Configure PBR with IP SLAs for DUAL ISP on FTD Managed by FMC

Contents

Introduction Requirements **Components Used Background Information** Configure **Network Diagram Configurations** Step 1. Configure PBR Access List Step 2. Configure PBR Route Map Step 3. Configure FlexConfig Text Objects Step 4. Configure SLA Monitor Step 4. Configure Static Routes with Route Track Step 5. Configure PBR FlexConfig Object Step 6. Assign PBR FlexConfig Object to FlexConfig Policy Verify **Troubleshoot**

Introduction

This document describes how to configure PBR along with IP SLAs on a FTD that is managed by (FMC).

Contributed by Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- PBR configuration on Cisco Adaptive Security Appliance (ASA)
- FlexConfig on Firepower
- IP SLAs

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes how to configure Policy Based Routing (PBR) along with Internet Protocol Service Level Agreement (IP SLA) on a Cisco Firepower Threat Defense (FTD) that is managed by Cisco Firepower Management Center (FMC).

The traditional routing takes forwarding decisions based on the destination IP addresses only. PBR is an alternative to routing protocols and static routing.

It provides more granular control over routing because it allows the use of parameters such as source IP addresses or source and destination ports as routing criteria besides the destination IP address.

Possible scenarios for PBR include source sensitive applications or traffic over dedicated links.

Along with PBR, IP SLAs can be implemented in order to ensure availability of the next hop. An IP SLA is a mechanism that monitors end to end connectivity through the exchange of regular packets.

At the time of publication, PBR is not directly supported through FMC **Graphical User Interface (GUI)**, the configuration of the feature requires the use of FlexConfig policies.

On the other hand, only Internet Control Message Protocol (ICMP) SLAs are supported by FTD.

In this example, PBR is used to route packets over a primary Internet Service Provider (ISP) circuit based on the source IP address.

In the meantime, an IP SLA monitors connectivity and forces a fallback to backup circuit in case of any failure.

Configure

Network Diagram

In this example, Cisco FTD has two outside interfaces: VLAN230 and VLAN232. Each one connects to a different ISP.

The traffic from internal network VLAN2813 is routed through the primary ISP which uses PBR.

The PBR route map takes forwarding decisions based on the source IP address only (everything received from VLAN2813 must be routed to 10.88.243.1 in VLAN230) and it is applied in interface GigabitEthernet 0/1 of FTD.

In the meantime, FTD uses IP SLAs in order to monitor connectivity to each ISP Gateway. In case of any failure in VLAN230, FTD failovers to the backup circuit on VLAN232.



Configurations

Step 1. Configure PBR Access List

At the first step of PBR configuration, define which packets must be subject of the routing policy. PBR makes use of route maps and access list to identify traffic.

In order to define an access list for the matching criteria navigate to Objects > Object Management and select Extended under the Access List category in the table of contents.



Click Add Extended Access List . In the New Extended Access List Object window, assign a name for the object, then select the Add button in order to start with access list configuration.

Overview Analysis Policies Devices Obj	ects AMI	P Intelligence				$igoplus_{13}$ Deploy	System 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 such as route n	a traffic to which a service will appl naps.	y. Standard-Identifies traffic based	I on destination address only. Iden	tifies traffic based on source and de	Add Extended Access	tist Filter	nd IPv6 addresse
AAA Server					Value	_	Override	
RADIUS Server Group New Extend	d Access L	ist Object				? ×		
Single Sign-on Server Name Name Entries (0)	PBR_ACL					Q add		
Address Pools Sequence	Action	Source	Source Port	Destination	Destination Port	0 100		
IPv4 Pools IPv6			No records to	display				
Individual Objects Allow Override								
Collect Groups					Save	Cancel		
VExternal Attributes Dynamic Object Security Group Tag File List								
A Gy FlexConfig						No data to display	K < Page 1	lof1>>
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.	68.13.2					Go to System in Contr	ol Panel to activate	Vindows cisco

In the Add Extended Access List Entry window, select the object that represents the inside network, in this case VLAN2813.

Click Add to Source to define it as the source of the access list.

Click Add to create the entry.

Overview Analysis Policies De	ovices Objects	AMP Intelligenc	e					loy System	Help 🔻 dpo	erezve 🔻
Object Management Intrusion Ru	les									
Extended An access list object, also known as an acce	Add Extended	Access List Entry	v				? ×	d ports. Suppor	Filter ts IPv4 and IPv	v6 address
AAA Server	Logging:	Default	~						override	-
Sangle sign-on Server Server Secss List Secses List Secses List Secses List Secses List	Log Level: Log Interval:	300	Sec.							
Address Pools IPv4 Pools IPv4 Pools IPv6 Pools Application Filters As Path Community List Distinguished Name Individual Objects Object Groups Disterver Group Disterver Group Disterver Johnson Disterver Johns	Available Network Search by nar IPv4-Private- IPv6-IPv4-Mi PP6-trivate- PP6-trivate- PP8-trivate	All-RFC1918 apped cal -Unique-Local-Addresses -Relay-Anycast	Add to Cource Add to Destination	Source Networks (1)	G Add	Destination Networks (0) any Enter an IP address	Add			
File List						Add	Cancel No data to	display K <	Page 1 of	1 > >
Last login on Thursday, 2021-11-25 at 20:35:0	7 PM from 192.168.13	.2					Go to System i	n Control Panel to	activate Windo	

Click save. The object must be added to object list.



Step 2. Configure PBR Route Map

Once the PBR access list is configured, assign it to a route map. Route map evaluates traffic against the match clauses defined in the access list.

After a match occurs, route map executes the actions defined in the routing policy.

To define route map, navigate to Objects > Object Management and select Route Map in the table of contents.



Click Add Route Map >. In the New Route Map Object assign a name for the object, then click Add to create a new route map entry.

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				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

In the Add Route Map Entry window, define a sequence number for the position of the new entry.

Navigate to IPv4 > Match Clauses and select Extended in the Available Access List drop down menu.

Select the access list object created in Step 1.

Click Add to create the entry.

Note: FTD supports up to 65536 (from 0 to 65535) different entries. The lower the number, the highest the priority evaluation.

Overview Analysis Policies Devices Object	Add Route Map Entry		? >	< Contract of the second se	🦺 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules	Comment New Tex				
	Sequence No: 10				Charles Man
Route Map	Redistribution: 🖌 Allo	w Y			And route map
Route maps are used when redistributing routes into any rout	Match Clauses Set Cla	auses		protocol are allowed to be redi-	tributed into the target routing process.
Name	Security Zones	Address (2) Next Hop (0) Route Source (0)		Value	Override
Geolocation	IPv4				
og Interface	IPv6	select addresses to match as access list or prefix list addresse	s of route.		
r Key Chain	BGP	Charles Int. O Burkella			
network	Others	Access List			
P presented		Available Access Lists :			
Policy List		Extended 🗸			
POR Port					
The stand Backwork late		Available Extended Access List C	Selected Extended Access List		
The the foreful list		Search	BR_ACL		
A Parte Man		B PBR_ACL			
A m Cecurity Intelligence					
DNS Lists and Feeds					
Network Lists and Feeds					
URL Lists and Feeds			-		
Sinkhole		Add			
A SLA Monitor					
Time Range					
Time Zone					
Z Tunnel Zone					
G URL					
S Variable Set					
S VLAN Tag					
- BO VPN					
ManyConnect File			Add Cancel		
R Certificate Map					No data to display K < Page 1 of 1 > > C
Last Josin on Thursday, 2021-11-25 at 20:35-07 PM from 102-168	112.2				ahaha

Click Save . Add the object to the object list.



Step 3. Configure FlexConfig Text Objects

The next step involves the definition of FlexConfig text objects that represent default Gateways for each circuit. These text objects are used later in the configuration of FlexConfig object that associates PBR with SLAs.

In order to define a FlexConfig text object navigate to Objects > Object Management and select Text Object under the FlexConfig category in the table of contents.

Overview Analysis Policie	es Devices Objects AMP Intelligence		🧛 Deploy Syste	em Help v dperezve
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	🔍 Filter
Y AS Path	Name	Value	Type O	lverride
Cipher Suite List	defaultDNSNameServerUst	1.1.1.1	System Defined	2 2 8
Distinguished Name Individual Objects Object Groups DNS Server Group VExternal Attributes	defaultDNSParameters	3 5 10 abc.com There are 1 more items.	System Defined 🏾 🏾 🏾	0 0 8
Dynamic Object	disableInspectProtocolList		System Defined	
Security Group Tag	dnsNameServerList	2.2.2.2	System Defined	28
Gy FlexConfig Gy FlexConfig Object Gy Text Object	dnsParameters	3 5 abc.com	System Defined) / 3
🙀 Geolocation 🧠 Interface	elgrpAS	1	System Defined	2 2 3
Key Chain	elgrpAuthKey		System Defined	2 2 3
Network PKI	eigrpAuthKeyId		System Defined	2 2 3
Policy List	eigrpDisableAutoSummary	false	System Defined	2 3
A D Prefix List	eigrpDisableSplitHorizon	false	System Defined	28
IPv4 Prefix List	eigrpHelloInterval	60	System Defined	2
Ø Route Map	eigrpHoldTime	180	System Defined	28
Security Intelligence DNS Lists and Feeds		A <mark>stij</mark> Go to	มู่มีคู่ Wigd doug fows เห System in Control Panel to เ	Page 1 of 3 > > C activate Windows.
Last login on Thursday, 2021-11-25 at	20:35:07 PM from 192.168.13.2			-11-11

Click Add Text Object . In the Add Text Object window, assign a name for the object that represents the primary Gateway and specify the IPv4 address for this device.

Click Save to add the new object.

Overview Analysis Polici	es Devices Objects AMP Intelligence			Page 10 Peploy 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. These objects co	in 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 Distinguished Name Individual Objects Object Groups DNS Server Group DNS Server Group	defaultDNSParameters	Add Text Object Name: Primary_GW	? × sm are 1 more items.	System Defined 🥥	18
Dynamic Object	disableInspectProtocolList	Description:		System Defined	18
Security Group Tag	dnsNameServerList		2	System Defined	08
Gy FlexConfig Gy FlexConfig Object Gy Text Object	dnsParameters	Variable Type Single Count 1	um.	System Defined	18
Geolocation	eigrpAS	1 10.88.243.1		System Defined 📀	08
Key Chain	eigrpAuthKey	Allow Overrides	-	System Defined 🕑	18
Network	eigrpAuthKeyId	Sive Carro		System Defined 🕑	08
Policy List	eigrpDisableAutoSummary		Talse	System Defined 🕑	08
Port 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			Display	og 1 - 20 of 43 rows K < Page 1	• • • • • • •
Last login on Thursday, 2021-11-25 a	t 20:35:07 PM from 192.168.13.2				dute

Click Add Text Object again to create a second object, this time for the Gateway on the backup circuit.

Fill the new object with the appropriate name and IP address and click $\ensuremath{\textit{save}}$.

Overview Analysis Policie Object Management Intru	Overview Analysis Policies Devices Objects AMP Intelligence Object Hanagement Intrusion Roles							
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 Obje	t Filter			
Y AS Path	Name		Value	Туре	Override			
Cipher Suite List	defaultDNSNameServerList		1.1.1.1	System Defined	0	2 8 É		
Distinguished Name Individual Objects Object Groups ONS Server Group	defaultDNSParameters	Add Text Object Name: <u>Secondary_GW</u>	? Y X	System Defined	0	18		
Dynamic Object	disableInspectProtocolList	Description:		System Defined	0	18		
Security Group Tag	dnsNameServerList			System Defined	0	08		
Gy FlexConfig 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	eigrpAuthKeyId	Allow Overnoes	-	System Defined	0	08		
Policy List	eigrpDisableAutoSummary	Save	Cancel	System Defined	0	18		
Port	eigrpDisableSplitHorizon		false	System Defined	0	18		
IPv4 Prefix List	eigrpHelloInterval		60	System Defined	0	13		
Route Map	eigrpHoldTime		180	System Defined	0	08		
Security Intelligence DNS Lists and Feeds Network Lists and Feeds	elgrpIntfList			System Defined Displaying 1 - 20 of 44 rows	C A Page 1	/ । d13 > >। C		
Last login on Friday, 2021-11-26 at 08						-11111-		

The two objects must be added to the list along with the default objects.



Step 4. Configure SLA Monitor

To define the SLA objects used to monitor connectivity to each Gateway, navigate to **Objects > Object** Management and select **SLA** Monitor in the table of contents.



Select the Add SLA Monitor Object.

In the New SLA Monitor window, define a name along with an identifier for the SLA operation, the IP address for the device that must be monitored (in this case the primary Gateway), and the interface or zone through which the device is reachable.

Additionally, it is also possible to adjust the timeout and threshold. Click save.

Note: FTD supports up to 2000 SLA operations. The values for the SLA ID range from 1 to 2147483647.

Note: If timeout and threshold values are not specified, FTD uses default timers: 5000 miliseconds in each case.

Overview Analysis Policies Devices Objects AMP Intelligence				Page 13 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 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 Lists and Feeds Genetic Genetic Time Range Time Range Time Cane T	Available Zones C Search Survay Survay Survay Alantasia VLAN2813		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

Select the Add SLA Monitor button once more in order to create a second object, this time for the Gateway on the backup circuit.

Fill the new object with the appropriate information, ensure the SLA ID is different from the one defined for the primary Gateway, and save changes.

Object Management Intraction Rules SLA Monitor Check SLA Monitor defices a connectivity to a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address and tacks the availability of an operativity of a monitored address address in a monitored address in a mon	Overview Analysis Policie	es Devices Objects AMP Intelligence					Participation Provide America Americ America America Americ America America Ame America America Ame	o v dperezve v
SLA Monitor BLA monitor defines a consectivity policy the monitored address and tracks the availability of an one P Mat P Mat Kulte P Mat Kul	Object Management Intru	sion Rules	New SLA Monitor Ob	oject		? ×		
Policy List Policy List </td <td>SLA Monitor SLA monitor defines a connectivity p</td> <td>olicy to a monitored address and tracks the availability of a rout</td> <td>Name: Description:</td> <td>Secondary_GW</td> <td></td> <td></td> <td>do not have the option to use SLA monitor via route tracking.</td> <td></td>	SLA Monitor SLA monitor defines a connectivity p	olicy 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.	
Interfer Lift Primary_GW Primar	Policy List	Name	Frequency (seconds): SLA Monitor ID*:	60 2	(1-604800)		Value Security Zone: VLAN230	
Des Perfes Lite Secure Nap	Prefix List IPv4 Prefix List	Primary_GW	Threshold (milliseconds):		(0-60000)		Monitor ID: 1 Monitor Address: 10.88.243.1	/ G m
 Security betiligence Biscurity betiligence When the stand Fields Status and Fields Status	IPv6 Prefix List Ø Route Map		Data Size (bytes):	28	(0-16384)			
Wenter k Lists and Freds Wenter Address*: Bishole Stat Monitor Stat Monitor Time Range Time Range Time Zone Time Zone Valable Zones Time Zone Valable Zones Time Zone Time Zone Valable Zones Time Zone Valable Zones Time Zone Valable Zones Valable Zones Time Zone Valable Zones Time Zone Valable Zones Valable Zones Valable Zones Time Zone Valable Zones Valable Zones Time Zone Valable Zones Valable Zones Valable Zones Time Zone Valable Zones Valable Zones Valable Zones Valable Zones Time Zone Valable Zones Valable Zones Time Zone Valable Zones Time Zone Valable Zones Time Zone Time Zone <tr< td=""><td>Security Intelligence DNS Lists and Feeds</td><td></td><td>ToS: Number of Packets:</td><td>1</td><td></td><td></td><td></td><td></td></tr<>	Security Intelligence DNS Lists and Feeds		ToS: Number of Packets:	1				
Available Zones C Available Zones C Time Ranges Time Zone Time Zone Tim	Network Lists and Feeds URL Lists and Feeds		Monitor Address*:	10.31.124.1	3			
Time Range Time Zange	Sinkhole		Available Zones C		Selected Zones/Interfaces			
WRL Stable Set Stable Set VLAN Tag VLAN Tag Adv LAN2813 Cuttificate Map Adv LAN28	Time Range		Search Search VLAN230 Search VLAN232		VLAN232	8		
Vice rag	URL Svariable Set							
Certificate Map © Cuttom Attribute © Group Palicy @ RKV1 IPsec Proposal © IREV1 Palicy @ RKV2 IPsec Proposal © IREV1 Palicy © IREV2 Palicy	AnyConnect File			Add				
© Cutom Attribute © Group Policy @ RKV1 Piec Proposal © IKEV1 Policy @ RKV2 Piec Proposal @ IKEV2 Policy	A Certificate Map							
Cancel	Custom Attribute							
Cancel Cance	KEv1 IPsec Proposal							
KRV2 Prec Proposal KV2 Prec Proposal KV2 Prec Proposal Cancel Can	IKEv1 Policy							
Save Cancel	IKEV2 IPsec Proposal						Displaying 1 - 1 of 1 rows 🔣 🤇 Page 🗓	of 1 > > C
					Save	Cancel	with system in control subjects activated	alkala

The two objects must be added to the list.

Overview Analysis Polic	es Devices Objects AMP Intelligence	🗛 Deploy System	i Help v	dperezve 🔻
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	a,	
D 🥜 PKI 🔹	Name Value			
Policy List Port Prefix List	Primary_GW Security Zone: VLAN230 Horitor ID: 1 Monitor Address: 10.88,243.	1		/ 5 m
Ibv4 Prefix List Ibv6 Prefix List Ø Route Map	Secondary_GW Security Zone: VLAN232 Mentor UD: 2 Mentor 40dress: 10.31.124.	1		/ 6 📾
Certificate Nap Certific Variable Set Certificate Nap Certifi	Artina Geno 2	1996년 02년 가 Tores K <	Page 1 o	ri>≯C
Last login on Friday, 2021-11-26 at 0	8:37:16 AM from 192.168.13.2			altala.

Step 4. Configure Static Routes with Route Track

Once the IP SLA objects are created, define a route for each Gateway and associate them to the SLAs.

These routes do not actually provide connectivity from inside to outside (all the routing is performed through PBR), instead, they are needed to track connectivity to the Gateways through SLAs.

In order to configure static routes, navigate to Devices > Device Management, edit the FTD at hand and select Static Route in the table of contents within the Routing tab.

Overview Analysis Policies D	evices Objects	AMP Intelligence					鵫 Deploy S	ystem Help v dperezve v
Device Management Device Upg	rade NAT Vi	PN • QoS Platform Settin	gs FlexConfig Certificates					
ftdvha-dperezve Cisco Firepower Threat Defense for VMware								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 OSPFv3	-							
RIP	▼ IPvo Routes							
A GP IPv4								
IPv6								
Static Route								
IGMP								
PIM Multicast Boutes								
Multicast Boundary Filter								
General Settings BGP								
507								
							Activate Windows	
							Go to System in Control Panel	to activate Windows.
Last login on Friday, 2021-11-26 at 08:37:16	AM from 192.168.13.2							-ili-ili- cisco

In the Add Static Route Configuration window, in the Interface drop down, specify the name for the interface through which the primary Gateway must be reachable.

Then select the destination network and the primary Gateway in the Gateway drop down.

Specify a metric for the route and in the Route Track drop down and select the SLA object for the primary gateway created in Step 3.

Click **OK** to add the new route.

Overview Analysis Policies Devices Objects AMP Intelligence		🧶 Deploy System Help 🛪 diperezve 🛪
Device Management Device Upgrade NAT VPN + QoS Platform Settings	FlexConfig Certificates	13
Overview Analysis Verview Objects Job Interligence Device Hanagement Device Upgrade NAT VPI QoS Platform Settings ftdvha-dperezve Ciso Firepower Threat Defense for VHware Device Routing Interfaces Inline Sets DHCP • Manage Virtual Routers Global Virtual Router Properties Virtual Router Properties Virtual Router Properties OSFF OSFF OSFF OSFF Virtual Router Sets Virtual Router Sets BGP Ibv6 Ibv6 Ibv6 Virtual Routers Ibv4 Ibv5 Static Route Virtual Routers	FlexConfig Certificates Add Static Route Configuration ? × Type: IDv4 O IPv6 Interface* VLAN230 • (Interface starting with this kon signifies it is available for route leak) Metric Available Network C Selected Network Search any-loyd Brdet, Lab, Theodore Add Gatemay, VLAN230 Add Brdet, Cab, Theodore Add	Cancel
IGNP FPM Multicast Routes Multicast Boundary Filter General Settings BGP	Browlink-local Browlink-local Browlink-stocal Betway Carlos Browlink Carcel Correction Correction Correction Carcel	Activate Windows Go to System in Control Panel to activate Windows.
		-iliili. cisco

A second static route must be configured for the backup Gateway.

Click Add Route to define a new static route.

Fill the Add Static Route Configuration with the information for the backup Gateway and ensure the metric for this route is higher than the one configured in the first route.

Device Management Device Upg	rade NAT VPN • QoS Platform Settin	gs FlexConfig Certificates				
bevice Nanagement Device Upp tdv/ha-dperezve Cisco Firepower Threat Defense for VHware Device Routing Interfaces Manage Virtual Routers Ciclual Virtual Router Properties OSPF OSPF OSPF OSPF Virtual Router Properties Virtual Router	Adde Net OPV QdS Platform Settin Inline Sets DHCP Interface Interface V IPv4 Routes any-lpv4 VLAN230 VLAN230 V IPv6 Routes Interface VLAN230 VLAN230	Add Static Route Configuration Type:	7 ×	Metric 1	You have unsaved change Tracked Primary_GW	S Save Cancel
DV4 DV5 Static Route Multicast Routing EGMP PIH Multicast Routes Multicast Routes BGP		Gateway Gateway, VAN232 IP+4-Benchmark/Tests IP+4-Holicast IP-4-Holicast IP-4-4-Holicast IP-4-4-4-Holicast IP-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4	ancel			
						•

The two routes must be added to the list.

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

Step 5. Configure PBR FlexConfig Object

Enable SLAs under the route map used for PBR and apply this route map in an interface of the FTD.

So far, route map has been only associated to the access list that defines the matching criteria. However, the last adjustments are not supported through FMC GUI so a FlexConfig object is needed.

To define the PBR FlexConfig object navigate to Objects > Object Management and select FlexConfig Object under the FlexConfig category in the table of contents.

Object Management Instruction Rules Prescript Object Impaired Rules Impaired	Overview Analysis Policie	s Devices Objects AMP Intelligence	🍕 Deploy System Help 🕶	dperezve *
Encode dotter Image: Code dotter A data Image: Code dotter Image:	Object Management Intru	ion Rules		
Mase Description V AS Path Object Cytops Configure Object Object Suite List Configure Usite List Configure Usite List Configure Object Oracys Configure Object Object Object Object Object Object Suite Advant DNS Parameter Disable Object Oracys Delable Default Inspection. Object Obj	FlexConfig Object RexConfig Object include device con	iguration commands, variables, and scripting language instructions. It is used in FlexConfig polices.	Add FlexConfig Object	
Option: Suite List Default, DNS_Configure Defau	Y AS Path	Name	Description	
I biddinguided Name Default_Inspection_Protocal_Disable Default_Inspection_Protocal_Disable Default_Inspection_Protocal_Inable I biddinguided Notests Default_Inspection_Protocal_Inable Enable Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Enable Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Enable Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Configure one outide (PD client) and one inside interface (recipient of default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection_Protocal_Inable Default_Inspection. Default_Inspection. Default_Inspection. I biddinguided Notests Default_Inspection. Default_Inspection. Default_Inspection. Default_Inspection. Default_Inspection. I biddinguide Notests Default_Inspection. Default_Inspection. Default_Inspection. Default_Inspection. I biddin Inspe	 Cipher Suite List Community List 	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNSParameter	Q 4 6 🕇
monologia Ugers PakeL Inspection_Protocol_Enable PakeL Inspection_Configure W DIS Server Croup DicPode_Fredix_Delegation_Configure Configure one outside (PD client) and one inside interface (ncipient of d c c c c c f gure no outside (PD client) and one inside interface (ncipient of d c c c c c f gure no outside (PD client) and one inside interface (ncipient of d c c c c f gure no outside (PD client) and one inside interface (ncipient of d c c c c f gure no outside (PD client) and one inside interface (ncipient of d c c c c f gure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure one outside (PD client) and one inside interface (ncipient of d c c c c f gure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters and dnsName: Image: Configure DNS with the help of TextDollets dnsParameters DNS configures auth-summary. Image: Configure DNS with the help of TextDollets dnsParameters DNS configures auth-summary. Image: Configure DNS with the help of TextDollets dnsParameters DNS configures auth-summary. Image: Configure DNS with the help of TextDollets dnsParameters DNS configures auth-summary. Image: Configure DNS with the help of TextDollets dnsParameters DNS configures auth-summary. Image: Configure DNS with th	Distinguished Name	Default_Inspection_Protocol_Disable	Disable Default Inspection.	🔁 🔍 🖯 👘
INS SErver Croup DicPode, Fredix, Delegation_Configure INS Server Croup DicPode, Fredix, Delegation_Configure INS Server Croup DicPode, Fredix, Delegation_Configure INS Server Croup DicPode, Fredix, Delegation_UnConfigure INS Server Croup DicPode, Fredix, Delegation_UnConfigure INS Server Croup DicPode, Fredix, Delegation_UnConfigure INS Server Croup DicEout INS Server Croup DicEout <td>Diject Groups</td> <td>Default_Inspection_Protocol_Enable</td> <td>Enable Default Inspection.</td> <td>B 🔍 🖯 👘</td>	Diject Groups	Default_Inspection_Protocol_Enable	Enable Default Inspection.	B 🔍 🖯 👘
Important Attributes Preck-offigure Remove configuration of one outside (PD client) and one inside interface () ,) Important Code Dis_Configure Dis_Configure Dis_Configure Important Code Dis_Configure Dis_Configure Remove configuration of one outside (PD client) and one inside interface (), , , , , , , , , , , , , , , , , ,	@ DNS Server Group	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de	E
Security Croup Tag Disconfigure Image: Security Croup Tag Dis_configure Image: Security Croup Tag Dis_con	External Attributes Dynamic Object	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (Q 4 8
Image: Configure Dis_Lun Configure Remove the DNS configures addes. Image: Configures addes. Image: Configure EppInterface_Configures Configures addes.summary. Image: Configures addes.summary. I	Security Group Tag	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName: (Q A B
Implementation EpspConfigure Configures signs, 1. Configures auto-summary, 3	4 🦫 FlexConfig	DNS_UnConfigure	Remove the DNS configurations. (B 4 6
Image: Configure Stateface Configures Stateface Parameters for eight 1: Configures Stateface Parameters for 1: Sis Configure Image: Configure Stateface Configure Image: Configure Stateface Parameters for 1: Sis Configure Image: Configure Stateface Configure Stateface Parameters for 1: Sis Configure Stateface Parameters for 1: Sis Configures Parameters Param	FlexConfig Object Text Object	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.	Q Q B
Bit retrative Egro _ Informityre Filter total Egro _ Informityre Bit Honds Egro _ Informityre	👿 Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m	D 4 6
In Sterhook Egop_Unconfigure_All In Spect_Unconfigure_All In Spect_Unconfigure_All In Spect_Unconfigure In Spect_Unconfigure In Spect_Unconfigure In S	Key Chain	Eigrp_UnConfigure	Clears eigrp configuration for an AS	G G
Implicit Ust Implicit Ust Configure Inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the soript are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an inspection for (jov 5 traffic. Used text objects in the sorie) are IP. Q. with an	Network	Eigrp_Unconfigure_All	Clears eigrp configuration.	Q 4 6
Print Unic Configure Inspect. Unic Configure Inspect. Unic Configure Inspect. In Print List ISIS_Configure ISIS_Configure In Print List ISIS_Configure Configures global parameters for IS-IS. In Print List ISIS_Interface_Configuration Interface level IS-IS parameters. In Print List Isis_Interface_Configuration Interface level IS-IS parameters.	Policy List	Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP (G 🔍 🖯
Iby-4 Prefix List ISIS_Configure Configures global parameters for IS-IS. Ibit Iby-3b Prefix List ISIS_Interface_Configuration Ibit Ibit Ibit Prode Natio Ibit Ibit Ibit Ibit Ibit Ibit	Port	Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.	Q 🔍 🖯 👘
🐚 IPv6 Prefix List ISIS_Interface_Configuration Interface level IS-IS parameters. By default configure ipv4 unless address 🐚 👊 📋	Drv4 Prefix List	ISIS_Configure	Configures global parameters for IS-IS.	D 4 B
	Brv6 Prefix List	ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless address	D A B
🗸 🐺 Security Intelligence 🛛 ISIS_Unconfigure IS-IS. 🗠 🕞 🐛 🔂 🗸	a 🥪 Security Intelligence	ISIS_Unconfigure	Unconfigures is-is.	🔁 🔍 🖯 🖕
Application of the second sec	DNS Lists and Feeds		Abial and B W 20 of 49 Yows K < Page 1 o Go to System in Control Panel to activate Windo	3 K < 5 h

Select the Add FlexConfig Object button. In the Add FlexConfig Object window assign a name and navigate to Insert > Insert Policy Object > Route Map .

Overview Analysis Policies D	Devices Objects	AMP Intelligence	🔒 Deploy System Help 🔻	dperezve v
Object Management Intrusion R	tules	Add FlexConfig Object ?>		
FlexConfig Object FlexConfig Object include device configurat	tion commands, variat	Name: PER	Add FlexConfig Object	
Individual Objects	me ault_DNS_Configure	Description:	the help of TextObjects defaultDNSParameter	D 4 8 *
DNS Server Group	ault Inspection Proto-	Opy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.		Do a B
Dynamic Object Defa	ault_Inspection_Proto	© Insett • E Deployment: Once ♥ Type: Append ♥		DA B
File List DHC	CPv6_Prefix_Delegatio	Insert Policy Object Fext Object Text Object Network	client) and one inside interface (recipient of de	D 4 6
C FlexConfig Object	CPv6_Prefix_Delegatio	Security Zones	ne outside (PD client) and one inside interface (D . 6
Carlocation	5_Configure	Standard ACL Object	p of TextObjects dnsParameters and dnsName:	D 4 6
M Interface DNS	5_UnConfigure	Route Map	tions.	G G
Key Chain Eign	p_Configure		ures next hop. 2. configures auto-summary. 3.	G & 6
Þ 🌽 PKI Eign	p_Interface_Configure		eters for eigrp. 1. Configures authentication m	D A 6
Policy List Eign	p_UnConfigure		or an AS	DA B
- De Prefix List Eign	p_Unconfigure_All			Q. 4 6
IPv4 Prefix List Insp	pect_IPv6_Configure	Variables Name Dimension Default Value Property (Type.,, Override Description	r6 traffic. Used text objects in the script are IP-	DA 6
@ Route Map Insp	pect_IPv6_UnConfigur		ipv6 traffic.	D A B
Security Intelligence DNS Lists and Feeds ISIS	5_Configure	No records to display	ers for IS-IS.	D3 4 5
Network Lists and Feeds ISIS	5_Interface_Configura		eters. By default configure ipv4 unless addres:	Da 9. 8
Sinkhole ISIS	5_Unconfigure			Q 4 6 -
Gia SLA Monitor		Save	piaying 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 192.168.13.3	2		dudo

In the Insert Route Map Variable window, assign a name for the variable and select the PBR object created in Step 2.

Click save to add the route map as part of the FlexConfig object.

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.	D 4 5
Key Chain	Eigrp_Configure Eigrp_Interface_Configure										ures next hop. 2. configures auto-summary. 3 reters for eigrp. 1. Configures authentication m	D 48
Policy List	Elgrp_UnConfigure										or an AS	D4 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	D4 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 Polici	es Devices Objects	AMP Intell	ligence							🔒 Deploy System Help 🔻	dperezve v
Object Management Intro	usion Rules	Add FlexConfig	g Object						? ×		
FlexConfig Object RexConfig Object include device co	nfiguration commands, variat	Name:	PBR.							Add FlexConfig Object	
Individual Objects Object Groups ONS Server Group	Name Default_DNS_Configure									the help of TextObjects defaultDNSParameter	6 4 8 ²
External Attributes	Default_Inspection_Proto-	Copy-pastin	g any rich text might introduce	line breaks while ge	nerating CLI. Please verify	the CLI before deploym	vent.				Da 9 0
Dynamic Object	Default_Inspection_Proto	 Insert • 	1				Deployment:	Once 👻 Type	Append ¥		0.46
File List	DHCPv6_Prefix_Delegatio	\$PBR_RouteMap	P							client) and one inside interface (recipient of de	Ca 4 6
FlexConfig FlexConfig Object	DHCPv6_Prefix_Delegatio									ne outside (PD client) and one inside interface (Da 4 6
Ca Text Object	DNS_Configure									p of TextObjects dnsParameters and dnsName:	D 4 6
Geolocation	DNS_UnConfigure									tions.	D 4 0
P Key Chain	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3.	Da 9. 8
Network PKI	Eigrp_Interface_Configure									eters for eigrp. 1. Configures authentication m	D 4 0
Policy List	Eigrp_UnConfigure									or an AS	D 4 8
A De Prefix List	Eigrp_Unconfigure_All										Da 9. 6
IPv4 Prefix List	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Property (Type	Override	Description	۲	r6 traffic. Used text objects in the script are IP	D 4 6
② Route Map	Inspect_IPv6_UnConfigur	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false		_	ipv6 traffic.	DA B
 Security Intelligence DNS Lists and Feeds 	ISIS_Configure									ers for IS-IS.	D 4 8
Network Lists and Feeds	ISIS_Interface_Configura									eters. By default configure ipv4 unless address	D 4 8
Sinkhole	ISIS_Unconfigure									The second second	D4 6 -
G SLA Monitor								- C	A	iplaying 1 - 20 of 49 rows K < Page 1	OK < E to
								Save	cancel		alada

Besides the route map variable, we must add the FlexConfig text objects that represent each Gateway (defined in Step 3). In the Add FlexConfig Object window navigate to Insert > Insert Policy Object > Text Object .

Overview Analysis P	Policies Devices Object	AMP Intel	ligence							🗛 Deploy System Help 🕯	r dperezve v
Object Management	Intrusion Rules	Add FlexConfi	g Object						? ×		
FlexConfig Object FlexConfig Object include devi	ice configuration commands, varia	Name: Description:	PBR							Add FlexConfig Object	
AAA Server RADIUS Server Grou Single Sign-on Server Access List	P Default_DNS_Configure Default_Inspection_Proto	🛆 Copy-pasti	ng any rich text	might introduce line breaks whil	le generating CLI. Please ve	ify the CLI before deploym	sent.			the help of TextObjects defaultDNSParamete	Q .5
Extended	Default_Inspection_Proto	 Insert • 					Deployr	ment: Everytime • Type: (Append 👻		048
Address Pools	DHCPv6_Prefix_Delegation	Insert Poli	tem Variable	Text Object						client) and one inside interface (recipient of d	- La 4 6
IPv4 Pools	DHCPv6_Prefix_Delegation	O Insert Sec	ret Key	Security Zones						e outside (PD client) and one inside interface	(D Q B
Application Filters	DNS_Configure			Standard ACL Object						p of TextObjects dnsParameters and dnsName	D 46
Dipher Suite List	DNS_UnConfigure			Route Map						tions.	Da 4, 6
Community List	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3	D A B
Individual Objects	Eigrp_Interface_Configur									eters for eigrp. 1. Configures authentication n	n 🖪 🔍 🗇
DNS Server Group	Eigrp_UnConfigure									or an AS	DA B
External Attributes	Eigrp_Unconfigure_All										D 4 6
Security Group Tag	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Property (Type	Override	Description	۲	/6 traffic. Used text objects in the script are IP	D A B
File List Ge FlexConfig	Inspect_IPv6_UnConfigur	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false		_	ipv6 traffic.	D A B
Se FlexConfig Object	ISIS_Configure									ws for 15-15.	D 4 6
Ca Text Object	ISIS_Interface_Configura									eters. By default configure ipv4 unless addres	H D 4 8
G Interface	ISIS_Unconfigure										Q Q 8 -
Key Chain	•							Save	Cancel G	playing 1 - 20 of 49 rows IC < Page 1	of 3 > > C
Last Issia on Saturday, 2021-11	1-27 at 11:06:56 AM from 102 169 1	3.3									alah

In the Insert Text Object Variable window assign a name for the variable and select the text object that represents the primary Gateway defined in Step 3.

Click save button in order to add it to the FlexConfig object.

Overview Analysis Polici	es Devices Objects	AMP Intel	ligence		<u> </u>					🔒 Deploy System Help 🔻	dperezve v
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			Insert Text Ob	iect Variable			7 ×		1 the help of TextObjects defaultDNSParameter	B4 6 1
Access List Extended Standard	Default_Inspection_Proto Default_Inspection_Proto	Copy-pastir	g any rich text	Variable Name: Description:	Primary_GW			YB	me 🕶 Type: Append 💌		
Address Pools	DHCPv6_Prefix_Delegatio									client) and one inside interface (recipient of de	D3 4 8
IPv6 Pools	DHCPv6_Prefix_Delegatio			Available Objects	c		Selected Object			te outside (PD client) and one inside interface	D 4 8
Application Filters	DNS_Configure			🔍 primar		×	Primary_GW	8		Ip of TextObjects dnsParameters and dnsName	D 4 6
Cipher Suite List	DNS_UnConfigure			Primary_GW						tions.	DA 6
Community List	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3.	DA B
Individual Objects	Eigrp_Interface_Configure									eters for eigrp. 1. Configures authentication m	DA B
Object Groups Object Group	Eigrp_UnConfigure									or an AS	D 4 6
External Attributes	Eigrp_Unconfigure_All										D 4 6
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	ion	ipv6 traffic.	DA 6
Gerenter FlexConfig Object	ISIS_Configure					No records to a	lisplay			irs for IS-IS.	D4 8
Ca Text Object	ISIS_Interface_Configura									ieters. By default configure ipv4 unless address	D 4 5
S Interface	ISIS_Unconfigure										Da 9. 6 -
Notwork									A Carat	splaying 1 - 20 of 49 rows K < Page 1	OK < Elo
Last login on Saturday, 2021-11-27 al	t 11:06:56 AM from 192.168.13	.2							Save		altala

Repeat these last steps for backup Gateway. At the end of the process, the two variables must be appended to the FlexConfig object.

Overview Analysis Polici	ies Devices Object	s AMP Intel	ligence							🐥 Deploy System Help 🔻	dperezve v
Object Management Intro	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									the help of TextObjects defaultDNSParameter	DA 8 ⁺
Access List	Default_Inspection_Proto	🔬 Copy-pastir	g any rich text might intro	duce line breaks while (generating CLI. Please veri	ify the CLI before deploym	ent.				Q 4 6
Standard	Default_Inspection_Proto	 Insert • 					Deploym	ent: Everytime 🖌 Type: Appe	end 👻		D A 6
Address Pools	DHCPv6_Prefix_Delegatio	SPBR_RouteMa SPrimary GW	p							dient) and one inside interface (recipient of de	Q 4 8
IPv6 Pools	DHCPv6_Prefix_Delegation	\$Secondary_GW	t.							e outside (PD client) and one inside interface (D 4 6
Application Filters	DNS_Configure									p of TextObjects dnsParameters and dnsName	045
Cipher Suite List	DNS_UnConfigure									tions.	B 4 6
Community List	Elgrp_Configure									ures next hop. 2. configures auto-summary. 3.	D 4 8
Individual Objects	Eigrp_Interface_Configur									eters for eigrp. 1. Configures authentication m	D 4 5
Object Groups Object Group	Elgrp_UnConfigure									or an AS	0.40
External Attributes	Eigrp_Unconfigure_All										0.46
Security Group Tag	Inspect_IPv6_Configure	Variables							۲	6 traffic. Used text objects in the script are IP	046
Tile List	Inspect_IPv6_UnConfigur	Name		Dimension	Default Value	Property (Type	Override	Description	_	ipv6 traffic.	0.9.6
FlexConfig Performer	ISIS Configure	Primary_GW		SINGLE	10.88.243.1	FREEFORM:Prim	false			ers for 15-15.	
C Text Object	Lots_compare	Secondary_GW		SINGLE	10.31.124.1	PREEFORM:Seco	false				40 40
Geolocation	ISIS_Interface_Configura	Per_Routeriap		STROFF	PBK_Routeriap	ROUTERWP:PBR	19126			ieters. By default configure ipv4 unless addres:	048
S Interface	ISIS_Unconfigure										Q 4 8 -
The Key Chain								Save	Action Ac	playing 1 - 20 of 49 rows 🔣 🗧 Page 1	of 3 > > C
Last login on Saturday, 2021-11-27 al	t 11:06:56 AM from 192.168.1	3.2									alaha

The syntax for the PBR configuration must be the same as in Cisco ASA. The sequence number for the route map must match the one configured in Step 2 (10 in this case) as well as the SLA IDs.

To configure PBR to check availability for the next hop, the set ip next-hop verify-availability command must be used.

Route map must be applied to the inside interface, in this case VLAN2813. Use **policy-route route-map** command under the interface configuration.

Click save when configuration is completed.



The FlexConfig object must be added to the list.



Step 6. Assign PBR FlexConfig Object to FlexConfig Policy

Navigate to Devices > FlexConfig and edit the FlexConfig policy at hand.

Select the PBR FlexConfig object in Available FlexConfig table of contents, save changes, and deploy changes to FTD.

Overview Analysis Policies Devices Objects Device Management Device Upgrade NAT VPN	AMP Ir	Platform Settings Fle	xConfig Certificates			%	Deploy System	Help 🔻 d	perezve v
ftdvha-dperezve						You have unsaved changes	Preview Config	🗄 Save	🙁 Cancel
Enter Description							3	Policy Assign	nments (1)
Available FlexConfig C S FlexConfig Object	T Selo	cted Prepend FlexConfi	Is						
×		Name			Description				
GUiser Defined Paper Paper Paper Pare Orbault_Dists_Configure Orbault_Inspection_Protocol_Enable Orbault_Inspection_Protocol_Enable Orbault_Inspection_Configure OHCPv6_Prefix_Delegation_Configure OHCPv6_Configure									
DNS_UnConfigure	Selo	cted Append FlexConfig	•						
Eigrp_Configure	<i>a.</i>	Name			Description				_
Eigrp_UnConfigure	1.	PBR							9.0
Eigrp_Unconfigure_All inspect_INV6_Configure inspect_INV6_UnConfigure insts_Lonconfigure insts_treatexe_Configuration insts_Unconfigure insts_Unconfigure_All Netflow_Add_Destination				Selected Append ResConfigs		Activate Win	clowe		
						Go to System in (Control Panel to activ		15.
Last Joan on Sahurday, 2021-11-27 at 11-06-56 JM from 102 168 13 2	,								սիսիւ

Verify

After the deployment finishes, FTD must send regular ICMP echo request to the monitored devices in order to ensure reachability. In the meantime, a tracked route to the primary Gateway must be added to the routing table.

Because connectivity to primary Gateway is up, traffic from internal subnet (VLAN2813) must be forwarded through the primary ISP circuit.

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

If the FTD does not receive an echo reply from primary Gateway within the threshold timer specified in the SLA Monitor object, the host is considered unreachable and marked as down. Tracked route to primary Gateway is also replaced by tracked route to backup peer.

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, 0 - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF Gateway of last resort is 10.31.124.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [2/0] via 10.31.124.1, VLAN232 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25 255.255.255.255 is directly connected, VLAN232 C 192.168.13.0 255.255.255.0 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813

route from routing table.

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 Now, all the traffic from VLAN2813 must be forwarded through the backup ISP circuit.

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

In order to validate which PBR entry is enforced in interesting traffic, run command **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