Konfiguration von PBR mit IP SLAs für DUAL ISP auf FTD, verwaltet von FMC

Inhalt

Einleitung **Anforderungen** Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm Konfigurationen Schritt 1: PBR-Zugriffsliste konfigurieren Schritt 2: Konfigurieren der PBR-Routenzuordnung Schritt 3: FlexConfig-Textobjekte konfigurieren Schritt 4: SLA-Monitor konfigurieren Schritt 4: Konfigurieren statischer Routen mit Route Track Schritt 5: PBR-FlexConfig-Objekt konfigurieren Schritt 6: Zuweisung eines PBR-FlexConfig-Objekts zur FlexConfig-Richtlinie Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie PBR zusammen mit IP SLAs auf einem FTD konfiguriert wird, das von (FMC) verwaltet wird.

Beitrag von Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- PBR-Konfiguration auf Cisco Adaptive Security Appliance (ASA)
- FlexConfig auf Firepower
- IP SLAs

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

Cisco FTD Version 7.0.0 (Build 94)

• Cisco FMC Version 7.0.0 (Build 94)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In diesem Dokument wird die Konfiguration Policy Based Routing (PBR) zusammen mit Internet Protocol Service Level Agreement (IP SLA) zu Cisco Firepower Threat Defense (FTD) verwaltet vom Cisco FirePOWER Management Center (FMC).

Beim herkömmlichen Routing werden Weiterleitungsentscheidungen nur auf Basis der Ziel-IP-Adressen getroffen. PBR ist eine Alternative zu Routing-Protokollen und statischem Routing.

Sie bietet eine detailliertere Kontrolle über das Routing, da sie die Verwendung von Parametern wie Quell-IP-Adressen oder Quell- und Ziel-Ports als Routing-Kriterien neben der Ziel-IP-Adresse ermöglicht.

Mögliche PBR-Szenarien umfassen Anwendungen, die auf die Quelle reagieren, oder Datenverkehr über dedizierte Verbindungen.

Zusammen mit PBR können IP SLAs implementiert werden, um die Verfügbarkeit des nächsten Hop sicherzustellen. Ein IP SLA ist ein Mechanismus, der eine End-to-End-Verbindung durch den Austausch regulärer Pakete überwacht.

Zum Zeitpunkt der Veröffentlichung wird PBR nicht direkt durch FMC unterstützt. Graphical User Interface (GUI) gesetzt ist, erfordert die Konfiguration der Funktion die Verwendung von FlexConfig-Richtlinien.

Auf der anderen Seite Internet Control Message Protocol (ICMP) SLAs werden von FTD unterstützt.

In diesem Beispiel wird PBR verwendet, um Pakete über eine primäre Internet Service Provider (ISP) auf Basis der IP-Quelladresse.

In der Zwischenzeit überwacht ein IP SLA die Konnektivität und erzwingt bei einem Ausfall ein Fallback zu einem Backup-Schaltkreis.

Konfigurieren

Netzwerkdiagramm

In diesem Beispiel hat Cisco FTD zwei externe Schnittstellen: VLAN230 und VLAN232. Jede Verbindung wird mit einem anderen ISP hergestellt.

Der Datenverkehr vom internen Netzwerk VLAN2813 wird über den primären ISP geroutet, der PBR verwendet.

Die PBR-Routenübersicht trifft Weiterleitungsentscheidungen ausschließlich auf Basis der Quell-IP-Adresse (alles, was von VLAN2813 empfangen wird, muss in VLAN230 zu 10.88.243.1 geroutet werden). Sie wird in der Schnittstelle GigabitEthernet 0/1 von FTD angewendet. In der Zwischenzeit verwendet FTD IP SLAs, um die Verbindungen zu den einzelnen ISP-Gateways zu überwachen. Bei einem Ausfall von VLAN230 erfolgt ein FTD-Failover zum Backup-Schaltkreis des VLAN232.



Konfigurationen

Schritt 1: PBR-Zugriffsliste konfigurieren

Legen Sie im ersten Schritt der PBR-Konfiguration fest, welche Pakete der Routing-Richtlinie unterliegen sollen. PBR nutzt Routing-Karten und Zugriffslisten, um Datenverkehr zu identifizieren.

Um eine Zugriffsliste für die Zuordnungskriterien zu definieren, navigieren Sie zu Objects > Object Management und wählen Extended unter dem Access List Kategorie im Inhaltsverzeichnis.



Klicken Sie auf Add Extended Access List . Im New Extended Access List Object ein, weisen Sie einen Namen für das Objekt zu, und wählen Sie dann Add um mit der Konfiguration der Zugriffsliste zu beginnen.

Overview Analysis Policies	Devices Obje	cts AM	• Intelligence				🧛 Deploy 🤮	System Help 🔻	dperezve 🔻
Object Management Intrusion	Rules								
Extended An access list object, also known as an ac You use these objects when configuring pi	cess control list (AC) articular features, su	L), selects the	traffic to which a service will app	ly. Standard-Identifies traffic base	d on destination address only. Iden	tifies traffic based on source and d	Add Extended Access	s List 🔍 Filter ts. Supports IPv4 an	d IPv6 addressi
A CAA Server	me					Value		Override	
RADIUS Server Group	New Extended	Access Li	st Object				? ×		
Single Sign-on Server	Name Entries (0)	PBR_ACL					Add		
Address Pools	Sequence	Action	Source	Source Port	Destination	Destination Port			
Pv4 Pools Pv6 Pools Pv6 Pools Page Pool				No records to	display				
Individual Objects	Allow Overrides								
 Object Groups ONS Server Group External Attributes Dynamic Object Security Group Tag 						Save	Cancel		
File List									
A Sp FlexConfig							No data to display	_ I< < Page 1	lof1 > > (
Last login on Thursday, 2021-11-25 at 20:3	5:07 PM from 192.168	3.13.2					Go to System in Contr	ol Panel to activate 1	Vindow cisco

Im Add Extended Access List Entry das Objekt aus, das das interne Netzwerk darstellt, in diesem Fall VLAN2813.

Klicken Sie auf Add to Source um sie als Quelle der Zugriffsliste zu definieren.

Klicken Sie auf Add um den Eintrag zu erstellen.

Overview Analysis Policies De	objects	AMP Intelligence							Help 🔻 🏼 di	perezve 🔻
Object Management Intrusion Rules										
Extended	Add Extended A	Access List Entry					? ×	ccess List	🔍 Filter	^
An access list object, also known as an acce You use these objects when configuring par	Action:	🖋 Allow	~					d ports. Suppo	rts IPv4 and I	Pv6 address(
AAA Server	Logging:	Default	¥						Override	
Single Sign-on Server	Log Level:	Informational	~							
Access List	Log Interval:		Sec.							
Standard	Network Per									
Address Pools	Available Networks	c	0	Source Networks (1)		Destination Networks (0)				
IPv4 Pools	Search by nam	ne or value		VLAN2813	8	any				
Application Filters			*							
Y AS Path	IPv4-Private-	All-RFC1918								
Cipher Suite List	IPv6-1PV4-Ma	ippeo	Add to Source							
Community List	IPv6-Private-	Unique Local-Addresses								
Individual Objects	IPv6-to-IPv4-	-Relay-Anycast	Destination							
Object Groups	PBR_Host									
DNS Server Group	VLAN230									
External Attributes	VLAN232									
Dynamic Object	VLAN2813			Enter an ID address	Add	Enter an ID address	Add			
Security Group Tag				Line all iP address	AUU		AUU			
File List						Add	Cancel			
4 Gy FlexConfig							No data to	display K K	Page 1	of 1 > > (*
0							Go to System i	in Control Panel t	to activate Win	dows
Last login on Thursday, 2021-11-25 at 20:35:0										diniti

Klicken Sie auf save. Das Objekt muss der Objektliste hinzugefügt werden.



Schritt 2: Konfigurieren der PBR-Routenzuordnung

Weisen Sie die PBR-Zugriffsliste nach der Konfiguration einer Routenübersicht zu. Die Routenzuordnung wertet den Datenverkehr anhand der Übereinstimmungsklauseln aus, die in der Zugriffsliste definiert sind.

Nach einer Übereinstimmung werden die in der Routing-Richtlinie definierten Aktionen von der Routing-Zuordnung ausgeführt.

Navigieren Sie zum Definieren der Routenübersicht zu Objects > Object Management und wählen Route Map im Inhaltsverzeichnis aufgeführt.



Klicken Sie auf Add Route Map > Im New Route Map Object einen Namen für das Objekt zuweisen, und klicken Sie dann auf Add um einen neuen Routenplaneintrag zu erstellen.

Overview Analysis Policies Devices Objects AM	1P 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 th	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 JP PKI J Policy List	Common No.	Dedict-likelike	Add	
and Port	sequence no =	Reustribution		
Im Prefix List IPv4 Prefix List		No records to display		
IPv6 Prefix List				
// Route Map				
DNS Lists and Feeds				
Vetwork Lists and Feeds	Allow Querrides			
Sinkhole	Allow Overrides			
Gan SLA Monitor		Save	Cancel	
Time Range				
Time Zone				
Tunnel Zone				
A HAR 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

Im Add Route Map Entry eine Folgenummer für die Position des neuen Eintrags definieren.

Navigieren Sie zu IPv4 > Match Clauses und "Erweitert" im Available Access List Dropdown-Menü.

Wählen Sie das in Schritt 1 erstellte Zugriffslistenobjekt aus.

Klicken Sie auf Add um den Eintrag zu erstellen.

Hinweis: FTD unterstützt bis zu 65536 (von 0 bis 65535) verschiedene Einträge. Je niedriger die Anzahl, desto höher die Priorität.

Overview Analysis Policies Devices Object	Add Route Map Entry				? ×		🐥 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules							
	Sequence No: 10						Canton and the Char
Route Map	Redistribution: 🖌 Alle	w *					Add Route Plap
Route maps are used when redistributing routes into any rout	Match Clauses Set Cl	auses				protocol are allowed to I	be redistributed into the target routing process.
Mama	Security Zones	Address (2) Next Hop (0) Route Sour	ce (0)			Value	Quarrida
Geolocation	IPv4					Talac	or critic
G Interface	IPv6	Select addresses to match as access list or pre	fix list addresses of	route.			
They Chain	BGP						
Network	Others	Access List O Prefix List					
Þ 🔑 PKI	Solitina .	Available Access Lists :					
Policy List		Extended					
JP Port							
4 Lip Prefix List		Available Extended Access List C		Selected Extended Access List			
IPv4 Prefix List		Search		BR_ACL	8		
IPv6 Prefix List		R PRP ACI					
@ Route Map		a record					
A Security Intelligence							
DNS Lists and Feeds							
Network Lists and Feeds							
URL Lists and Feeds			Add				
Sinkhole							
SLA Pionitor							
Cartine runge							
Time Zone							
ec rome zone							
C Andable Cat							
S Variable Set							
P NON							
M AnyConnect File					Cancel		
8. Certificate Map				DDA	Cancel		No data to deviav 16 6 Page 1 of 1 > 31 0
							No data to display int it indige 1 of 1 / / G
							alaha

Klicken Sie auf save. Fügen Sie das Objekt der Objektliste hinzu.



Schritt 3: FlexConfig-Textobjekte konfigurieren

Im nächsten Schritt werden FlexConfig-Textobjekte definiert, die Standard-Gateways für die einzelnen Leitungen darstellen. Diese Textobjekte werden später in der Konfiguration des FlexConfig-Objekts verwendet, das PBR mit SLAs verknüpft.

Zum Definieren eines FlexConfig-Textobjekts navigieren Sie zu Objects > Object Management und wählen Text Object unter dem FlexConfig Kategorie im Inhaltsverzeichnis.

Overview Analysis Polici	es Devices Objects AMP Intelligence		🧛 Deploy Sys	tem Help 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	🔍 Filter	
Y AS Path	Name	Value	Туре	Override	
Cipher Suite List	defaultDNSNameServerList	1.1.1.1	System Defined	0	2 B -
Distinguished Name Individual Objects Object Groups DNS Server Group Z External Attributes	defaultDNSParameters	3 5 10 15 abc.com There are 1 more items.	System Defined	0	• 8
Dynamic Object	disableInspectProtocolList		System Defined	0	/8
Group Tag	dnsNameServerList	2.2.2.2	System Defined	0	18
Gy FlexConfig Gy FlexConfig Object Gy Text Object	dnsParameters	3 5 abc.com	System Defined	•	/ 8
👿 Geolocation 🍓 Interface	elgrpAS	1	System Defined	0	08
Ney Chain	eigrpAuthKey		System Defined	0	/ 8
Network P PKI	eigrpAuthKeyId		System Defined	0	18
Policy List	elgrpDisableAutoSummary	false	System Defined	0	18
A 🛐 Prefix List	eigrpDisableSplitHorizon	false	System Defined	0	08
IPv4 Prefix List	eigrpHellotnterval	60	System Defined	0	18
Ø Route Map	eigrpHoldTime	180	System Defined	0	28
Security Intelligence DNS Lists and Feeds		Asija Go to	ining Wild drag fows K System in Control Panel to	< Page 1	of 3 > > C
Last login on Thursday, 2021-11-25 at	20:35:07 PM from 192:168.13.2				-11-11-

Klicken Sie auf Add Text Object . Im Add Text Object einen Namen für das Objekt zuweisen, das das primäre Gateway darstellt, und die IPv4-Adresse für dieses Gerät angeben.

Klicken Sie auf save um das neue Objekt hinzuzufügen.

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 Restantial 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

Klicken Sie auf Add Text Object um ein zweites Objekt zu erstellen, diesmal für das Gateway auf der Sicherungsschaltung.

Füllen Sie das neue Objekt mit dem entsprechenden Namen und der entsprechenden IP-Adresse aus, und klicken Sie auf save.

Overview Analysis Polici Object Management Intro	es Devices Objects AMP Intelligent	e		93 Dep	oy System Help	v dperezve v
Text Object Text objects define free-form text st	trings that you use as variables in a FlexConfig object. Tl	ese objects can have single values or be a list of multiple values.		Add Tex	t Object	
Y AS Path	Name		Value	Туре	Override	
Cipher Suite List	defaultDNSNameServerList		1.1.1.1	System Defined	0	18 1
Distinguished Name Individual Objects Object Groups DNS Server Group	defaultDNSParameters	Add Text Object Name: Secondary_GW	? ? X	System Defined	o	18
Dynamic Object	disableInspectProtocolList	Description:		System Defined	0	18
Security Group Tag	dnsNameServerList			System Defined	0	08
Gy FlexConfig Gy FlexConfig Object Gy Text Object	dnsParameters	Variable Type Single v Count 1	0	System Defined	0	18
Geolocation	elgrpAS			System Defined	0	08
Key Chain	eigrpAuthKey	1 10.31.124.1		System Defined	0	18
Network	eigrpAuthKeyId	Allow Overhoes		System Defined	0	08
Policy List	eigrpDisableAutoSummary		Save Cancel	System Defined	0	18
Port	eigrpDisableSplitHorizon		false	System Defined	0	08
IPv4 Prefix List	eigrpHelloInterval		60	System Defined	0	18
Route Map	eigrpHoldTime		180	System Defined	0	08
Security Intelligence DNS Lists and Feeds Network Lists and Feeds	eigrpIntfList			System Defined Displaying 1 - 20 of 44 r	ows K < Page 1	/
Last login on Friday, 2021-11-26 at 0	8:37:16 AM from 192.168.13.2					-1 1-1 1- cisco

Die beiden Objekte müssen der Liste zusammen mit den Standardobjekten hinzugefügt werden.



Schritt 4: SLA-Monitor konfigurieren

Um die SLA-Objekte zu definieren, die zum Überwachen der Verbindungen zu den einzelnen Gateways verwendet werden, navigieren Sie zu Objects > Object Management und wählen SLA Monitor im Inhaltsverzeichnis aufgeführt.



Wählen Sie Add SLA Monitor - Objekt.

Im New SLA Monitor einen Namen zusammen mit einer Kennung für den SLA-Vorgang, die IP-Adresse für das zu überwachende Gerät (in diesem Fall das primäre Gateway) und die Schnittstelle oder Zone, über die das Gerät erreichbar ist, definieren.

Zusätzlich ist es auch möglich, das Timeout und den Schwellenwert anzupassen. Klicken Sie auf Save .

Hinweis: FTD unterstützt bis zu 2000 SLA-Vorgänge. Die Werte für die SLA-ID liegen zwischen 1 und 2147483647.

Hinweis: Wenn keine Timeout- und Schwellenwerte angegeben werden, verwendet FTD Standard-Timer: jeweils 5000 Millisekunden.

Overview Analysis Policies Devices Objects AMP Intelligence				👫 Deploy System Help 🔻 dperezve 🔻
Object Management Intrusion Rules	New SLA Monitor Ob	ject	? ×	
SLA Monitor SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rout	Name: Description:	Primary_GW]	Add SLA Monitor
Name Name Name Name Name Name Name Name	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) (0-60000) (0-604800000) (0-16384)	Value
UIL Lists and Freds Sidolo Lists A Honitor Linne Range Time Zone Time Zone Time Zone UIL Variable Set VLAN Tag AnyConnect File Conflictate Man Conflictate Man Conf	Available Zones C Search Sa VLAN230 ch VLAN232 ch VLAN2813		Selected Zones/Interfaces	
B IKEV2 Policy			Sauge Cancel	No data to display 🔣 🤇 Page 1 🗌 of 1 🗦 💥 🕻
Last login on Friday, 2021-11-26 at 08:37:16 AH from 192.168.13.2			Jave Canter	ajtajta 61500

Wählen Sie Add SLA Monitor - Taste erneut ein, um ein zweites Objekt zu erstellen, diesmal für das Gateway auf der Backup-Schaltung.

Füllen Sie das neue Objekt mit den entsprechenden Informationen aus, stellen Sie sicher, dass sich die SLA-ID von der für das primäre Gateway definierten ID unterscheidet, und speichern Sie die Änderungen.

Overview Analysis Policie	es Devices Objects AMP Intelligence					🅀 Deploy System Help 🕶	dperezve +
Object Management Intru	usion Rules	New SLA Monitor Ob	ject		? ×		
SLA Monitor SLA monitor defines a connectivity p	policy to a monitored address and tracks the availability of a rout	Name: Description:	Secondary_GW			do not have the option to use SLA monitor via route tracking.	
PKI S Policy List	Name	Frequency (seconds):	60	(1-604800)		Value	
Port	Primary_GW	SLA Monitor ID*:	2]		Security Zone: VLAN230 Monitor ID: 1	/ 6 m
Prefix List Prefix List		Threshold (milliseconds):		(0-60000)		Monitor Address: 10.88.243.1	
B IPv6 Prefix List		Data Size (hytes):	5000	(0-16384)			
Route Map Security Intelligence		ToS:					
DNS Lists and Feeds		Number of Packets:	1				
Network Lists and Feeds		Monitor Address*:	10.31.124.1	1			
URL Lists and Feeds Sinkhole		Available Tener 🕐		Enlasted Tenne Returbane			
Gia SLA Monitor		Search		A VLAN232			
Time Range		A VLAN230					
Tunnel Zone		Julan232					
O URL		1 VLAN2813					
S Variable Set			Add				
- D VPN							
AnyConnect File							
Custom Attribute							
Group Policy							
KEV1 IPsec Proposal							
REv2 IPsec Proposal						Activities and a strength of the second s	
R IKEv2 Policy				Save Cance		Craptaying 1 - 1 of 1 rows IK K Page [1] o	1 7 7 6
Last login on Friday, 2021-11-26 at 08	8:37:16 AM from 192.168.13.2						alulu

Die beiden Objekte müssen der Liste hinzugefügt werden.

Overview Analysis Polic	es Devices Objects AMP Intelligence	鵫 Deploy System	Help 🔻	dperezve +
Object Management Intr	sion Rules			
SLA Monitor SLA monitor defines a connectivity	policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via	Add SLA Monitor	9,	
PKI Realizy List	Name Value			
Port	Security Zone: VLA/230 Primary_GW Primary_GW 10.82 Honitor 10:1 Honitor Address: 10.88.243.1			/ 5 m
Iby IPv4 Prefix List Iby6 Prefix List If Route Map	Secondary_GW Secon			/ 6 📾
Security Intelligence Dis Lists and Feeds Interview Lists and Feeds URL Lists and Feeds URL Lists and Feeds URL Lists and Feeds URL Stand Feeds Time Range Time Rang				
IKEv2 IPsec Proposal IKEv2 Policy	Actively of the system	Minglorg Fows K < r	Page 1 o	f1>> €
Last login on Friday, 2021-11-26 at 0	c:37:16 AM from 192.168.13.2			-duala-

Schritt 4: Konfigurieren statischer Routen mit Route Track

Nachdem die IP SLA-Objekte erstellt wurden, definieren Sie eine Route für jedes Gateway, und ordnen Sie sie den SLAs zu.

Diese Routen bieten keine internen und externen Verbindungen (das gesamte Routing wird über PBR durchgeführt), sondern sind erforderlich, um die Verbindungen zu den Gateways über SLAs nachzuverfolgen.

Um statische Routen zu konfigurieren, navigieren Sie zu Devices > Device Management, die vorliegende FTD bearbeiten und Static Route im Inhaltsverzeichnis des Routing aus.

Overview Analysis Policies D	evices Objects	AMP Intelligence					🔒 Deploy Sy	stem Help v dperezve v
Device Management Device Upg	rade NAT VP	PN QoS Platform Setting	s FlexConfig Certificates					
ftdvha-dperezve Cisco Firepower Threat Defense for VMware								Save Cancel
Device Routing Interfaces	Inline Sets D	HCP						
Manage Virtual Routers								Add Route
Global	Network +	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
OSPF OSPF/3								
RIP	▼ IPv6 Routes							
a 💋 BGP								
IPv6								
Static Route								
IGMP								
PIM								
Multicast Routes Multicast Boundary Filter								
General Settings								
BGP								
							Activate Windows Go to System in Control Panel t	o activate Windows.
Last login on Friday, 2021-11-26 at 08:37:16	AM from 192.168.13.2							ultulu cisco

Im Add Static Route Configuration geben Sie im Dropdown-Menü Interface (Schnittstelle) den Namen der Schnittstelle an, über die das primäre Gateway erreichbar sein muss.

Wählen Sie dann das Zielnetzwerk und das primäre Gateway im Gateway Dropdown-Liste.

Geben Sie eine Metrik für die Route und in der Route Track das SLA-Objekt für das in Schritt 3 erstellte primäre Gateway aus.

Klicken Sie auf OK, um die neue Route hinzuzufügen.

Overview Analysis Policies Devices Object	cts AMP Intelligence		♣ Deploy System Help ▼ dperezve ▼
ftdvha-dperezve	VPN QoS Platform Settings	FlexConfig Certificates	Save Save
Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets	DHCP	Add Static Route Configuration ? ×	
Manage Virtual Routers		Type: Prie O Prie Interface" VLAN220 V	Add Route
Cicbal Vittual Router Properties OSFF OSFFV RIP OSFFV RIP OSFV RIP OSP RIP RIP RIP RIP RIP RIP RIP RIP RIP RI	Interface	(Interface starting with this Ico 🔹 signifies it is available for roote leak) Metric Available Network Image: Search Image: Search <	Tracked
Last login on Friday, 2021-11-26 at 08:37:16 AM from 192.168.13.	1.2		-ili-ili- cisco

Für das Backup-Gateway muss eine zweite statische Route konfiguriert werden.

Klicken Sie auf Add Route um eine neue statische Route zu definieren.

Füllen Sie das Add Static Route Configuration mit den Informationen für das Backup-Gateway, und stellen Sie sicher, dass die Kennzahl für diese Route höher ist als die für die erste Route konfigurierte.

Device Management Device Upg	rade NAT VPN •	QoS Platform Settings	FlexConfig	Certificates						
ftdvha-dperezve Cisco Firepower Threat Defense for VMware			Add Static	Route Configuration	on		? ×		You have unsaved chang	save 🔀 Cancel
Device Routing Interfaces	Inline Sets DHCP		Type:	● IPv4 O IPv	6					
Manage Virtual Routers			Interface*	VLAN232		*				🔾 Add Route 🔒
Global	Network +	Interface		(Interface starting	with this icon 👩 sig	nifies it is available for rou	te leak)	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes		Available	Network C	0	Selected Network				
OSPF	any-ipv4	VLAN230	Search	5		any-ipv4	6	1	Primary_GW	/ 8
OSPFV3 RIP	▼ IPv6 Routes		any-ip	w4 v						
# 🤪 BGP IPv4			FMC_L	ab_Theodore						
IPv6			Gatew	ay_VLAN230						
Static Route			IPv4-E	Benchmark-Tests						
IGMP			IPv4-L	ink-Local						
PIM			IPv4-1	fulticast						
Multicast Routes			IPv4-P	mvate-10.0.0.0-8	•					
manutable boundary rices			Gateway*	Gateway_VLAN23	2	- O				
General Settings			Metric:	2		(1 - 254)				
BGP			Tunneled:	(Used only for d	lefault Route)					
			Route Tracking	2: Secondary_GW		~ 0				
						OK	Cancel			

Die beiden Routen müssen der Liste hinzugefügt werden.

Overview Analysis Policies D	evices Objects AMP	Intelligence					🦺 Deploy System Help	v dperezve v
Device Management Device Upg	rade NAT VPN v Qo	5 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								
PIM Multiszet Poutes								
Multicast Boundary Filter								
General Settings								
BGP								
								-
						Activate	Windows	
						Go to Syste	em in Control Panel to activate V	Vindows.
Last login on Friday, 2021-11-26 at 16:34:30	PM from 192.168.13.2							շվերիչ

Schritt 5: PBR-FlexConfig-Objekt konfigurieren

Aktivieren Sie SLAs unter der für PBR verwendeten Routenübersicht, und wenden Sie diese Routenübersicht in einer Schnittstelle des FTD an.

Bisher wurde die Route Map nur der Zugriffsliste zugeordnet, in der die Zuordnungskriterien definiert sind. Die letzten Anpassungen werden jedoch nicht über die FMC-GUI unterstützt, sodass ein FlexConfig-Objekt erforderlich ist.

Navigieren Sie zum PBR-FlexConfig-Objekt Objects > Object Management und wählen FlexConfig Object unter dem FlexConfig Kategorie im Inhaltsverzeichnis.

Overview Analysis Polici	es Devices Objects AMP Intelligence	💁 Deploy System Help 🔻	dperezve *
Object Management Intr	sion Rules		
FlexConfig Object RexConfig Object include device co	figuration 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	Da 4 6 📍
Distinguished Name	Default_Inspection_Protocol_Disable	Disable Default Inspection.	🔁 🔍 🖯 👘
Object Groups	Default_Inspection_Protocol_Enable	Enable Default Inspection.	B 🔍 🗗
@ DNS Server Group	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de	Da 🔍 🖯 👘
External Attributes Dynamic Object	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (D 4 8
Security Group Tag	DKS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName	G G G
Generation	DNS_UnConfigure	Remove the DNS configurations.	6 4 8
G Text Object	Elgrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.	D 4 8
Geolocation	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m	B 4 6
Key Chain	Eigrp_UnConfigure	Clears eigrp configuration for an AS	Q 4 6
Retwork	Elgrp_Unconfigure_All	Clears eigrp configuration.	🕒 🔍 🖯 👘
PKI Bolicy List	Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP-	D A B
Port	Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.	D A B
IPv4 Prefix List	1515_Configure	Configures global parameters for IS-IS.	D 4 8
IPv6 Prefix List IRv6 Map	ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless address	Da 🔍 🖯
4 💞 Security Intelligence	1515_Unconfigure	Unconfigures is-is.	Q Q 0 -
DNS Lists and Feeds		Abisblaving Wildows K < Page 1 Go to System in Control Panel to activate Windo	5 K < εh
Last login on Friday, 2021-11-26 at 1	1:34:30 PM from 192.168.13.2		aludo

Wählen Sie Add FlexConfig Object - Taste. Im Add FlexConfig Object einen Namen zuzuweisen und zu navigieren, Insert > Insert Policy Object > Route Map.

Overview Analysis Polici	es Devices Object	AMP Intelligence	👫 Deploy System Help 🔻 dperezve 🔻
Object Management Intru	sion Rules	Add FlexConfig Object ? ×	
FlexConfig Object FlexConfig Object include device con	ifiguration commands, varial	Name: PER	Add FlexConfig Object
Individual Objects Object Groups DNS Server Group	Name Default_DNS_Configure Default_Inspection_Proto	Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.	the help of TextObjects defaultDNSParameter
External Attributes Dynamic Object	Default Inspection Proto	Deployment: Once v Type: Append v	
Security Group Tag	DHCPv6_Prefix_Delegatio	Insert Falley Object Text Object Text Object Network	client) and one inside interface (recipient of de 🗋 🛶 📋
G FlexConfig Object	DHCPv6_Prefix_Delegatio	Insert Serret Key Security Zones Standard AC, Object Consolid AC, Object	e outside (PD client) and one inside interface (👘 👊 🕤 in the second se
Geolocation	DNS_UnConfigure	Route Map	tions. D 🔍 🖯
Key Chain	Eigrp_Configure		ures next hop. 2. configures auto-summary. 3. 👔 🔩 📋
Þ 🌽 PKI	Eigrp_Interface_Configure		eters for eigrp. 1. Configures authentication m
Policy List	Eigrp_UnConfigure		or an AS
🖌 📴 Prefix List	Eigrp_Unconfigure_All		D 4 5
IPv4 Prefix List	Inspect_IPv6_Configure	Variables Name Dimension Default Value Property (Type Override Description	r6 traffic. Used text objects in the script are IP 🛛 🔯 🏐
⑦ Route Map	Inspect_IPv6_UnConfigur	нине оплатия основ спорату (треш отентов основного	ipvő traffic. 🔯 🔍 🖯
Security Intelligence DNS Lists and Feeds	ISIS_Configure	No records to display	ers for IS-IS.
Network Lists and Feeds	ISIS_Interface_Configura		veters.By default configure ipv4 unless address 👔 🔍 🍵
Sinkhole	ISIS_Unconfigure		D 4 3 -
Gia SLA Monitor		Save Cancel	□ playing 1 - 20 of 49 rows K < Page 1 of 3 > > C
Last login on Saturday, 2021-11-27 at	09:15:30 AM from 192.168.1		alight

Im Insert Route Map Variable einen Namen für die Variable zuweisen und das in Schritt 2 erstellte PBR-Objekt auswählen.

Klicken Sie auf save um die Routenübersicht als Teil des FlexConfig-Objekts hinzuzufügen.

Overview Analysis Policie	es Devices Objects	AMP Intel	ligence								P3 Deploy System Help	• dperezve •
Object Management Intru	ision Rules	Add FlexConfig	g Object							? ×		
FlexConfig Object FlexConfig Object include device con	ifiguration 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-pastin	g 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_Prefix_Delegatio DHCPv6_Prefix_Delegatio			Available Objects	c		Selected Object				client) and one inside interface (recipient of o	
Ca Text Object	DNS_Configure DNS_UnConfigure			Search	0		Ø PBR_RouteMap	8			Ip of TextObjects dnsParameters and dnsNam tions.	• D • 6
Key Chain Network Poper List	Eigrp_Configure Eigrp_Interface_Configure										ures next hop. 2. configures auto-summary.	
Port Prefix List Prefix List	Elgrp_UnConfigure	Variables									for an AS	
B IPv6 Prefix List Route Map	Inspect_IPv6_Configure Inspect_IPv6_UnConfigur	Name					Save	Cancel	ption		/6 traffic. Used text objects in the script are I ipv6 traffic.	D4 6
 Security Intelligence DNS Lists and Feeds Network Lists and Feeds 	ISIS_Configure ISIS_Interface_Configura										ers for IS-IS. reters. By default configure jov4 unless addre	
URL Lists and Feeds	ISIS_Unconfigure										splaying 1 - 20 of 49 rows 🔣 🐇 Page 1	ра б. оз у с
Last login on Saturday, 2021-11-27 at	: 09:15:30 AM from 192.168.13.	2							Save	Cancel	Management Constant Same to according we	altalu

Overview Analysis Policies	s Devices Objects	AMP Intell	igence							🔒 Deploy System Help 🔻	dperezve v
Object Management Intrus	ion Rules	Add FlexConfig) Object						? ×		
FlexConfig Object RexConfig Object include device confi	iguration commands, variat	Name:	PBR							Add FlexConfig Object	
Individual Objects	Name Default_DNS_Configure	Conv-nastin	a any rich test might introdu	e line breaks while or	nerating CLL Please verify	the CLI before deploym	sent.			the help of TextObjects defaultDNSParameter	B 4 6 ⁺
External Attributes Dynamic Object Security Group Tag	Default_Inspection_Proto	O Insert •					Deployme	nt: Once 👻 Type: [Append 👻		
Tile List	DHCPv6_Prefix_Delegatio	\$PBR_RouteMag	2							client) and one inside interface (recipient of de	Di 9. 6
Gy FlexConfig Gy FlexConfig Object	DHCPv6_Prefix_Delegatio									e outside (PD client) and one inside interface (Da 4, 6
Ca Text Object	DNS_Configure									ip of TextObjects dnsParameters and dnsName:	0.46
Geolocation	DNS_UnConfigure									tions.	D 4 6
Key Chain	Eigrp_Configure									ures next hop. 2. configures auto-summary. 3.	D 4 8
PKI	Eigrp_Interface_Configure									eters for eigrp. 1. Configures authentication m	D 4 6
Policy List	Eigrp_UnConfigure									or an AS	D A B
4 🗓 Prefix List	Eigrp_Unconfigure_All										D 4 6
IPv6 Prefix List	Inspect_IPv6_Configure	Variables		Dimension	Default Value	Property (Type	Override	Description		/6 traffic. Used text objects in the script are IP	D A B
Ø Route Map	Inspect_IPv6_UnConfigur	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false			ipv6 traffic.	G G G
Security Intelligence DNS Lists and Feeds	1515_Configure									ers for 15-15.	D 4 8
Network Lists and Feeds	ISIS_Interface_Configura									eters. By default configure ipv4 unless address	Q 4 6
Sinkhole	ISIS_Unconfigure								A.	Seate Mindows	D4 6 .
Gia SLA Monitor								Save	Cancel GD	iplaying 1 - 20 of 49 rows K < Page 1	of 3 > X C
Last losis as Cabuchy 2021-11-22 at 0	0.15.20 AM from 102 168 12								Control		ahaha

Neben der Routing-Map-Variablen müssen die FlexConfig-Textobjekte hinzugefügt werden, die die einzelnen Gateways darstellen (wie in Schritt 3 definiert). Im Add FlexConfig Object Fenster navigieren Insert > Insert Policy Object > Text Object .

Overview Analysis Poli	cies Devices Objects	s AMP Intellig	ence							Participation Provides A statement of the statement of	dperezve +
Object Management Int	trusion Rules	Add FlexConfig (Object						? ×		
FlexConfig Object RexConfig Object include device of	configuration commands, variat	Name: F	BR							Add FlexCorfig Object	
RADIUS Server Group Single Sign-on Server	Default_DNS_Configure Default_Inspection_Proto	Copy-pasting a	ny rich text might introduce	line breaks while g	enerating CLI. Please veri	y the CLI before deploym	ent.			the help of TextObjects defaultDNSParameter	
Address Pools	Default_Inspection_Proto	 Insert Policy C Insert System 	bject Text Object Variable Network				Deproymen	nc <u>Everyome v</u> type:	Append ¥	client) and one inside interface (recipient of de	
As Path	DHCPv6_Prefix_Delegatio	Insert Secret I	Security Z Standard / Extended	ones ACL Object ACL Object						te outside (PD client) and one inside interface (p of TextObjects dnsParameters and dnsName tions	640
Community List	Eigrp_Configure		Route Map							ures next hop. 2. configures auto-summary. 3 eters for eiorp. 1. Configures authentication m	D4 5
Object Groups Object Group DNS Server Group Z External Attributes	Elgrp_UnConfigure Elgrp_Unconfigure_All									or an AS	048
Dynamic Object Security Group Tag File List	Inspect_IPv6_Configure Inspect_IPv6_UnConfigur	Variables Name		Dimension	Default Value	Property (Type	Override	Description	۲	r6 traffic. Used text objects in the script are IP	048
GexConfig GexConfig Object GexConfig Object	ISIS_Configure	Per_Routemap		SINGLE	PER_Routemap	ROUTEMAPOPER	raise			ers for 15-15.	DQ B
Geolocation Interface Key Chain	ISIS_Unconfigure								Δ.	Capaving 1 - 20 of 49 rows K < Page 1	
Maharak								Save	Cancel G		alulu

Im Insert Text Object Variable einen Namen für die Variable zuweisen und das Textobjekt auswählen, das das in Schritt 3 definierte primäre Gateway darstellt.

Klicken Sie auf save um sie dem FlexConfig-Objekt hinzuzufügen.

Overview Analysis Polici	es Devices Objects	AMP Intelli	igence							Page 1 - Page 1 - Page 1 - Page 2 -		dperezve +
Object Management Intro	usion Rules	Add FlexConfig) Object						1	? ×		
FlexConfig Object FlexConfig Object include device co	nfiguration commands, varial	Name: Description:	PBR							Add FlexConfig Object	Rilter	
AAA Server	Name											
Single Sign-on Server	Default_DNS_Configure			Insert Text Ob	ect Variable			? ×		the help of TextObjects defaultD	SParameter	b 4 6 *
Access List	Default_Inspection_Proto	🔬 Copy-pasting	g any rich text	Usrishia Namar	Driver City							B B B
Extended Standard	Default_Inspection_Proto	O Insert •		Description:	Primary_GW	_		v	ime 🕶 Type: Append			0.4.6
Address Pools	DHCPv6_Prefix_Delegatio									client) and one inside interface (re	cipient of de	B 4 6
IPv6 Pools	DHCPv6_Prefix_Delegatio			Available Objects	c		Selected Object			ve outside (PD client) and one insi	de interface (6.0
Application Filters	DNS_Configure			🔍 primar		×	Primary_GW	8		lp of TextObjects dnsParameters a	nd dnsName:	346
Dipher Suite List	DNS_UnConfigure			Primary_GW						tions.		646
Community List	Eigrp_Configure									ures next hop. 2. configures auto-	summary. 3.	6.00
Individual Objects	Eigrp_Interface_Configure									eters for eigrp. 1. Configures auth	entication m	045
Object Groups Object Group	Eigrp_UnConfigure									'or an AS		348
External Attributes	Elgrp_Unconfigure_All											6.0
Security Group Tag	Inspect_IPv6_Configure	Variables							lan	/6 traffic. Used text objects in the	script are IP	6.00
File List	Inspect_IPv6_UnConfigur	reame					Save	Cancel	aon	ipv6 traffic.		3 46
Generating FlexConfig Object	ISIS_Configure					No records to a	lisplay			ars for 15-15.		0.46
Geolocation	ISIS_Interface_Configura									ieters. By default configure ipv4 u	nless addres:	346
Interface	ISIS_Unconfigure											b 4 6 -
Key Chain										splaying 1 - 20 of 49 rows K <	Page 1 of	2 K < E
Last login on Saturday, 2021-11-27 a	t 11:06:56 AM from 192.168.13	.2							Save Cancel			alah

Wiederholen Sie die letzten Schritte für das Backup-Gateway. Am Ende des Prozesses müssen die beiden Variablen an das FlexConfig-Objekt angehängt werden.

Overview Analysis Polici	ies Devices Object	s AMP Intel	ligence						P3 Deploy System Help •	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								the help of TextObjects defaultDNSParamete	D A S ^
Access List	Default_Inspection_Proto	Copy-pastir	ig any rich text might	introduce line breaks while	generating CLI. Please ver	ify the CLI before deploym	ent. Deploym	ent: Everytime 🛩 Type: Append	-	D 46 D 46
Address Pools IPv4 Pools IPv6 Pools	DHCPv6_Prefix_Delegatio	SPBR_RouteMa SPrimary_GW SSecondary_GW	p C						client) and one inside interface (recipient of d	048 048
Application Filters	DNS_Configure								lp of TextObjects dnsParameters and dnsName	098
Copher Suite List	Elgrp_Configure								tions. ures next hop. 2. configures auto-summary. 3	1040 1040
Individual Objects	Eigrp_Interface_Configur								eters for eigrp. 1. Configures authentication n	D 4 6
Dbject Groups	Eigrp_UnConfigure								ior an AS	D 4 8
Dynamic Object	Eigrp_Unconfigure_All									
Security Group Tag	Inspect_IPv6_Configure	Variables		Dimension	Default Malue	Property (Truce	Output	Deceleties	.6 traffic. Used text objects in the script are IF	D A B
File List	Inspect_IPv6_UnConfigur	Primary GW		SINGLE	10.99.243.1	EPEEEOPM-Prim	Overnide	Description	ipv6 traffic.	DA B
FlexConfig FlexConfig Object	ISIS_Configure	Secondary GW		SINGLE	10.31.124.1	FREEFORM:Seco	false		ers for IS-IS.	Do G. G
Ga Text Object	ISIS_Interface_Configura	PBR_RouteMap		SINGLE	PBR_RouteMap	ROUTEMAP:PBR	false		eters. By default configure ipv4 unless addres	DA B
Interface	ISIS_Unconfigure									Q. 4. 6 -
Key Chain								Save Cance	AC playing 1 - 20 of 49 rows K < Page 1] of 3 > X C
Last login on Saturday, 2021-11-27 a		3.2								- dualte

Die Syntax für die PBR-Konfiguration muss mit der Syntax in Cisco ASA übereinstimmen. Die Sequenznummer für die Routenzuordnung muss mit der in Schritt 2 (in diesem Fall mit Schritt 10) konfigurierten Nummer sowie den SLA-IDs übereinstimmen.

Um die PBR-Funktion so zu konfigurieren, dass die Verfügbarkeit für den nächsten Hop geprüft wird, set ip next-hop verify-availability muss verwendet werden.

Die Routenzuordnung muss auf die interne Schnittstelle angewendet werden, in diesem Fall VLAN2813. Nutzung policy-route route-map unter der Schnittstellenkonfiguration ein.

Klicken Sie auf save wenn die Konfiguration abgeschlossen ist.



Das FlexConfig-Objekt muss der Liste hinzugefügt werden.



Schritt 6: Zuweisung eines PBR-FlexConfig-Objekts zur FlexConfig-Richtlinie

Navigieren Sie zu Devices > FlexConfig und die vorliegende FlexConfig-Richtlinie bearbeiten.

Wählen Sie das PBR-FlexConfig-Objekt in Available FlexConfig Inhaltsverzeichnis zu erstellen, Änderungen zu speichern und Änderungen in FTD bereitzustellen.

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							5	Policy Assign	nments (1)
Available FlexConfig C StexConfig Object	T Selo	cted Prepend FlexConfi	Is						
×		Name			Description				
GUiser Defined Paper Paper Paper System Defined Ordault_Dists_Configure Ordault_Inspection_Protocol_Enable Ordault_Inspection_Protocol_Enable Ordault_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_Linterface_Configure insts_Unconfigure 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

Überprüfung

Nach Abschluss der Bereitstellung muss FTD eine regelmäßige ICMP-Echoanfrage an die überwachten Geräte senden, um die Erreichbarkeit sicherzustellen. In der Zwischenzeit muss eine verfolgte Route zum primären Gateway der Routing-Tabelle hinzugefügt werden.

Da die Verbindung zum primären Gateway aktiv ist, muss der Datenverkehr vom internen Subnetz (VLAN2813) über den primären ISP-Schaltkreis weitergeleitet werden.

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

Wenn der FTD innerhalb des im SLA Monitor-Objekt angegebenen Timer-Schwellenwerts keine Echoantwort vom primären Gateway empfängt, gilt der Host als nicht erreichbar und wird als inaktiv markiert. Die verfolgte Route zum primären Gateway wird auch durch die verfolgte Route zum Backup-Peer ersetzt.

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 is directly connected, VLAN231 L 192.168.13.1 255.255.255 is directly connected, VLAN2813

Die Informationsmeldung 622001 wird jedes Mal generiert, wenn FTD eine verfolgte Route der Routing-Tabelle hinzufügt oder daraus entfernt.

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 Nun muss der gesamte Datenverkehr von VLAN2813 über den Backup-ISP-Schaltkreis weitergeleitet werden.

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, nsq_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

Fehlerbehebung

Um zu überprüfen, welcher PBR-Eintrag in interesting traffic, Befehl debug policy-route ausführen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.