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

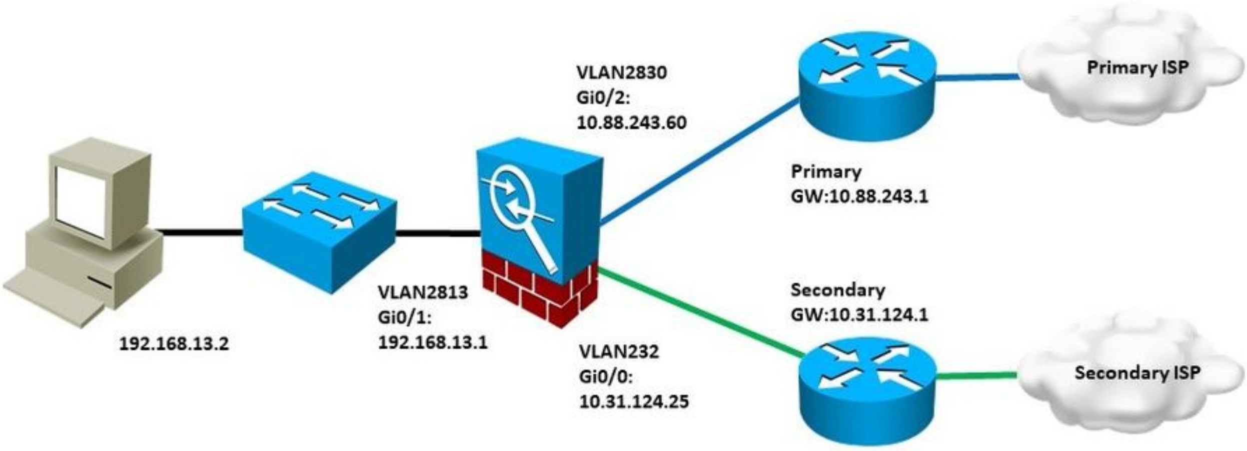
Netzwerkdiagramm

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.

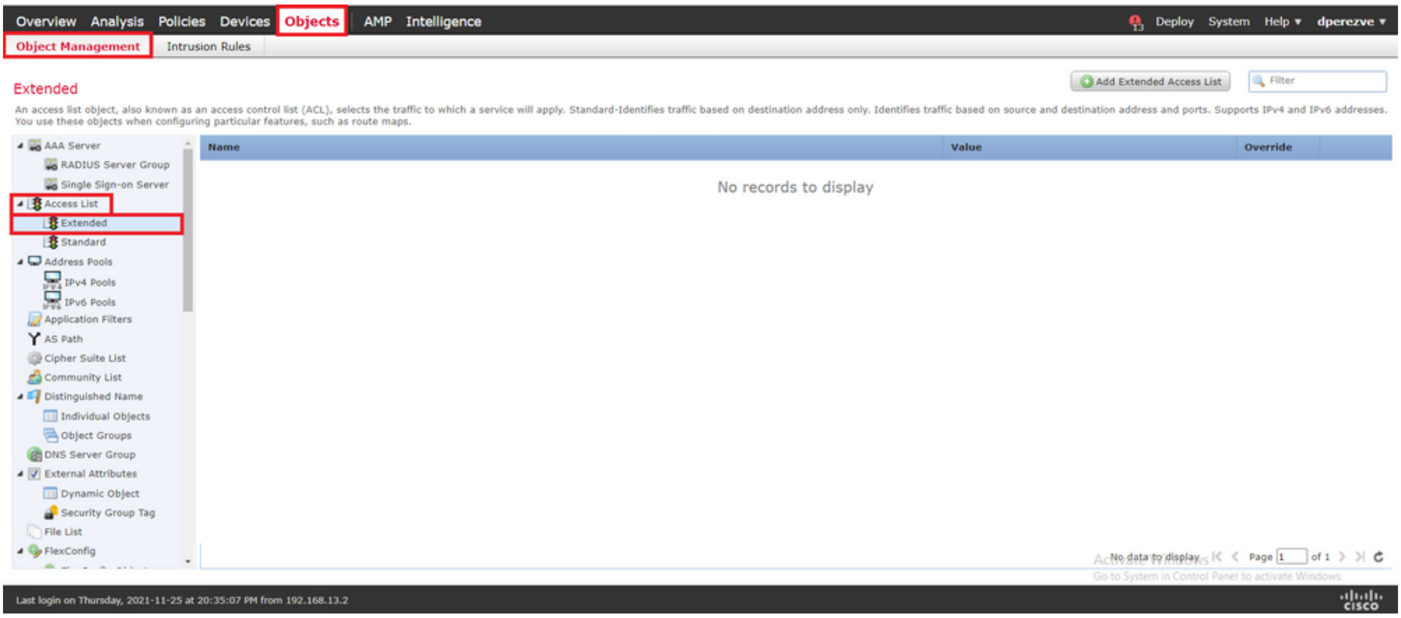


Konfigurationen

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.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

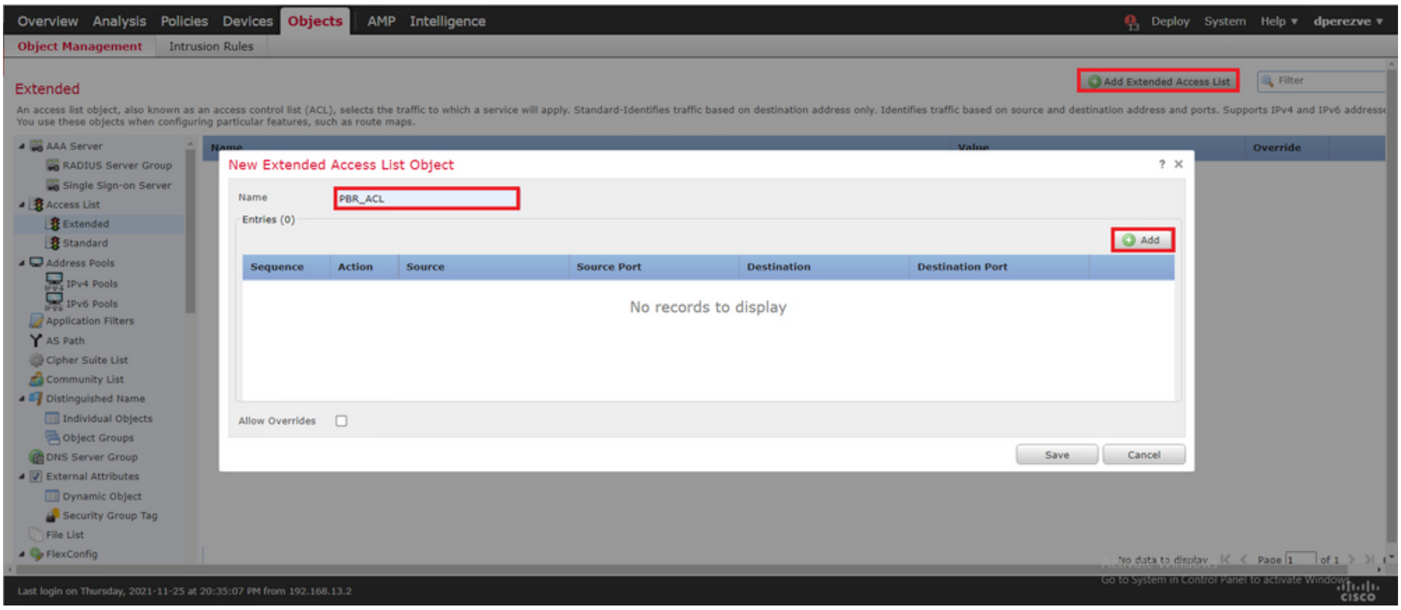
Name	Value	Override

No records to display

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

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

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.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

New Extended Access List Object

Name: PBR_ACL

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port

No records to display

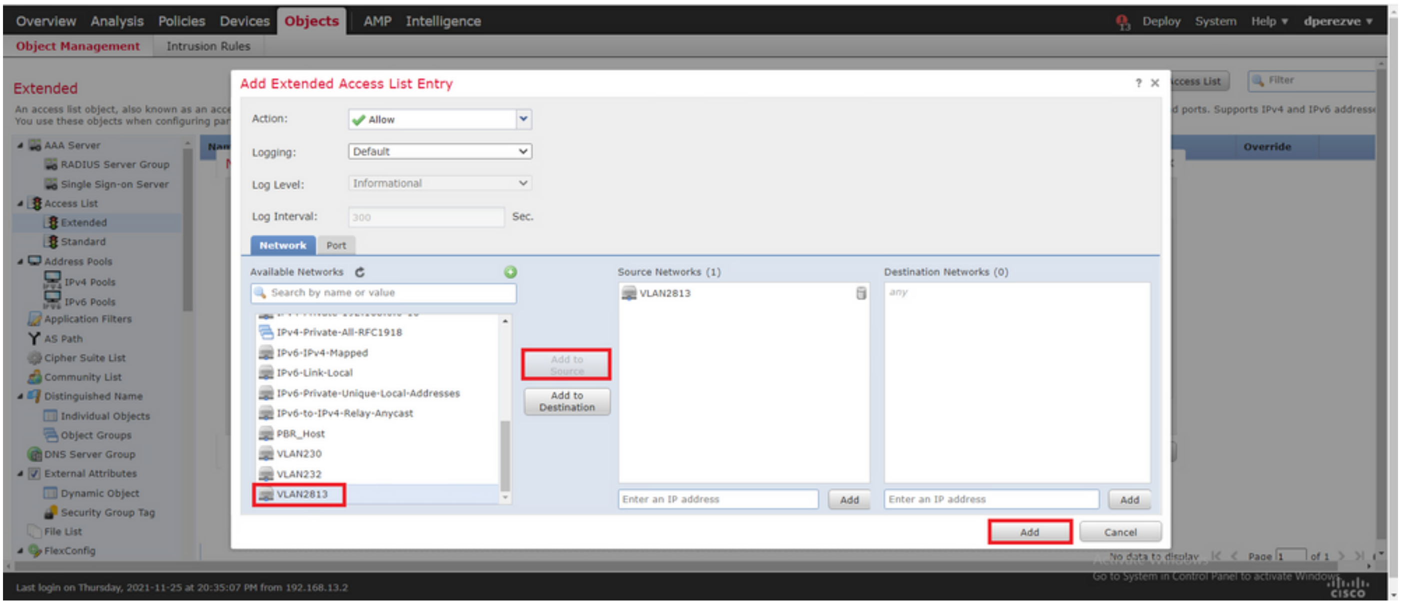
Allow Overrides ☐

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

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.



Add Extended Access List Entry

Action: ✓ Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Available Networks

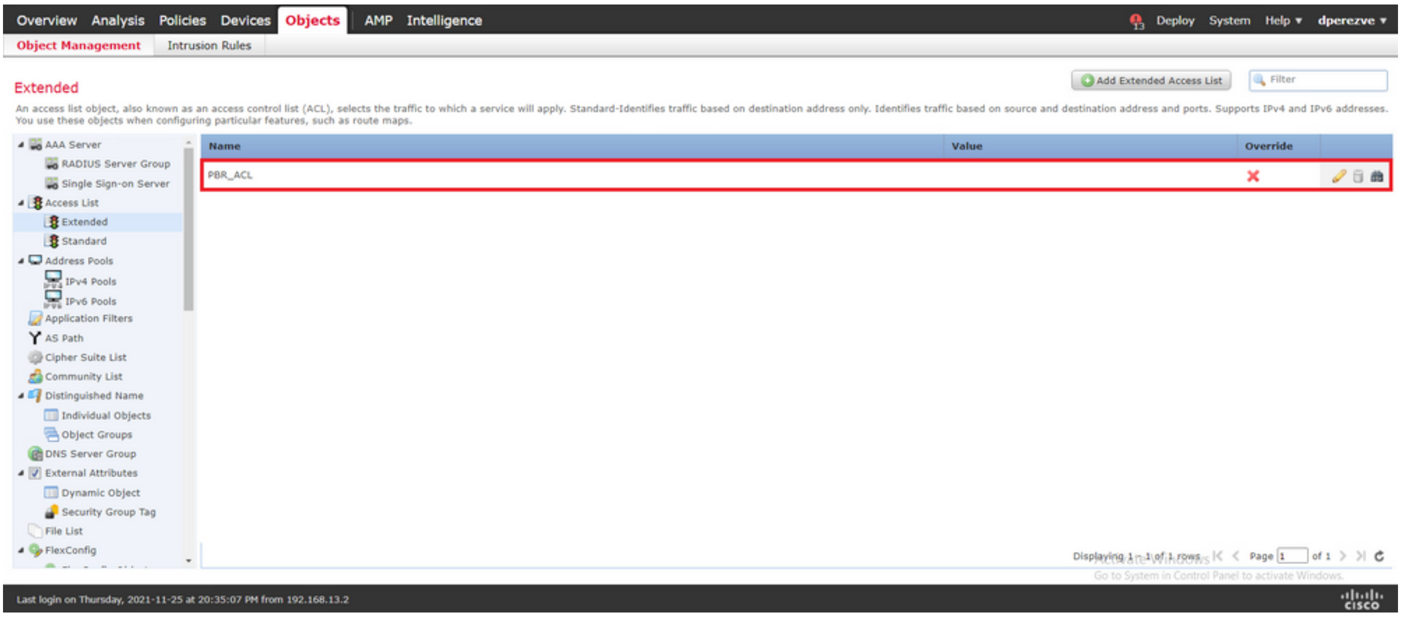
- IPv4-Private-All-RFC1918
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- PBR_Host
- VLAN230
- VLAN232
- VLAN2813

Source Networks (1): VLAN2813

Destination Networks (0): any

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

Klicken Sie auf **Save** . Das Objekt muss der Objektliste hinzugefügt werden.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
PBR_ACL		✗

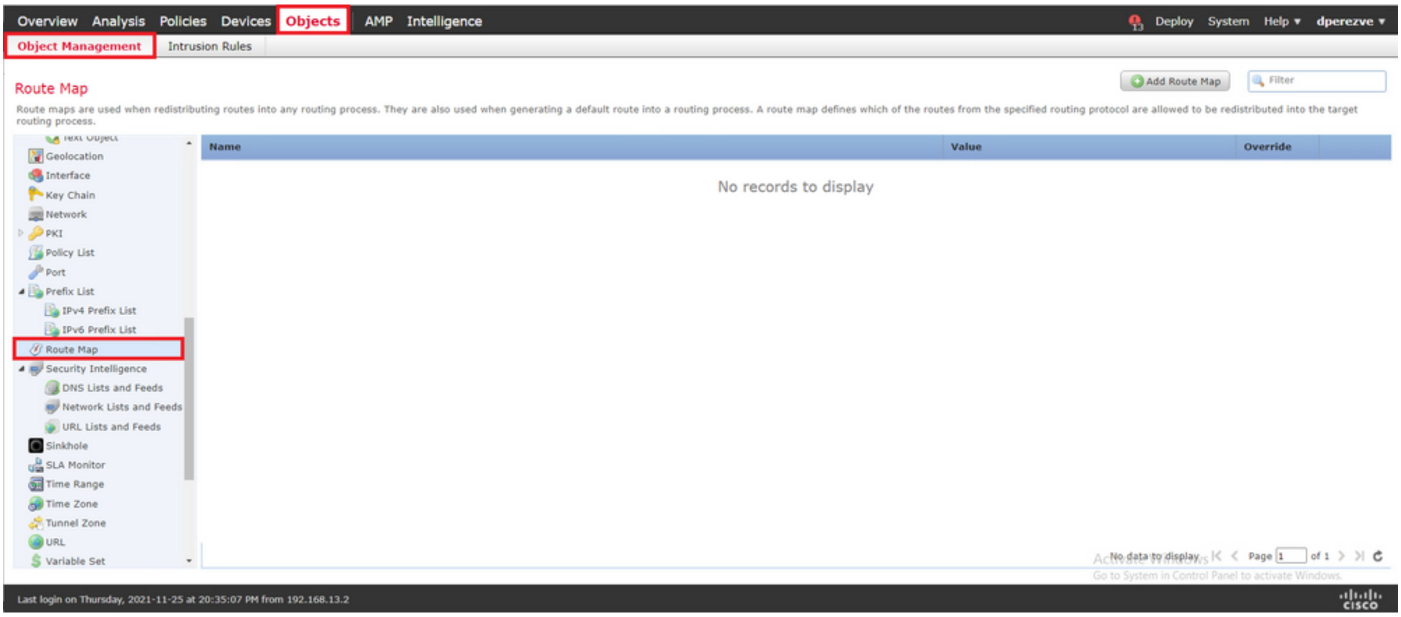
Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

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.



Route Map

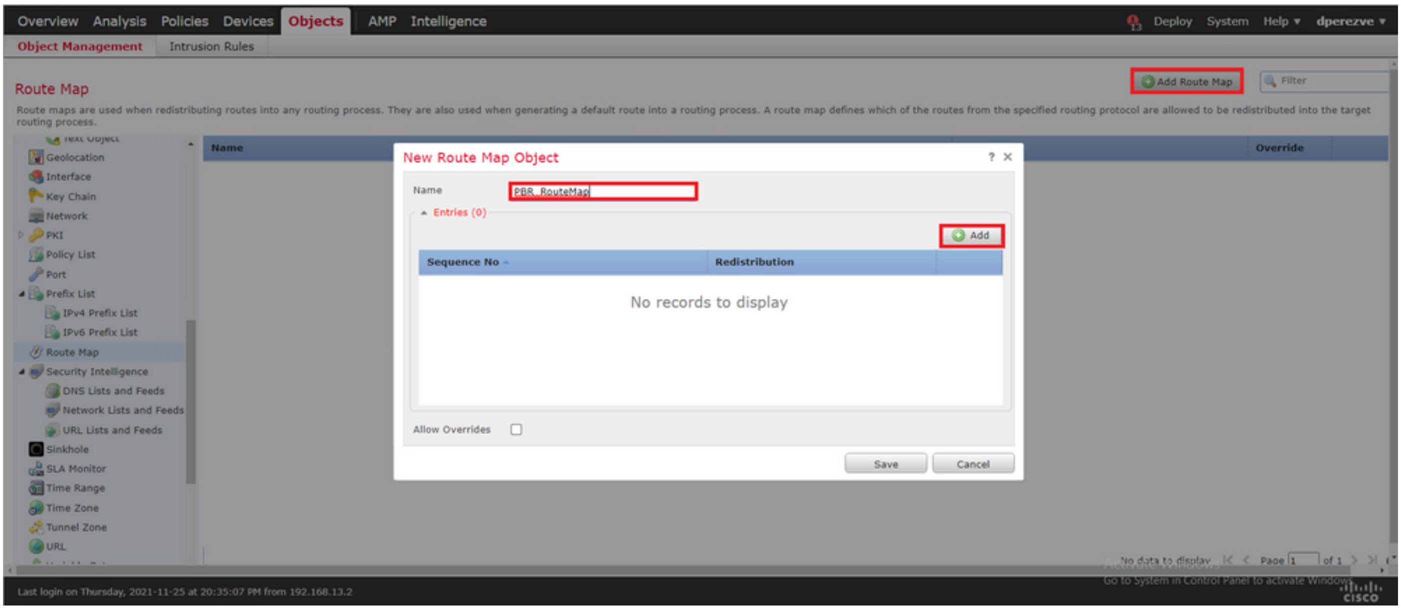
Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Name	Value	Override

No records to display

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

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 AMP Intelligence
Deploy System Help dperezve
Object Management Intrusion Rules
Add Route Map
Filter
Override
Add
Sequence No
Redistribution
Save
Cancel

Route Map

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

New Route Map Object

Name: PBR_RouteMap

Entries (0)

No records to display

Allow Overrides ☐

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

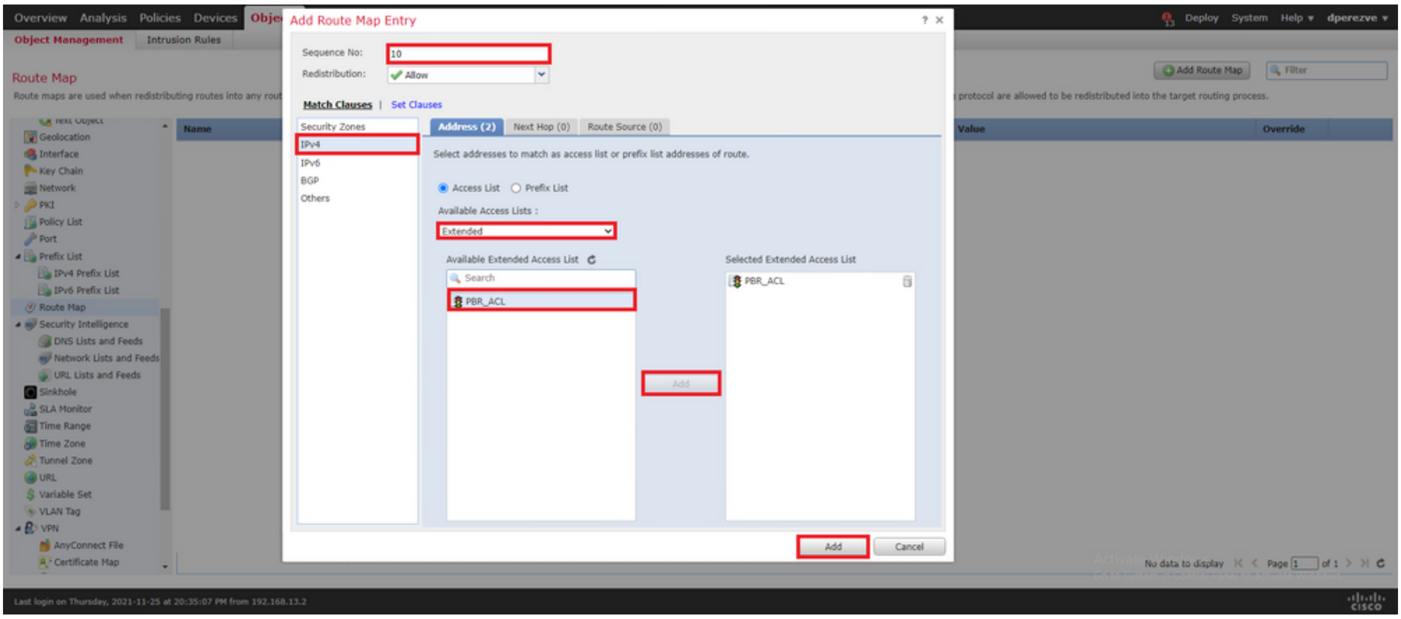
Im **Add Route Map Entry** eine Folgenummer für die Position des neuen Eintrags definieren.

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 Objects
Deploy System Help dperezve
Object Management Intrusion Rules
Add Route Map
Filter
Match Clauses | Set Clauses
Security Zones
IPv4
IPv6
BGP
Others
Address (2) Next Hop (0) Route Source (0)
Search
Add
Cancel

Add Route Map Entry

Sequence No: 10

Redistribution: Allow

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

● Access List ○ Prefix List

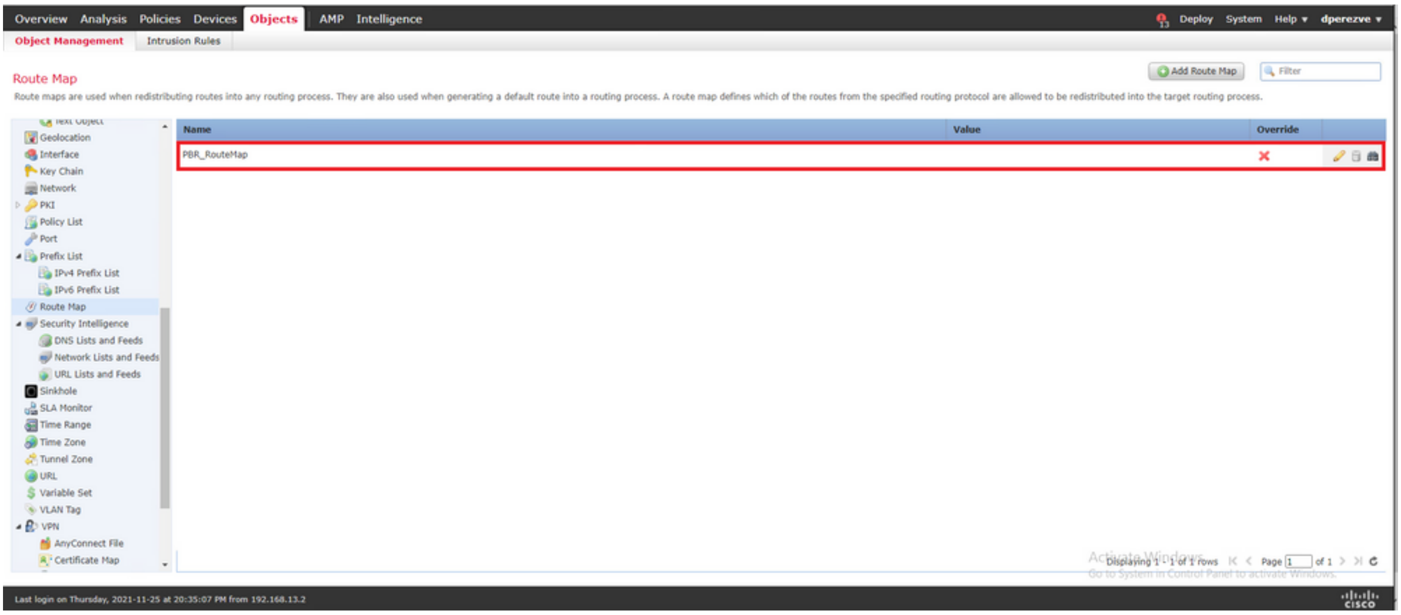
Available Access Lists : Extended

Available Extended Access List: PBR_ACL

Selected Extended Access List: PBR_ACL

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

Klicken Sie auf **Save** . Fügen Sie das Objekt der Objektliste hinzu.



Route Map

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

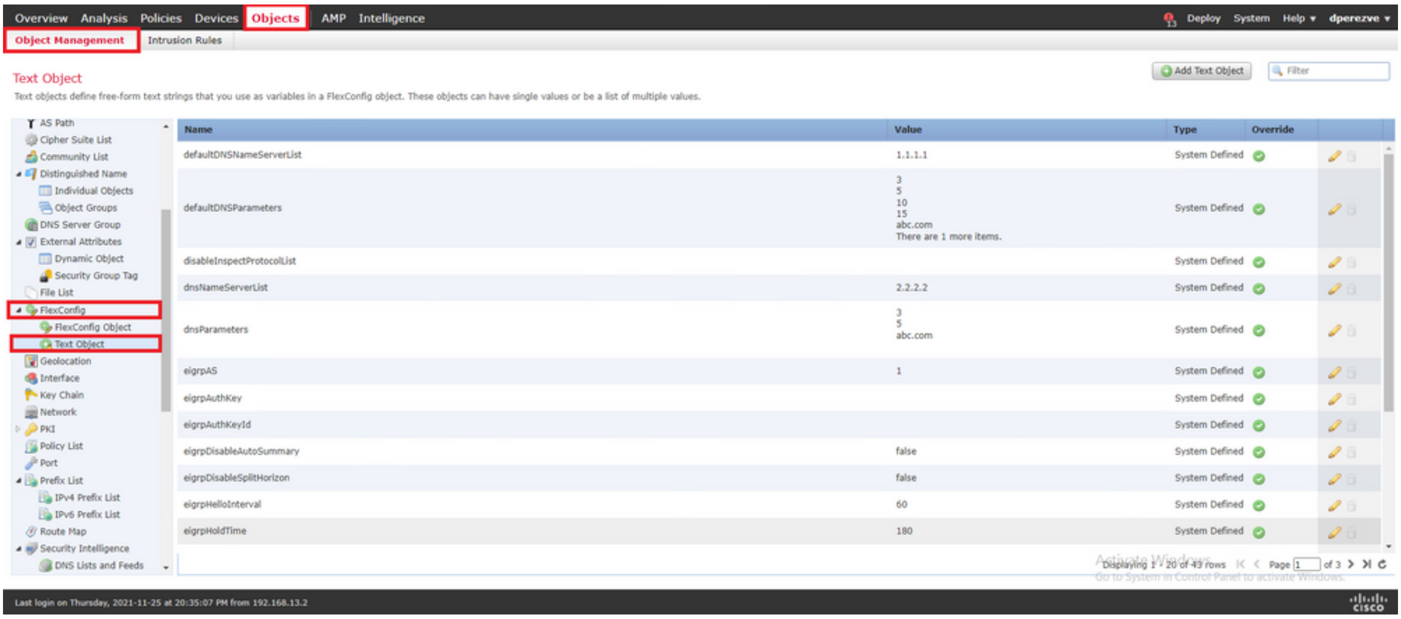
Name	Value	Override
PBR_RouteMap		✗

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

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.



Text Object

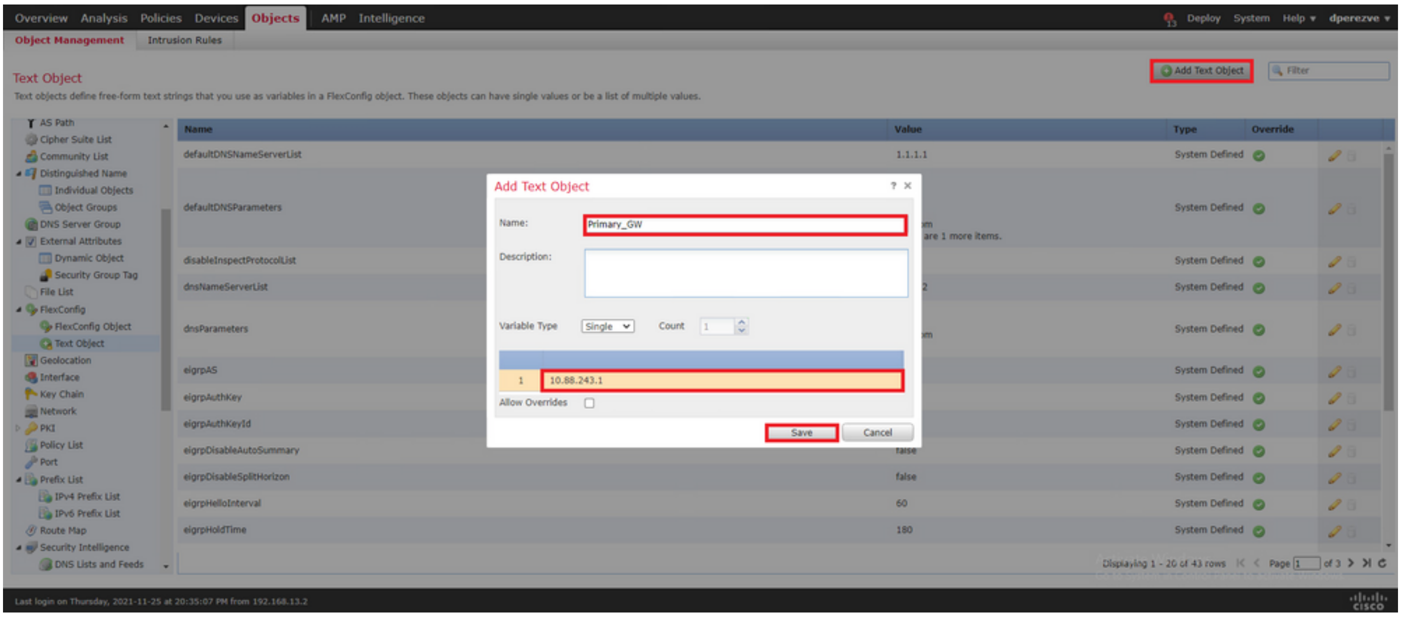
Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	✓
defaultDNSParameters	3 5 10 15 abc.com There are 1 more items.	System Defined	✓
disableInspectProtocolList		System Defined	✓
dnsNameServerList	2.2.2.2	System Defined	✓
dnsParameters	3 5 abc.com	System Defined	✓
eigrpAS	1	System Defined	✓
eigrpAuthKey		System Defined	✓
eigrpAuthKeyId		System Defined	✓
eigrpDisableAutoSummary	false	System Defined	✓
eigrpDisableSplitHorizon	false	System Defined	✓
eigrpHelloInterval	60	System Defined	✓
eigrpHoldTime	180	System Defined	✓

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

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.



Text Object

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

Add Text Object

Name: Primary_GW

Description:

Variable Type: Single Count: 1

1	10.88.243.1

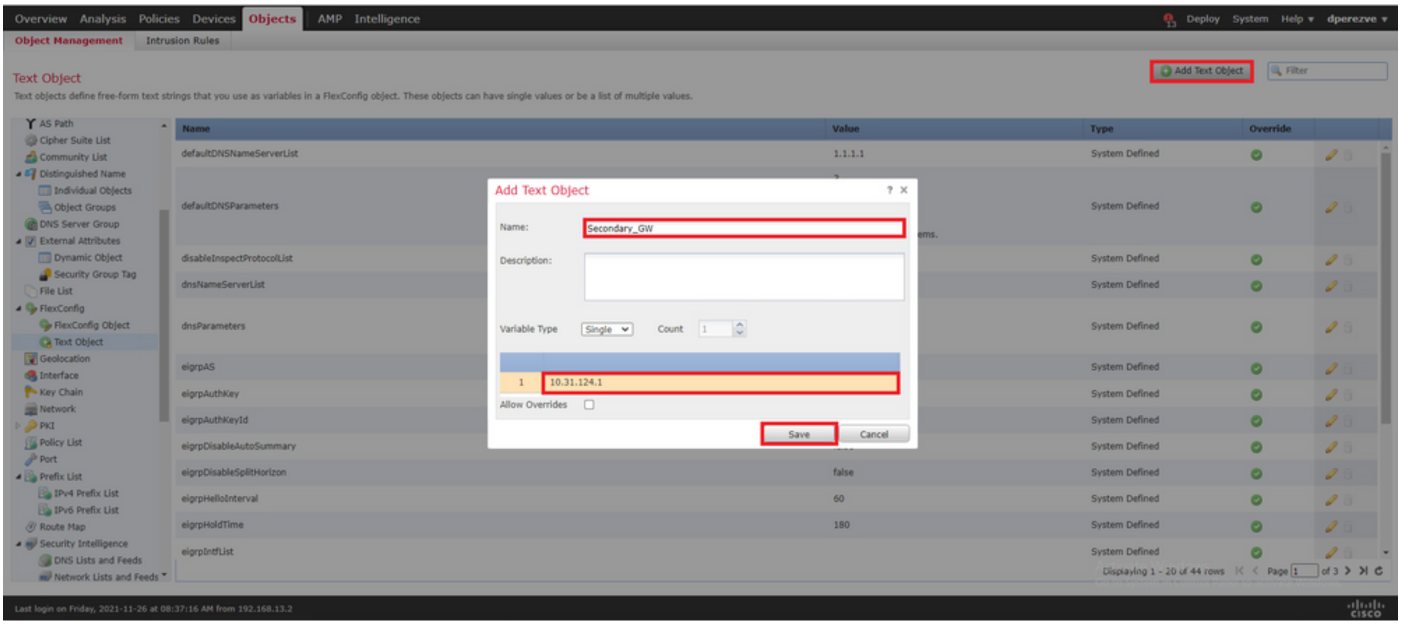
Allow Overrides □

Save Cancel

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

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** .



Text Object

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

Add Text Object

Name: Secondary_GW

Description:

Variable Type: Single Count: 1

1	10.31.124.1

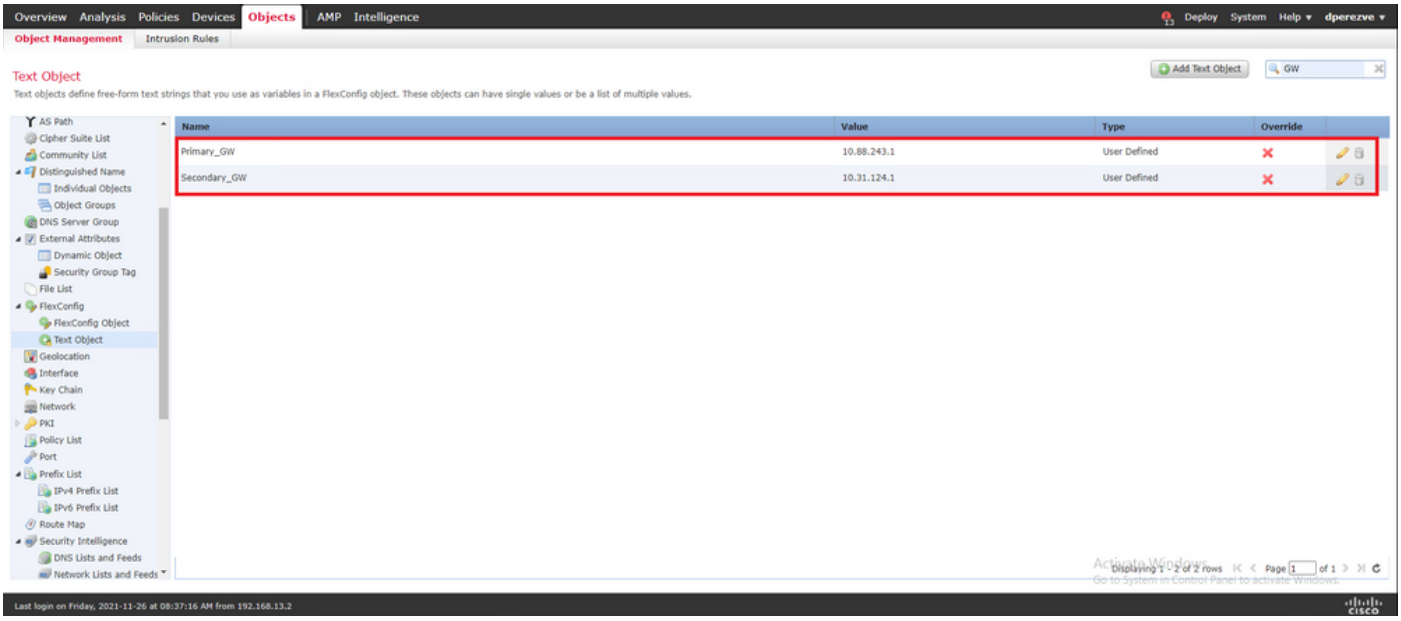
Allow Overrides □

Save Cancel

Displaying 1 - 20 of 44 rows

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

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



Text Object

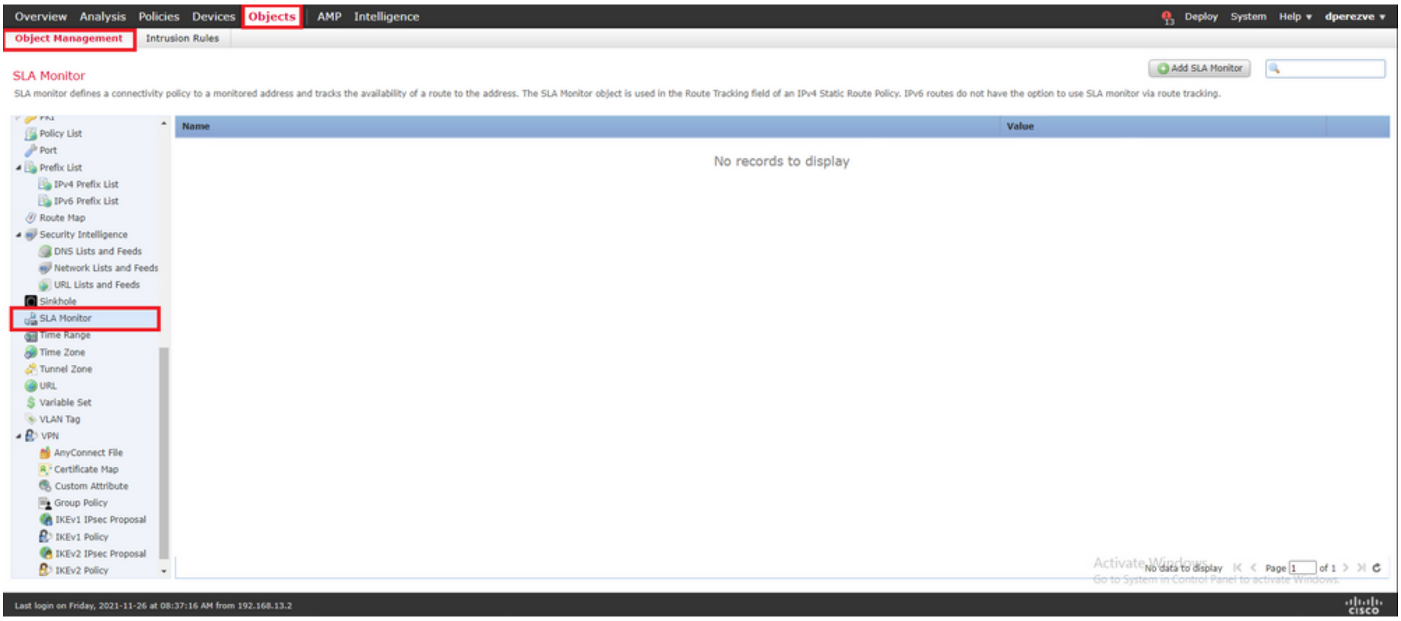
Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

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

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

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.



SLA Monitor

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value

No records to display

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

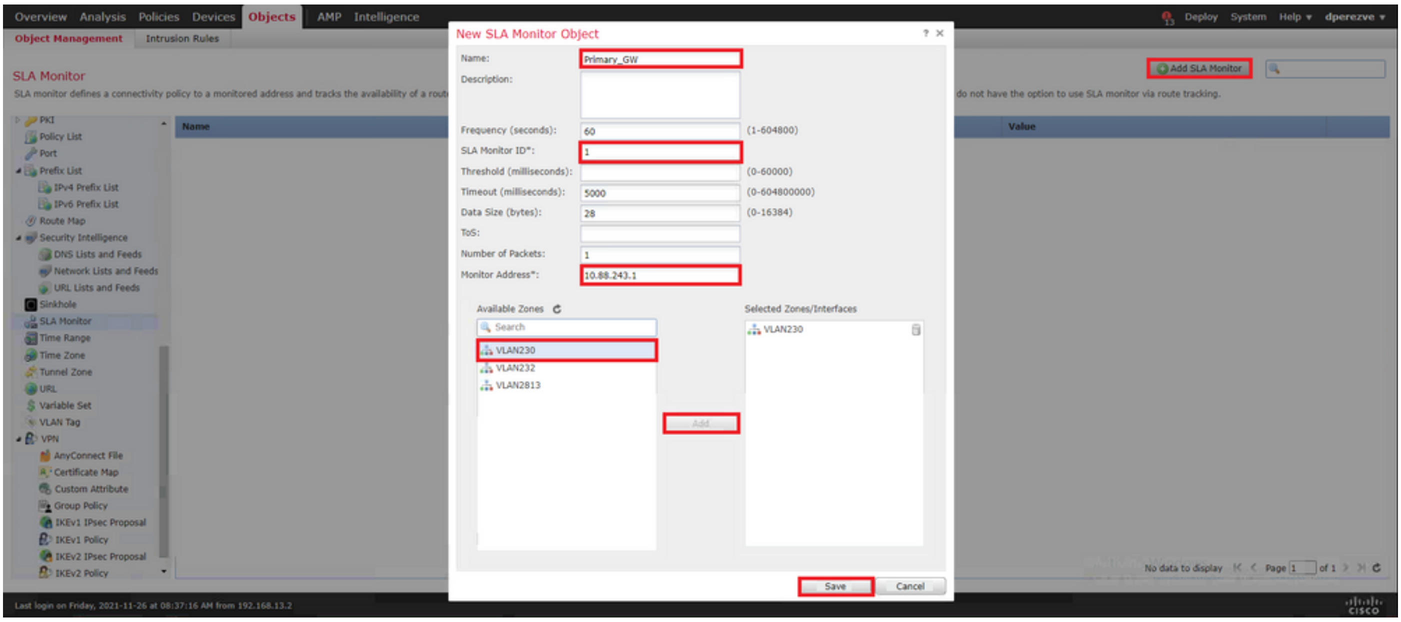
Wählen Sie **Add SLA Monitor** -Objekt.

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.



SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rout… do not have the option to use SLA monitor via route tracking.

New SLA Monitor Object

Name: Primary_GW

Description:

Frequency (seconds): 60 (1-604800)

SLA Monitor ID*: 1

Threshold (milliseconds): (0-60000)

Timeout (milliseconds): 5000 (0-604800000)

Data Size (bytes): 28 (0-16384)

ToS:

Number of Packets: 1

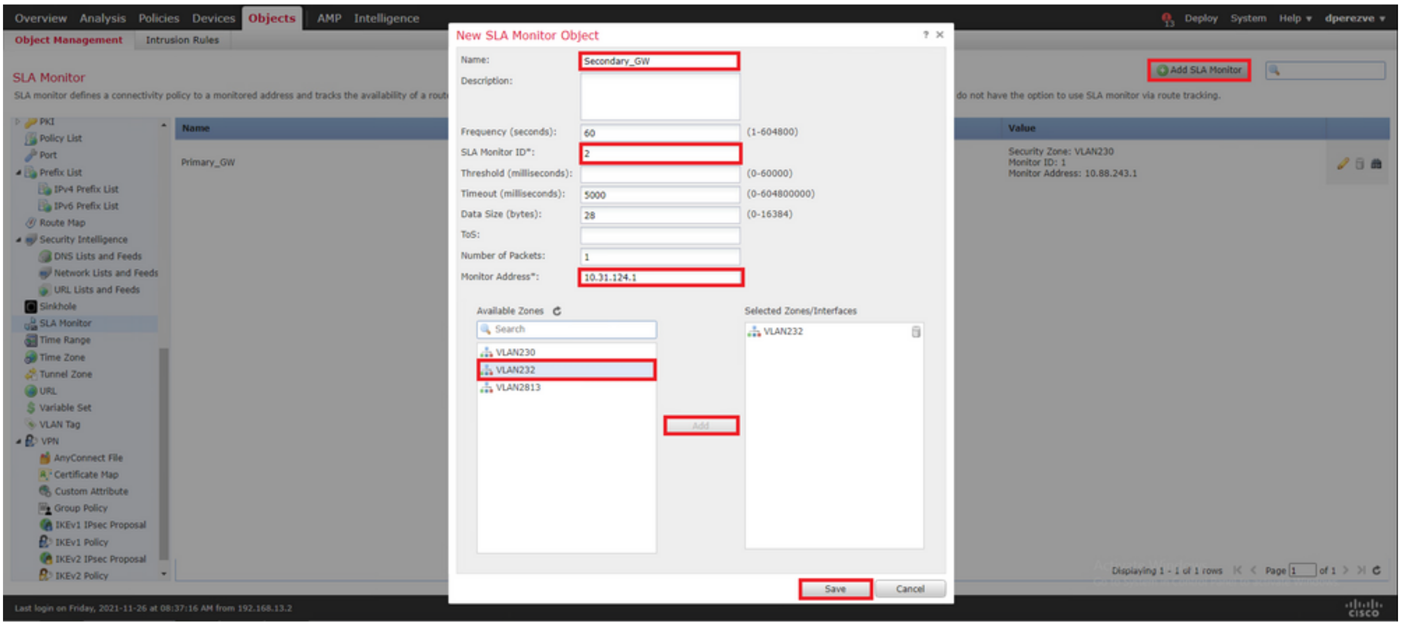
Monitor Address*: 10.88.243.1

Available Zones: VLAN230, VLAN232, VLAN2813

Selected Zones/Interfaces: VLAN230

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.



SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a rout… do not have the option to use SLA monitor via route tracking.

Primary_GW — Security Zone: VLAN230
Monitor ID: 1
Monitor Address: 10.88.243.1

New SLA Monitor Object

Name: Secondary_GW

Description:

Frequency (seconds): 60 (1-604800)

SLA Monitor ID*: 2

Threshold (milliseconds): (0-60000)

Timeout (milliseconds): 5000 (0-604800000)

Data Size (bytes): 28 (0-16384)

ToS:

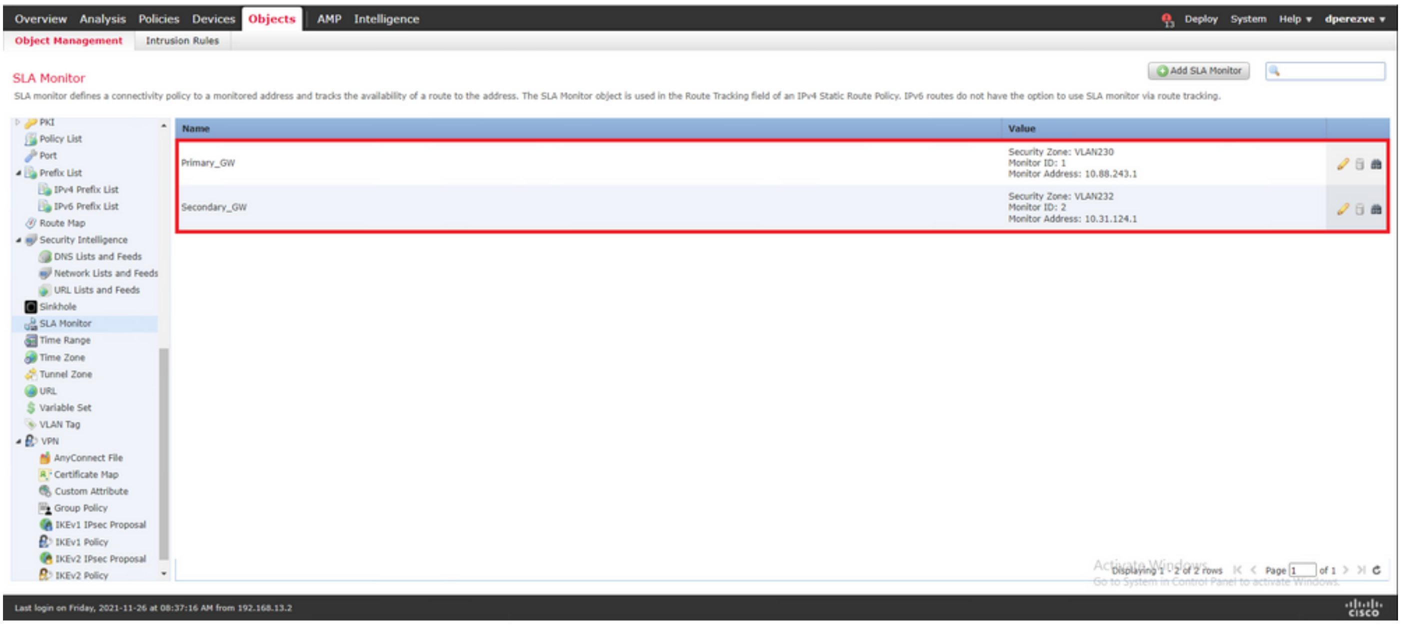
Number of Packets: 1

Monitor Address*: 10.31.124.1

Available Zones: VLAN230, VLAN232, VLAN2813

Selected Zones/Interfaces: VLAN232

Die beiden Objekte müssen der Liste hinzugefügt werden.



SLA Monitor

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

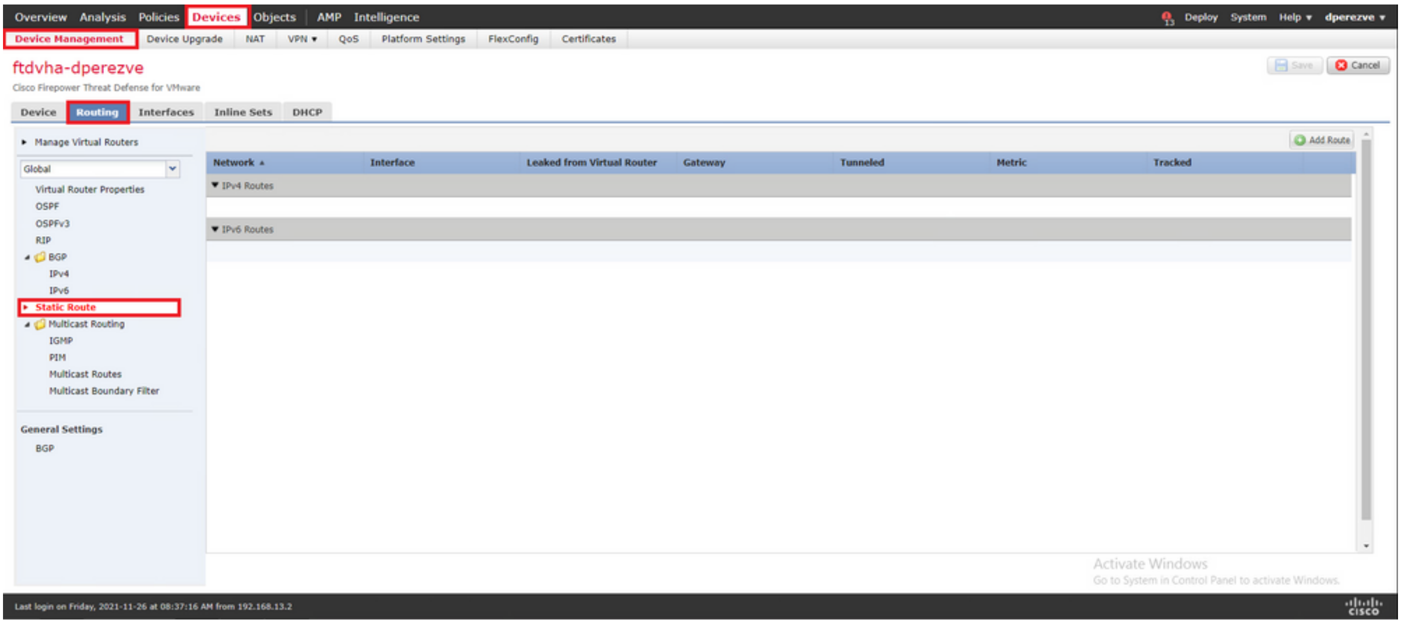
Name	Value
Primary_GW	Security Zone: VLAN230 Monitor ID: 1 Monitor Address: 10.88.243.1
Secondary_GW	Security Zone: VLAN232 Monitor ID: 2 Monitor Address: 10.31.124.1

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.



ftdvha-dperezve

Cisco Firepower Threat Defense for VMware

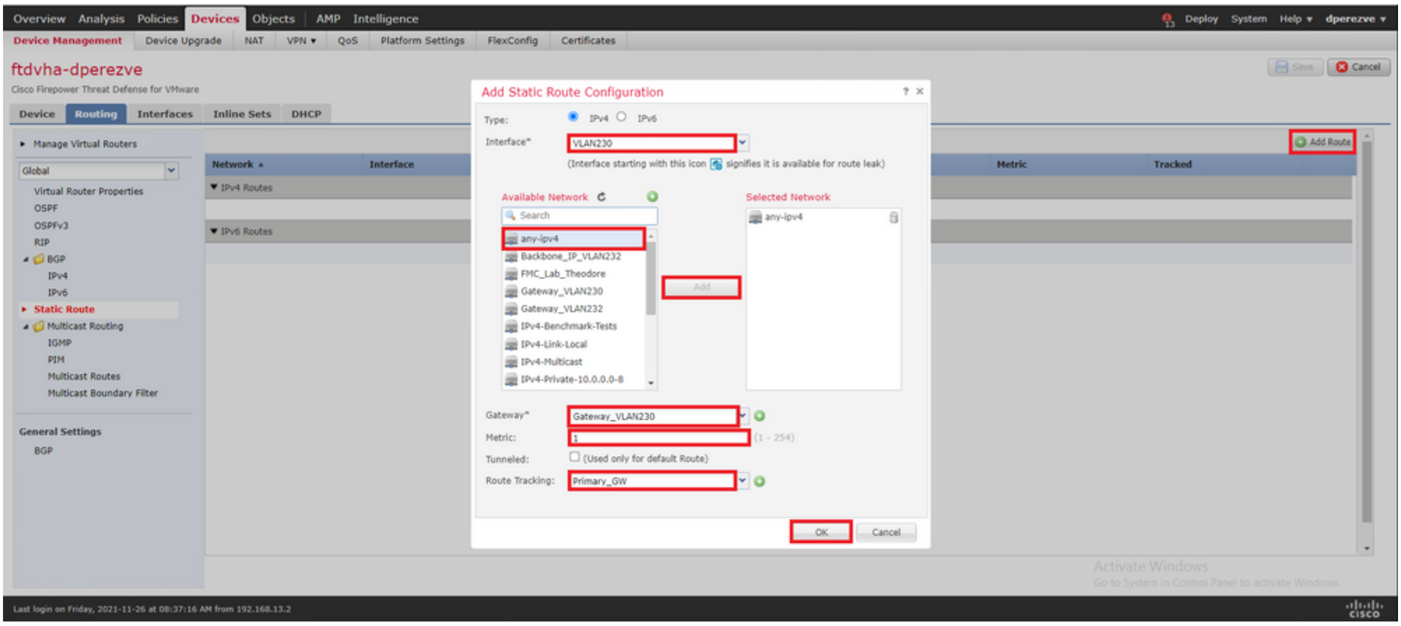
Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
▼ IPv6 Routes						

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.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: VLAN230

(Interface starting with this icon signifies it is available for route leak)

Available Network: any-ipv4, Backbone_IP_VLAN232, FMC_Lab_Theodore, Gateway_VLAN230, Gateway_VLAN232, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8

Selected Network: any-ipv4

Gateway*: Gateway_VLAN230

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

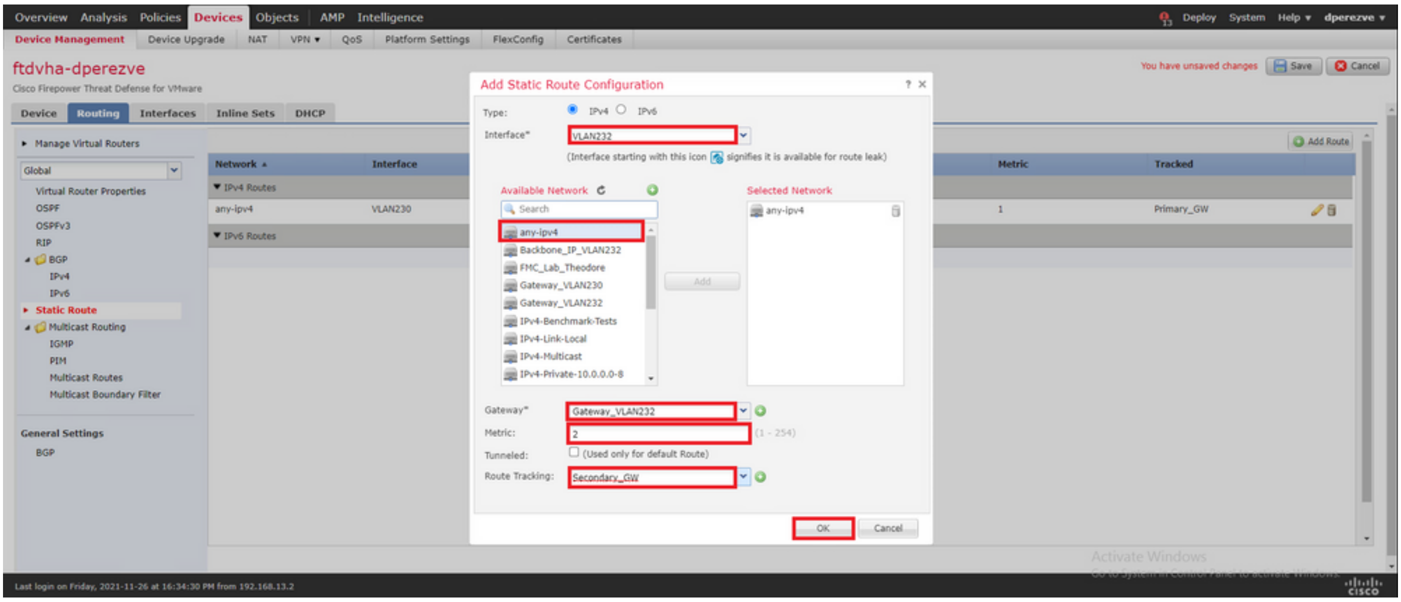
Route Tracking: Primary_GW

OK Cancel

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.



Network	Interface	Metric	Tracked
IPv4 Routes			
any-ipv4	VLAN230	1	Primary_GW
IPv6 Routes			

Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: VLAN232

(Interface starting with this icon signifies it is available for route leak)

Available Network: any-ipv4, Backbone_IP_VLAN232, FMC_Lab_Theodore, Gateway_VLAN230, Gateway_VLAN232, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8

Selected Network: any-ipv4

Gateway*: Gateway_VLAN232

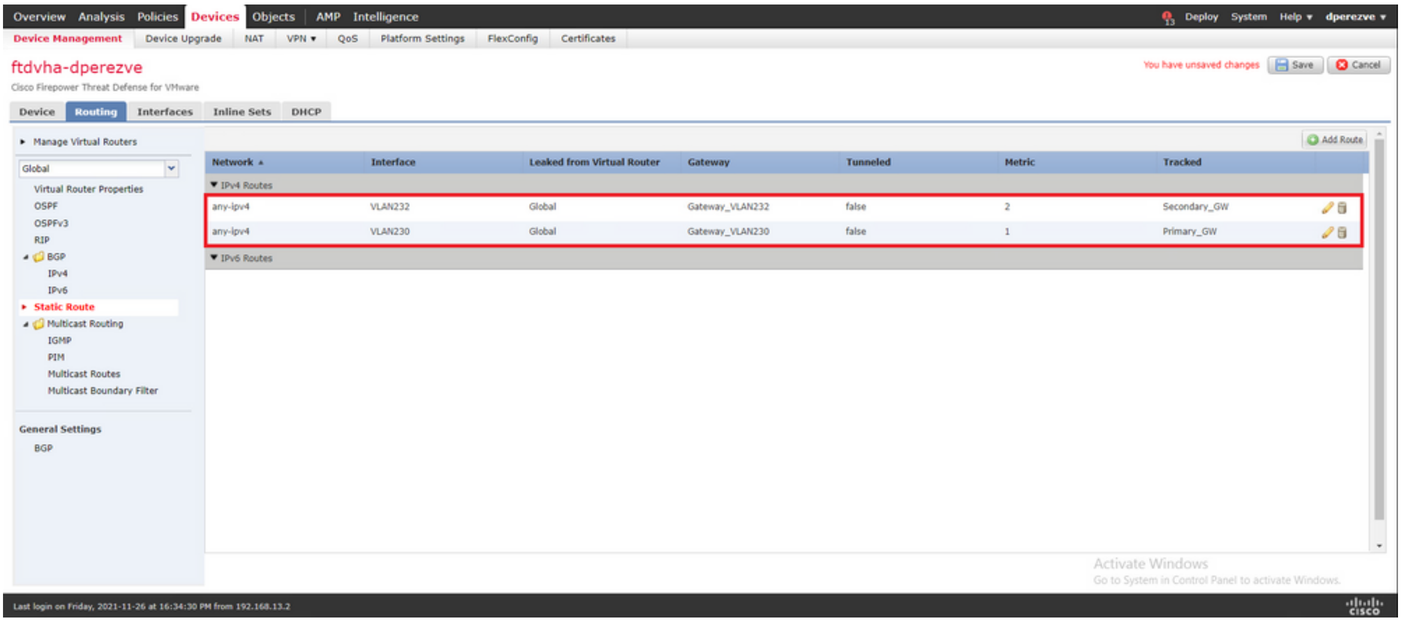
Metric: 2 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking: Secondary_GW

OK Cancel

Die beiden Routen müssen der Liste hinzugefügt werden.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
ftdvha-dperezve
Cisco Firepower Threat Defense for VMware
You have unsaved changes
Save
Cancel
Device Routing Interfaces Inline Sets DHCP
Manage Virtual Routers
Global
Virtual Router Properties
OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter
General Settings
BGP
Add Route
Activate Windows
Go to System in Control Panel to activate Windows.
Last login on Friday, 2021-11-26 at 16:34:30 PM from 192.168.13.2

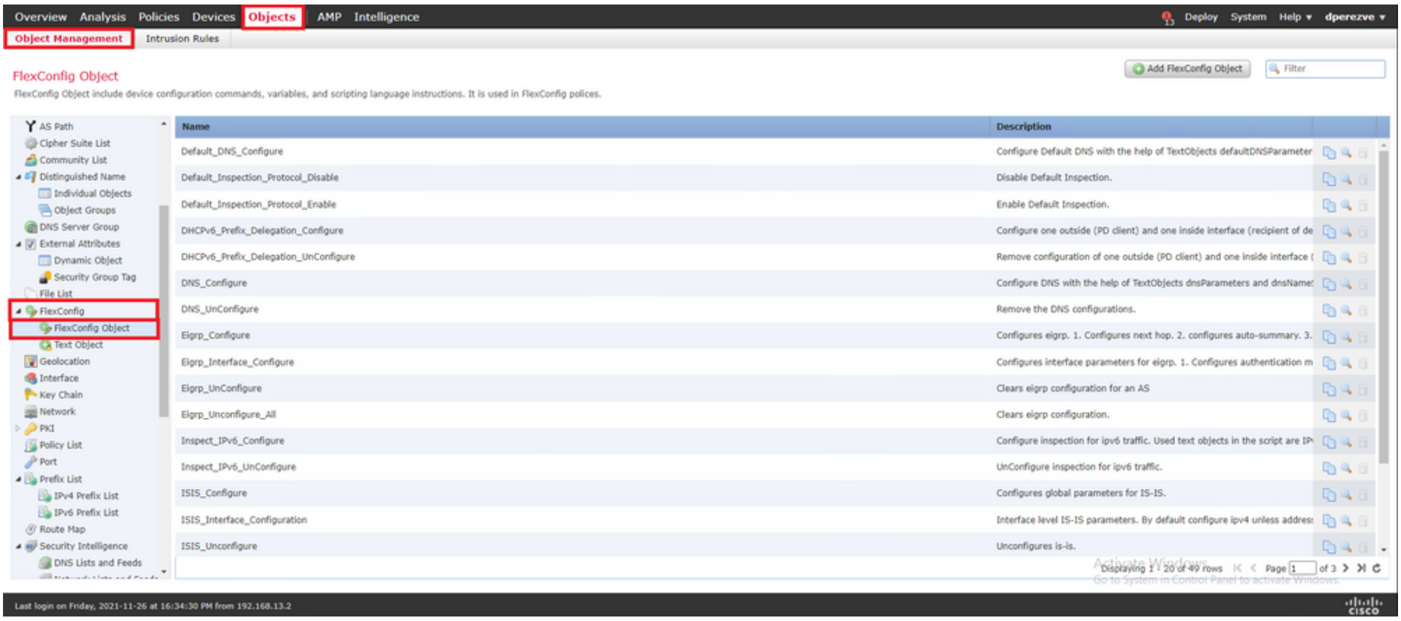
Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	VLAN232	Global	Gateway_VLAN232	false	2	Secondary_GW
any-ipv4	VLAN230	Global	Gateway_VLAN230	false	1	Primary_GW
▼ IPv6 Routes						

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.



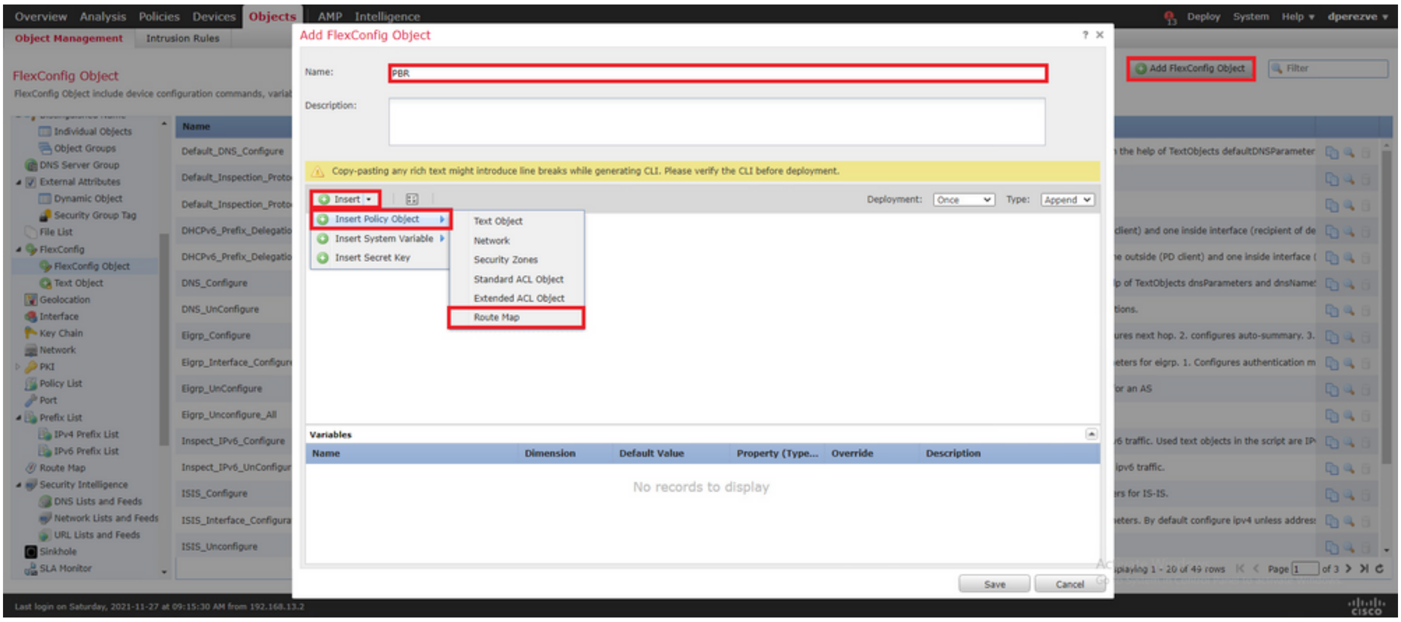
FlexConfig Object

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

Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNSParameter
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface (recipient of de
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside interface (
DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and dnsName:
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-summary. 3.
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures authentication m
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in the script are IP
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv4 unless addres:
ISIS_Unconfigure	Unconfigures is-is.

Displaying 1 - 20 of 49 rows Page 1 of 3

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



Add FlexConfig Object

Name: PBR

Description:

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

Deployment: Once Type: Append

Variables

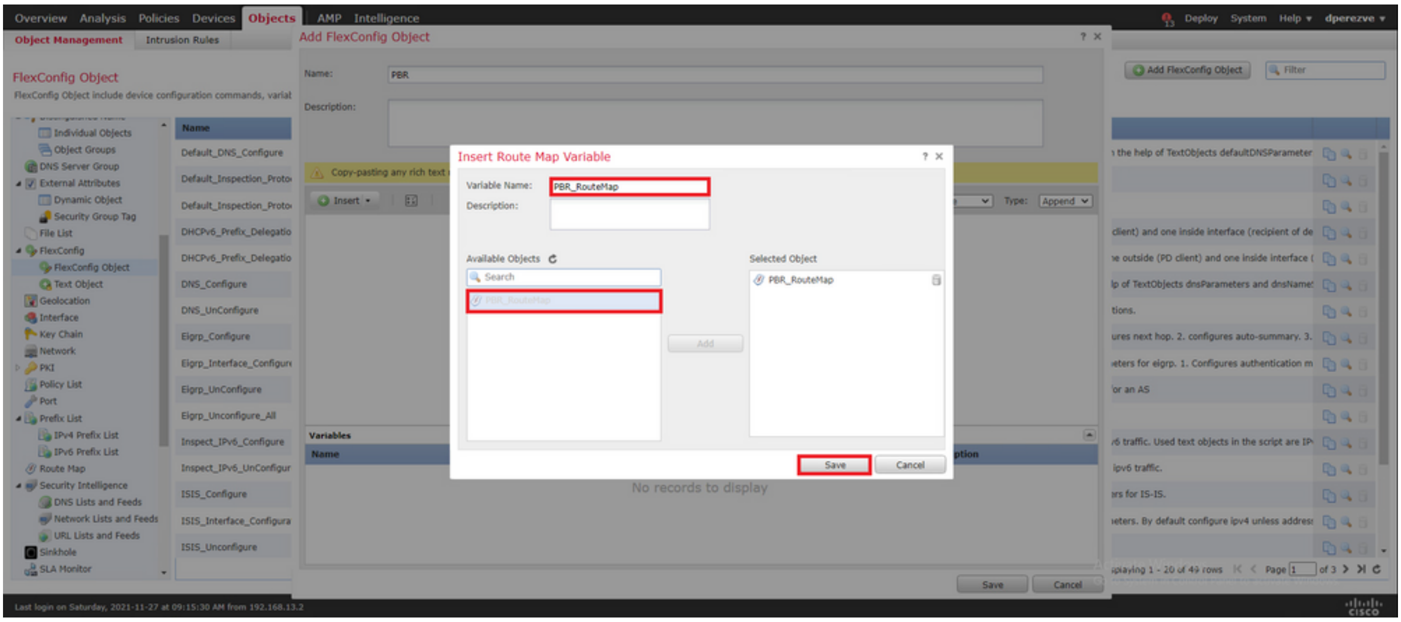
Name	Dimension	Default Value	Property (Type...	Override	Description

No records to display

Last login on Saturday, 2021-11-27 at 09:15:30 AM from 192.168.13.2

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 Policies Devices Objects AMP Intelligence
Deploy System Help ▾ dperezve ▾
Object Management Intrusion Rules
FlexConfig Object
Add FlexConfig Object
Insert Route Map Variable
Available Objects
Search
Add
Save
Cancel

Add FlexConfig Object

Name: PBR

Insert Route Map Variable

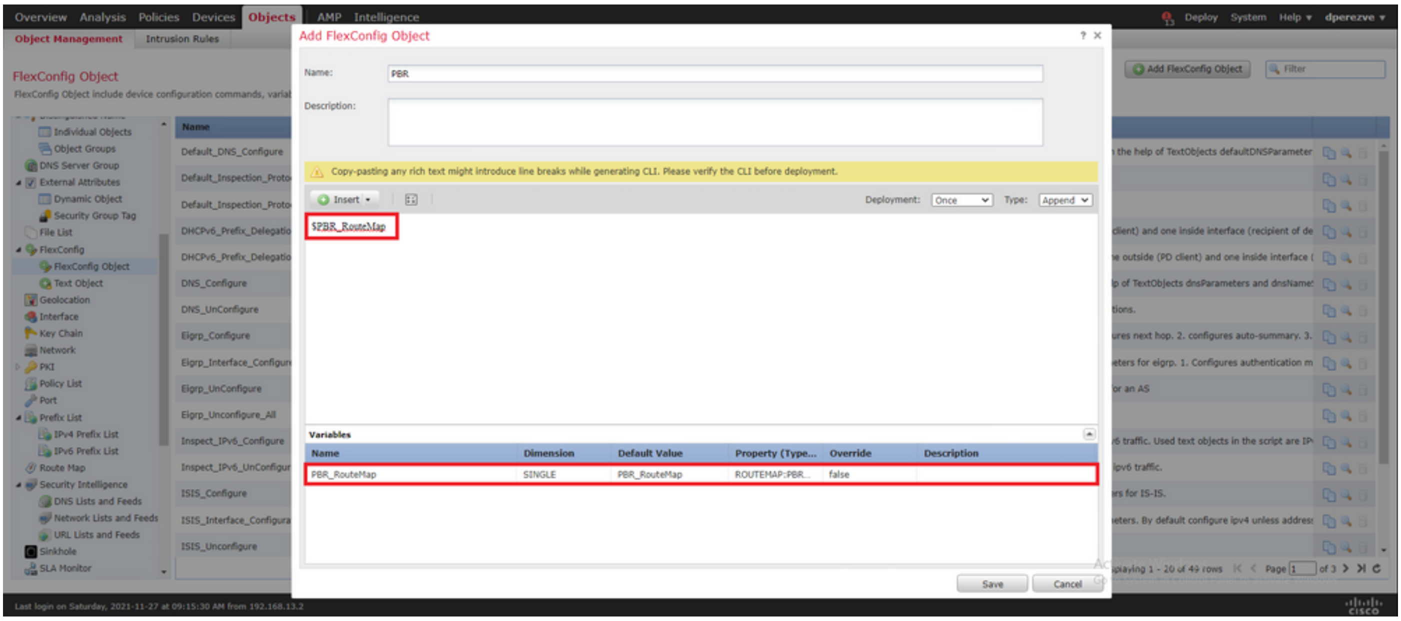
Variable Name: PBR_RouteMap

Description:

Selected Object: PBR_RouteMap

No records to display

Last login on Saturday, 2021-11-27 at 09:15:30 AM from 192.168.13.2



Name: PBR

Description:

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

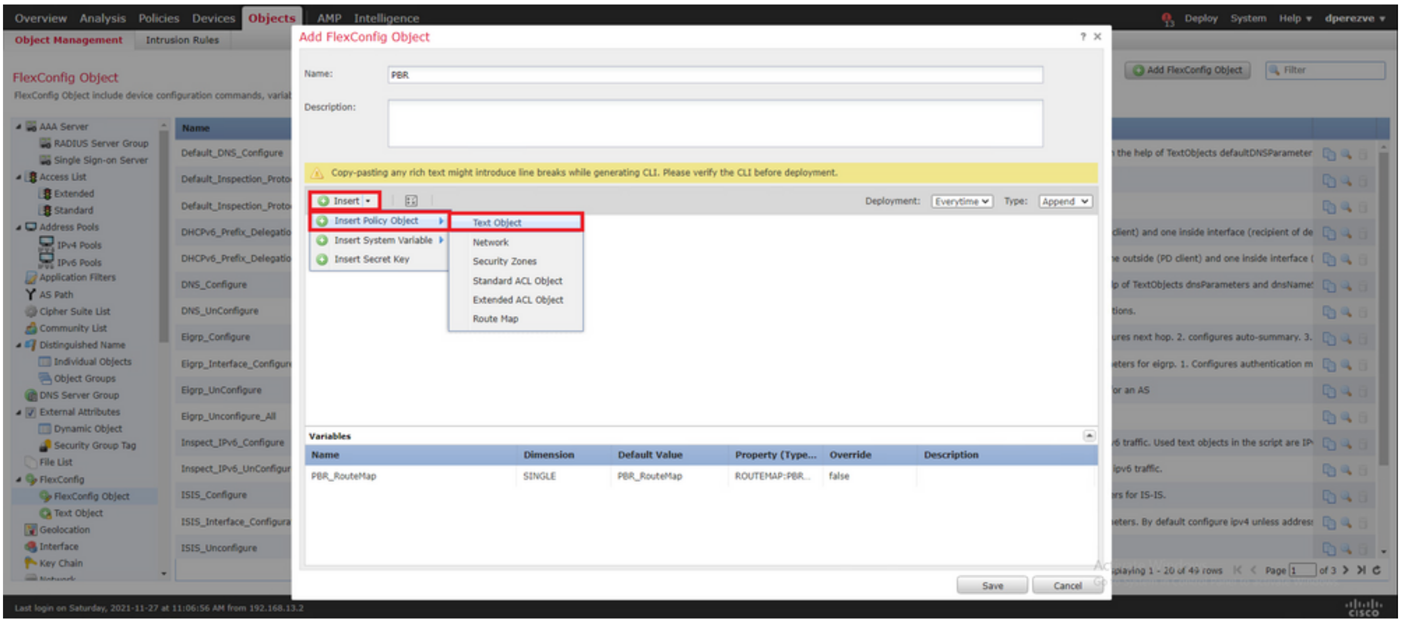
Deployment: Once   Type: Append

```
$PBR_RouteMap
```

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

Last login on Saturday, 2021-11-27 at 09:15:30 AM from 192.168.13.2

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 .**



Name: PBR

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

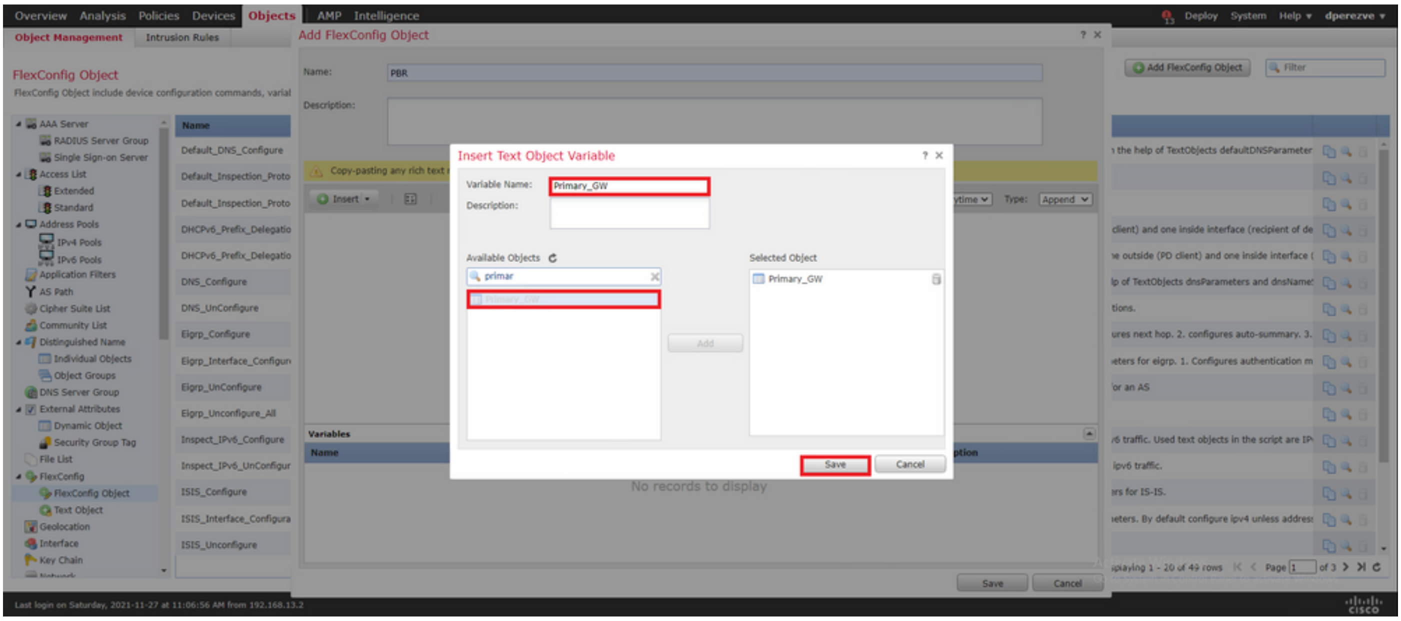
Deployment: Everytime   Type: Append

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

Last login on Saturday, 2021-11-27 at 11:06:56 AM from 192.168.13.2

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.



Insert Text Object Variable

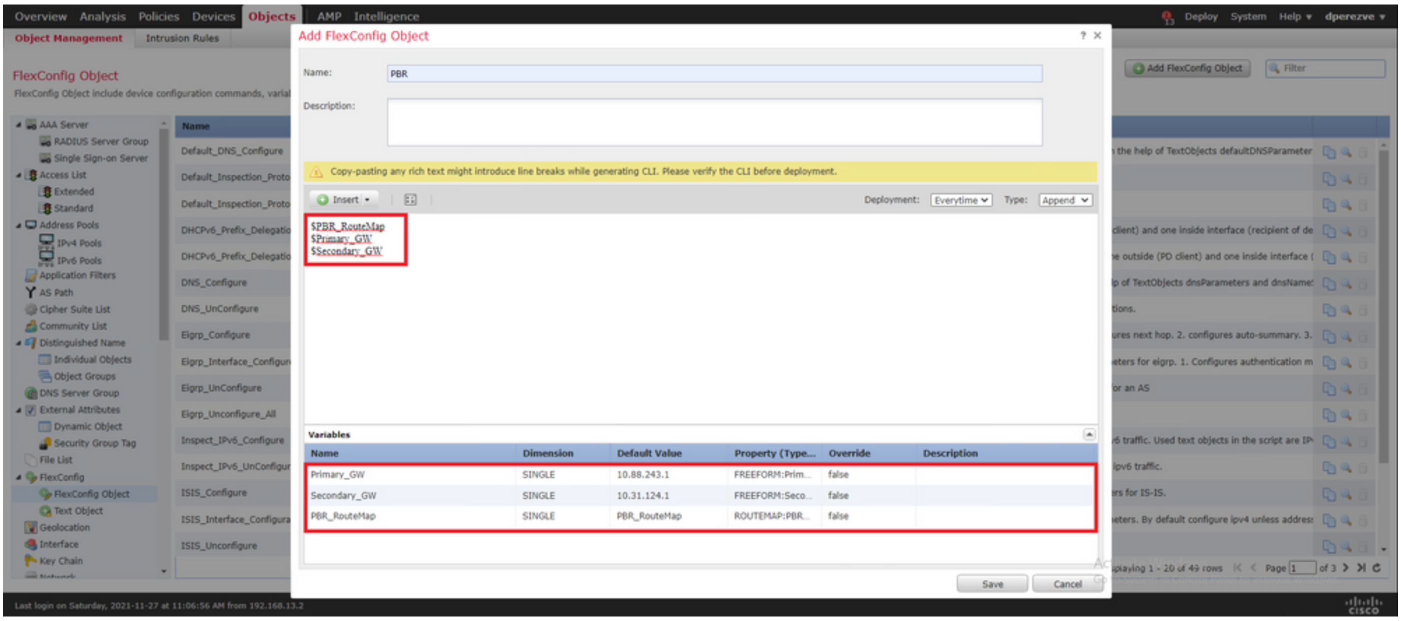
Variable Name: Primary_GW

Description:

Available Objects: primar

Selected Object: Primary_GW

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



Add FlexConfig Object

Name: PBR

Description:

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

Deployment: Everytime Type: Append

```
$PBR_RouteMap
$Primary_GW
$Secondary_GW
```

Variables

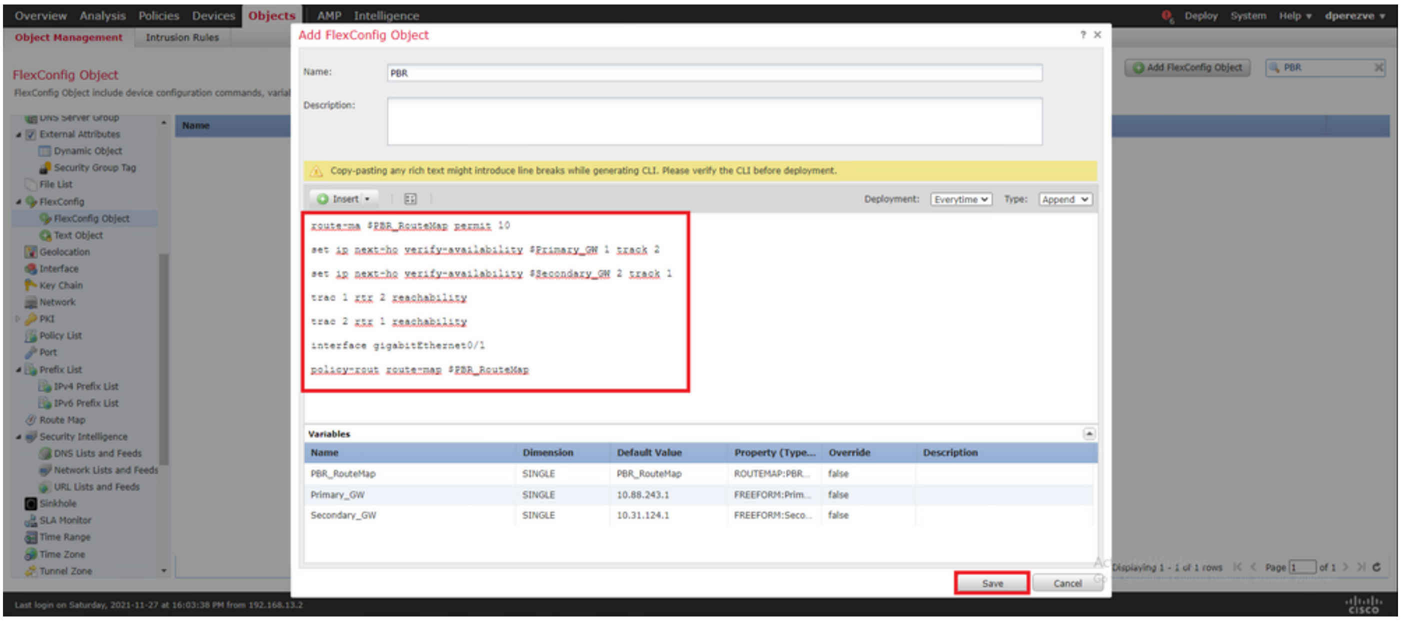
Name	Dimension	Default Value	Property (Type...	Override	Description
Primary_GW	SINGLE	10.88.243.1	FREEFORM:Prim...	false	
Secondary_GW	SINGLE	10.31.124.1	FREEFORM:Seco...	false	
PBR_RouteMap	SINGLE	PBR_RouteMap	ROUTEMAP:PBR...	false	

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.



Add FlexConfig Object

Name: PBR

Description:

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

Deployment: Everytime Type: Append

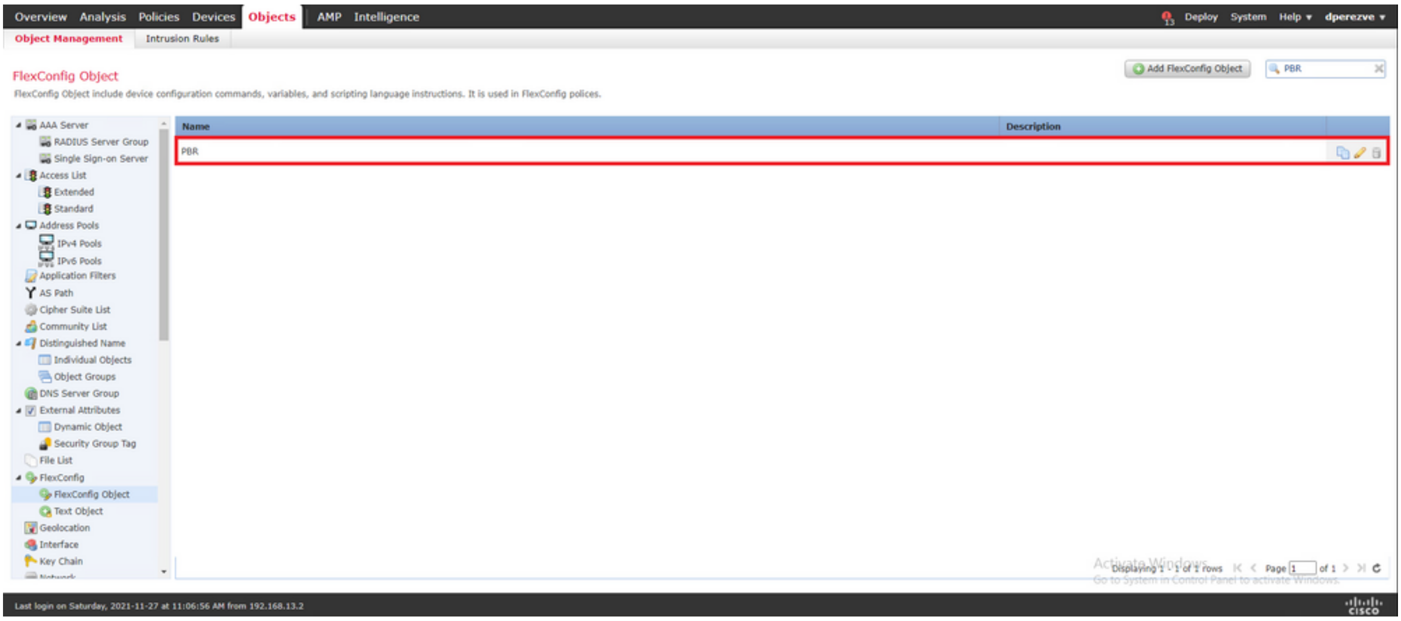
```
route-ma $PBR_RouteMap permit 10

set ip next-ho verify-availability $Primary_GW 1 track 2

set ip next-ho verify-availability $Secondary_GW 2 track 1

trac 1 rtr 2 reachability

trac 2 rtr 1 reachability

interface gigabitEthernet0/1

policy-rout route-map $PBR_RouteMap
```

Variables

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

Last login on Saturday, 2021-11-27 at 16:03:38 PM from 192.168.13.2

Das FlexConfig-Objekt muss der Liste hinzugefügt werden.



FlexConfig Object

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

Name	Description
PBR	

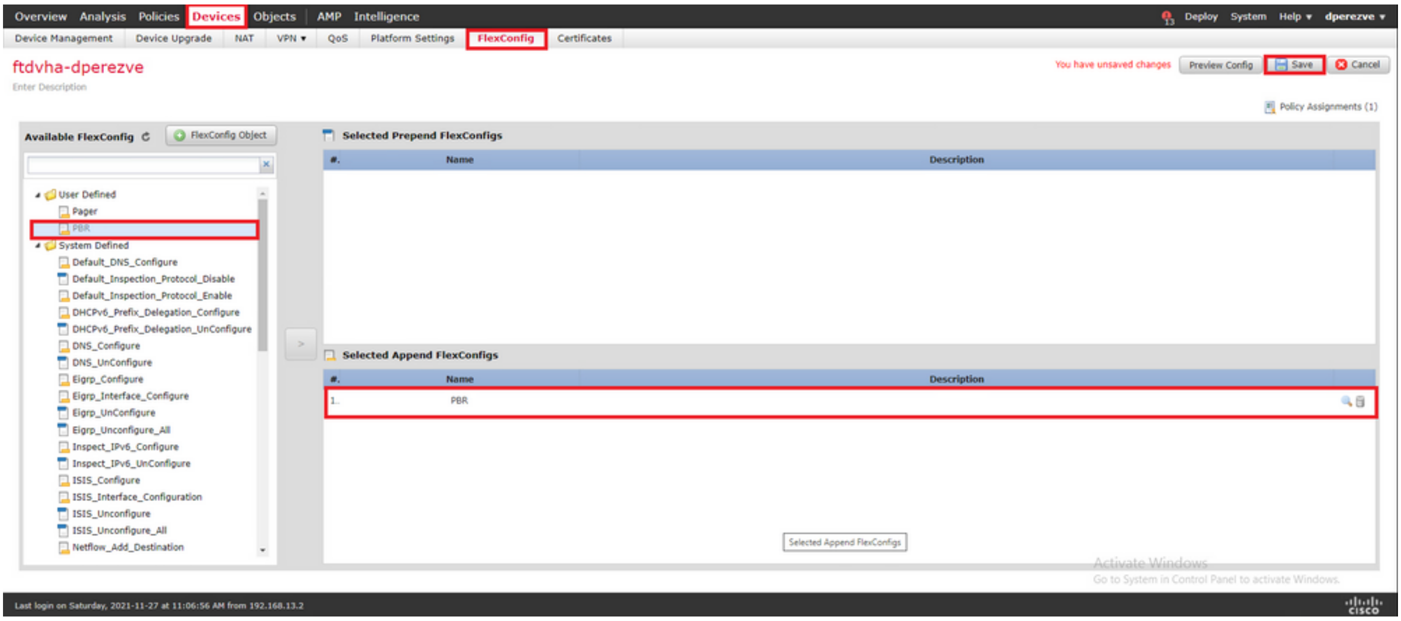
Displaying 1 - 1 of 1 rows Page 1 of 1

Last login on Saturday, 2021-11-27 at 11:06:56 AM from 192.168.13.2

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 AMP Intelligence
Deploy System Help ▾ dperezve ▾
Device Management Device Upgrade NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
ftdvha-dperezve
Enter Description
You have unsaved changes Preview Config Save Cancel
Policy Assignments (1)
Available FlexConfig
FlexConfig Object
User Defined
Pager
PBR
System Defined
Default_DNS_Configure
Default_Inspection_Protocol_Disable
Default_Inspection_Protocol_Enable
DHCPv6_Prefix_Delegation_Configure
DHCPv6_Prefix_Delegation_UnConfigure
DNS_Configure
DNS_UnConfigure
Eigrp_Configure
Eigrp_Interface_Configure
Eigrp_UnConfigure
Eigrp_Unconfigure_All
Inspect_IPv6_Configure
Inspect_IPv6_UnConfigure
ISIS_Configure
ISIS_Interface_Configuration
ISIS_Unconfigure
ISIS_Unconfigure_All
Netflow_Add_Destination
Selected Prepend FlexConfigs
# Name Description
Selected Append FlexConfigs
# Name Description
1 PBR
Selected Append FlexConfigs
Activate Windows
Go to System in Control Panel to activate Windows.
Last login on Saturday, 2021-11-27 at 11:06:56 AM from 192.168.13.2

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.

```
firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address
(access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2 [up]
ip next-hop verify-availability 10.31.124.1 2 track 1 [up] firepower# show route Codes: L -
local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O
- OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 -
OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-
IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static
route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF
Gateway of last resort is 10.88.243.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [1/0] via
10.88.243.1, VLAN230 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25
255.255.255.255 is directly connected, VLAN232 C 10.88.243.0 255.255.255.0 is directly
connected, VLAN230 L 10.88.243.60 255.255.255.255 is directly connected, VLAN230 C 192.168.13.0
255.255.255.0 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly
connected, VLAN2813
```

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 flow-
end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-
list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information:
Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust
hits=172250, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
```

```
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176701, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176711, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=anyError: not enough
buffer space to print ASP rule Result: input-interface: VLAN2813(vrfid:0) input-status: up
input-line-status: up output-interface: VLAN230(vrfid:0) output-status: up output-line-status:
up Action: allow
```

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
255.255.255.255 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
```

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 flow-
end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-
list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information:
Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust
hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177180, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
```

```
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177190, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Result: input-interface:
VLAN2813(vrfid:0) input-status: up input-line-status: up output-interface: VLAN232(vrfid:0)
output-status: up output-line-status: up Action: allow
```

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 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
```