
Policy List Port Prefix List	Primary_GW	Security Zone: VLAN230 Monitor ID: 1 Monitor Address: 10.80.243.1
Iby IPv4 Prefix List Iby IPv6 Prefix List Ø Route Map	Secondary_OW	Security Zone: VLAN232 Monitor ID: 2 Monitor Address: 10.31.124.1
Security Intelligence     Gross Lists and Feeds     URL Lists and Feeds     URL Lists and Feeds     URL Lists and Feeds     Graduate     Graduate     Graduate     Graduate     Graduate     Time Zone     URL     Variable Set     VAriable Se		ActiveJapa산102년양양ines K < Page 1 > 거 호 Go to System in Control Panel to activate Windows.
Last login on Friday, 2021-11-26 at 0	38:37:16 AM from 192.165.13.2	-duala-

#### 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 D	evices Objects A	MP Intelligence					🦺 Deploy Sys	tem Help v dperezve v
Device Management Device Upg	rade NAT VPN •	QoS Platform Settings	FlexConfig Certificates					
ftdvha-dperezve Cisco Firepower Threat Defense for VMware	Talling Cold. DUCD							Save Cancel
Device Routing Interfaces	Inline Sets DHCP							[
<ul> <li>Manage Virtual Routers</li> </ul>					The second se			Add Route
Global 👻	Network A	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	<ul> <li>IPV4 Routes</li> </ul>							
OSPFv3	▼ IPv6 Routes							
RIP								
IPv4								
IPv6								
Static Route     Multicast Routing								
IGMP								
PIM Multilenet Deuten								
Multicast Boundary Filter								
General Settings								
BGP								
							A stiuste Mindaue	•
							Go to System in Control Panel to	activate Windows.
Last login on Friday, 2021-11-26 at 08:37:16	VM from 192.168.13.2							-ili.ili. cisco

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 v dperezve v
Device Management Device Upgrade NAT VPN • QoS Platform Settings	FlexConfig Certificates	
ftdvha-dperezve Cisco Firepower Threat Defense for VMware	Add Static Route Configuration 7 ×	Save Cancel
Device Routing Interfaces Inline Sets DHCP	Туре: • IPv4 О IPv6	
Manage Virtual Routers	Interface" VLAN230	Add Route
Global V Network A Interface	(Interface starting with this icon 🚯 signifies it is available for route leak) Metric	Tracked
Virtual Router Properties - and Routes	Available Network C Selected Network	
OSPFv3 VIPv6 Routes	ary-lpv4	
BOP IPv4	FMC_Lab_Theodore	
IPv6  Static Route	Gateway_VLAN230 Gateway_VLAN232	
a 💋 Multicast Routing IGMP	IPv4-Benchmark-Tests     IPv4-Unk-Local	
PIM Multicast Routes	IPv4-Multicast	
Multicast Boundary Filter	Gateway* Gateway VLAN230	
General Settings	Metric: 1 (1 - 254)	
DVF	Tunneled: Utsed only for default Route)	
	OK Cancel	
Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.2		-11:-11:- cisco

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 D	Devices Objects AMP Intelligence	Elevende Catilicates			913 Deploy System	n Help v dperezve v
ftdvha-dperezve Cisco Firepower Threat Defense for VMware		Add Static Route Configuration	? ×		You have unsaved changes	Save Save
Device Routing Interfaces	Inline Sets DHCP	Type:  IPv4 O IPv6				i
Manage Virtual Routers		Interface" VLAN232				Add Route
Global	Network * Interface	(Interface starting with this icon 👩 signifies it is available for route lea	ak)	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes	Available Network C 3 Selected Network				
OSPF	any-ipv4 VLAN230	Search any-lpv4	8	1	Primary_GW	/8
USHYY3 RIP Ø BGP IPv4 IPv6	▼ IPv6 Routes	any-lip4 Bis3bon_IP_VLAV232 FMC_Lab_Theodore Gateway_VLAV230 Add				
State Routing     IGMP     PIM     Multicast Routes     Multicast Boundary Filter		Prv4-BenchmarkoTests Prv4-Unik-Local Prv4-Wilcast Prv4-Private-10.0.0.0-8				
General Settings BGP		Metric:     2     (1 - 254)       Tunneled:     Used only for default Route)       Route Tracking:     Eecondary_GW				
		OK	Cancel			
Last login on Friday, 2021-11-26 at 16:34:30	PM from 192.168.13.2				Go to system in control Parier to a	- uluilu

As duas rotas devem ser adicionadas à lista.

Overview Analysis Policies D	evices Objects AMP	Intelligence					🧛 Deploy System Help	p v dperezve v
Device Management Device Upg	rade NAT VPN VQ0	S Platform Settings FlexC	onfig Certificates					
ftdvha-dperezve Cisco Firepower Threat Defense for VMware							You have unsaved changes 📔 S	ave Cancel
Device Routing Interfaces	Inline Sets DHCP							
Manage Virtual Routers								Add Route
Global	Network +	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
OSPF	any-ipv4	VLAN232	Global	Gateway_VLAN232	false	2	Secondary_GW	/8
OSPFV3 RIP	any-ipv4	VLAN230	Global	Gateway_VLAN230	false	1	Primary_GW	/8
a 💋 BGP	▼ IPv6 Routes							
IPv4								
Static Route								
a 💋 Multicast Routing								
IGMP								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
BGP								
								*
						Activat	e Windows	
						Go to Sys	tem in control Panel to activate V	Annaows.
Last login on Friday, 2021-11-26 at 16:34:30	M from 192.168.13.2							0.000

#### 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.

Overview Analysis Policie	s Devices Objects AMP Intelligence	👫 Deploy System Help 🕶	dperezve 🔻
Object Management Intru	ion Rules		
FlexConfig Object FlexConfig Object include device con	iguration commands, variables, and scripting language instructions. It is used in RexConfig polices.	Add FlexConfig Object Riter	
Y AS Path	Name	Description	
<ul> <li>Cipher Suite List</li> <li>Community List</li> </ul>	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNSParameter	<b>a 4</b> 6 🔒
A 🗐 Distinguished Name	Default_Inspection_Protocol_Disable	Disable Default Inspection.	a 🔍 🖯 👘
Dbject Groups	Default_Inspection_Protocol_Enable	Enable Default Inspection.	a 🤹 🖯 👘
@ DNS Server Group	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de	696
External Attributes     Dynamic Object	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (	<b>b</b> 4 6
Security Group Tag	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName:	<b>a</b> e e <b>e</b>
4 🦻 FlexConfig	DNS_UnConfigure	Remove the DNS configurations.	0.0
G Text Object	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.	046
👿 Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m	a 🤹 💧 👘
Key Chain	Eigrp_UnConfigure	Clears eigrp configuration for an AS	<b>a</b> a a -
Retwork	Eigrp_Unconfigure_All	Clears eigrp configuration.	<b>a</b> e e
Policy List	Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP-	<b>a</b> a a 👘
Port	Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.	<b>b</b> 4 6 📕
IPv4 Prefix List	ISIS_Configure	Configures global parameters for IS-IS.	<b>a</b> a
IPv6 Prefix List     Ø Route Map	ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless address	<b>a</b> 4 6
4 🛒 Security Intelligence	ISIS_Unconfigure	Unconfigures is-is.	<b>a</b> e .
DNS Lists and Feeds		Abiataling W200449 rows IK < Page 1 of Go to System in Control Panel to activate Windo	5 K < 61
Last Ionin on Friday, 2021-11-26 at 16	34/30 PM from 192.168.11.2		սիսիս

Selecione a opção Add FlexConfig Object botão. No Add FlexConfig Object janela atribuir um nome e navegar até Insert > Insert Policy Object > Route Map .

Overview Analysis Policies Devices Obje	ts AMP Intelligence	👫 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules	Add FlexConfig Object ? ×	
FlexConfig Object FlexConfig Object include device configuration commands, va	Name: PBR	Add FlexConfig Object
Individual Objects Object Groups Default_DNS_Configur	Description:	s the help of TextObjects defaultDNSParameter 🛛 🗣 🗃 着
DNS Server Group Default_Inspection_Pro	🔝 Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.	Disk G
Dynamic Object     Default_Inspection_Pro	Deployment: Once V Type: Append V	048
File List DHCPv6_Prefix_Delega	Insert Policy Object     Fext Object     Insert System Variable      Network	dient) and one inside interface (recipient of de 🛛 👔 🔍 🍵
C FlexConfig Object DHCPv6_Prefix_Delega	Security Zones Security Zones	e outside (PD client) and one inside interface ( 🛛 🔒 📋
Ca Text Object DNS_Configure	Standard ACL Object	ip of TextObjects dnsParameters and dnsName: 👔 🔍 🕤
Geolocation DNS_UnConfigure	Externed ALL Ubject Route Map	tions. 🔁 🔍 🖯
Key Chain Eigrp_Configure		ures next hop. 2. configures auto-summary. 3. 👔 🔩 📋
Bigrp_Interface_Config	n	eters for eigrp. 1. Configures authentication m 🛛 🐚 🧠 📋
Policy List Eigrp_UnConfigure		or an AS
Prefix List     Eigrp_Unconfigure_All		<b>D</b> 4 6
Inspect_IPv6_Configur	Variables Name Dimension Default Value Property (Type,,, Override Description	r6 traffic. Used text objects in the script are IP 🛛 🖓 🚳
@ Route Map Inspect_IPv6_UnConfig		ipvő traffic. 🔯 🔍 🖯
Security Intelligence     DNS Lists and Feeds     ISIS_Configure	No records to display	ers for IS-IS.
Network Lists and Feeds ISIS_Interface_Config	a	ieters. By default configure ipv4 unless addres: 🌇 🔍 🖯
Sinkhole ISIS_Unconfigure		<b>D</b> 9.8 -
Use SLA Monitor +	A Save Cancel G	→ playing 1 - 20 of 49 rows K < Page 1 of 3 > > C
Last Ionin on Saharday, 2021-11-22 at 09-15-10 AM from 192-16		ahaha

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 Policie	s Devices Objects	AMP Intelli	gence								💁 Deploy System Help 🕯	dperezve +
Object Management Intru	sion Rules	Add FlexConfig	Object							? ×		
FlexConfig Object RexConfig Object include device con	figuration commands, variat	Name: Description:	PBR								Add FlexConfig Object	
Individual Objects     Object Groups     DNS Server Group      External Attributes     Dynamic Object	Name Default_DNS_Configure Default_Inspection_Proto Default_Inspection_Proto	Copy-pasting	any rich text	Insert Route M Variable Name: Description:	ap Variable PBR_RouteMap	-		? ×	Type:	Append V	1 the help of TextObjects defaultDNSParamete	
File List	DHCPv6_Prefbc_Delegatio DHCPv6_Prefbc_Delegatio			Available Objects	c		Selected Object				client) and one inside interface (recipient of d re outside (PD client) and one inside interface	
C Text Object	DNS_Configure			Search	0		@ PBR_RouteMap	8			Ip of TextObjects dnsParameters and dnsName tions.	<b>D</b> 45
Key Chain	Eigrp_Configure Eigrp_Interface_Configure										ures next hop. 2. configures auto-summary. 3 reters for eigrp. 1. Configures authentication m	<b>D</b> 48
Policy List	Elgrp_UnConfigure										or an AS	<b>D4</b> 0
IPv4 Prefix List	Inspect_IPv6_Configure	Variables Name					Save	Cancel	ption	۲	r6 traffic. Used text objects in the script are IP	048
Security Intelligence     DNS Lists and Feeds	ISIS_Configure				No	records to dis	play				ers for 15-15.	
Wetwork Lists and Feeds	ISIS_Interface_Configura ISIS_Unconfigure										ieters. By default configure ipv4 unless addres	<b>D4</b> 5
Last login on Saturday, 2021-11-27 at	09:15:30 AM from 192.168.13.	.2							Save	Cancel	splaying 1 - 20 of 49 rows 🥂 🦿 Page 1	

Overview Analysis Policies Device	es Objects AMP Intell	ligence				🔒 Deploy System Help 🔻	dperezve v
Object Management Intrusion Rules	Add FlexConfig	ig Object			? ×		
FlexConfig Object RexConfig Object include device configuration con	Name: mmands, variat Description:	PBR				Add FlexConfig Object	
Individual Objects  Object Groups  Default_DN  DNS Server Group  Default_Int  Defa	NS_Configure Ispection_Proto	ng any rich text might introduce line breaks while	generating CLI. Please verify the	CLI before deployment.		1 the help of TextObjects defaultDNSParameter	
Dynamic Object Default_In	spection_Proto			Deployme	ent: Once 👻 Type: Append 💙		<b>DA B</b>
File List DHCPv6_P	vefix_Delegatio	¢				client) and one inside interface (recipient of de	<b>D A B</b>
FlexConfig     DHCPv6_P      DHCPv6_P	Prefix_Delegatio					ne outside (PD client) and one inside interface (	Da 9. 8
Ca Text Object DNS_Confi	igure					p of TextObjects dnsParameters and dnsName:	<b>D</b> 4 6
Geolocation DNS_UnCo	onfigure					tions.	<b>D</b> 4 8
Key Chain Eigrp_Conf	figure					ures next hop. 2. configures auto-summary. 3.	0.48
PKI Eigrp_Inter	erface_Configure					eters for eigrp. 1. Configures authentication m	<b>DA</b> 6
Policy List Eigrp_UnCo	Configure					or an AS	<b>G G</b>
Prefix List     Eigrp_Unco	onfigure_All						<b>DA</b> 6
IPv4 Prefix List Inspect_IP	V6_Configure Name	Dimension	Default Value	Property (Type Override	Description	/6 traffic. Used text objects in the script are IP-	<b>D</b> 4 3
@ Route Map Inspect_IP	Pv6_UnConfigur PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR false		ipv6 traffic.	<b>G G G</b>
Security Intelligence ISIS_Confi	igure					ers for 15-15.	<b>D A B</b>
Network Lists and Feeds ISIS_Inter	rface_Configura					eters. By default configure ipv4 unless address	<b>D A B</b>
Sinkhole ISIS_Unco	onfigure						<b>DAG</b> -
Gin SLA Monitor					A	splaying 1 - 20 of 49 rows K < Page 1	OK < Elo
	Aug. 103 148 13 3				Save Cancel		ahaha

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 .

Overview Analysis Polic	cies Devices Object	s AMP Intel	ligence							🗛 Deploy System Help <del>v</del>	dperezve +
Object Management Intr	rusion Rules	Add FlexConfi	g Object						? ×		
FlexConfig Object RexConfig Object include device co	onfiguration commands, varial	Name:	PBR							Add FlexConfig Object	
AAA Server	Name     Default_DNS_Configure									the help of TextObjects defaultDNSParameter	<b>6</b> 48
Access List     Extended     Standard	Default_Inspection_Proto	Copy-pastin	ig any rich text i	night introduce line breaks while	e generating CLI. Please ver	ify the CLI before deploym	ent. Deploym	ent: Everytime V Type: 7	ippend 💌		048 048
Address Pools     IPv4 Pools	DHCPv6_Prefix_Delegatio	<ul> <li>Insert Syst</li> </ul>	em Variable 🕨	Network						client) and one inside interface (recipient of de	D 4 6
Pvs IPv6 Pools	DHCPv6_Prefix_Delegatio	<ul> <li>Insert Secr</li> </ul>	et Key	Security Zones						re outside (PD client) and one inside interface (	<b>D A</b> B
Application Filters	DNS_Configure			Standard ACL Object						Ip of TextObjects dnsParameters and dnsName	<b>D 4</b> 8
Cipher Suite List	DNS_UnConfigure			Route Map						tions.	D 4 6
Community List	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3.	Q 4 6
Individual Objects	Eigrp_Interface_Configur									eters for eigrp. 1. Configures authentication m	Da 9. 6
DNS Server Group	Eigrp_UnConfigure									or an AS	<b>Q 4</b> 8
External Attributes	Eigrp_Unconfigure_All										0.46
Security Group Tag	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Property (Type	Override	Description	۲	r6 traffic. Used text objects in the script are IP-	<b>D 4</b> 8
File List	Inspect_IPv6_UnConfigur	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PER	false			ipv6 traffic.	<b>D G F</b>
Gerentig Object	ISIS_Configure									ws for IS-15.	D 4 5
Ga Text Object	ISIS_Interface_Configura									ieters. By default configure ipv4 unless address	<b>D 4</b> 8
4 Interface	ISIS_Unconfigure										D. G. G .
Metuwek	-							Save	Cancel G	splaying 1 - 20 of 49 rows K < Page 1	of 3 > > C
Last Inde on Caburday, 2021, 11, 22	ab 11:06:07 AM from 102 160 1										ahaha

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.

Overview Analysis Polici	es Devices Objects	AMP Intel	ligence							🔒 Deploy System Help 🔻	dperezve +
Object Management Intru	usion Rules	Add FlexConfi	g Object						? ×		
FlexConfig Object RexConfig Object include device co	nfiguration commands, varial	Name: Description:	PBR							Add FlexConfig Object	
AAA Server	Name Default_DNS_Configure			Jacost Text Ob	le et Mariable					1 the help of TextObjects defaultDNSParameter	<b>DQ</b> 0 <b>±</b>
Single Sign-on Server     Server     Server     Server	Default_Inspection_Proto	Copy-pastir	g any rich text	Variable Name: Description:	Primary_GW			ytim	e 🕶 Type: Append 💌		<b>D</b> 46
Address Pools	DHCPv6_Prefix_Delegatio									client) and one inside interface (recipient of de	
Application Filters	DHCPv6_Prefix_Delegatio			Available Objects	¢	×	Selected Object	8		te outside (PD client) and one inside interface (	<b>D</b> 46
Dipher Suite List	DNS_UnConfigure			Primary_CW						tions.	Q 4 6
Community List	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3.	048
Individual Objects	Eigrp_Interface_Configure									eters for eigrp. 1. Configures authentication m	D 4 5
Object Groups     Object Group	Eigrp_UnConfigure									'or an AS	046
External Attributes	Elgrp_Unconfigure_All										048
Security Group Tag	Inspect_IPv6_Configure	Variables								/6 traffic. Used text objects in the script are IP	D 4 5
File List	Inspect_IPv6_UnConfigur	Name					Save	Cancel		ipvő traffic.	<b>Q4</b> 6
Gerenter FlexConfig Object	ISIS_Configure					No records to	display			ws for 15-15.	<b>D4</b> 6
Geolocation	ISIS_Interface_Configura									ieters. By default configure ipv4 unless address	<b>D 4</b> 8
Interface	ISIS_Unconfigure										<b>D4</b> 6 -
Key Chain									A Comment	splaying 1 - 20 of 49 rows K < Page 1	SK < € lo
Last login on Saturday, 2021-11-27 al	t 11:06:56 AM from 192.168.13	.2							Save Cance		altalta

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

Overview Analysis Polici	ies Devices Object	s AMP Intel	lligence							🧛 Deploy System	Help v dperezve v
Object Management Intro	usion Rules	Add FlexConfi	g Object						? ×		
FlexConfig Object RexConfig Object include device co	nfiguration commands, varia	Name: Description:	PBR							Add FlexConfig Object	Filter
AAA Server	Name Default_DNS_Configure									the help of TextObjects defaultDNSPa	rameter 🕞 🔍 🗃 🍈
🖌 📑 Access List	Default_Inspection_Proto	🔬 Copy-pastir	ng any rich text mig	ht introduce line breaks while	generating CLI. Please ver	ify the CLI before deploym	ent.				Q 4 6
Extended     Standard	Default_Inspection_Proto	O Insert •					Deploym	ent: Everytime 🕶 Type:	Append 👻		<b>D 4</b> 8
Address Pools	DHCPv6_Prefix_Delegation	SPBR_RouteMa SPrimary_GW	p.							client) and one inside interface (recipie	ent of de 🛯 🕞 🔒 📋
IPv6 Pools	DHCPv6_Prefix_Delegation	\$Secondary_GW	X.							ne outside (PD client) and one inside in	iterface ( 👔 🔍 🖯
Application Filters	DNS_Configure									p of TextObjects dnsParameters and d	nsNamet 🗈 🔍 🖯
Cipher Suite List	DNS_UnConfigure									tions.	Da 🔍 🗇
Community List	Elgrp_Configure									ures next hop. 2. configures auto-sum	mary. 3. 👔 🔍 📋
Individual Objects	Eigrp_Interface_Configur									eters for eigrp. 1. Configures authentic	cation m 🗈 🔍 🕤
DNS Server Group	Eigrp_UnConfigure									or an AS	<b>D A B</b>
External Attributes	Eigrp_Unconfigure_All										D 4 6
Security Group Tag	Inspect_IPv6_Configure	Variables							۲	6 traffic. Used text objects in the scrip	t are IP 🕞 🔍 🖯
File List	Inspect_IPv6_UnConfigur	Name		Dimension	Default Value	Property (Type	Override	Description	_	ipv6 traffic.	<b>DA</b> B
4 Sp FlexConfig	Mart Configure	Primary_GW		SINGLE	10.88.243.1	FREEFORM:Prim	false				0.00
FlexConfig Object	ISIS_Configure	Secondary_GW		SINGLE	10.31.124.1	FREEFORM:Seco	false			ers for IS-IS.	43 44 8
Geolocation	ISIS_Interface_Configura	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false			eters. By default configure ipv4 unless	s address 👔 🔍 🖯
G Interface	ISIS_Unconfigure										Q 4 8 -
The Key Chain								Save	Cancel G	opiaying 1 - 20 of 49 rows K < Pa	ge 1 of 3 > > C
Last login on Saturday, 2021-11-27 al	t 11:06:56 AM from 192.168.1	3.2									սիսիս

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.



O objeto FlexConfig deve ser adicionado à lista.



#### 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.

Device Management Device Upgrade NAT	VPN •	QoS Platfor	m Settings FlexConfig	ificates
tdvha-dperezve				You have unsaved changes Preview Config 📔 Save 🚺 🖸 Cancel
nter Description				Policy Assignments (1)
Available FlexConfig C G FlexConfig Obje	ct	Selected P	repend FlexConfigs	
	×	#.	Name	Description
Suser Defined     Pager     Suser Defined     Default_DNS_Configure     Default_Inspection_Protocol_Etable     Default_Inspection_Protocol_Etable     DHCPv6_Prefix_Delegation_UnConfigure     DNS_Configure     DNS_Configure     DNS_Configure		Selected A	opend FlexConfigs	
Eigrp_Configure		a.	Name	Description
Eigrp_Interface_Configure Eigrp_UnConfigure		1.	PBR	48
Eigrp_Unconfigure_All     Inspect_UPvG_Configure     Inspect_UPvG_Unconfigure     ISIS_Configure     ISIS_Interface_Configuration     ISIS_Unconfigure     ISIS_Unconfigure     ISIS_Unconfigure_All     Netflow_Add_Destination				Selected Append RexConfigs
				Go to System in Control Panel to activate Windows.

# 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.

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 flowend access-list CSM\_FW\_ACL\_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve accesslist 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: classmap 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 ruleid 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: classmap 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 ruleid 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 ruleid 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 ruleid 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, VLAN231 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 flowend access-list CSM\_FW\_ACL\_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve accesslist 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: classmap 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 ruleid 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: classmap 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 ruleid 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 ruleid 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 ruleid 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 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

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.