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

Table des matières

Introduction **Exigences** Composants utilisés Informations générales Configurer Diagramme du réseau Configurations Étape 1. Configurer la liste d'accès PBR Étape 2. Configurer la carte de routage PBR Étape 3. Configurer des objets texte FlexConfig Étape 4. Configurer le Moniteur SLA Étape 4. Configuration de routes statiques avec route track Étape 5. Configurer l'objet PBR FlexConfig Étape 6. Attribuer l'objet FlexConfig PBR à la politique FlexConfig Vérifier Dépannage

Introduction

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

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

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- Cisco FTD version 7.0.0 (build 94)
- Cisco FMC version 7.0.0 (build 94)

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

Informations générales

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

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

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

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

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

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

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

Dans cet exemple, PBR est utilisé pour acheminer des paquets sur un Internet Service Provider (ISP) basé sur l'adresse IP source.

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

Configurer

Diagramme du réseau

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

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

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

En attendant, FTD utilise des SLA IP afin de surveiller la connectivité à chaque passerelle ISP. En

cas de panne dans VLAN230, le FTD bascule vers le circuit de secours sur VLAN232.



Configurations

Étape 1. Configurer la liste d'accès PBR

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

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



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

Overview Analysis Policies Devices Ob	ects AM	P Intelligence				🗛 Deploy Sy	stem 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 features,	CL), selects the	e traffic to which a service will apply naps.	. Standard-Identifies traffic based	on destination address only. Ident	tifies traffic based on source and d	Add Extended Access L	ist Filter	d IPv6 address
AAA Server					Value	_	Override	
RADIUS Server Group New Extend	ed Access L	ist Object				? ×		
Single Sign-on Server Agencess List Extended Entries (0)	PBR_ACL							
3 Standard						Add		
Address Pools Sequence	Action	Source	Source Port	Destination	Destination Port			
Invé Pools Invé Pools Application Filters Y AS Path Cipher Suite List			No records to	display				
Distinguished Name Individual Objects Allow Override Object Groups								
C DNS Server Group					Save	Cancel		
V External Attributes Dynamic Object Piecurity Group Tag File List								
4 Set FlexConfig						No data to display	IC < Page 1	lof1>>
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.	68.13.2					Go to System in Control	Panel to activate 1	Vindows cisco

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

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

Cliquer Add pour créer l'entrée.

Overview Analysis Policies De	ovices Objects	AMP Intelligence						loy System Help v dperezve v
Object Management Intrusion Ru	les							
Extended	Add Extended	Access List Entry					? ×	ccess List
An access list object, also known as an acce You use these objects when configuring par	Action:	🖋 Allow	•					d ports. Supports IPv4 and IPv6 addresse
AAA Server Nam	Logging:	Default	~					Override
Single Sign-on Server	Log Level:	Informational	~					
4 S Access List	Log Interval:		Sec.					
Standard								
Address Pools	Network Por	rt		a				
IPv4 Pools	Available Networks	s C		Source Networks (1)	8	Destination Networks (0)		
IPV6 Pools					3			
AS Dath	E IPv4-Private-	-All-RFC1918	-					
Cipher Suite List	IPv6-IPv4-Ma	apped	Add to	1				
Community List	IPv6-Link-Lor	cal	Source	1				
A 🗐 Distinguished Name	IPv6-Private-	-Unique-Local-Addresses	Add to					
Individual Objects	IPv6-to-IPv4	-Relay-Anycast	Destination					
Contract Groups	PBR_Host							
DNS Server Group	VLAN230							
4 📝 External Attributes	VLAN232							
Dynamic Object	WLAN2813			Enter an IP address	bba	Enter an IP address	bbb	
Security Group Tag								
File List						Add	Cancel	
4 🎭 FlexConfig							No data to	display I< < Page 1 of 1 > > (*
	_				_		Go to System #	Control Panel to activate Windows
Last login on Thursday, 2021-11-25 at 20:35:0								cisco.

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



Étape 2. Configurer la carte de routage PBR

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

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

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



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

Overview Analysis Policies Devic	es Objects AMP In	telligence			🧛 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules					
Route Map					Add Route Map
Route maps are used when redistributing routes routing process.	into any routing process. They ar	e also used when generating a default route into a routi	ng process. A route map defines which of the r	routes from the specified routing pro	tocol are allowed to be redistributed into the target
Geolocation	Ne	w Route Map Object		? ×	Override
G Interface	Na	me PBR_RouteMap		_	
■ Network P PKI		Entries (0)		bbA 🕥	
Dolicy List		Sequence No 🗠	Redistribution		
IPv4 Prefix List		No record	s to display		
🕒 IPv6 Prefix List 🕖 Route Map					
Security Intelligence DNS Lists and Feeds					
Network Lists and Feeds URL Lists and Feeds	AI	low Overrides		_	
G Sinkhole Gas SLA Monitor			Save	Cancel	
🚮 Time Range					
🚓 Tunnel Zone 🍘 URL					
4				A	No data to display IC < Page 1 of 1 > >
					to system in control Panel to activate Windows cisco

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

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

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

Cliquer Add pour créer l'entrée.

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

Overview Analysis Policies Devices Obje	Add Route Map Entry		? ×	👫 Deploy System	n Help v dperezve v
Object Management Intrusion Rules	Sequence No:				
Daula Man	Redistribution:			Add Route Map	🔍 Filter
Route Map		•			
Route maps are used when redistributing routes into any rout	Match Clauses Set Cla	uses		protocol are allowed to be redistributed into the target routing process	*
Name	Security Zones	Address (2) Next Hop (0) Route Source (0)		Value	Override
Celocation	IPv4	Colored and designed as a second link on second link of a second second			
og interrace	IPv6	Select addresses to match as access list or prefix list addresses of route.			
r Key Chain	BGP				
Network Network	Others	Access List O Prefix List			
🖻 🍻 PKI		Available Access Lists :			
Delicy List		Extended			
Port .					
 Prefix List 		Available Extended Access List C Selected Extended Acc	ess List		
IPv4 Prefix List		Search	8		
🔓 IPv6 Prefix List					
@ Route Map		8 PBR_ACL			
A Security Intelligence					
DNS Lists and Feeds					
Network Lists and Feeds					
URL Lists and Feeds					
Sinkhole		bbA			
SLA Monitor					
Time Range					
Time Zone					
2 Tunnel Zone					
(URL					
S Variable Set					
C. VI AN THE					
A RI VON					
AnyConnect File			Add Cancel		
8 Certificate Man			Cancel	Activation design of a	Page 1 of 1)) (*
Ex constant may				NO data to display 14 4	sale T out > > 0
Last Josin on Thursday. 2021-11-25 at 20:35-07 PM from 102.168	13.2				ahaha

Cliquer save . Ajoutez l'objet à la liste d'objets.



Étape 3. Configurer des objets texte FlexConfig

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

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

Overview Analysis Policie	es Devices Objects AMP Intelligence		$egin{array}{c} {f P}_3 & {f Deploy} & {f System} & {f H} \end{array}$	slp v 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 can have single values or be a list of multiple values.		Add Text Object	lter
Y AS Path	Name	Value	Type Override	
Cipher Suite List Community List	defaultDNSNameServerList	1.1.1.1	System Defined 👩	2 B -
 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 📀	18
Dynamic Object	disableInspectProtocolList		System Defined	18
Group Tag	dnsNameServerList	2.2.2.2	System Defined 🕥	18
Gy FlexConfig Gy FlexConfig Object Gy Text Object	dnsParameters	3 5 abc.com	System Defined 🥥	/ 8
Geolocation	elgrpAS	1	System Defined 📀	08
Key Chain	eigrpAuthKey		System Defined 🥥	18
Network PKI	eigrpAuthKeyId		System Defined 🙄	18
Policy List	elgrpDisableAutoSummary	false	System Defined 📀	/8
 Prefix List 	eigrpDisableSplitHorizon	false	System Defined 📀	08
IPv4 Prefix List	eigrpHelloInterval	60	System Defined 📀	18
Ø Route Map	eigrpHoldTime	180	System Defined 📀	08
Security Intelligence DNS Lists and Feeds			Apisphiliping W2010749/Yows IC < Page Go to System in Control Panel to activate	1 of 3 > X C Windows.
Last login on Thursday, 2021-11-25 at	20:35:07 PM from 192.168.13.2			-dude

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

Cliquer save pour ajouter le nouvel objet.

Overview Analysis Polic	cies Devices Objects AMP Intelligence	2		93 Deploy System Help •	dperezve +
Text Object Text objects define free-form text	strings 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 Restanced Attributes	defaultDNSParameters	Add Text Object Name: Primary_GW	? × m are 1 more items.	System Defined 🥥	18
Dynamic Object	disableInspectProtocolList	Description:		System Defined	08
Security Group Tag	dnsNameServerList		2	System Defined	08
GexConfig GexConfig Object GexConfig Object	dosParameters	Variable Type Single Count	m	System Defined 🥥	18
Geolocation	eigrpAS	1 10 99 242 1		System Defined 📀	08
🏊 Key Chain	eigrpluthKey	Allow Overrides		System Defined	18
Network PKI	eigrpAuthKeyId		Save Carrel	System Defined	08
Policy List	eigrpDisableAutoSummary		Taise	System Defined	18
Port Prefix List	eigrpDisableSplitHorizon		false	System Defined 👩	08
IPv4 Prefix List	eigrpHelloInterval		60	System Defined	18
@ Route Map	eigrpHoldTime		180	System Defined	08
Security Intelligence DNS Lists and Feeds				Displaying 1 - 20 of 43 rows IC < Page 1]of3 > X C
Last login on Thursday, 2021-11-25					aludo

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

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

Overview Analysis Policie	es Devices Objects AMP Intelligence			9 Deploy	System Help v	dperezve *
Object Management Intru Text Object Text objects define free-form text st	sion Rules	have single values or be a list of multiple values.		Add Text Obje	tt. Filter	
Y AS Path	Name		Value	Туре	Override	
Cipher Suite List	defaultDNSNameServerList		1.1.1.1	System Defined	0	2 8 ÷
Distinguished Name Individual Objects Object Groups DNS Server Group External Attributes	defaultDNSParameters	Add Text Object Name: Secondary_GW	? ×	System Defined	0	18
Dynamic Object	disableInspectProtocolList	Description:		System Defined	0	18
Security Group Tag	dnsNameServerList			System Defined	0	08
Preconfig PlexConfig PlexConfig Object Config Object Config Object	drsParameters	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
INetwork ▷	eigrpAuthKeyId	Allow Otenhoes		System Defined	0	08
Policy List	eigrpDisableAutoSummary	Save	Cancel	System Defined	0	18
Prefix List	eigrpDisableSplitHorizon		false	System Defined	0	18
IPv4 Prefix List	eigrpHelloInterval		60	System Defined	0	18
@ Route Map	eigrpHoldTime		180	System Defined	0	18
Security Intelligence DNS Lists and Feeds Network Lists and Feeds	eigrpIntfList			System Defined Displaying 1 - 20 of 44 rows	⊘ < < Page 1	0 3 × X С
Last login on Friday, 2021-11-26 at 08						111111

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



Étape 4. Configurer le Moniteur SLA

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



Sélectionnez le Add SLA Monitor Objet.

Dans la New SLA Monitor, définissez un nom ainsi qu'un identifiant pour l'opération SLA, l'adresse IP du périphérique qui doit être surveillé (dans ce cas, la passerelle principale) et l'interface ou la zone par laquelle le périphérique est accessible.

En outre, il est également possible d'ajuster le délai d'attente et le seuil. Cliquer save.

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

Remarque : si les valeurs de délai d'attente et de seuil ne sont pas spécifiées, FTD utilise des compteurs par défaut : 5 000 milisecondes dans chaque cas.

Overview Analysis Policies Devices Objects AMP Intelligence				👫 Deploy System Help 🔻 dperezve 🕷
Object Management Intrusion Rules	New SLA Monitor Ob	ject	? 3	
SLA Monitor SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route	Name: Description:	Primary_GW	1	Add SLA Monitor
Roley List Port Prot Prot Prot Prot Prot Prot Prot Prot Prot Port Prot Port P	Frequency (seconds): SLA Monitor ID*: Threshold (milliseconds): Timeout (milliseconds): Data Size (bytes): ToS: Number of Packets: Monitor Address*:	60 1 5000 28 1 10.88.243.1	(1-604800) (0-60480000) (0-604800000) (0-16384)	Value
URL Lists and Freds GinAbide GinAbide GinAbide Time Zone Time Zone Time Zone Wrabbe Set VLAN Tag Cutton Attribute Group Pelicy Cutton Attribute Group Pelicy Discut Libley Group Pelicy Discut Libley	Available Zones C G Search St VLAN230 ds VLAN230 ds VLAN2913		Selected Zones/Interfaces	
B IKEV2 Policy *				No data to display K < Page 1 of 1 > > C
Last bein an Diday 2021-11-26 at 08:37:16 AM from 102.168-13.2			Save Cancel	Jululu

Sélectionnez le Add SLA Monitor afin de créer un deuxième objet, cette fois pour le modem routeur sur le circuit de sauvegarde.

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

Overview Analysis Polici	es Devices Objects AMP Intelligence				🧛 Deploy Sy	rstem Help v dperezve v
Object Management Intru	usion Rules	New SLA Monitor Ol	oject	?	×	
SLA Monitor SLA monitor defines a connectivity (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.	
P PKI	Name	Frequency (seconds):	60	(1-604800)	Value	
Protocy List Protocy List Protocy List Protocy List Protocy List Protocy Protocy List Protocy Protocy List Protocy Lists and Feeds URL Lists and Feeds URL Lists and Feeds Sistahole Sistahole Sistahole Sistahole	Primary_GW	SLA Monitor ID*: Threshold (milliseconds): Timeout (milliseconds): Data Size (bytes): ToS: Number of Packets: Monitor Address*: Available Zones C Search	2 5000 28 1 10.31.124.1	(0-60000) (0-604800000) (0-16384) Selected Zones/Interfaces	Security Zone: VLAN230 Heniter ID: 1 Henitor Address: 10.88.243.1	/0.
Time Range Time Zone Time Zone Time Zone Tome Zone VRL VRI VVRI VVRI Molonnect File Custon Attribute Coston Attribute Ciston Policy Ciston Policy	1	े 2000 के VLAN230 के VLAN232 के VLAN2813				
DCP TKEV2 Policy *				Save Cancel		
Last login on Friday, 2021-11-26 at 08	8:37:16 AM from 192.168.13.2					aludo

Les deux objets doivent être ajoutés à la liste.

Overview Analysis Polic	es Devices Objects AMP Intelligence	🗛 Deploy Syste	em Help v	dperezve v
Object Management Intr	usion 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 IP+4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor	Add SLA Monitor	۹,	
D 🌽 PKI .	Name Value			
Policy List Port Port Prefix List	Primary_GW Security Zone: VLAV230 Moritor 10: 1 Moritor 40: 19: 10: 1	1		/ 5 m
Drv4 Prefix List	Secondary_GW Security Zone: VLAN232 Monitor UD: 2 Monitor ddress: 10.31.124	1		/ 6 m
Conter Hap Conter Hap	Pointor Adoresi: 10.3.1.124.			
IKEV1 IPsec Proposal IKEV1 Policy IKEV1 Policy IKEV2 Policy IKEV2 Policy IKEV2 Policy	Active Ge to Sy	GAVI 이외 여행 Kows K 《 stem in Control Panel to ?	Page 1	of1 >>> C ows.
Last login on Friday, 2021-11-26 at 0	8:37:16 AM from 192.168.13.2			-ili-ili-

Étape 4. Configuration de routes statiques avec route track

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

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

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

Overview Analysis Policies D	evices Object	s AMP Intelligen	ce					鵫 Deploy S	ystem Help 🔻	dperezve v
Device Management Device Upg	rade NAT V	VPN VOS Platfo	rm Settings FlexCor	fig Certificates						
ftdvha-dperezve Cisco Firepower Threat Defense for VMware									Save	Cancel
Device Routing Interfaces	Inline Sets	DHCP								
 Manage Virtual Routers 									C Ad	1 Route
Global 👻	Network *	Interfa	e	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked		
Virtual Router Properties	 IPv4 Routes 									
OSPF OSPFv3	- 10 / 0 · · · · ·									- 1. 1
RIP	▼ IPvo Routes									
# 🤪 BGP										
IP∨6										
Static Route										
IGMP										
PIM										
Multicast Routes Multicast Boundary Filter										
General Settings										
BGP										
								A stiuste Mindour		*
								Go to System in Control Panel	to activate Wind	ows.
Last login on Friday, 2021-11-26 at 08:37:16	AM from 192.168.13.2	2								altalta cisco

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

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

Spécifiez une mesure pour la route et dans la zone Route Track et sélectionnez l'objet SLA pour la

passerelle principale créée à l'étape 3.

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

Overview Analysis Policies De	evices Objects AMP Intelligence		🧛 Deploy System Help 🔻 dperezve 🔻
Device Management Device Upgr	rade NAT VPN QoS Platform Settings	FlexConfig Certificates	
Cisco Firepower Threat Defense for VMware		Add Static Route Configuration 7 ×	Save Cancel
Device Routing Interfaces	Inline Sets DHCP	Туре: 🖲 IРv4 О IРv6	
Manage Virtual Routers	Natural - Tatadas	Interface" VLAN230 V (Interface studies with this icen (* desilier it is well-this for rests icel) to the last	Add Route
Ciceal Vitual Router Properties OSPF OSPF/3 RP P BOP IP/4 IP/6 • Static Route • Static Route IOHP PIN Multicast Routes Multicast Routes Multicast Boundary Filter Cemeral Settings BOP	Network + Interface	Available Network Image: Search Search Selected Network Search any-lipv4 Phy-Lendmark-Tests any-lipv4 Phy-Hendmark-Tests Image: Phy-Hubbark Phy-Hendmark-Tests Image: Phy-Hubbark Phy-Hendmark-Tests Image: Phy-Hubbark Phy-Hendmark-Tests Image: Phy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Bhy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Bhy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Bhy-Hubbark Image: Phy-Hubbark Image: Phy-Hubbark Image: Phy-Hub	
		OK. Cancel	Activate Windows
			Go to System in Control Panel to activate Windows.
Last login on Friday, 2021-11-26 at 08:37:16 /	U4 from 192-168-13-2		CISCO

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

Cliquer Add Route pour définir une nouvelle route statique.

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

Overview Analysis Policies D	Devices Objects AMP Intelligence	s FlexConfig Certificates	0 15 Deploy System Help v diperezve v
ftdvha-dperezve Cisco Firepower Threat Defense for VMware		Add Static Route Configuration ? ×	You have unsaved changes 📑 Save Cancel
Kouting Interfaces Manage Virtual Routers Global	Network + Interface	Interface" VLAN222 (Interface starting with this icon is signifies it is available for route leak)	Add Route
Virtual Router Properties OSPFV3 RIP © BCP IPv4 Pv6 • Static Route @ Multicast Routing IG4P PIM Multicast Routes Multicast Boundary Filter Ceneral Settings BGP	▼IPv4 Routes any-ipv4 VLAN230 ▼IPv6 Routes	Available Network Selected Network Sanchet Sanchet Sanchet any-loyd Backbons, JP, UAN232 any-loyd Gateway, VAN230 Add Gateway, VAN230 Add Drvd-hink-Local Drvd-hink-Local Drvd-hink-Local Inverted (1-254) Tunneled: Cused only for default Route) Route Tracking: Secondary_GW OK Cancel	1 Primary_GW
Last Josin on Feder, 2021;11:26 at 16:34:30	PM from 102 1/8 13 2		Activate Windows

Les deux routes doivent être ajoutées à la liste.

Overview Analysis Policies D	evices Objects AMF	P Intelligence					🧛 Deploy System I	Help v dperezve v
Device Management Device Upg	rade NAT VPN •	QoS Platform Settings I	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								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-lpv4	VLAN230	Global	Gateway_VLAN230	false	1	Primary_GW	/8
a 🤪 BGP	▼ IPv6 Routes							
IPv4								
IPv6								
A G Multicast Routing								
IGMP								
PIM								
Multicast Roundary Filter								
General Settings								
BGP								
								v
							So to System in Control Panel to activa	te Windows.
Last login on Friday, 2021-11-26 at 16:34:30 F	PM from 192.168.13.2							վերի

Étape 5. Configurer l'objet PBR FlexConfig

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

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

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

Overview Analysis Policie	s Devices Objects AMP Intelligence	🗛 Deploy System Help 🔻	dperezve v
Object Management Intru	ion Rules		
FlexConfig Object RexConfig Object include device con	iguration commands, variables, and scripting language instructions. It is used in RexConfig polices.	Add FlexConfig Object	
Y AS Path	Name	Description	
Cipher Suite List Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNSParameter	D 4 6 *
A 🌍 Distinguished Name	Default_Inspection_Protocol_Disable	Disable Default Inspection.	Da 🔍 🖯 👘
Individual Objects Object Groups	Default_Inspection_Protocol_Enable	Enable Default Inspection.	Da 🔍 🖯 👘
DNS Server Group	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de	D 4 6
External Attributes Dynamic Object	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (D A B
Security Group Tag	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName:	Q 4 6
A G FlexConfig	DNS_UnConfigure	Remove the DNS configurations.	D A B
G Text Object	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.	Q 4 6
Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m	Da 🔍 🖯 👘
S Interface	Eigrp_UnConfigure	Clears eigrp configuration for an AS	Da 4, 6
Retwork	Eigrp_Unconfigure_All	Clears eigrp configuration.	D 4 8
P PRI	Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP	DA B
Port	Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.	D A B
IPv4 Prefix List	1515_Configure	Configures global parameters for IS-IS.	DA B
IPv6 Prefix List Route Map	ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless address	Da 🔍 🖯 👘
a 🥪 Security Intelligence	1515_Unconfigure	Unconfigures is-is.	D4 6 -
DNS Lists and Feeds		Abiabian W 20 (14) for a city of the second	of 3 > > C
Last login on Friday, 2021-11-26 at 16	34:30 PM from 192.168.13.2		aluto

Sélectionnez le Add FlexConfig Object s'affiche. Dans la Add FlexConfig Object attribuer un nom et accéder à 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		D 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		D 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

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

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

Overview Analysis Polici	es Devices Objects	AMP Intel	ligence								🔒 Deploy System Help 🕯	dperezve +
Object Management Intru	ision Rules	Add FlexConfi	g Object							? ×		
FlexConfig Object RexConfig Object include device cor	ifiguration commands, variat	Name: Description:	PBR								Add FlexConfig Object	
Diplect Groups	Name Default_DNS_Configure			Insert Route M	an Variable			7 X			1 the help of TextObjects defaultDNSParameter	99
DNS Server Group Z External Attributes	Default_Inspection_Proto	🔬 Copy-pastin	g any rich text	Variable Name:	PBR. RouteMap	_						D4 6
Dynamic Object	Default_Inspection_Proto	O Insert •		Description:					Type:	Append V		D A B
File List	DHCPv6_Prefix_Delegatio										client) and one inside interface (recipient of de	D3 4 6
Gy FlexConfig Gy FlexConfig Object	DHCPv6_Prefix_Delegatio			Available Objects	c		Selected Object				te outside (PD client) and one inside interface	DA 8
Ca Text Object	DNS_Configure			Search		_	Ø PBR_RouteMap	8			lp of TextObjects dnsParameters and dnsName	B 4 8
Geolocation	DNS_UnConfigure			Ø PBR_RouteMa	P						tions.	D 4 6
Key Chain	Eigrp_Configure										ures next hop. 2. configures auto-summary. 3	D 4 6
Network PKI	Eigrp_Interface_Configure										eters for eigrp. 1. Configures authentication m	DA 6
Policy List	Eigrp_UnConfigure										or an AS	D A B
4 🕒 Prefix List	Eigrp_Unconfigure_All											0.6
IPv6 Prefix List	Inspect_IPv6_Configure	Variables							ption	۲	/6 traffic. Used text objects in the script are IP	DA B
@ Route Map	Inspect_IPv6_UnConfigur						Save	Cancel			ipv6 traffic.	B4 6
Security Intelligence DNS Lists and Feeds	ISIS_Configure					o records to dis	blay				ars for IS-IS.	DA B
Network Lists and Feeds	ISIS_Interface_Configura										ieters. By default configure ipv4 unless addres	DA 6
URL Lists and Feeds Sinkhole	ISIS_Unconfigure											DA 0 -
Gia SLA Monitor									(From	Concel	splaying 1 - 20 of 49 rows K < Page 1	of 3 > X C
Last login on Saturday, 2021-11-27 at	: 09:15:30 AM from 192.168.13.	2							5916	Cancel		-iltilii cisco

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 💙		DA A
File List DHCPv6_P	vefix_Delegatio	¢				client) and one inside interface (recipient of de	D A B
FlexConfig DHCPv6_P DHCPv6_P	Prefix_Delegatio					ne outside (PD client) and one inside interface (Da 9. 8
G Text Object DNS_Confi	igure					p of TextObjects dnsParameters and dnsName:	D 4 6
Geolocation DNS_UnCo	onfigure					tions.	D 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	DA 6
Policy List Eigrp_UnCo	Configure					or an AS	G G
Prefix List Eigrp_Unco	onfigure_All						D A B
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-	D 4 3
@ Route Map Inspect_IP	Pv6_UnConfigur PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR false		ipv6 traffic.	G G G
Security Intelligence ISIS_Confi	igure					ers for 15-15.	D A B
Network Lists and Feeds ISIS_Inter	rface_Configura					eters. By default configure ipv4 unless address	D A B
Sinkhole ISIS_Unco	onfigure						DAG -
Gin SLA Monitor					A	splaying 1 - 20 of 49 rows K < Page 1	OK < Elo
	Aug. 103 148 13 3				Save Cancel		ahaha

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

Overview Analysis Polic	cies Devices Objects	AMP Intel	ligence							🔒 Deploy System Help 🔻	dperezve +
Object Management Intr	rusion Rules	Add FlexConfig	g Object						? ×		
FlexConfig Object FlexConfig Object include device or	onfiguration commands, varial	Name:	PBR							Add FlexConfig Object	
AAA Server	Name Default_DNS_Configure	Description.								the help of TextObjects defaultDNSParameter	D A B
▲ Standard	Default_Inspection_Proto	Copy-pastin	g any rich text i	night introduce line breaks while	generating CLI. Please ver	ify the CLI before deploym	ent. Deployr	nent: Everytime 💙 Type: Appe	nd 💌		645 645
Address Pools	DHCPv6_Prefix_Delegatio	 Insert Polic Insert Syst 	em Variable	Text Object Network						client) and one inside interface (recipient of de	D 4 B
Application Filters	DNS_Configure	Unsert Secr	et key	Security Zones Standard ACL Object						ip of TextObjects dnsParameters and dnsName:	6948
Cipher Suite List Community List	DNS_UnConfigure			Route Map						tions. ures next hop. 2. configures auto-summary. 3.	D 4 6
Distinguished Name Individual Objects Object Groups	Eigrp_Interface_Configure									eters for eigrp. 1. Configures authentication m	040
DNS Server Group External Attributes	Elgrp_UnConfigure									or an AS	D4 0
Dynamic Object Security Group Tag	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Property (Type	Override	Description	۲	of traffic. Used text objects in the script are IP-	0.4.5
Gy FlexConfig Gy FlexConfig Object	Inspect_IPv6_UnConfigur ISIS_Configure	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false			ipv6 traffic. nrs for IS-IS.	D 4 6
G Text Object	ISIS_Interface_Configura									eters. By default configure ipv4 unless address	D 4 5
Key Chain	ISIS_Unconfigure							Com Co	Ax GD	iplaying 1 - 20 of 49 rows K < Page 1	of 3 > X C
								Save	in can		ahaha

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

Cliquer save afin de l'ajouter à l'objet FlexConfig.

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	leat Mariable					1 the help of TextObjects defaultDNSParameter	DQ 0 ±
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 💌		D 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 (D 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	Q 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.	Q4 6
Gerenter FlexConfig Object	ISIS_Configure					No records to	display			ws for 15-15.	D4 6
Geolocation	ISIS_Interface_Configura									ieters. By default configure ipv4 unless address	D 4 8
Interface	ISIS_Unconfigure										D4 6 -
Key Chain									A Comment	splaying 1 - 20 of 49 rows K < Page 1	SK < £ to
Last login on Saturday, 2021-11-27 al	t 11:06:56 AM from 192.168.13	.2							Save Cance		altalta

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

Overview Analysis Polici	ies Devices Object	s AMP Inte	lligence								dperezve v
Object Management Intri	usion Rules	Add FlexConfi	g Object						? ×		
FlexConfig Object RexConfig Object include device co	nfiguration commands, varia	Name: Description:	PBR							Add FlexConfig Object	
AAA Server	Name Default_DNS_Configure	Come antibility		akt lateradore Han beenla ookila	erenties CI I News	di the CIT before destroyed				the help of TextObjects defaultDNSParameter	D A B
Access List	Default_Inspection_Proto	Insert -	i 🗉 i	nt nu ouoce nire breaks white	generating cci. Hease ve	ny the CLI before deployin	Deploym	nent: Everytime 🕶 Type: Append	1 ¥		
Address Pools IPv4 Pools IPv6 Pools	DHCPv6_Prefix_Delegation	SPBR_RouteMa SPrimary_GW SSecondary_GW	р Х						d	lient) and one inside interface (recipient of de outside (PD client) and one inside interface	
Application Filters	DNS_Configure								10	of TextObjects dnsParameters and dnsName	DA B
Community List	Elgrp_Configure								u	res next hop. 2. configures auto-summary. 3.	048
Individual Objects	Eigrp_Interface_Configur									ters for eigrp. 1. Configures authentication m	
DNS Server Group	Elgrp_UnConfigure								0	r an AS	D4 6
External Attributes	Eigrp_Unconfigure_All								_11		0.48
Security Group Tag	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Broperty (Tupe	Override	Description		traffic. Used text objects in the script are IP	048
File List	Inspect_IPv6_UnConfigu	Primary GW		SINGLE	10.88.243.1	FREEFORM:Prim	false	Description		ov6 traffic.	DA 6
FlexConfig Object	ISIS_Configure	Secondary_GW		SINGLE	10.31.124.1	FREEFORM:Seco	false			s for IS-IS.	Da 6
Geolocation	ISIS_Interface_Configura	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false		10	ters. By default configure ipv4 unless addres	D4 8
S Interface	ISIS_Unconfigure								- 11		048 -
Maturd								Save Can	Aici _e	Naying 1 - 20 of 49 rows K < Page 1] of 3 > > C
Last login on Saturday, 2021-11-27 a		3.2									

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

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

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

Cliquer save lorsque la configuration est terminée.



L'objet FlexConfig doit être ajouté à la liste.



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

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

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

evice Management Device Upgrade 1	LAT VPI	V V QoS Platfo	rm Settings FlexConfig Cert	tes
dvha-dperezve				You have unsaved changes Preview Config Save Cancel
ter Description				Policy Assignments (1)
Ausilable FlowConfin & O FlexConfin	Object	Selected B	tropond ElevConfins	
Available Prexcound C			Name	Description
	×		Nonine	vescapion
4 📢 User Defined				
Paper				
PBR	- 1			
4 🥥 System Defined	-			
Default_DNS_Configure				
Default_Inspection_Protocol_Disable				
Default_Inspection_Protocol_Enable				
DHCPv6_Prefix_Delegation_Configure				
DHCPv6_Prefix_Delegation_UnConfig	ure C			
DNS_Configure		> D Selected 4	anond ElevConfigs	
DNS_UnConfigure		derected F	append r texcomigs	
Eigrp_Configure		<i>a.</i>	Name	Description
Eigrp_Interface_Configure		1.	PBR	4.5
Eigrp_UnConfigure				
Eigrp_Unconfigure_All				
Inspect_IPv6_Configure				
Inspect_IPV6_Unconfigure				
ISIS_Configure				
ISIS_Interface_Computation				
ISIS Unconfigure All				Selected Append FlexConfigs
ISIS_Unconfigure_All				
ISIS_Unconfigure_All ISIS_Vector_Add_Destination				Activate Windows

Vérifier

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

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

firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed Phase: 1 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop verify-availability 10.31.124.1 2 track 1 Additional Information: Matched route-map PBR_RouteMap, sequence 10, permit Found next-hop 10.88.243.1 using egress ifc VLAN230 Phase: 2 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log 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

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

firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address (access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2 [down] ip next-hop verify-availability 10.31.124.1 2 track 1 [up] firepower# show route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF Gateway of last resort is 10.31.124.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [2/0] via 10.31.124.1, VLAN232 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25 255.255.255.255 is directly connected, VLAN232 C 192.168.13.0 255.255.255.0 is directly connected, VLAN2813

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

firepower# show logg | i 622001 %FTD-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.31.124.1, distance 2, table default, on interface VLAN232%FTD-6-305012: Teardown dynamic UDP translation from VLAN2813:192.168.13.5/49641 to VLAN230:10.88.243.60/49641 duration 0:02:10 Maintenant, tout le trafic provenant du VLAN2813 doit être transféré via le circuit ISP de secours.

firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed Phase: 1 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop verify-availability 10.31.124.1 2 track 1 Additional Information: Matched route-map PBR_RouteMap, sequence 10, permit Found next-hop 10.31.124.1 using egress ifc VLAN232 Phase: 2 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log 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

Dépannage

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

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

À propos de cette traduction

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

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