

PBR met IP SLA's voor DUBBELE ISP configureren op FTD beheerd door FMC

Inhoud

[Inleiding](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 1. PBR-toegangslijst configureren](#)

[Stap 2. PBR-routekaart configureren](#)

[Stap 3. FlexConfig-tekstobjecten configureren](#)

[Stap 4. SLA-monitor configureren](#)

[Stap 4. Configureer statische routes met routespoor](#)

[Stap 5. PBR FlexConfig-object configureren](#)

[Stap 6. PBR FlexConfig-object toewijzen aan FlexConfig-beleid](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u PBR samen met IP SLA's kunt configureren op een FTD die wordt beheerd door FMC.

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PBR-configuratie op **Cisco Adaptive Security Appliance (ASA)**
- FlexConfig aan **Firepower**
- IP SLA's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD versie 7.0.0 (Build 94)
- Cisco FMC versie 7.0.0 (Build 94)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft hoe u het volgende kunt configureren **Policy Based Routing (PBR)** samen met **Internet Protocol Service Level Agreement (IP SLA)** op een Cisco-scherm **Firepower Threat Defense (FTD)** die wordt beheerd door Cisco **Firepower Management Center (FMC)**.

De traditionele routing neemt doorsturen beslissingen die alleen op de IP-adressen van de bestemmingen zijn gebaseerd. PBR is een alternatief voor het routeren van protocollen en statische routing.

Het verstrekt meer korrelige controle over het routing omdat het het gebruik van parameters zoals bron IP adressen of bron en bestemmingshavens als routeringscriteria naast het bestemming IP adres toestaat.

De mogelijke scenario's voor PBR omvatten brongevoelige toepassingen of verkeer over specifieke verbindingen.

Samen met PBR kunnen IP SLA's worden geïmplementeerd om de beschikbaarheid van de volgende hop te garanderen. Een IP SLA is een mechanisme dat de end-to-end connectiviteit bewaakt door de uitwisseling van reguliere pakketten.

Op het moment van publicatie wordt PBR niet rechtstreeks ondersteund door het VCC **Graphical User Interface (GUI)** Voor de configuratie van deze functie moet u gebruik maken van FlexConfig-beleid.

Aan de andere kant **Internet Control Message Protocol (ICMP)** SLA's worden ondersteund door FTD.

In dit voorbeeld wordt PBR gebruikt om pakketten via een primaire **Internet Service Provider (ISP)** circuit gebaseerd op het IP-adres van de bron.

Ondertussen bewaakt een IP SLA de connectiviteit en dwingt hij een reservestroomkring in geval van een storing.

Configureren

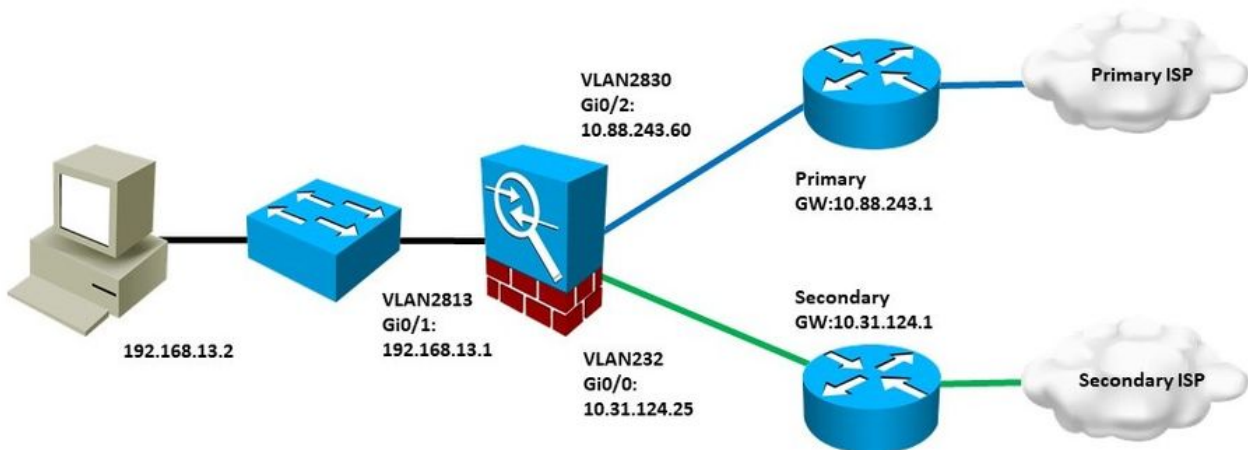
Netwerkdigram

In dit voorbeeld heeft Cisco FTD twee externe interfaces: VLAN230 en VLAN232. Elke maakt verbinding met een andere ISP.

Het verkeer vanuit het interne netwerk VLAN2813 wordt via de primaire ISP gerouteerd die PBR gebruikt.

De PBR routekaart neemt doorsturen beslissingen alleen op basis van het IP-bronadres (alles van VLAN2813 moet worden gerouteerd naar 10.88.243.1 in VLAN230) en wordt toegepast in de interface Gigabit Ethernet 0/1 van FTD.

Ondertussen gebruikt FTD IP SLA's om de connectiviteit met elke ISP-gateway te bewaken. In het geval van een storing in VLAN230, FTD failover naar het back-upcircuit op VLAN232.



Configuraties

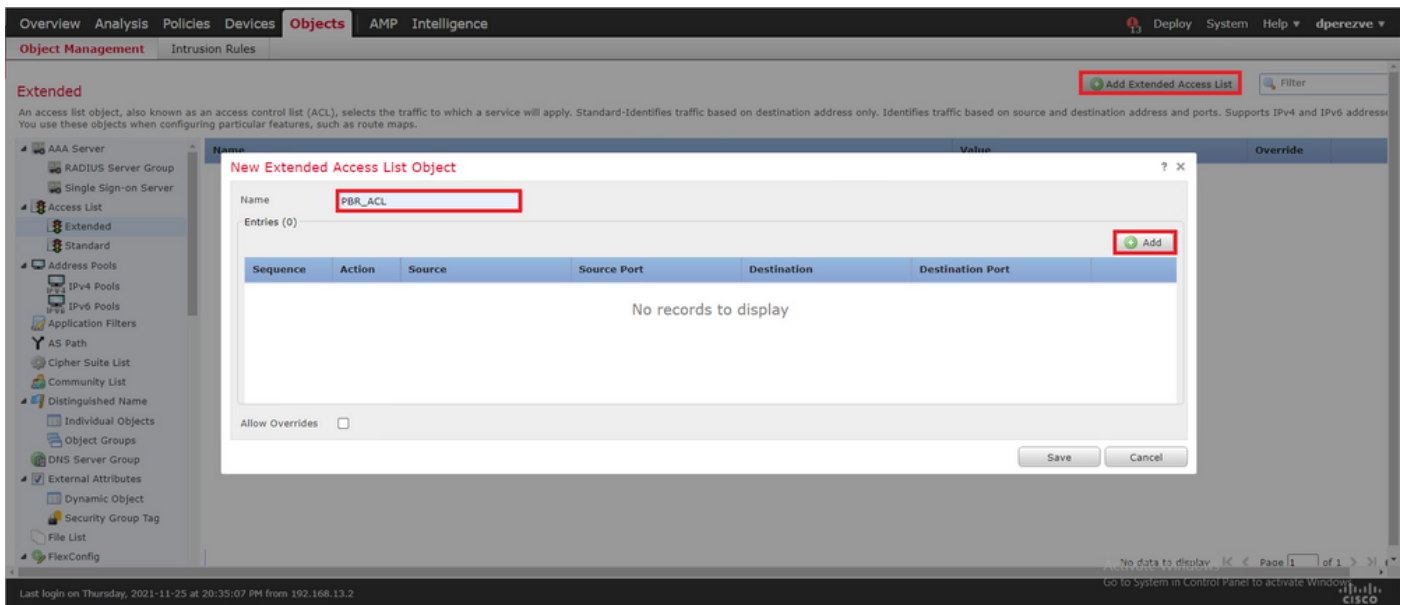
Stap 1. PBR-toegangslijst configureren

Bij de eerste stap van configuratie PBR, definieer welke pakketten onderwerp moeten zijn van het routingsbeleid. PBR maakt gebruik van routekaarten en toegangslijsten om verkeer te identificeren.

Om een toegangslijst voor de bijbehorende criteria te definiëren, bladert u naar **Objects > Object Management** en selecteer **Extended** in het kader **Access List** categorie in de inhoudsopgave.

The screenshot shows the Cisco FTD web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is active. Below the navigation bar, there are tabs for 'Object Management' and 'Intrusion Rules'. The 'Object Management' page displays a list of object categories on the left sidebar, with 'Access List' selected and 'Extended' highlighted. The main content area shows a table with the header 'Name', 'Value', and 'Override', and the text 'No records to display'. The bottom status bar indicates 'Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2'.

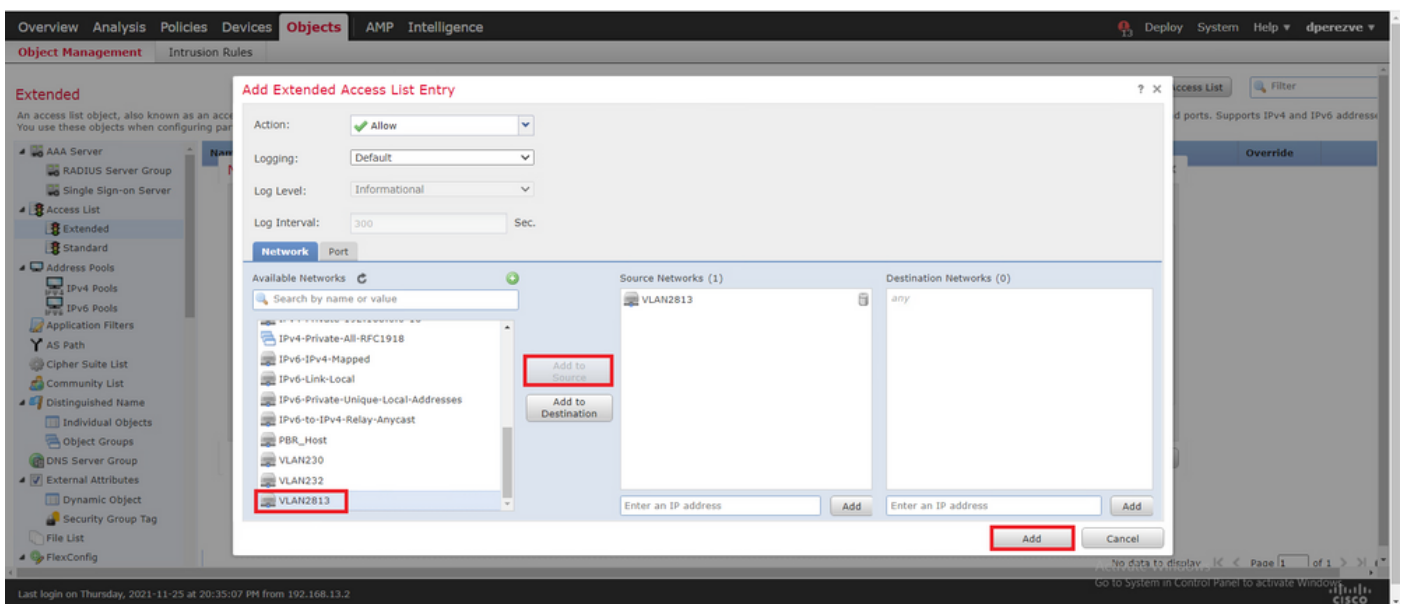
Klik **Add Extended Access List**. In het **New Extended Access List Object** venster, een naam voor het object toewijzen en vervolgens de **Add** om met de configuratie van de toegangslijst te beginnen.



In het Add Extended Access List Entry selecteer in het venster het object dat het binnennetwerk vertegenwoordigt, in dit geval VLAN2813.

Klik Add to Source om het als bron van de toegangslijst te definiëren.

Klik Add om de ingang te creëren.



Klik save . Het object moet worden toegevoegd aan de objectlijst.

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		X

Displaying 1 of 1 rows | Page 1 of 1

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

Stap 2. PBR-routekaart configureren

Zodra de PBR toegangslijst is geconfigureerd, wijs deze toe aan een routekaart. De routekaart evalueert verkeer tegen de matchclausules die in de toegangslijst worden bepaald.

Nadat een gelijke voorkomt, voert de routekaart de acties uit die in het routeringsbeleid worden bepaald.

Om routekaart te bepalen, navigeer aan **Objects > Object Management** en selecteer **Route Map** in de inhoudsopgave.

Route Map

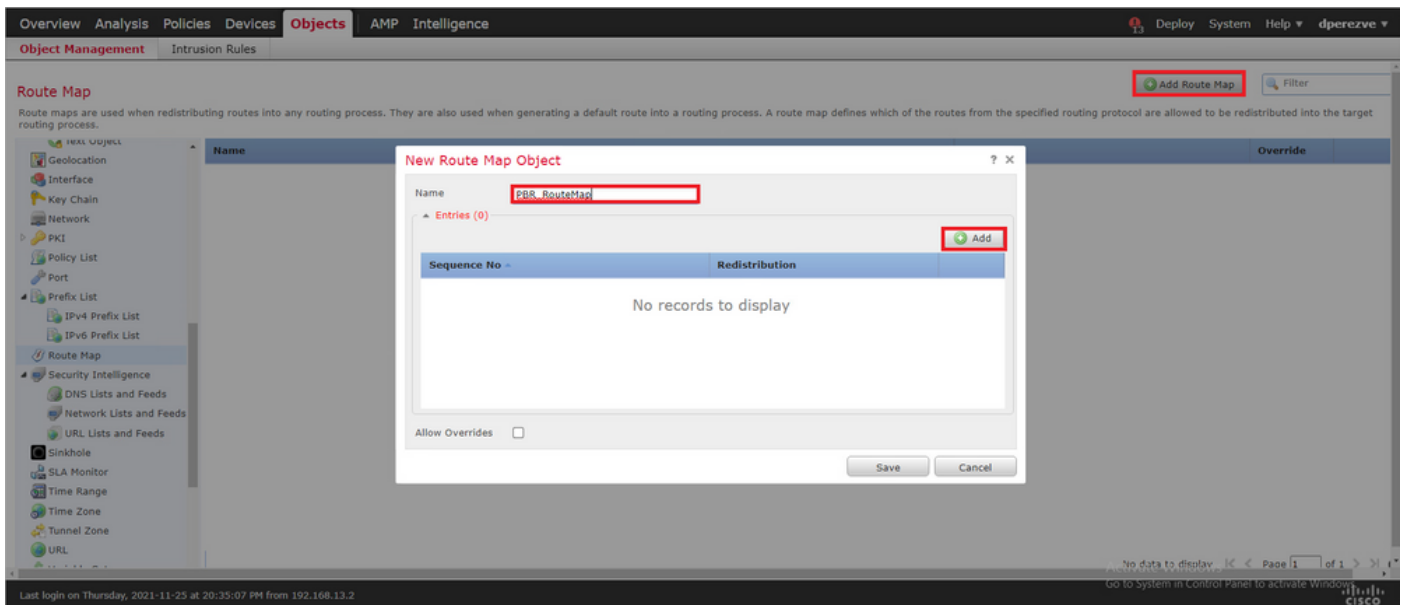
Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Name	Value	Override
No records to display		

AC: No data to display | Page 1 of 1

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

Klik **Add Route Map >**. In het **New Route Map Object** een naam voor het object toewijzen en vervolgens op klikken **Add** om een nieuwe routekaartingang te creëren.



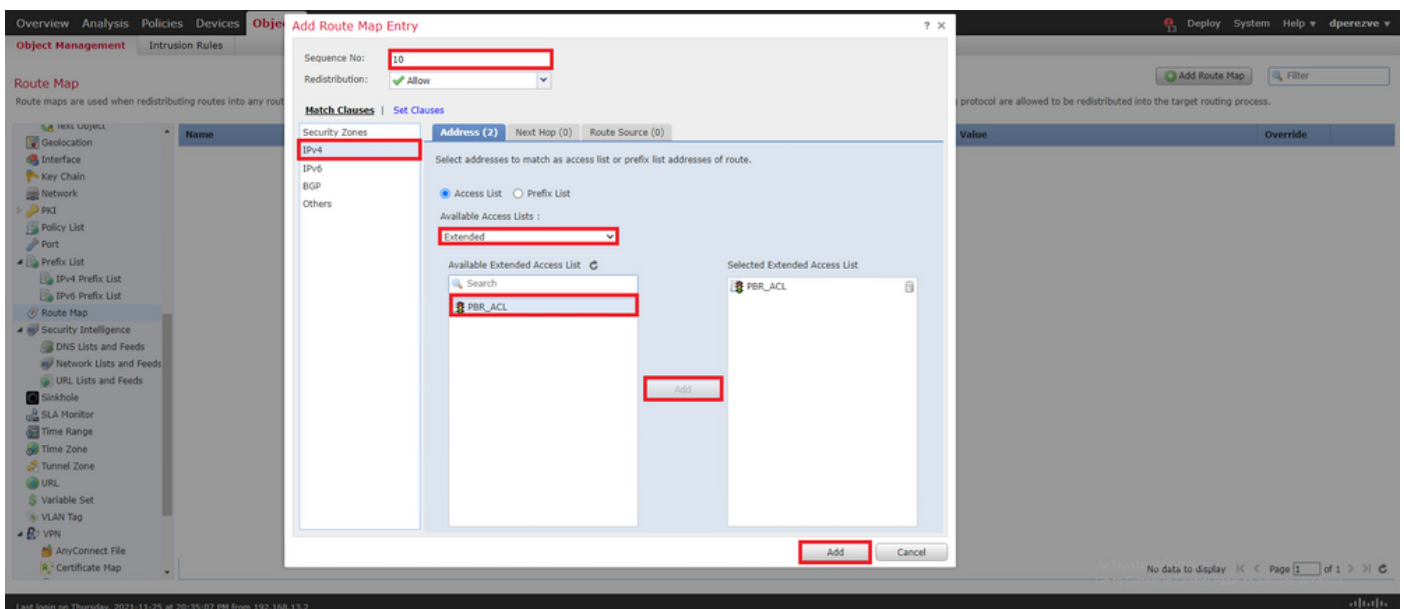
In het **Add Route Map Entry** bepaald een volgnummer voor de positie van de nieuwe vermelding.

Naar navigeren **IPv4-server > Match Clauses** en selecteer **Uitgebreid** in het Available Access List vervolgkeuzelijst.

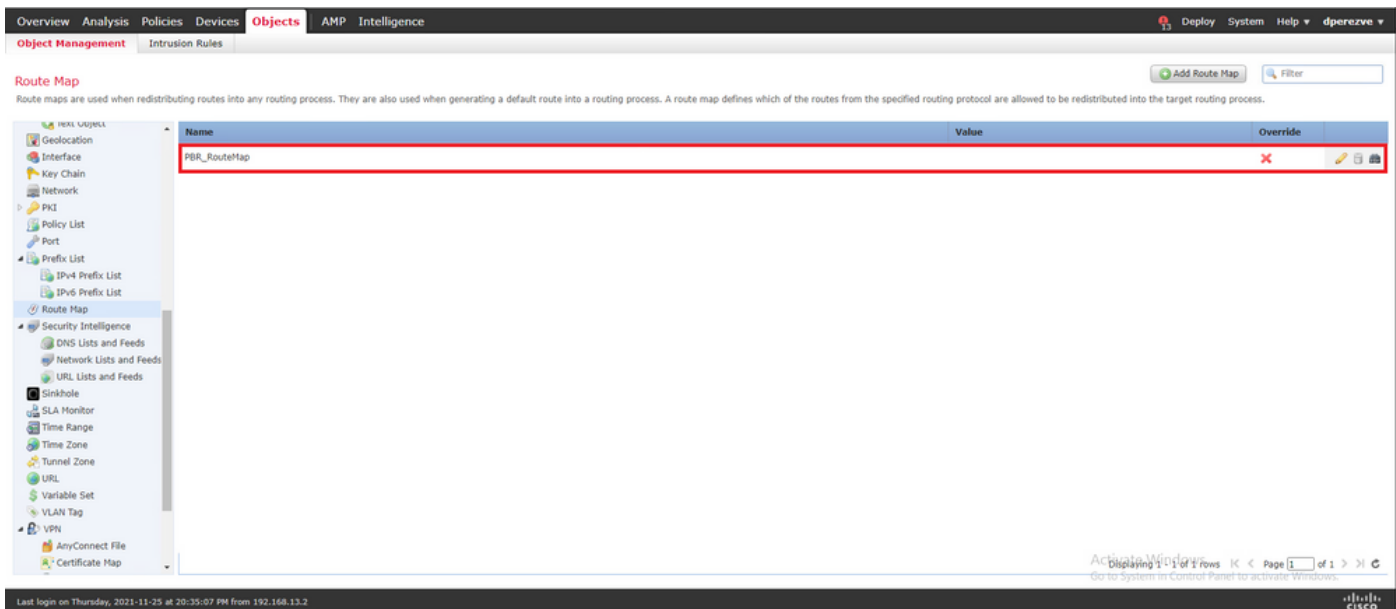
Selecteer het object van de toegangslijst dat in Stap 1 is gemaakt.

Klik **Add** om de ingang te creëren.

Opmerking: FTD ondersteunt maximaal 65536 (van 0 tot 65535) verschillende vermeldingen. Hoe lager het aantal, hoe hoger de prioriteitsevaluatie.



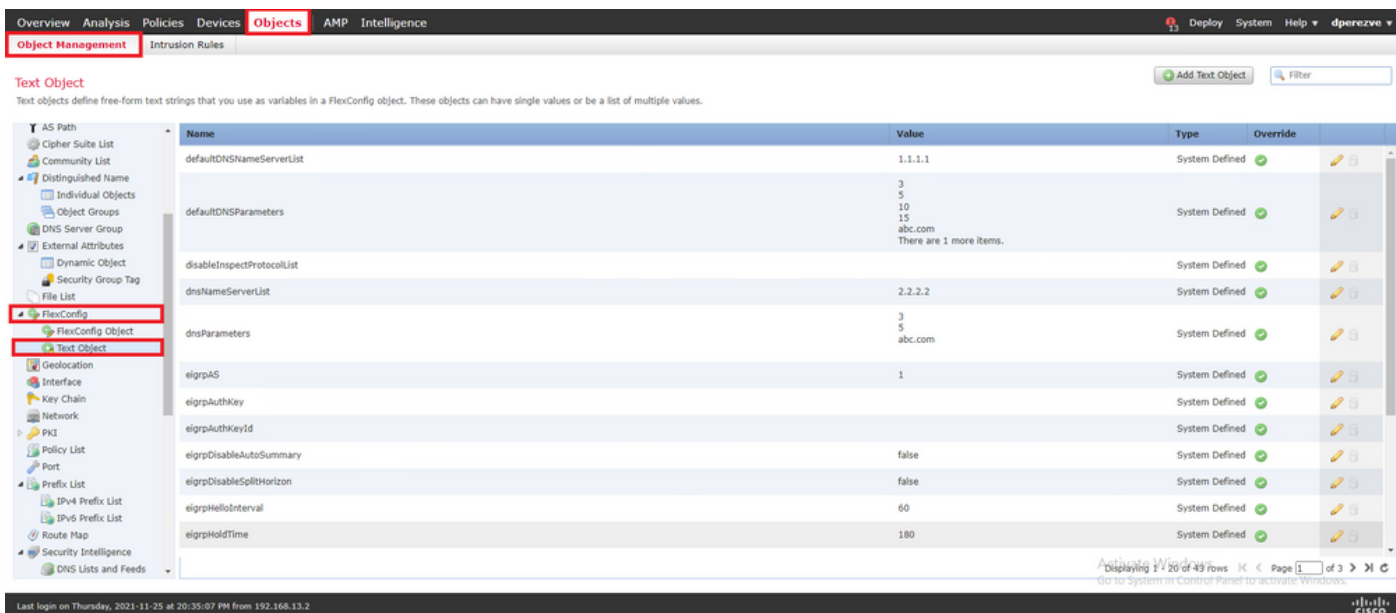
Klik **save** . Voeg het object toe aan de lijst van objecten.



Stap 3. FlexConfig-tekstobjecten configureren

De volgende stap omvat de definitie van FlexConfig-tekstobjecten die de standaardgateways voor elk circuit vertegenwoordigen. Deze tekstobjecten worden later gebruikt in de configuratie van FlexConfig-object dat PBR aan SLA's koppelt.

Om een FlexConfig-tekstobject te definiëren, navigeert u naar **Objects > Object Management** en selecteert u **Text Object** in het kader **FlexConfig** categorie in de inhoudsopgave.



Klik **Add Text Object** . In het **Add Text Object** venster, een naam toewijzen voor het object dat de primaire gateway vertegenwoordigt en het IPv4-adres voor dit apparaat specificeren.

Klik **save** om het nieuwe object toe te voegen.

Object Management | Intrusion Rules

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

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	<input checked="" type="checkbox"/>
defaultDNSParameters		System Defined	<input checked="" type="checkbox"/>
disableInspectProtocolList		System Defined	<input checked="" type="checkbox"/>
dnsNameServerList		System Defined	<input checked="" type="checkbox"/>
dnsParameters		System Defined	<input checked="" type="checkbox"/>
eigrpAS		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKey		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKeyId		System Defined	<input checked="" type="checkbox"/>
eigrpDisableAutoSummary		System Defined	<input checked="" type="checkbox"/>
eigrpDisableSplitHorizon	false	System Defined	<input checked="" type="checkbox"/>
eigrpHelloInterval	60	System Defined	<input checked="" type="checkbox"/>
eigrpHoldTime	180	System Defined	<input checked="" type="checkbox"/>

Displaying 1 - 20 of 43 rows Page 1 of 3

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

Klik **Add Text Object** opnieuw om een tweede object te maken, dit keer voor de Gateway in het back-circuit.

Vul het nieuwe object in met de juiste naam en IP-adres en klik op **save**.

Object Management | Intrusion Rules

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

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	<input checked="" type="checkbox"/>
defaultDNSParameters		System Defined	<input checked="" type="checkbox"/>
disableInspectProtocolList		System Defined	<input checked="" type="checkbox"/>
dnsNameServerList		System Defined	<input checked="" type="checkbox"/>
dnsParameters		System Defined	<input checked="" type="checkbox"/>
eigrpAS		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKey		System Defined	<input checked="" type="checkbox"/>
eigrpAuthKeyId		System Defined	<input checked="" type="checkbox"/>
eigrpDisableAutoSummary		System Defined	<input checked="" type="checkbox"/>
eigrpDisableSplitHorizon	false	System Defined	<input checked="" type="checkbox"/>
eigrpHelloInterval	60	System Defined	<input checked="" type="checkbox"/>
eigrpHoldTime	180	System Defined	<input checked="" type="checkbox"/>
eigrpIntfList		System Defined	<input checked="" type="checkbox"/>

Displaying 1 - 20 of 44 rows Page 1 of 3

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

De twee objecten moeten samen met de standaardobjecten aan de lijst worden toegevoegd.

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	<input checked="" type="checkbox"/>
Secondary_GW	10.31.124.1	User Defined	<input checked="" type="checkbox"/>

Step 4. SLA-monitor configureren

Om de SLA-objecten te definiëren die worden gebruikt om de connectiviteit met elke gateway te bewaken, navigeert u naar **Objects > Object Management** en selecteert u **SLA Monitor** in de inhoudsopgave.

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.

No records to display

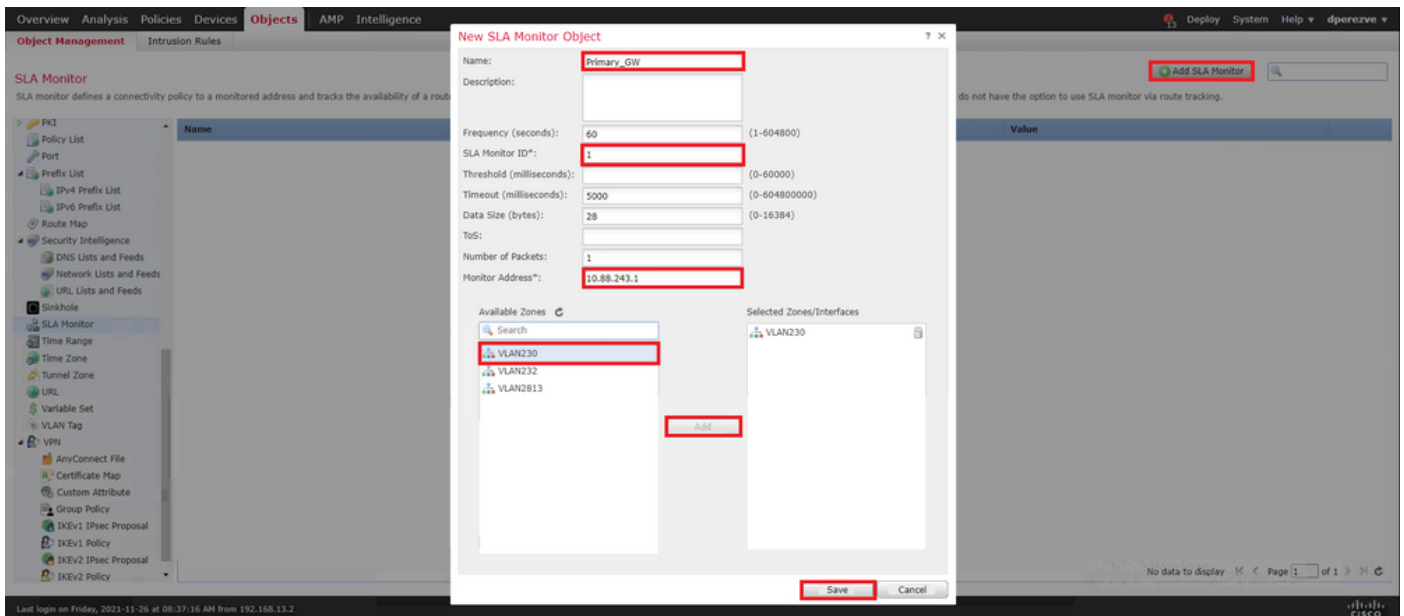
Selecteer de **Add SLA Monitor** voorwerp.

In het **New SLA Monitor** definieert u een naam samen met een identificatie voor de SLA-handeling, het IP-adres voor het apparaat dat moet worden bewaakt (in dit geval de primaire gateway) en de interface of zone waardoor het apparaat bereikbaar is.

Bovendien is het ook mogelijk om de timeout en de drempel aan te passen. Klik **Save**.

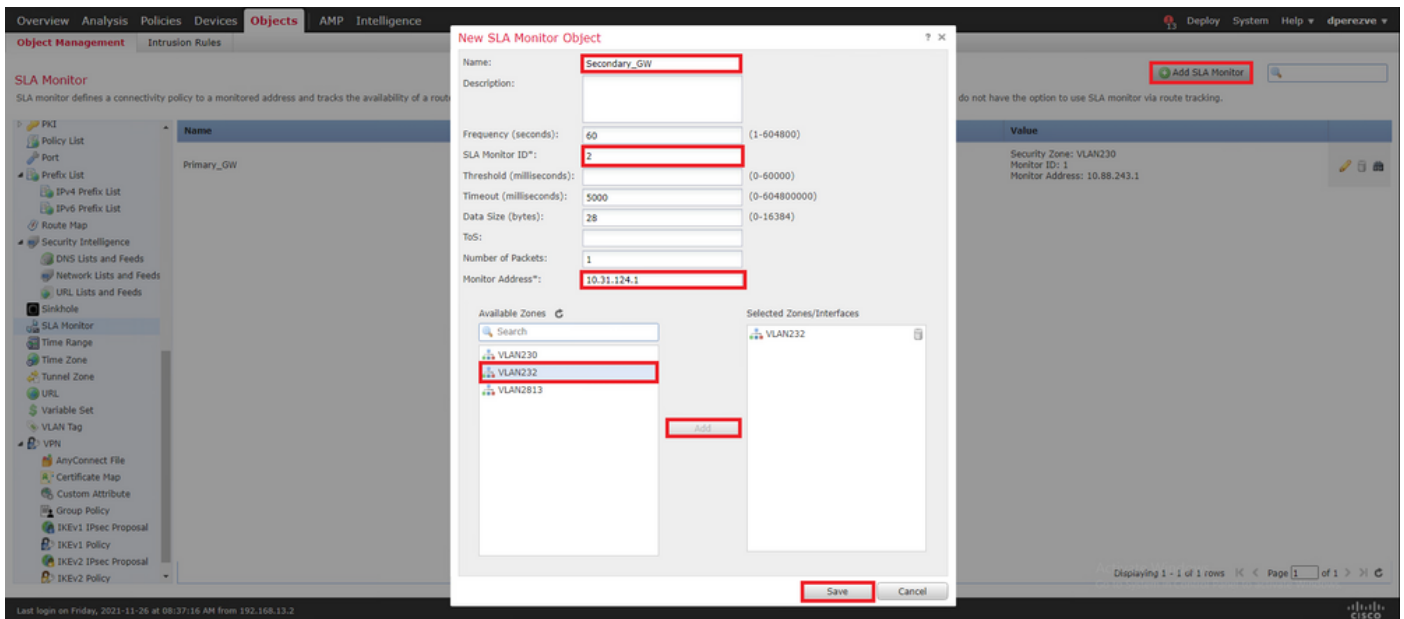
Opmerking: FTD ondersteunt maximaal 2000 SLA-bewerkingen. De waarden voor de SLA-ID variëren van 1 tot 2147483647.

Opmerking: Als de waarden voor time-out en drempelwaarden niet zijn gespecificeerd, gebruikt FTD de standaardtimers: 5000 miliseconden per geval.

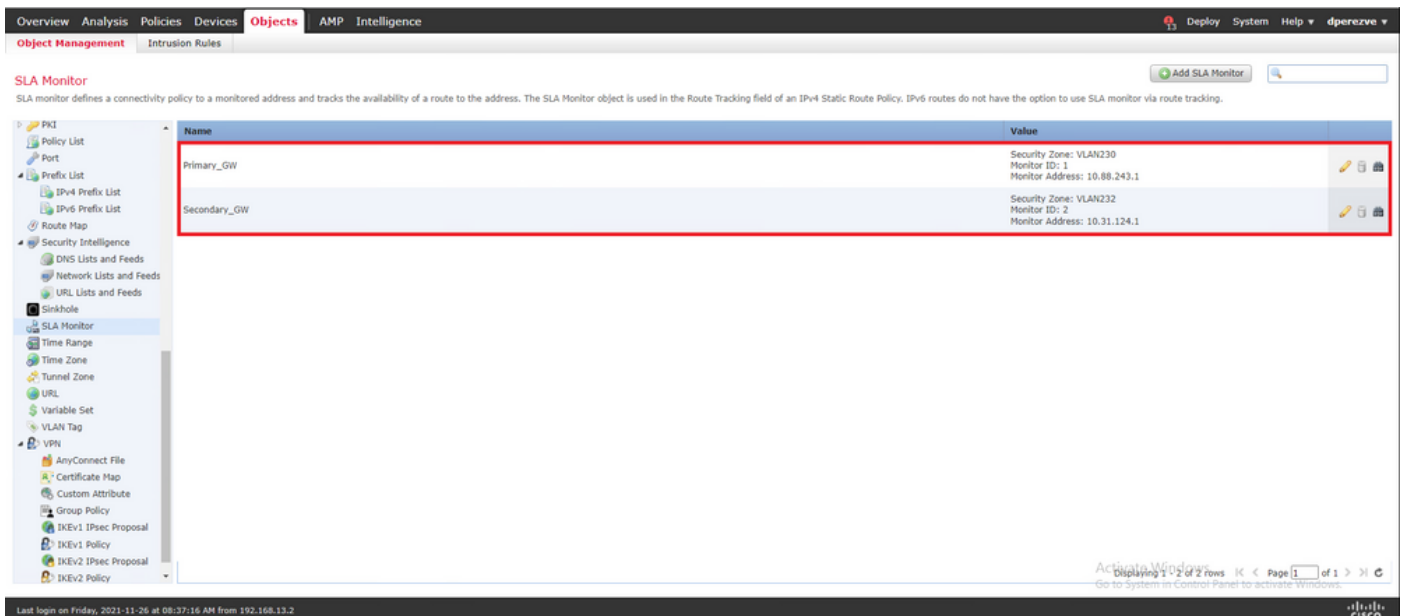


Selecteer de **Add SLA Monitor** knop nogmaals om een tweede object te maken, dit keer voor de Gateway in het back-upcircuit.

Vul het nieuwe object met de juiste informatie, zorg ervoor dat de SLA-id anders is dan de voor de primaire gateway gedefinieerde id en sla de wijzigingen op.



De twee objecten moeten aan de lijst worden toegevoegd.

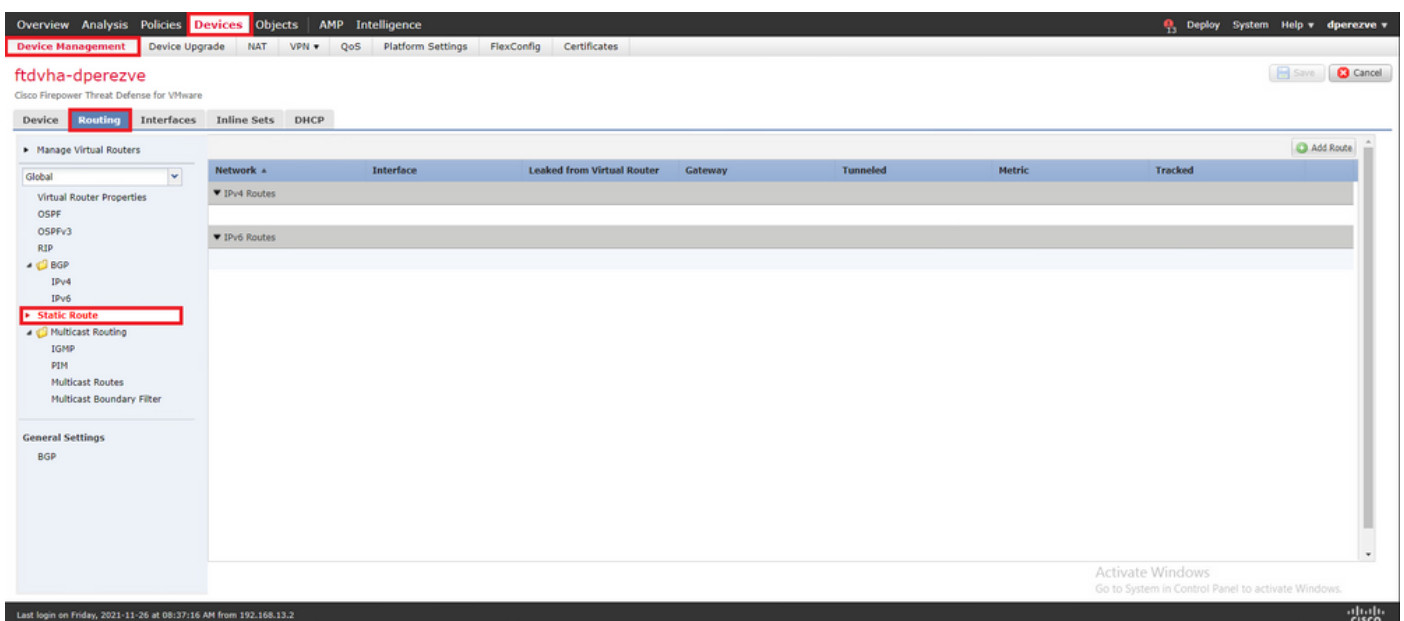


Step 4. Configureer statische routes met routespoor

Zodra de IP SLA-objecten zijn gemaakt, definieert u een route voor elke gateway en koppelt u deze aan de SLA's.

Deze routes bieden niet echt connectiviteit van binnen naar buiten (alle routing wordt uitgevoerd via PBR). In plaats daarvan zijn ze nodig om connectiviteit met de gateways via SLA's te volgen.

Om statische routes te configureren navigeert u naar **Devices > Device Management**, bewerk het FTD en selecteer **Static Route** in de inhoudsopgave binnen het **Routing** tabblad.

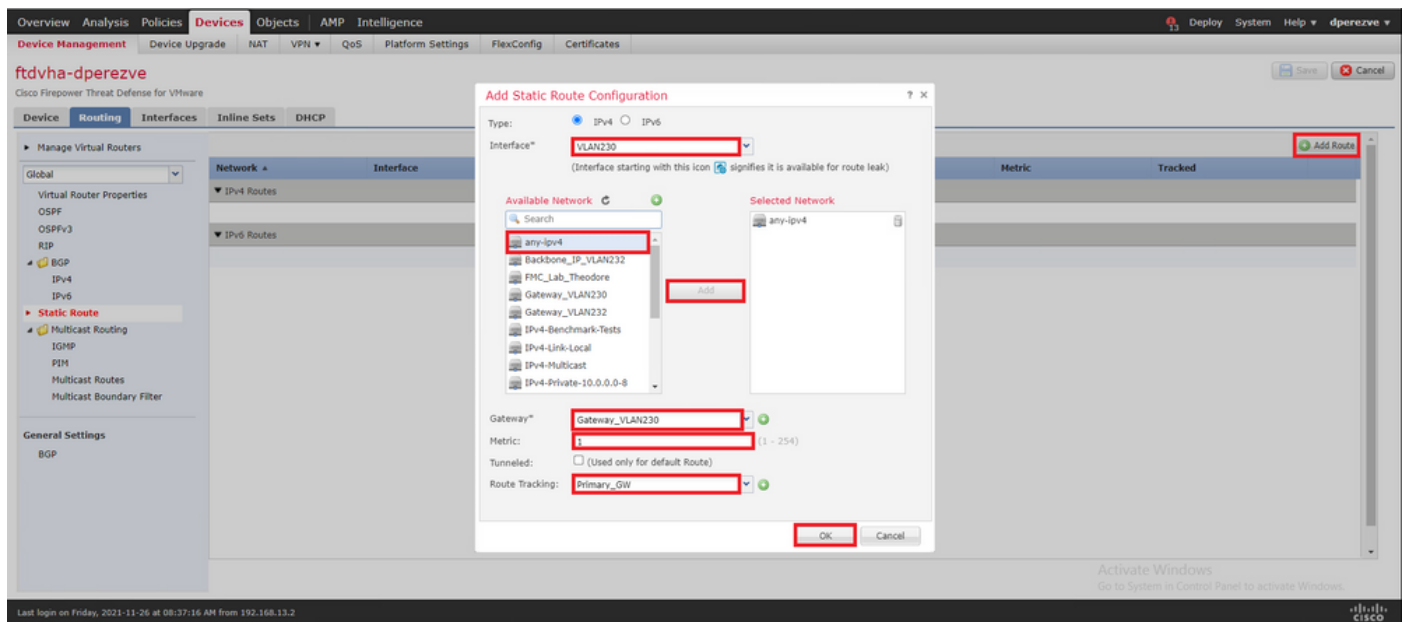


In het **Add Static Route Configuration** venster, in de **interfacedaling**, specificeert de naam voor de interface waardoor de primaire gateway bereikbaar moet zijn.

Selecteer vervolgens het doelnetwerk en de primaire gateway in het **Gateway** naar beneden.

Specificeer een metriek voor de route en in **Route Track** vervolgkeuzelijst en selecteer het SLA-object voor de primaire gateway die in **Stap 3** is gemaakt.

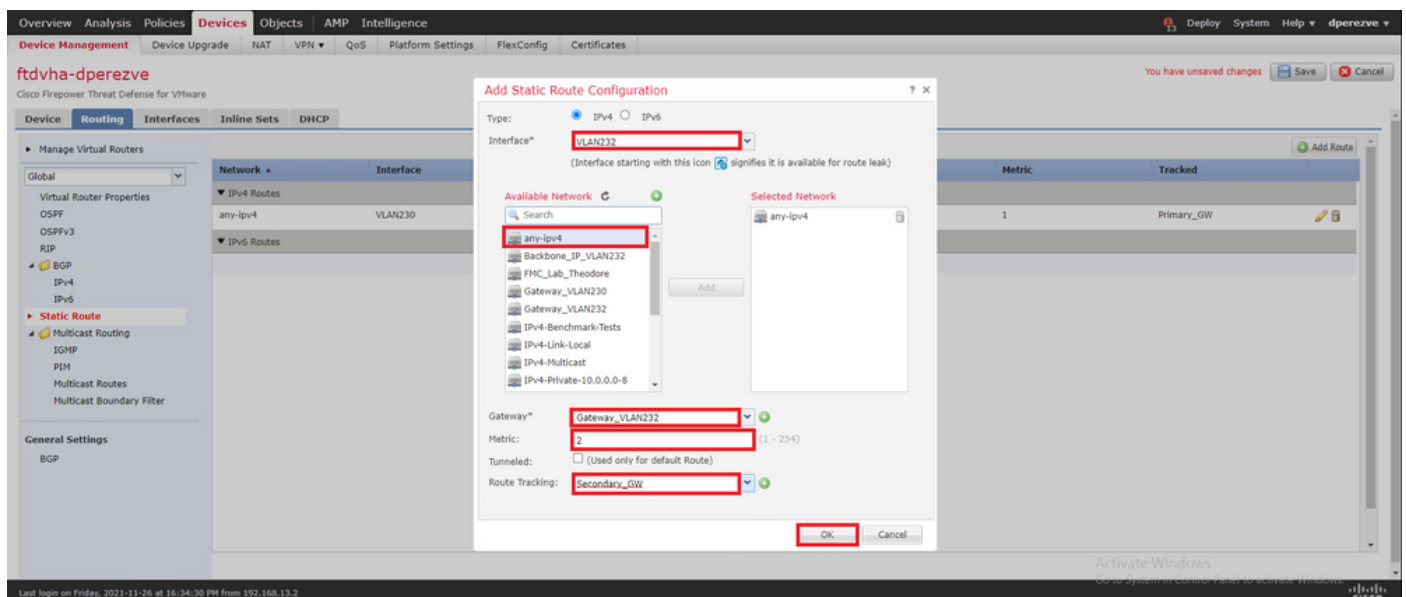
Klik op **OK** om de nieuwe route toe te voegen.



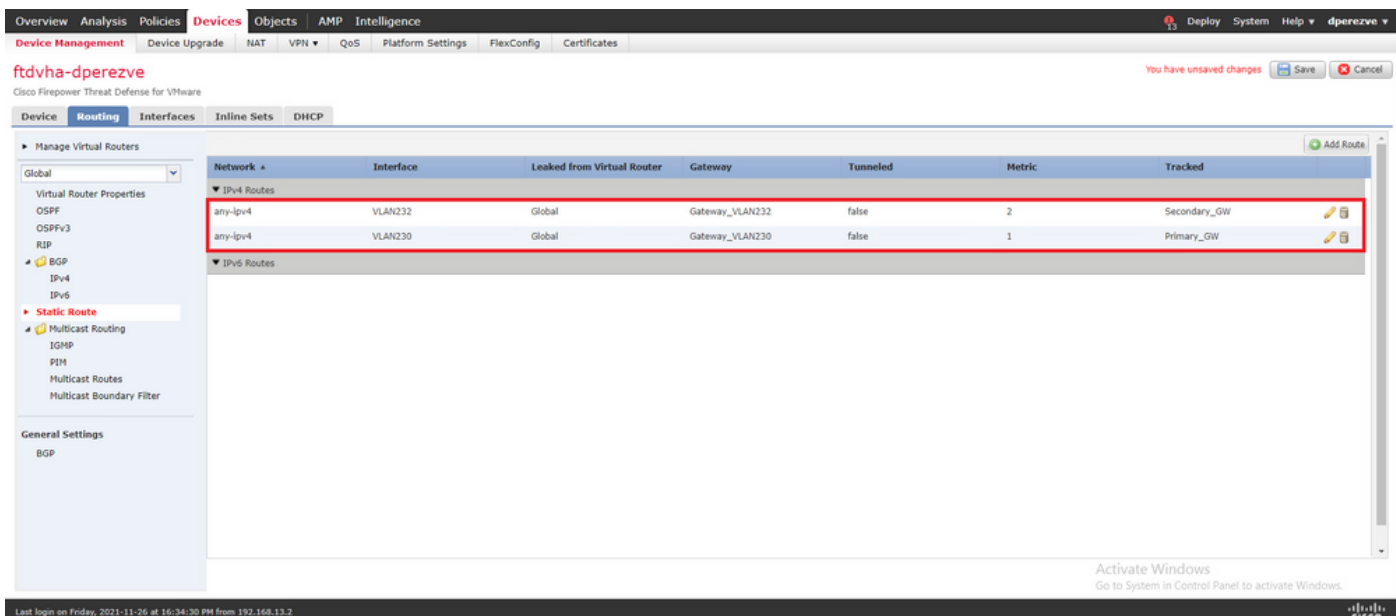
Er moet een tweede statische route worden geconfigureerd voor de back-upgateway.

Klik **Add Route** om een nieuwe statische route te bepalen.

Vul het **Add Static Route Configuration** met de informatie voor de back-upgateway en ervoor zorgen dat de metriek voor deze route hoger is dan die in de eerste route is geconfigureerd.



De twee routes moeten aan de lijst worden toegevoegd.

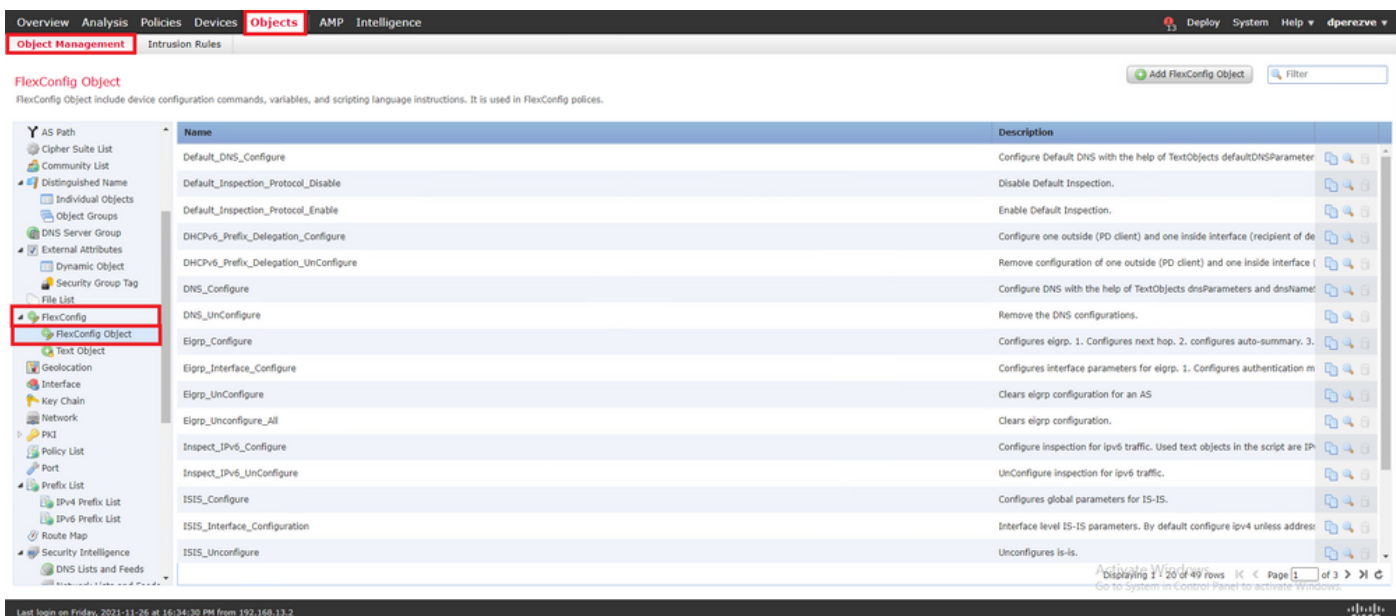


Stap 5. PBR FlexConfig-object configureren

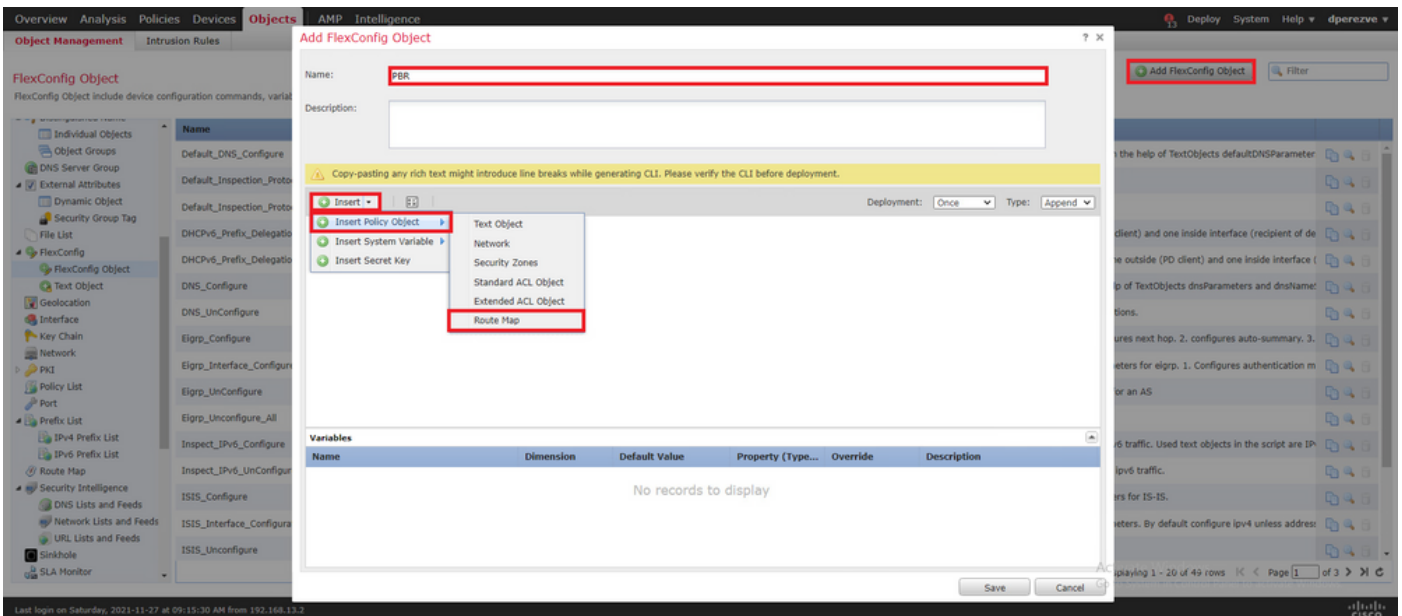
Schakel SLA's in onder de routekaart die voor PBR wordt gebruikt en pas deze routekaart toe in een interface van de FTD.

Tot nu toe is routekaart alleen gekoppeld aan de toegangslijst die de bijbehorende criteria definieert. De laatste aanpassingen worden echter niet ondersteund via FMC GUI, zodat een FlexConfig-object nodig is.

U kunt als volgt het object PBR FlexConfig definiëren: **Objects > Object Management** en selecteer **FlexConfig Object** in het kader **FlexConfig** categorie in de inhoudsopgave.

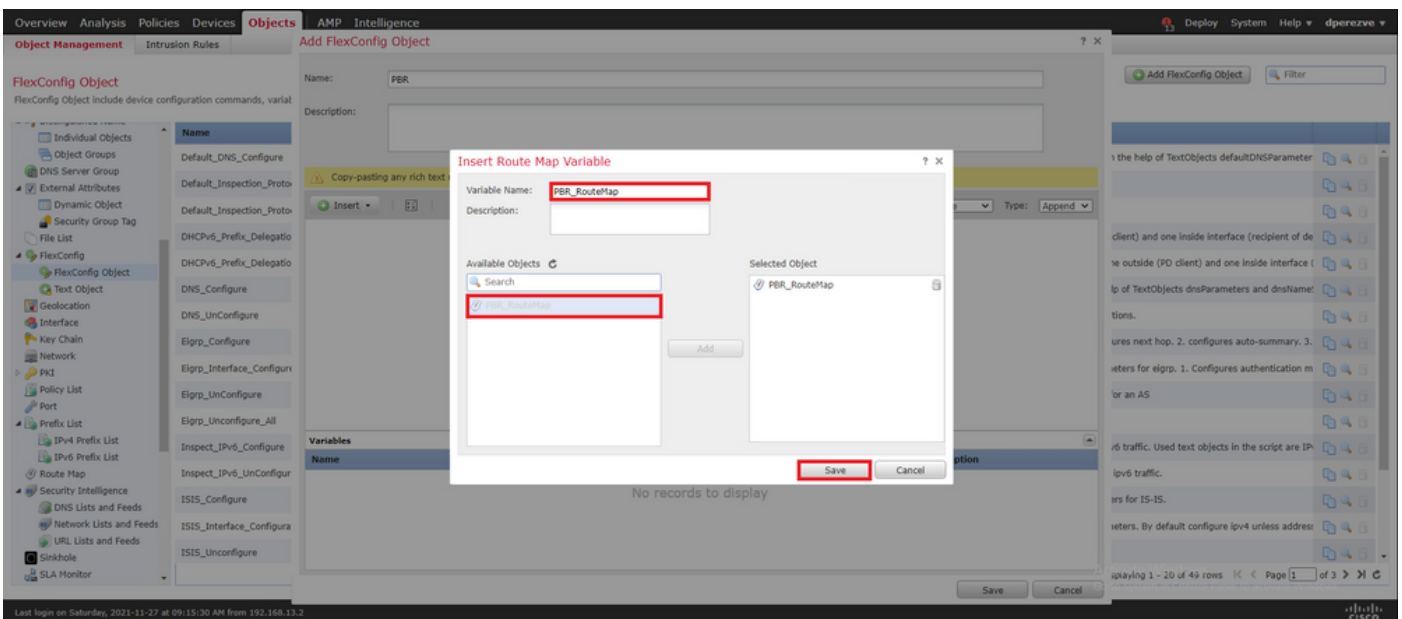


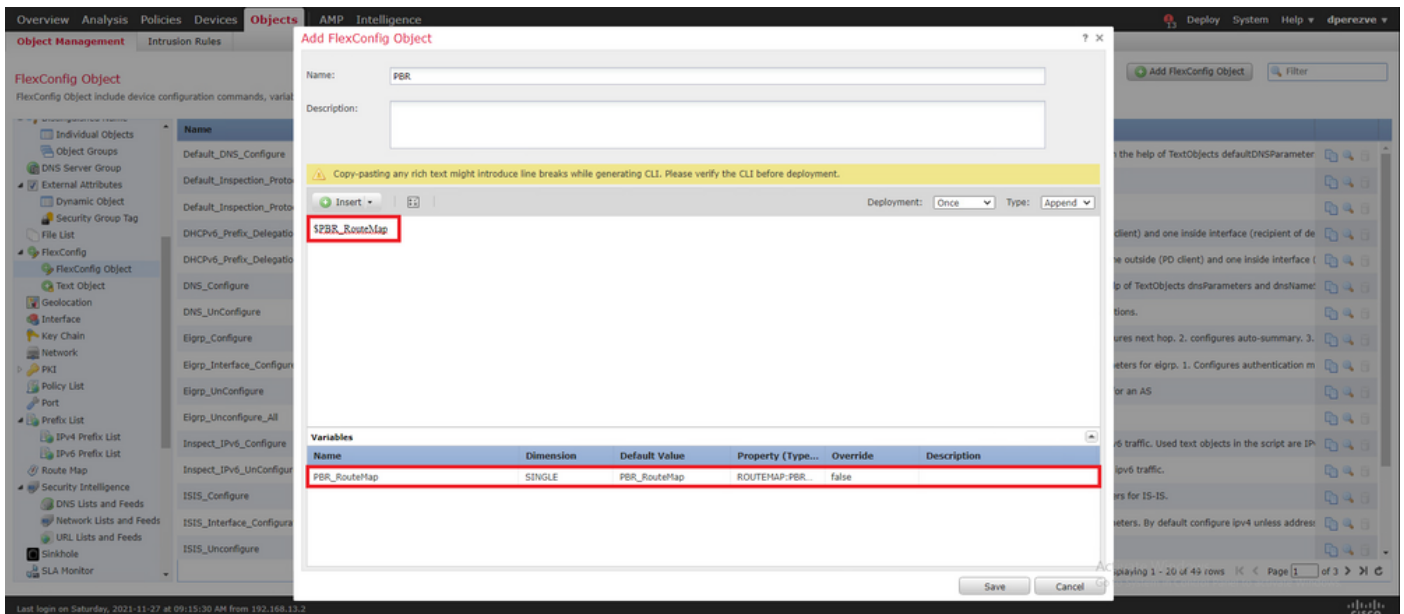
Selecteer de **Add FlexConfig Object** knop. In het **Add FlexConfig Object** venster een naam toewijzen en navigeren naar **Insert > Insert Policy Object > Route Map**.



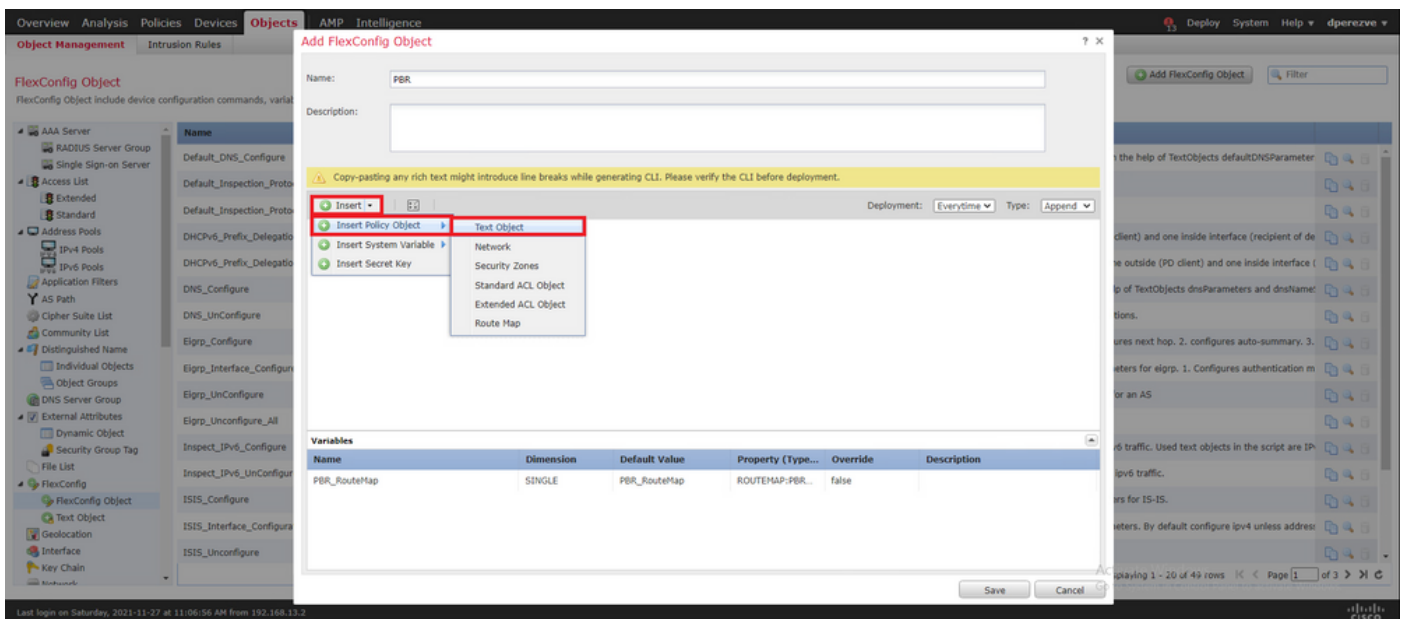
In het Insert Route Map Variable venster, een naam voor de variabele toewijzen en het PBR object selecteren dat in Stap 2 gemaakt is.

Klik **save** om de routekaart toe te voegen als deel van het object FlexConfig.



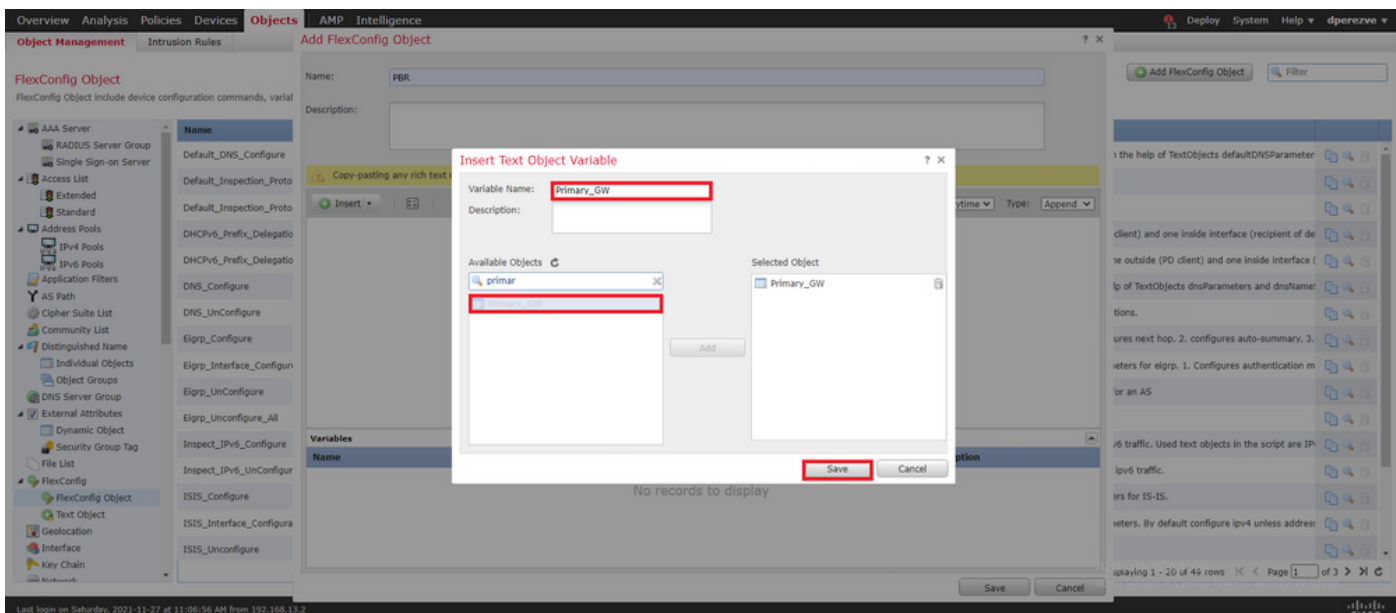


Naast de routekaartvariabele moeten we de FlexConfig tekstobjecten toevoegen die elke gateway vertegenwoordigen (gedefinieerd in stap 3). In het Add FlexConfig Object venster navigeren naar **Insert > Insert Policy Object > Text Object**.

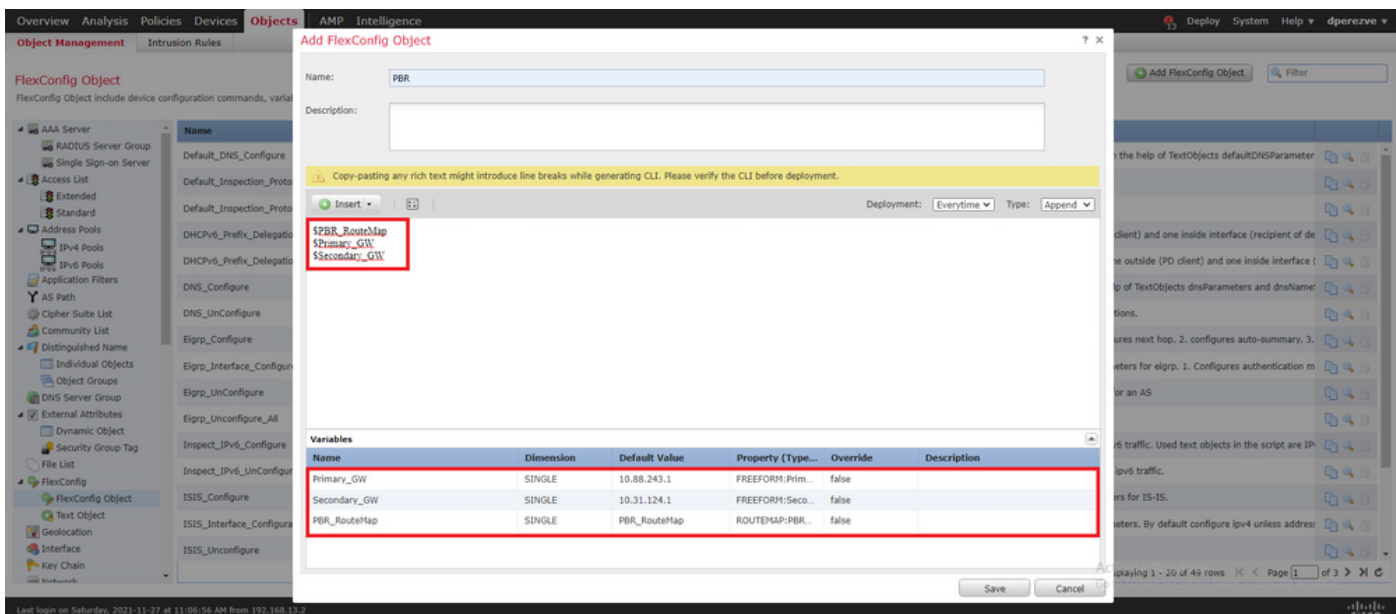


In het **Insert Text Object Variable** venster een naam voor de variabele toewijzen en het tekstobject selecteren dat de primaire gateway vertegenwoordigt die in Stap 3 is gedefinieerd.

Klik **save** om deze toe te voegen aan het object FlexConfig.



Herhaal deze laatste stappen voor back-upgateway. Aan het eind van het proces moeten de twee variabelen worden toegevoegd aan het object FlexConfig.



De syntaxis voor de PBR-configuratie moet gelijk zijn aan die in Cisco ASA. Het volgnummer voor de routekaart moet overeenkomen met het nummer dat in Stap 2 (in dit geval 10) is geconfigureerd, evenals met de SLA-ID's.

Om PBR te configureren om de beschikbaarheid van de volgende hop te controleren, drukt u op `set ip next-hop verify-availability` de opdracht moet worden gebruikt.

De routekaart moet op de binneninterface worden toegepast, in dit geval VLAN2813. Gebruik `policy-route route-map` bevel onder de interfaceconfiguratie.

Klik **save** wanneer de configuratie is voltooid.

Add FlexConfig Object

Name: PBR

Description:

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

Insert Deployment: Type:

```

route-map PBR_RouteMap permit 10
set ip next-hop verify-availability #Primary_GW 1 track 2
set ip next-hop verify-availability #Secondary_GW 2 track 1
track 1 ip 2 reachability
track 2 ip 1 reachability
interface gigabitEthernet0/1
policy-map PBR_RouteMap

```

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	

Save Cancel

Het object FlexConfig moet aan de lijst worden toegevoegd.

FlexConfig Object

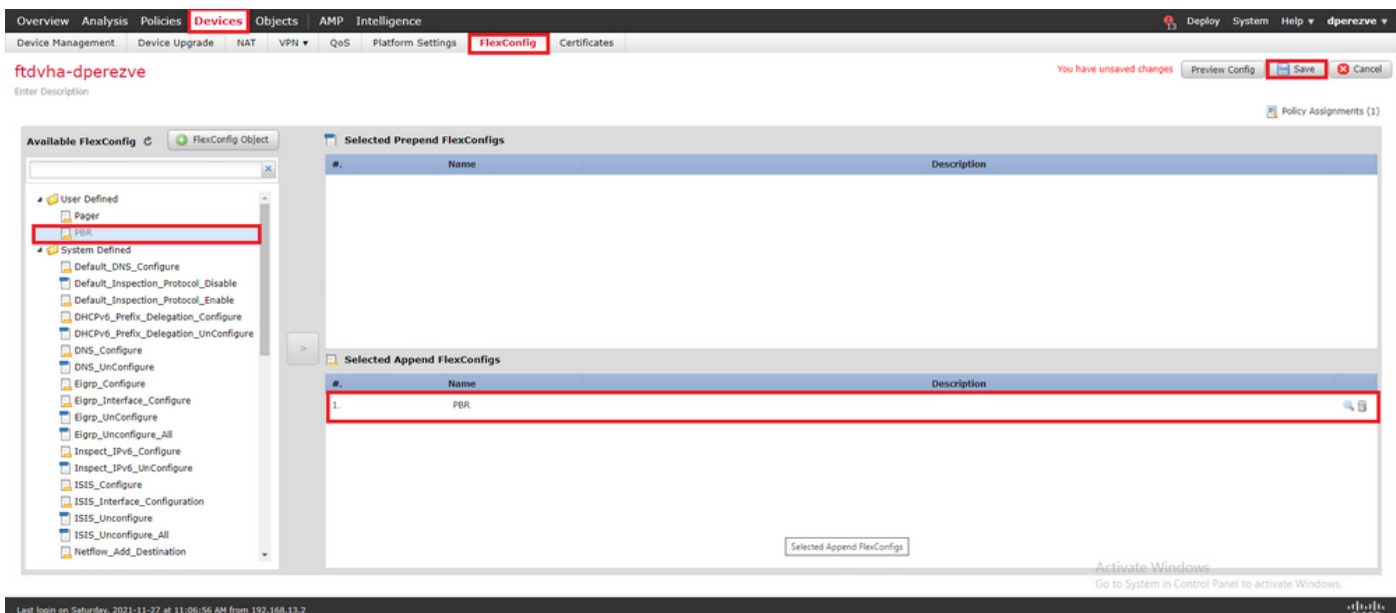
FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

Name	Description
PBR	

Stap 6. PBR FlexConfig-object toewijzen aan FlexConfig-beleid

Naar navigeren **Devices > FlexConfig** en bewerk het FlexConfig-beleid.

Selecteer het object PBR FlexConfig in **Available FlexConfig** inhoudsopgave, wijzigingen opslaan en wijzigingen in FTD implementeren.



Verifiëren

Nadat de implementatie is voltooid, moet FTD regelmatig een ICMP-echoverzoek verzenden naar de bewaakte apparaten om de bereikbaarheid te garanderen. Ondertussen moet een gevolgde route naar de primaire gateway aan de routingstabel worden toegevoegd.

```
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
```

Omdat de connectiviteit met de primaire gateway omhoog is, moet het verkeer van interne Subnet (VLAN2813) door de primaire ISP kring worden verstuurd.

```
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
```

Als de FTD geen echoantwoord ontvangt van de primaire gateway binnen de drempeltimer die in het SLA Monitor-object is gespecificeerd, wordt de host als onbereikbaar beschouwd en als down gemarkeerd. De getraceerde route naar primaire gateway wordt ook vervangen door een getraceerde route naar back-uppeer.

```
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
```

Informatiebericht 622001 wordt gegenereerd elke keer dat FTD een getraceerde route toevoegt of verwijdert uit een routingstabel.

```
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
```

Nu, moet al verkeer van VLAN2813 door de reservelSP kring worden verstuurd.

```
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=0xl46laf9c3320, 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=0xl46laff02da0, 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=0xl461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0xl46183cf8380, 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=0xl46170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0xl46170d413f0, 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=0xl46170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0xl46laf306740, 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=0xl46laf9c3320, 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=0xl46laff02da0, 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=0xl461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0xl46183cf8380, 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=0xl46170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0xl46170d413f0, 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=0xl46170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0xl46laf306740, 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=0xl46laf9c3320, 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
```

Problemen oplossen

Om te valideren welke PBR-vermelding in **interesting traffic** , open bevel **zuiveren beleid-route**.

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


Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.