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

Contents

Introduction

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

Contributed by Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

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

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

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

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

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

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

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

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

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

Configure

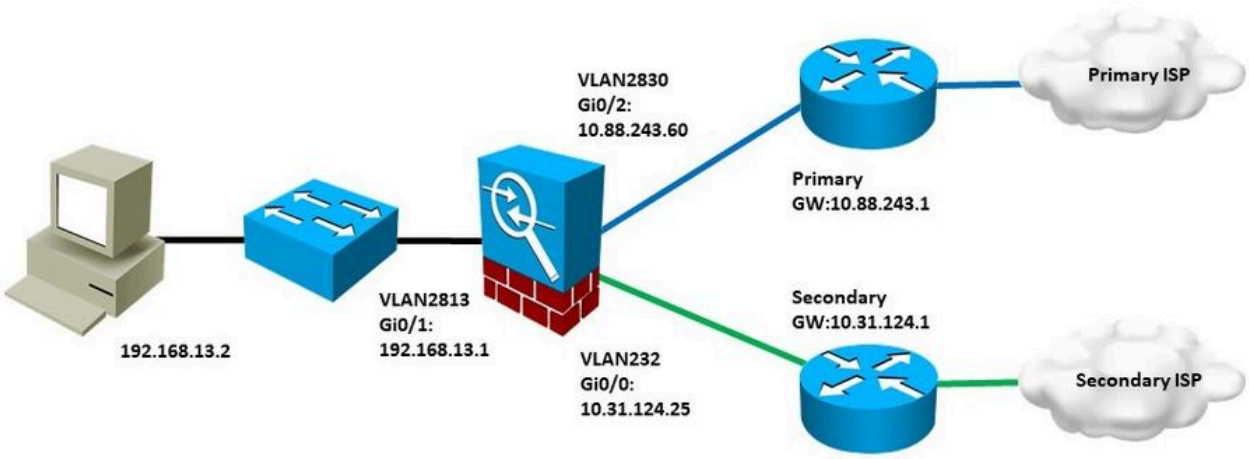
Network Diagram

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

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

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

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

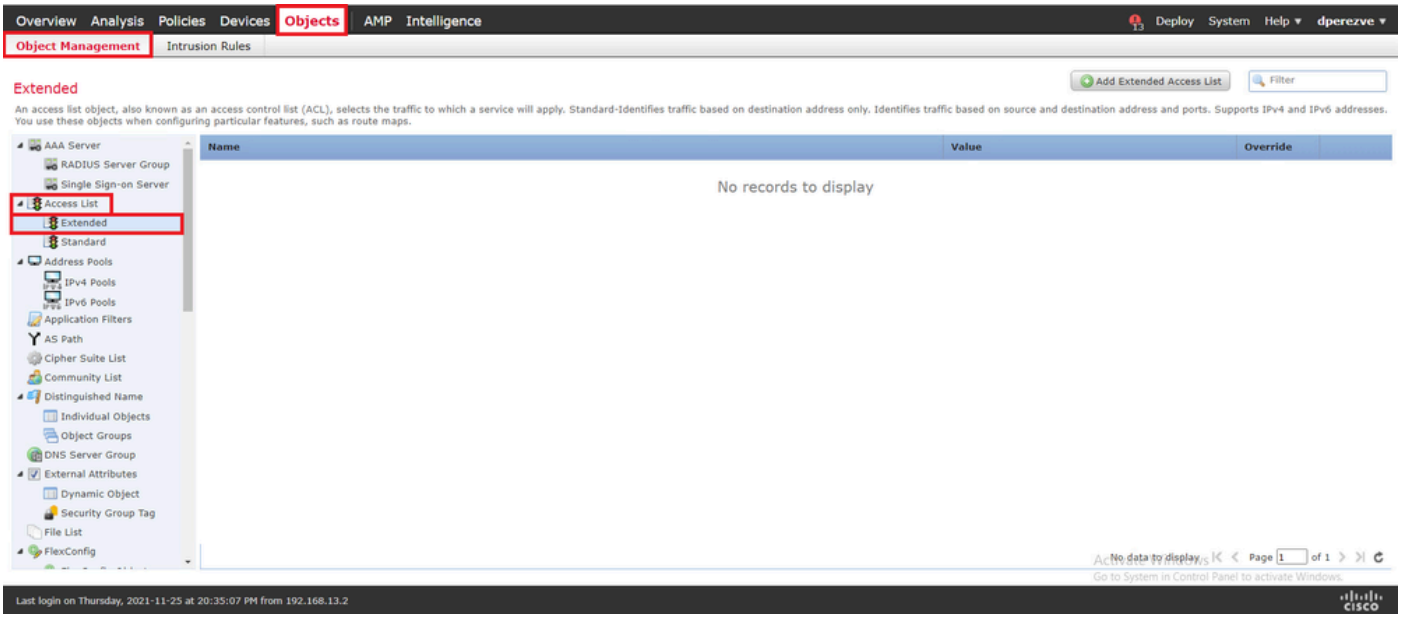


Configurations

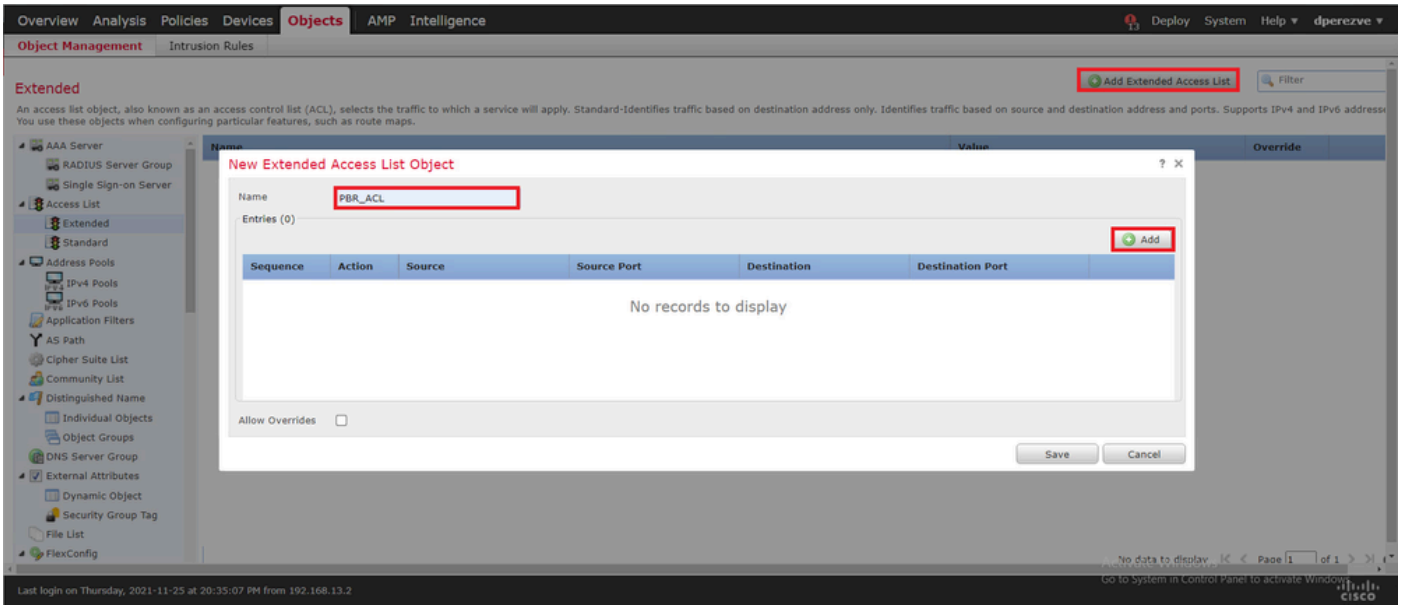
Step 1. Configure PBR Access List

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

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



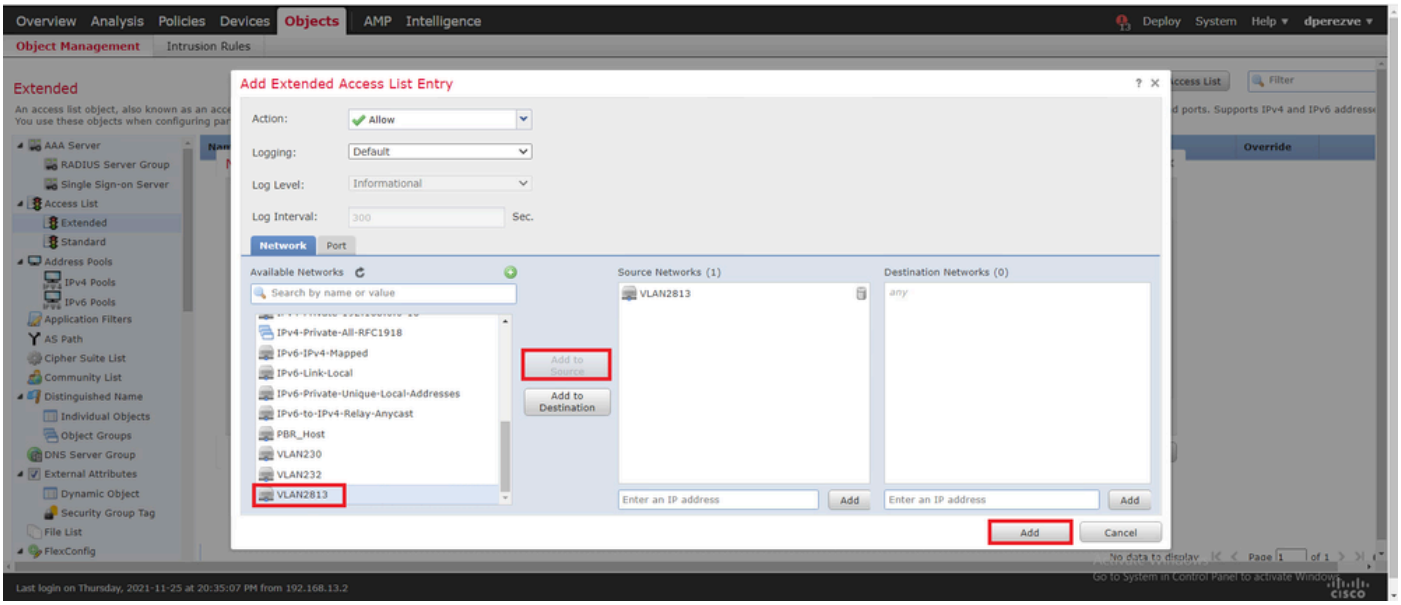
Click **Add Extended Access List .** In the **New Extended Access List Object** window, assign a name for the object, then select the **Add** button in order to start with access list configuration.



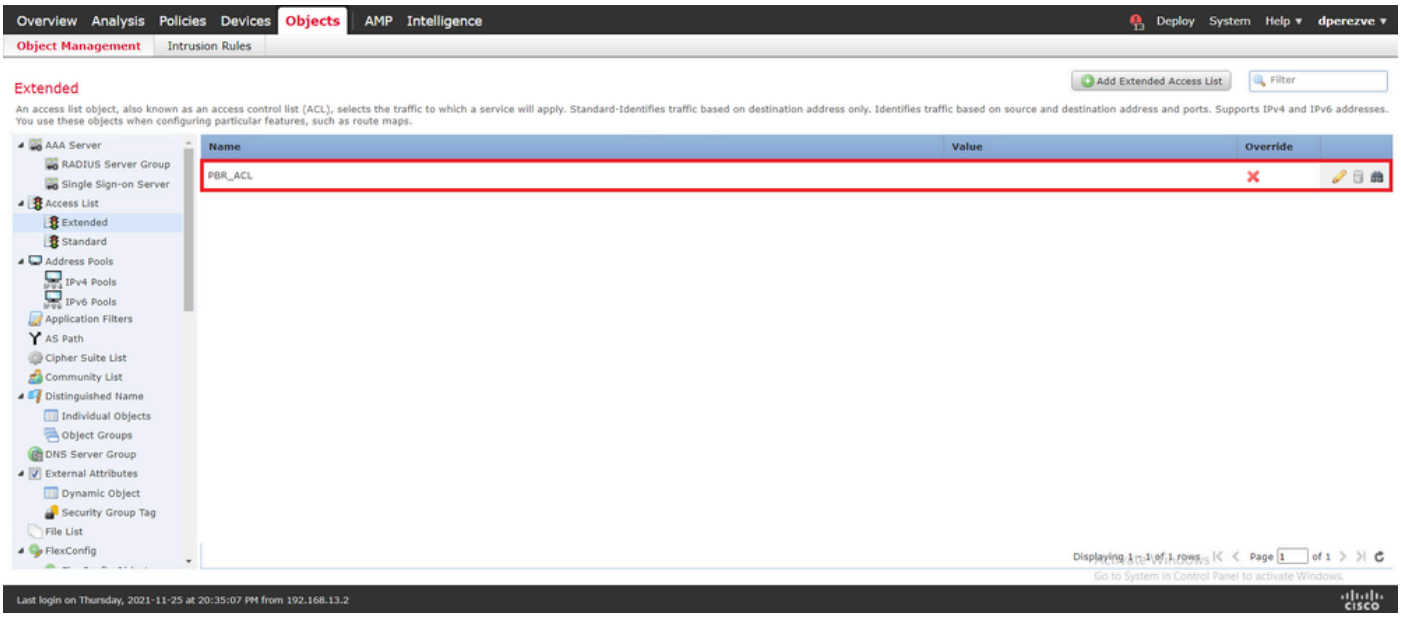
In the **Add Extended Access List Entry** window, select the object that represents the inside network, in this case VLAN2813.

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

Click **Add** to create the entry.



Click **Save** . The object must be added to object list.

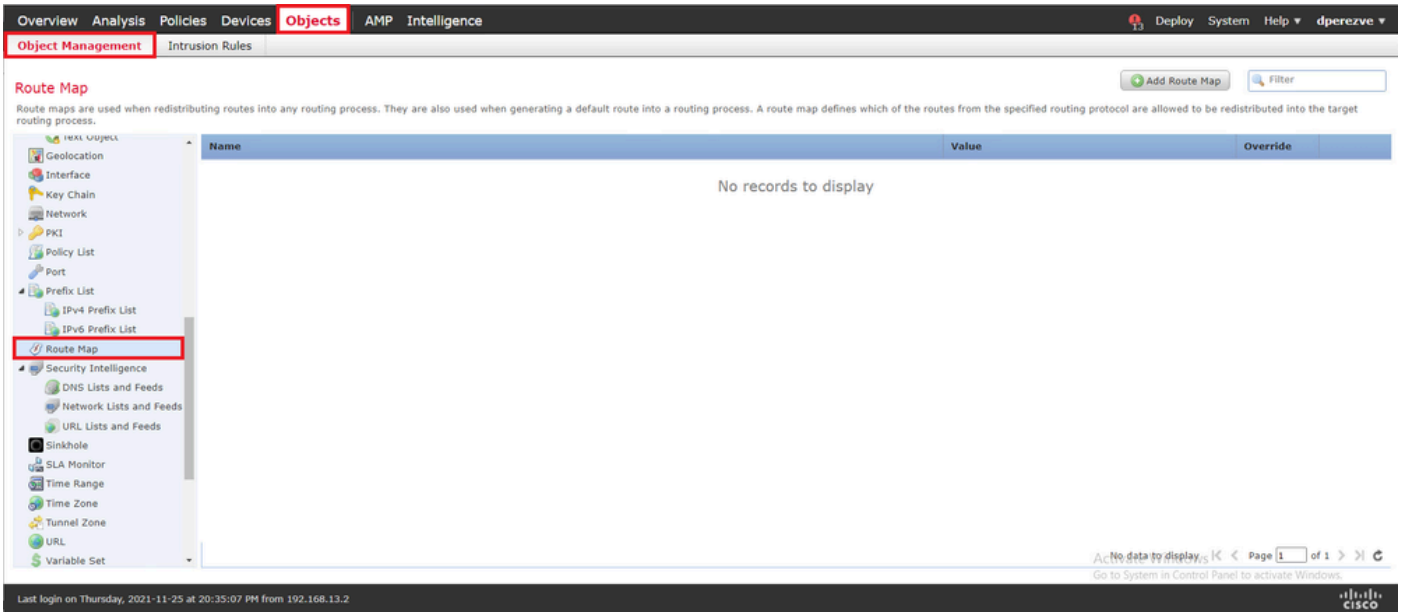


Step 2. Configure PBR Route Map

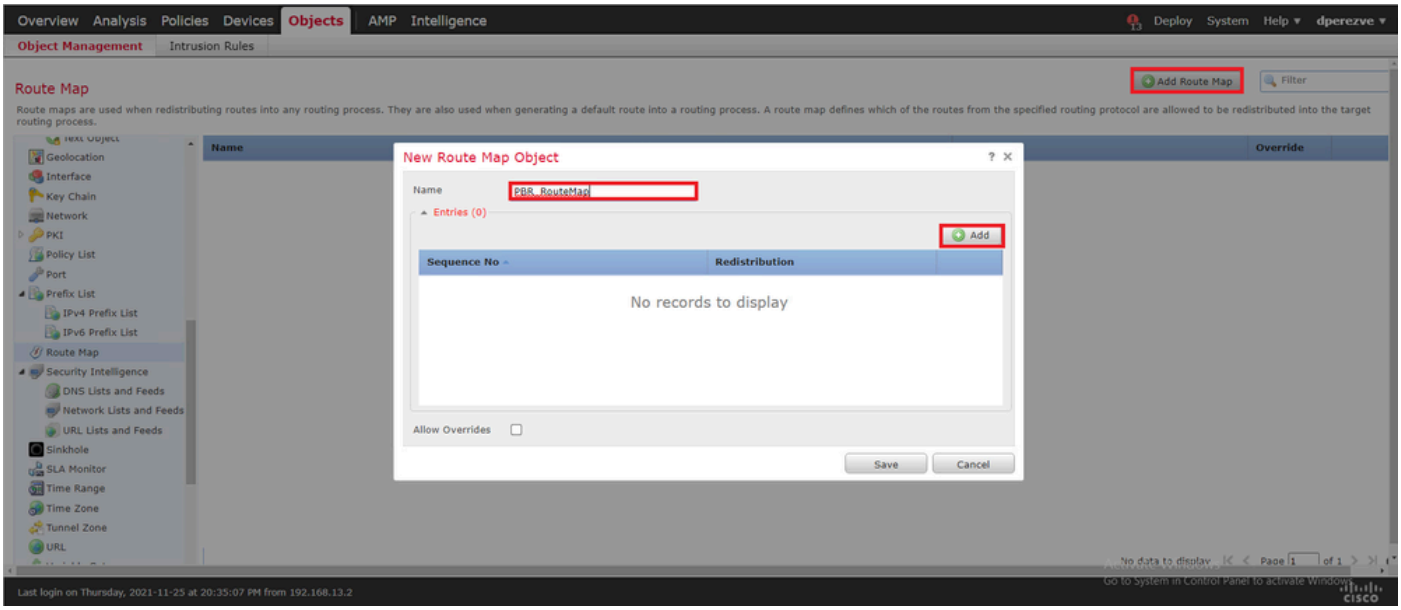
Once the PBR access list is configured, assign it to a route map. Route map evaluates traffic against the match clauses defined in the access list.

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

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



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



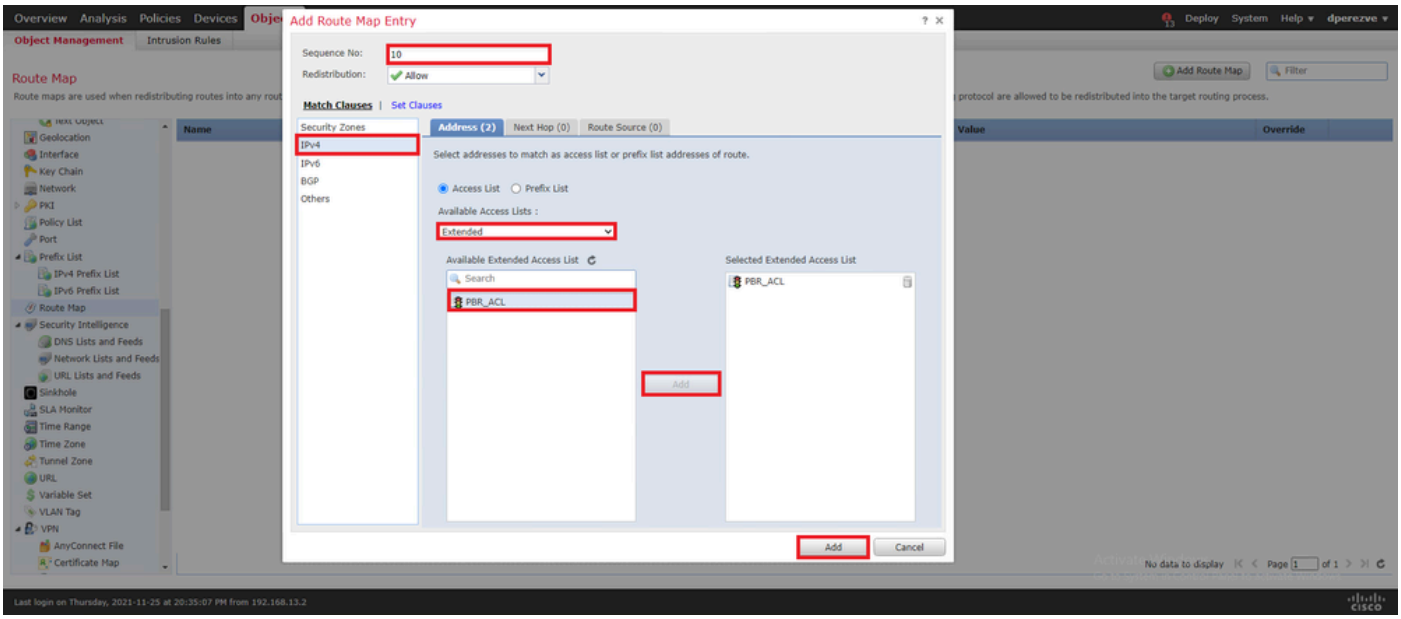
In the **Add Route Map Entry** window, define a sequence number for the position of the new entry.

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

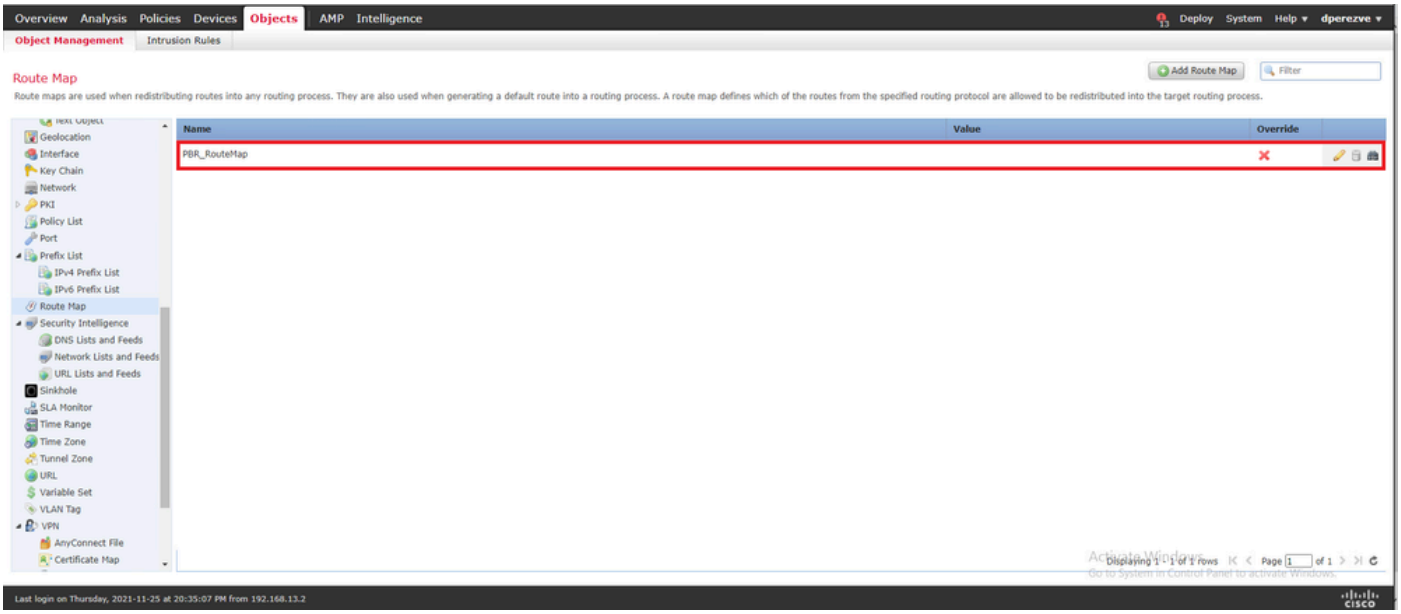
Select the access list object created in Step 1.

Click **Add** to create the entry.

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



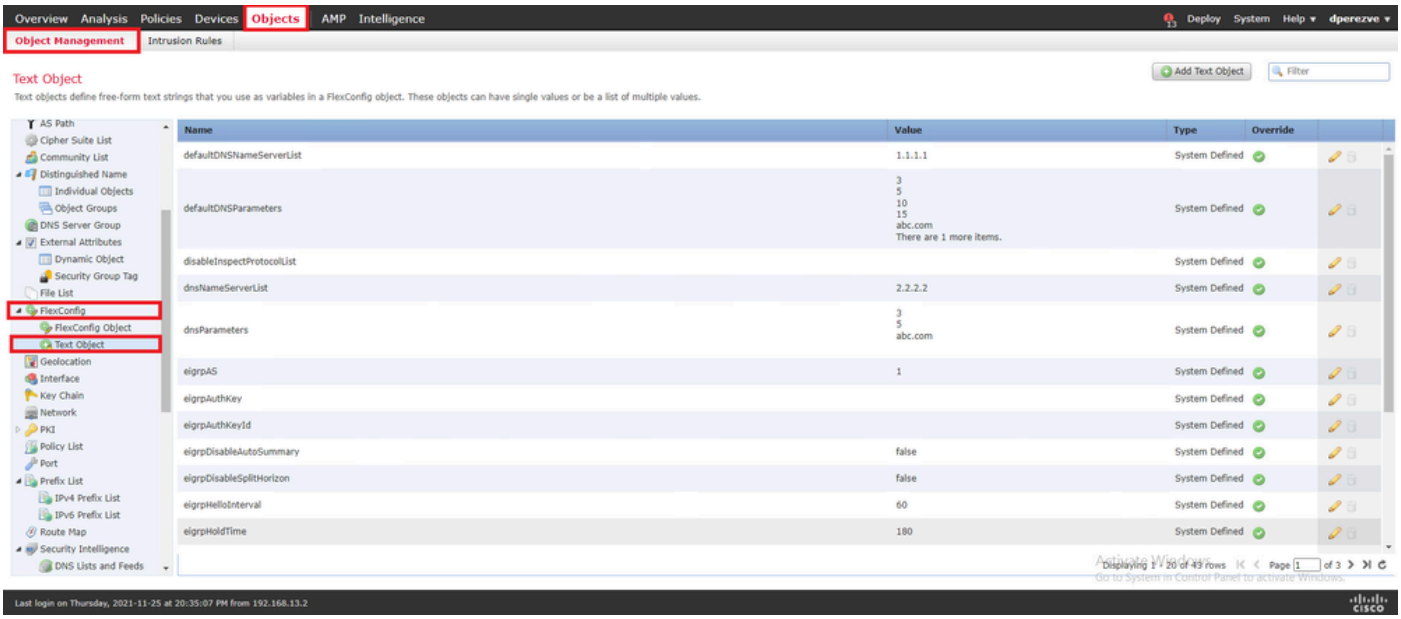
Click **Save** . Add the object to the object list.



Step 3. Configure FlexConfig Text Objects

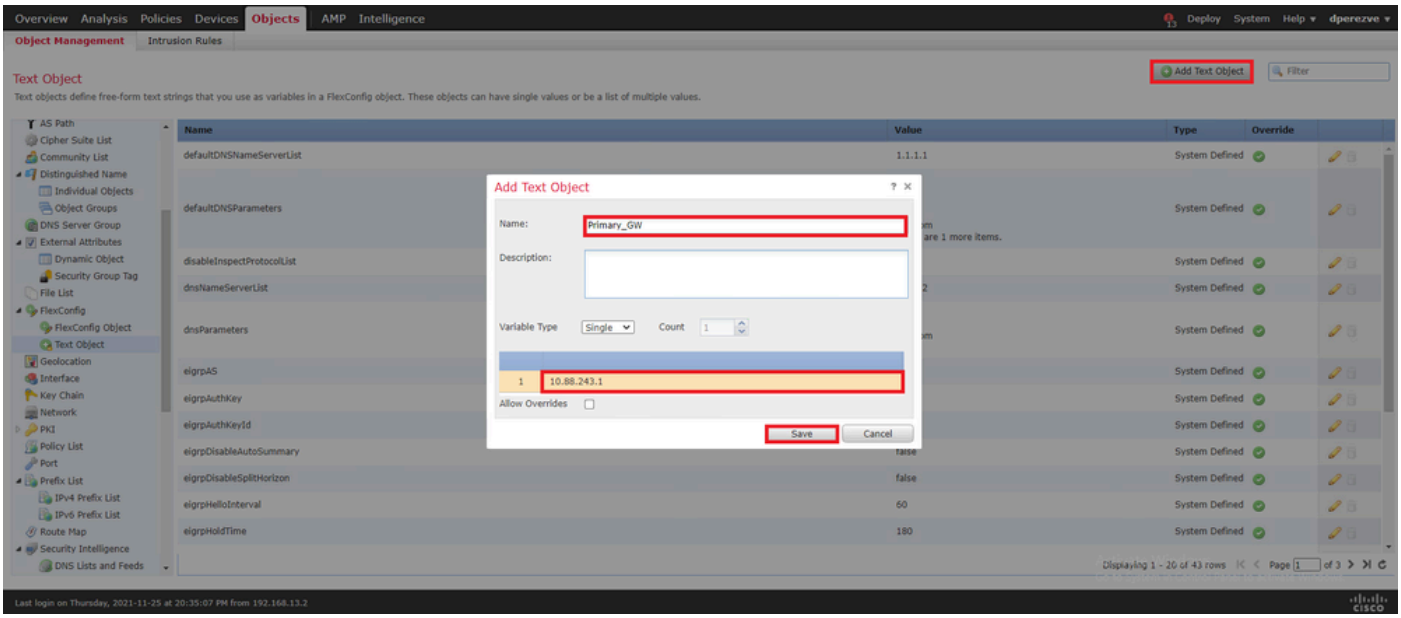
The next step involves the definition of FlexConfig text objects that represent default Gateways for each circuit. These text objects are used later in the configuration of FlexConfig object that associates PBR with SLAs.

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



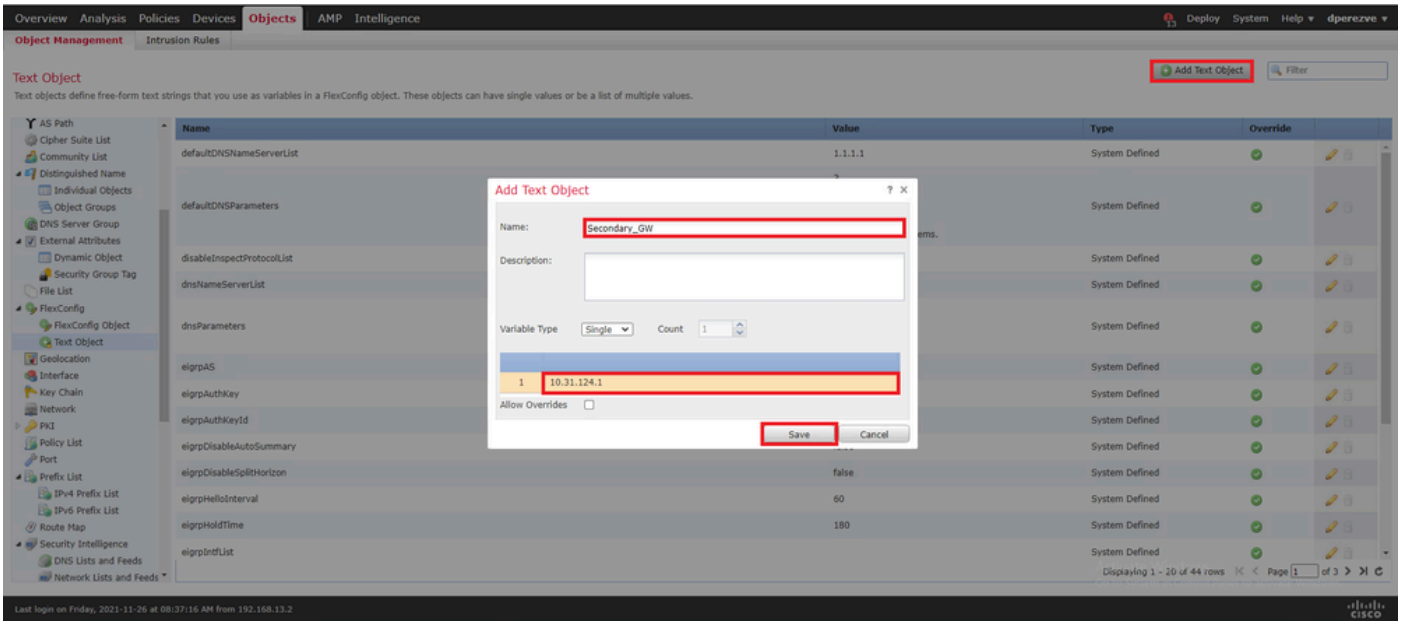
Click **Add Text Object** . In the **Add Text Object** window, assign a name for the object that represents the primary Gateway and specify the IPv4 address for this device.

Click **Save** to add the new object.

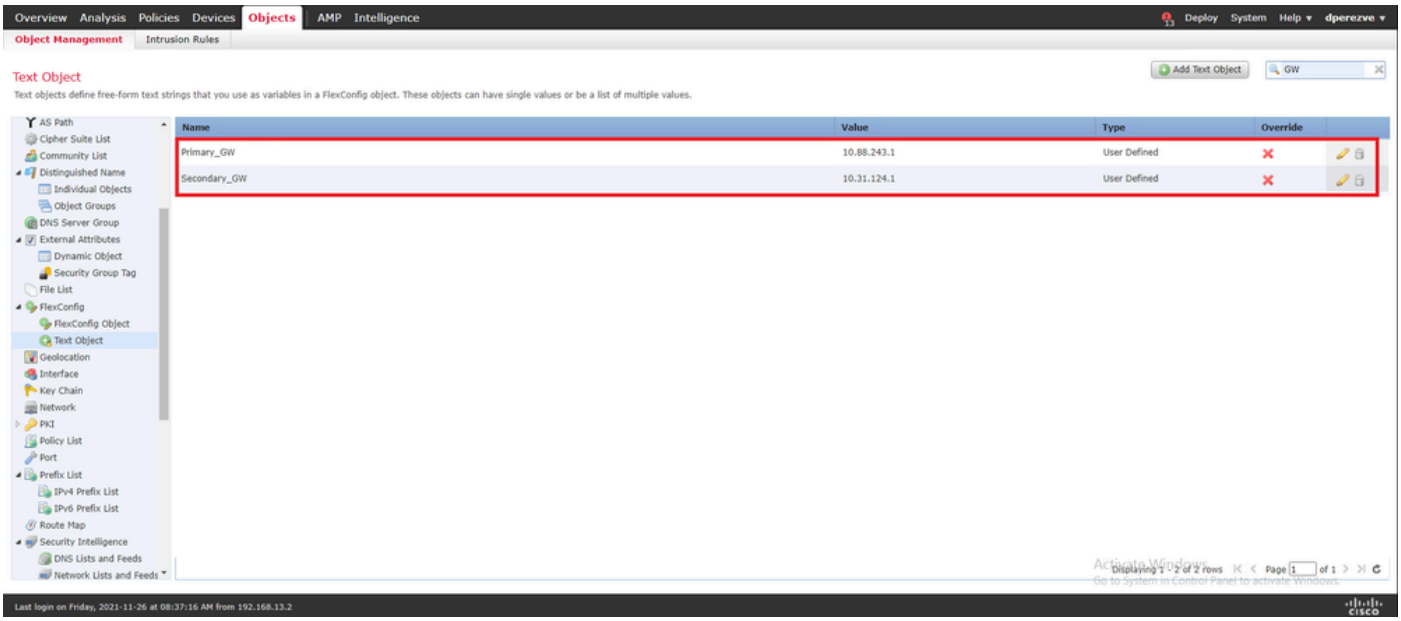


Click **Add Text Object** again to create a second object, this time for the Gateway on the backup circuit.

Fill the new object with the appropriate name and IP address and click **Save** .

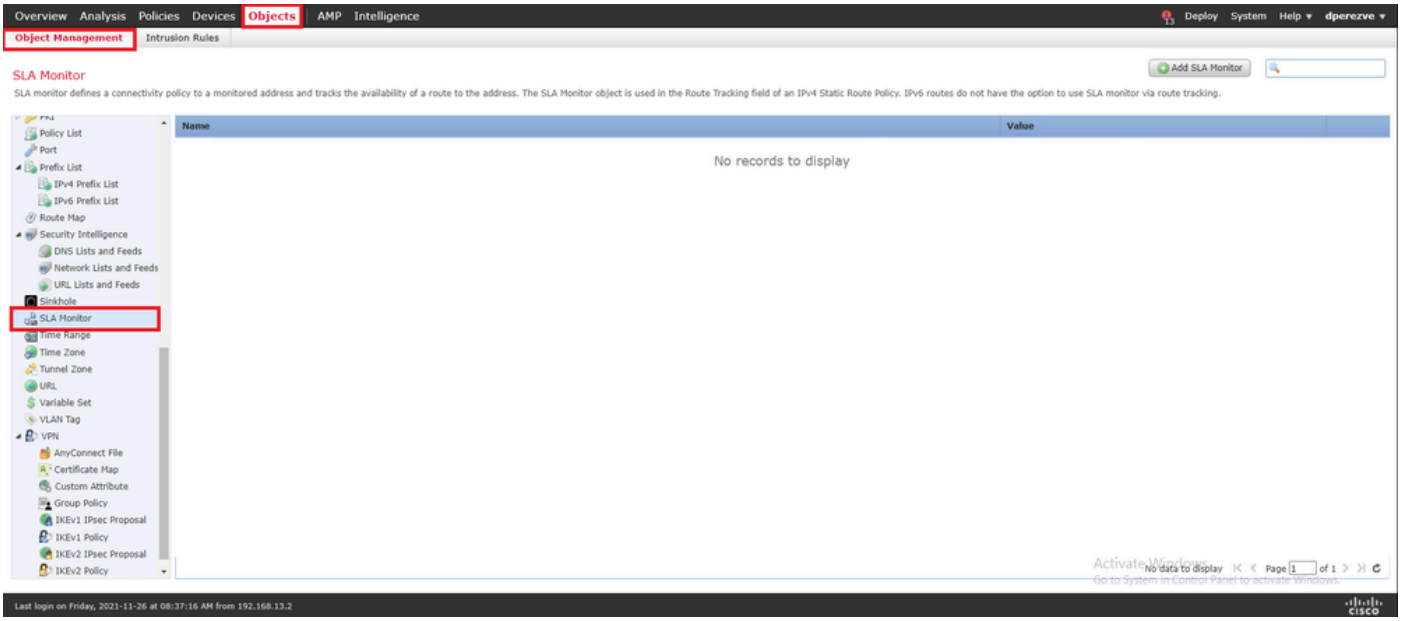


The two objects must be added to the list along with the default objects.



Step 4. Configure SLA Monitor

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



Select the **Add SLA Monitor** object.

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

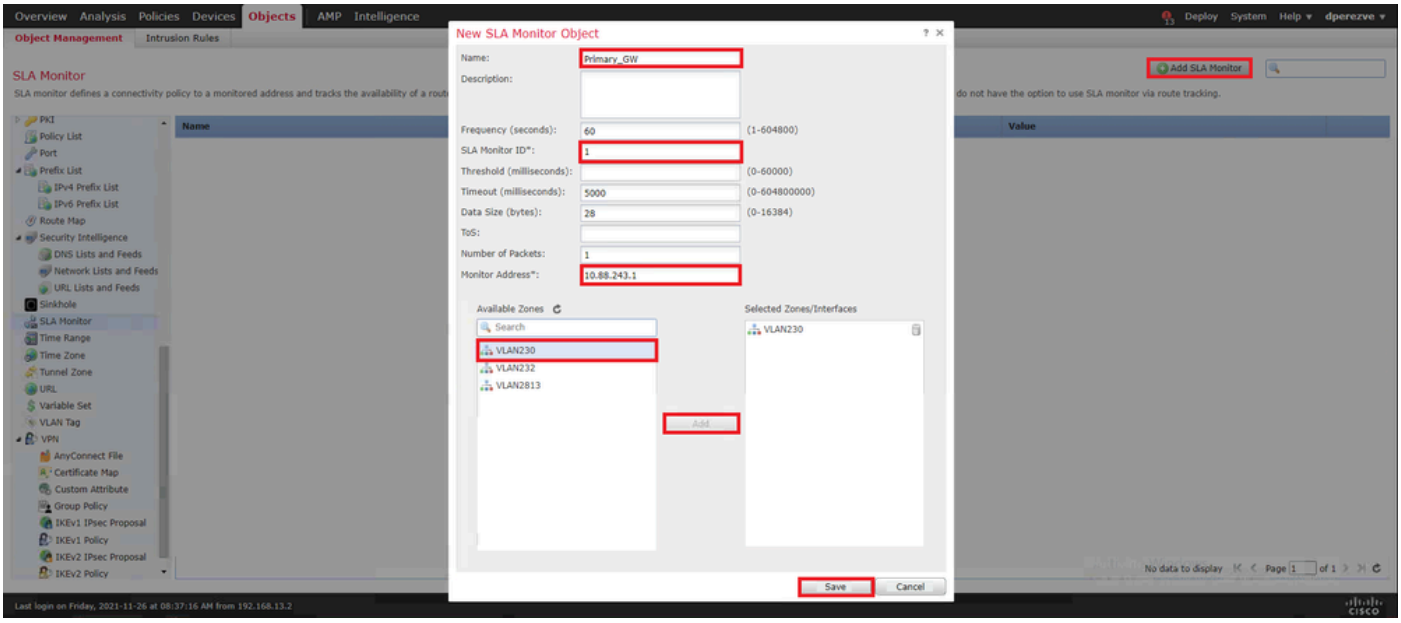
Additionally, it is also possible to adjust the timeout and threshold. Click **Save** .

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

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

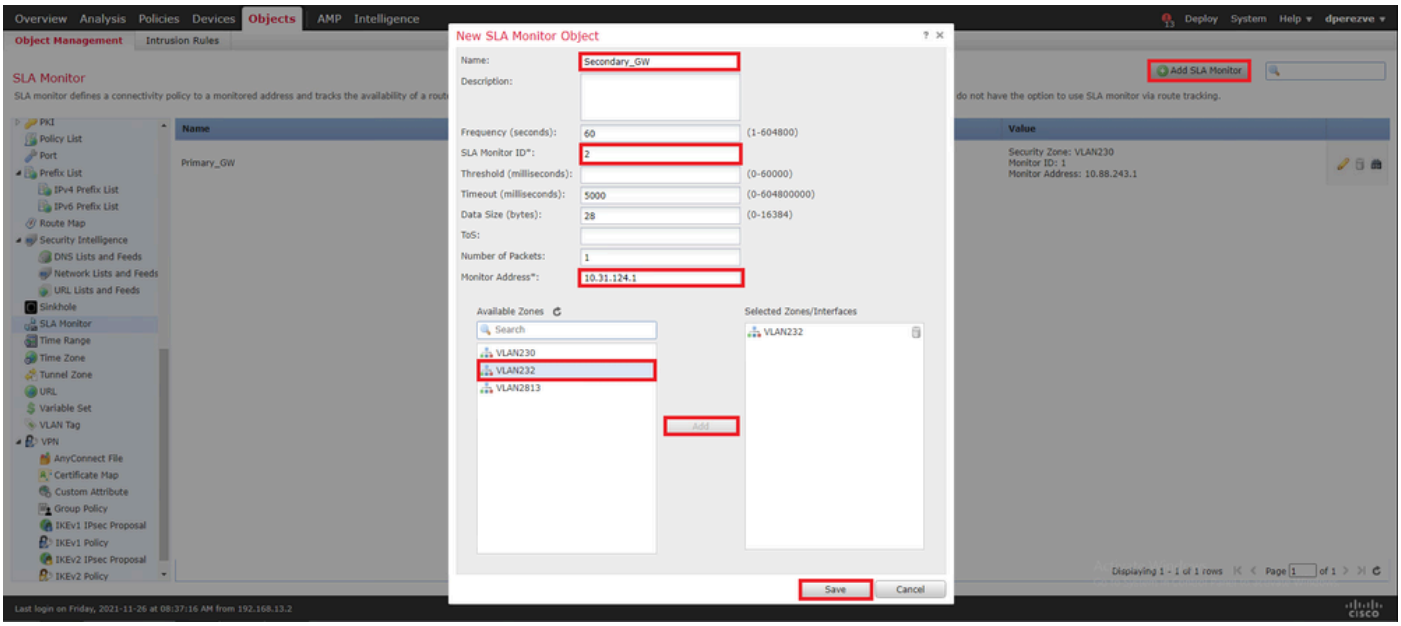
---

each case.

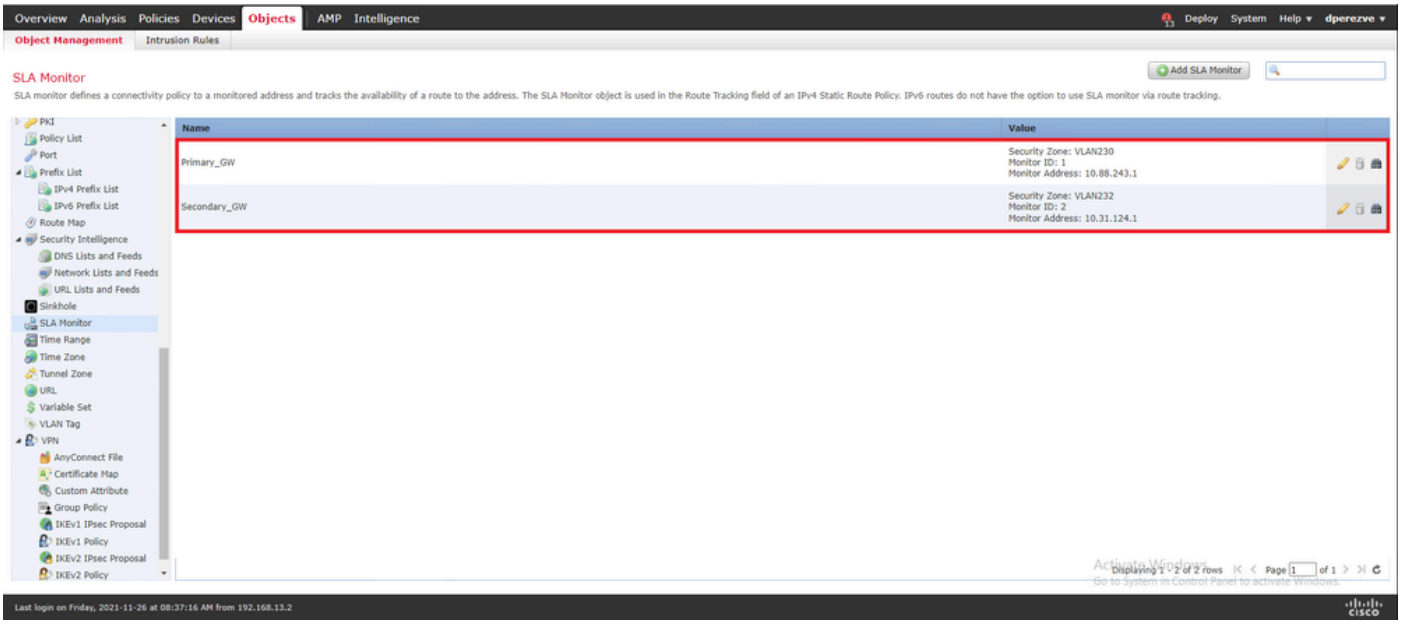


Select the **Add SLA Monitor** button once more in order to create a second object, this time for the Gateway on the backup circuit.

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



The two objects must be added to the list.

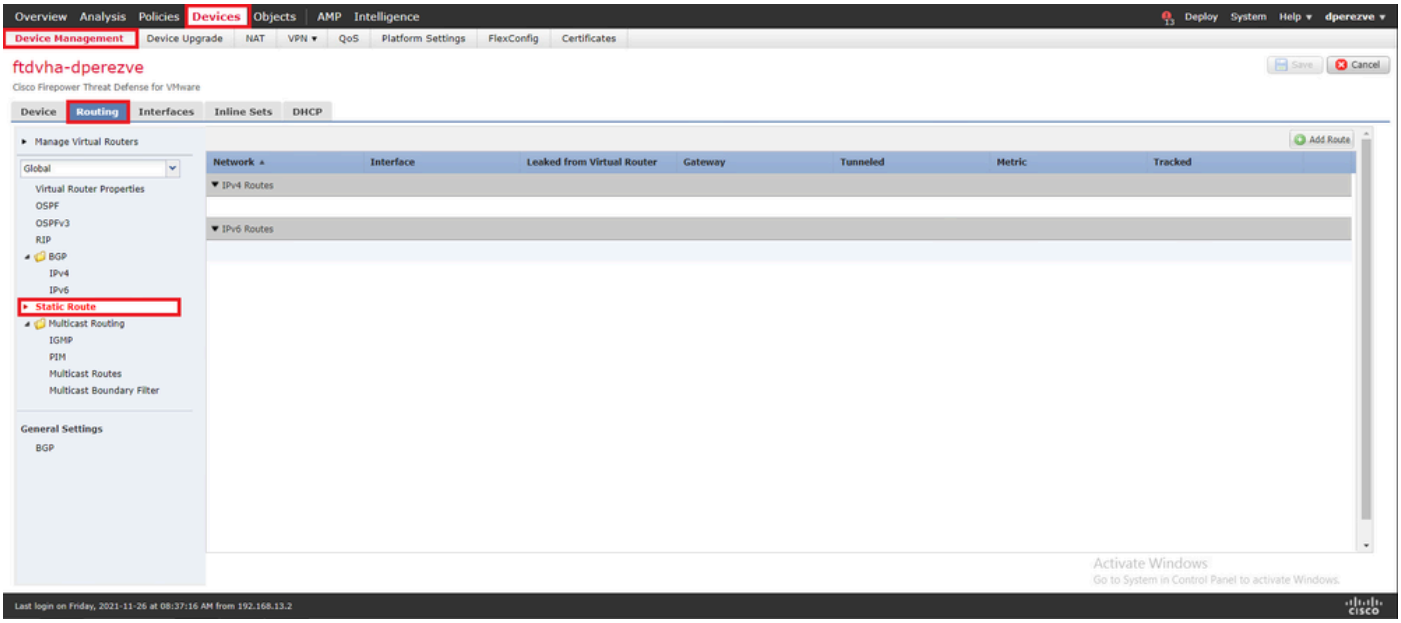


Step 4. Configure Static Routes with Route Track

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

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

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

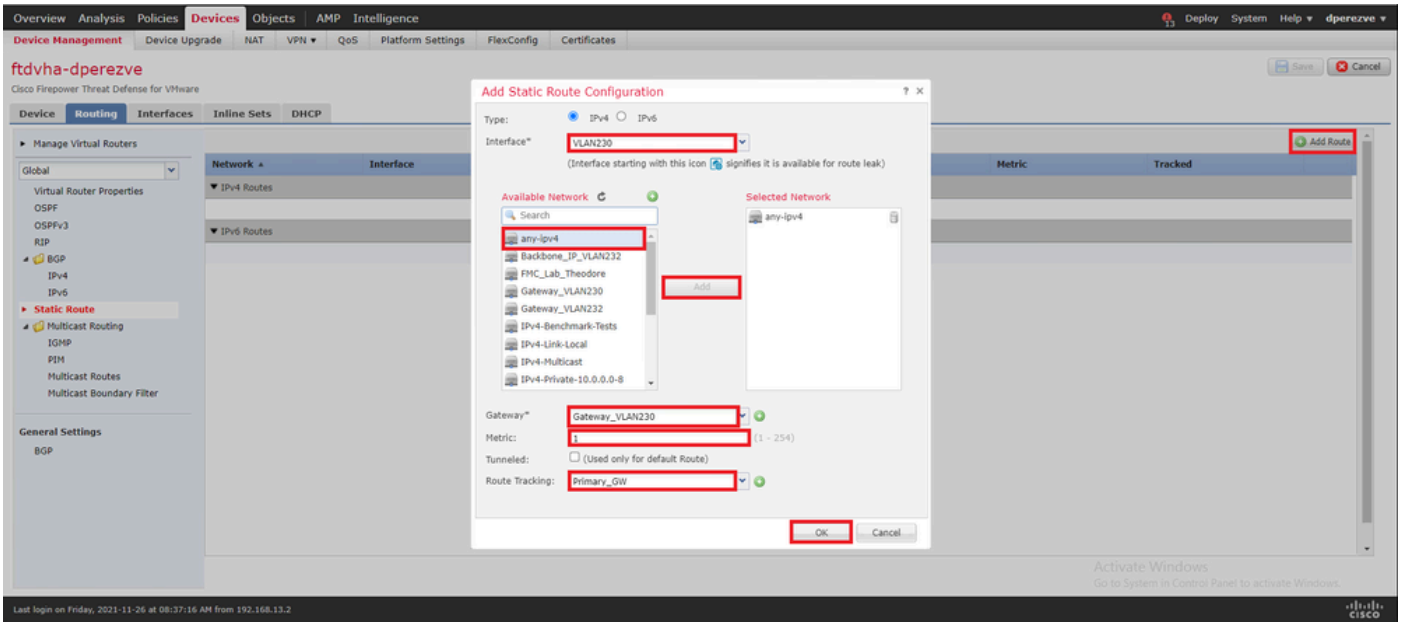


In the **Add Static Route Configuration** window, in the **Interface** drop down, specify the name for the interface through which the primary Gateway must be reachable.

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

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

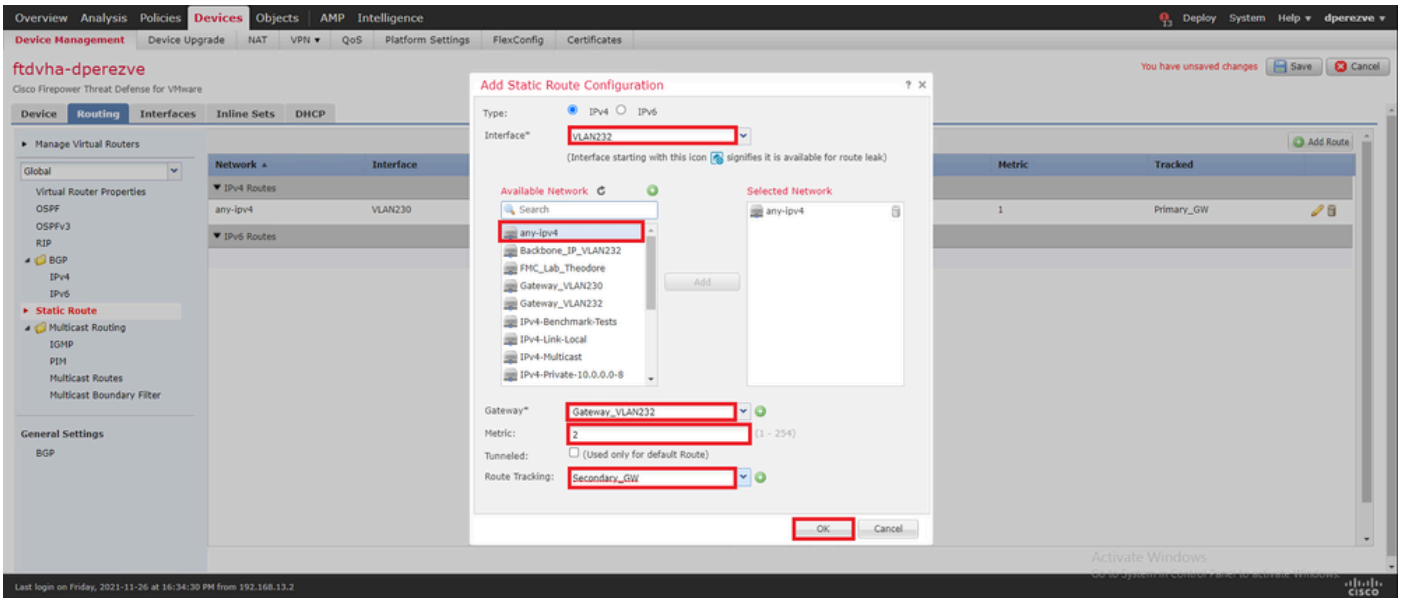
Click **OK** to add the new route.



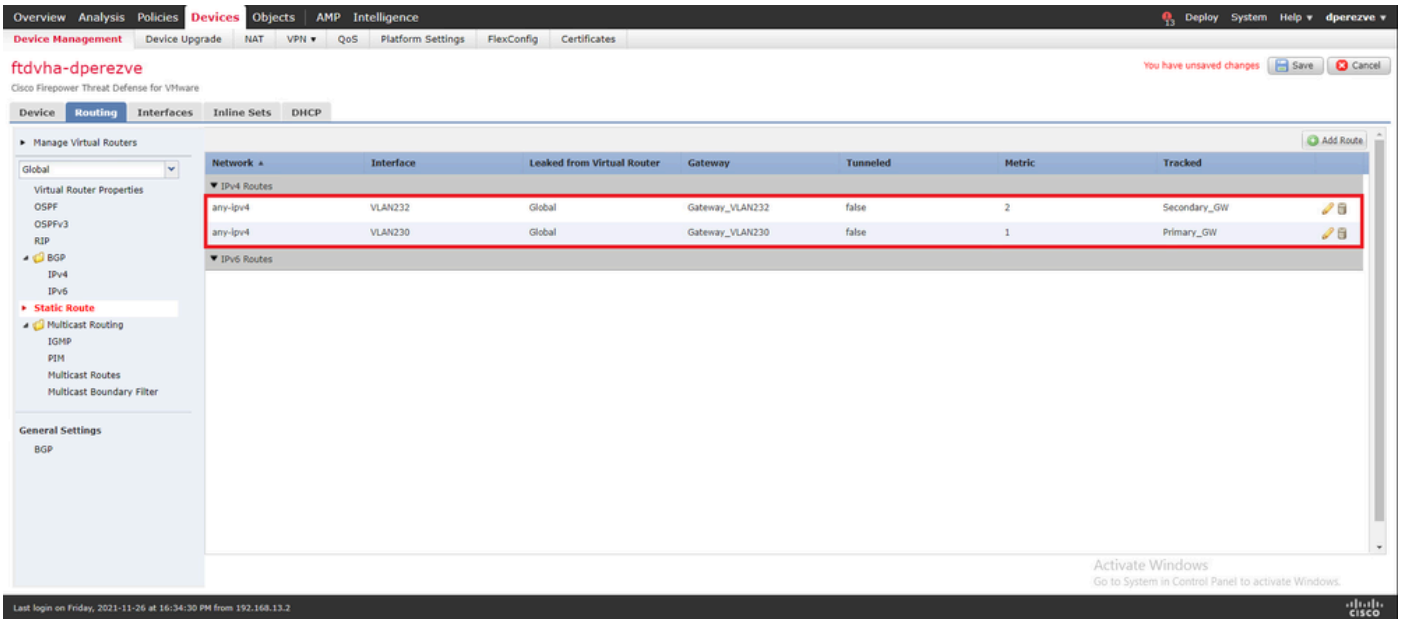
A second static route must be configured for the backup Gateway.

Click **Add Route** to define a new static route.

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



The two routes must be added to the list.

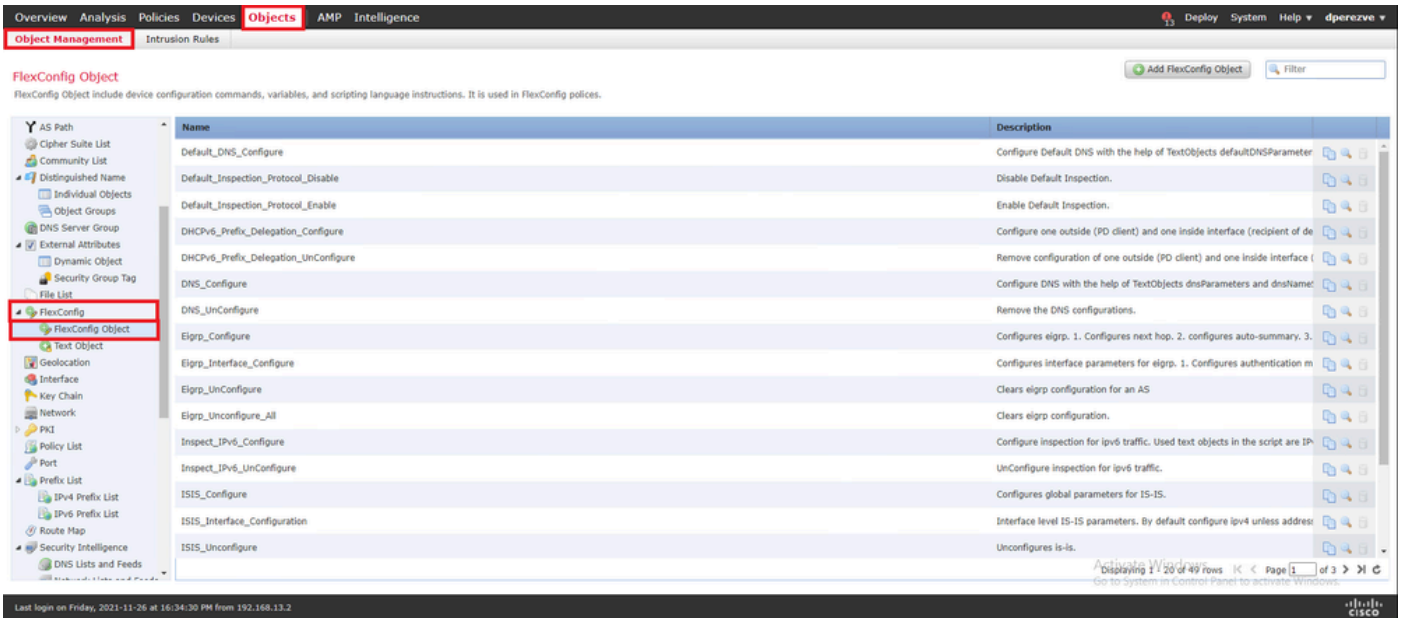


Step 5. Configure PBR FlexConfig Object

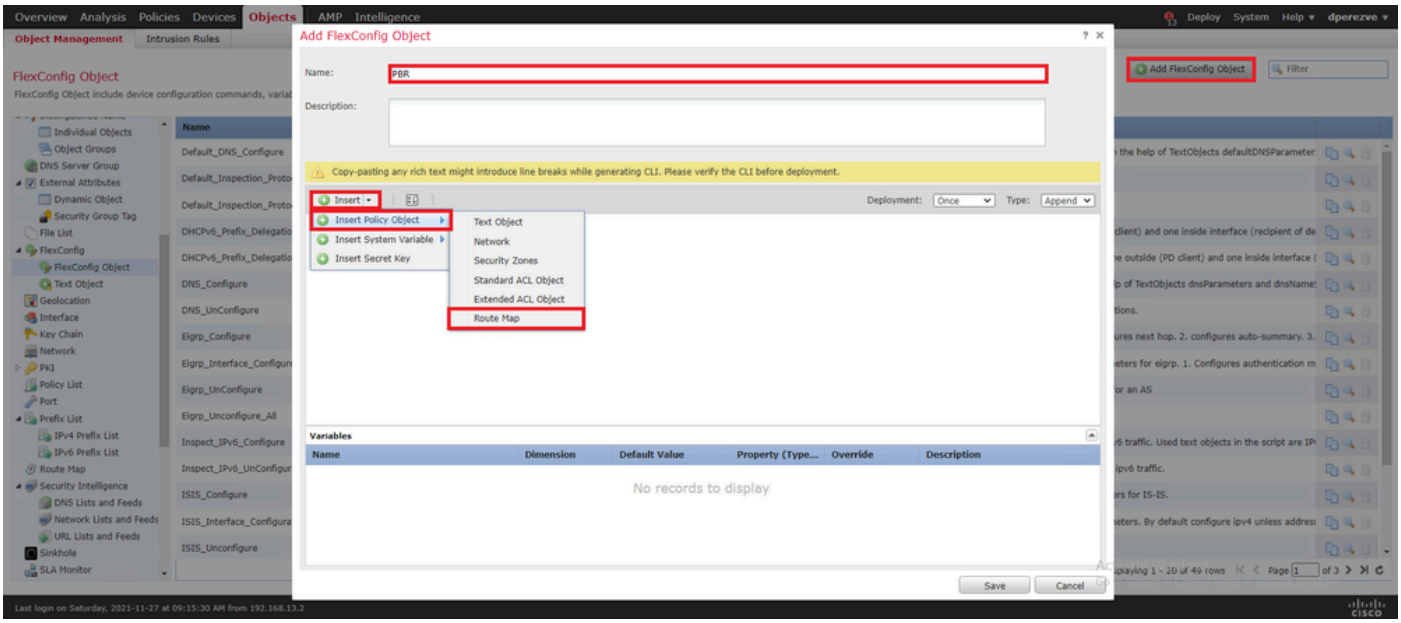
Enable SLAs under the route map used for PBR and apply this route map in an interface of the FTD.

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

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

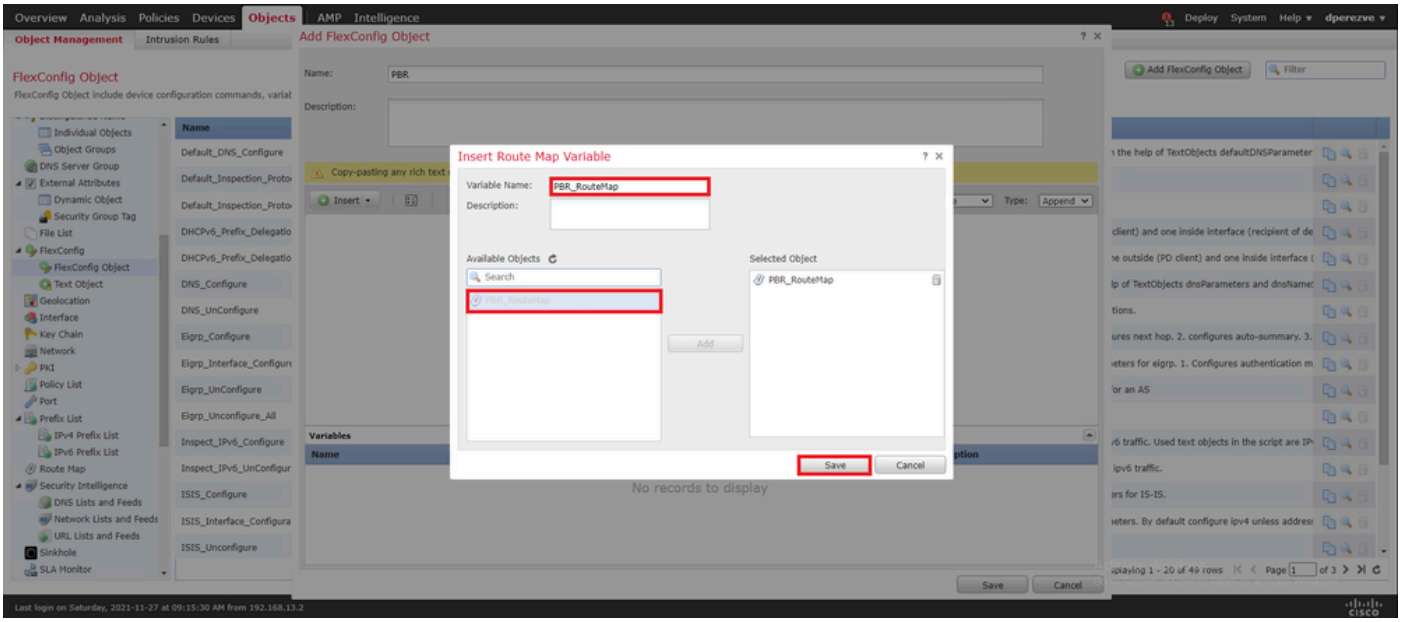


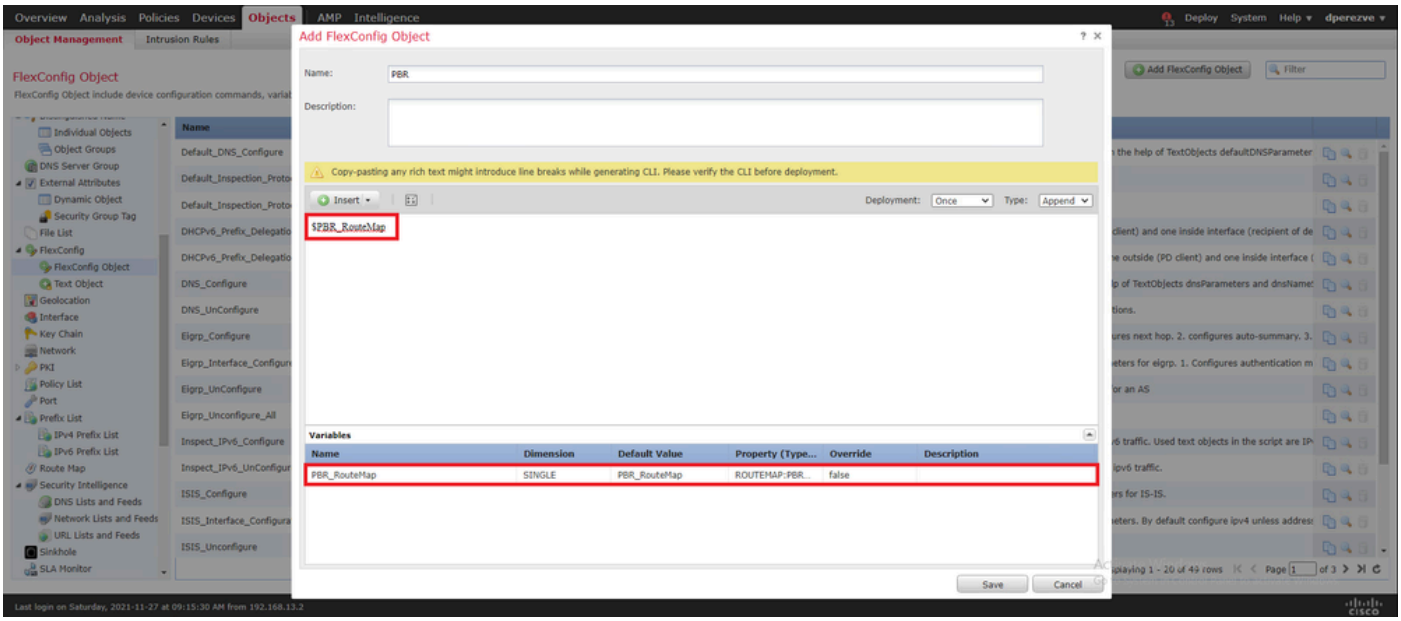
Select the **Add FlexConfig Object** button. In the **Add FlexConfig Object** window assign a name and navigate to **Insert > Insert Policy Object > Route Map .**



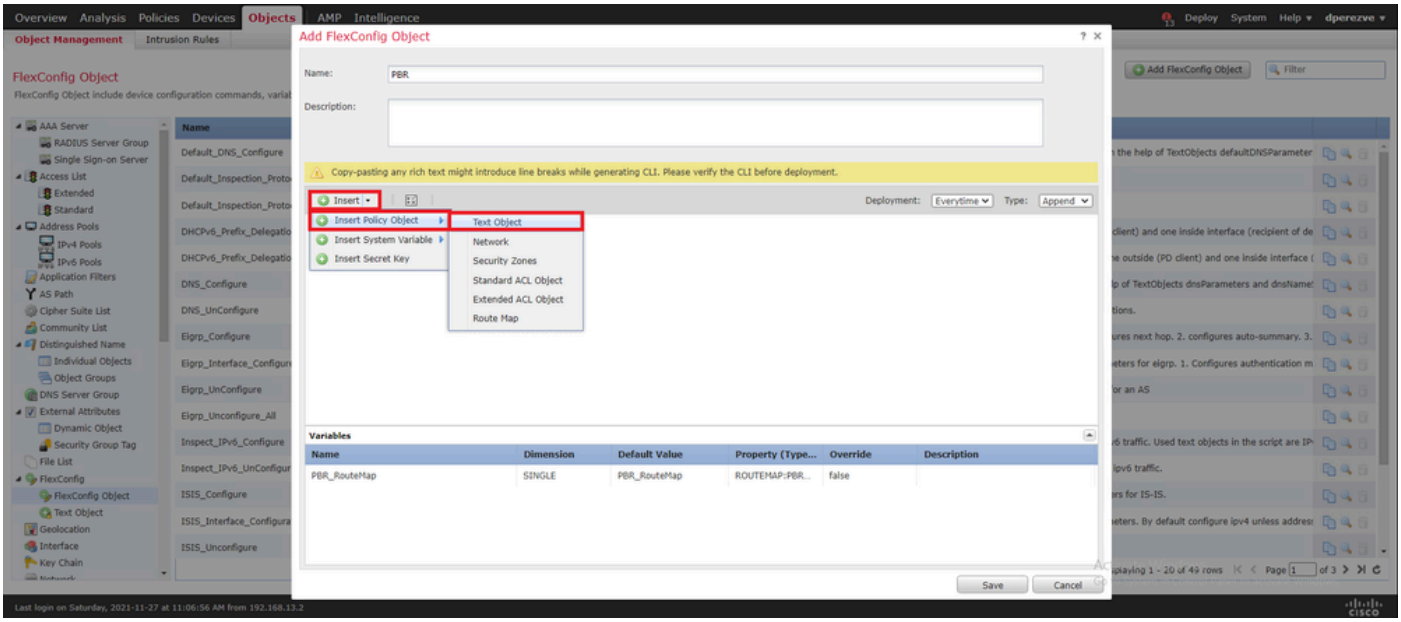
In the **Insert Route Map Variable** window, assign a name for the variable and select the PBR object created in Step 2.

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



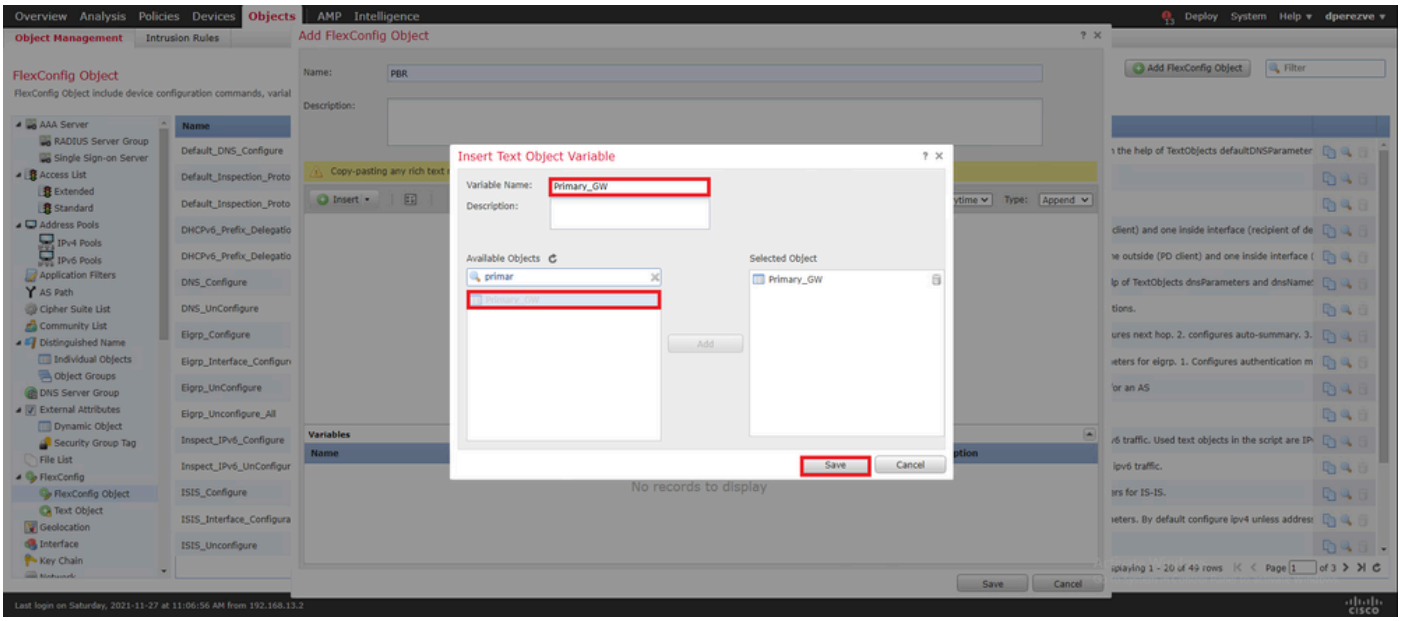


Besides the route map variable, we must add the FlexConfig text objects that represent each Gateway (defined in Step 3). In the **Add FlexConfig Object** window navigate to **Insert > Insert Policy Object > Text Object .**

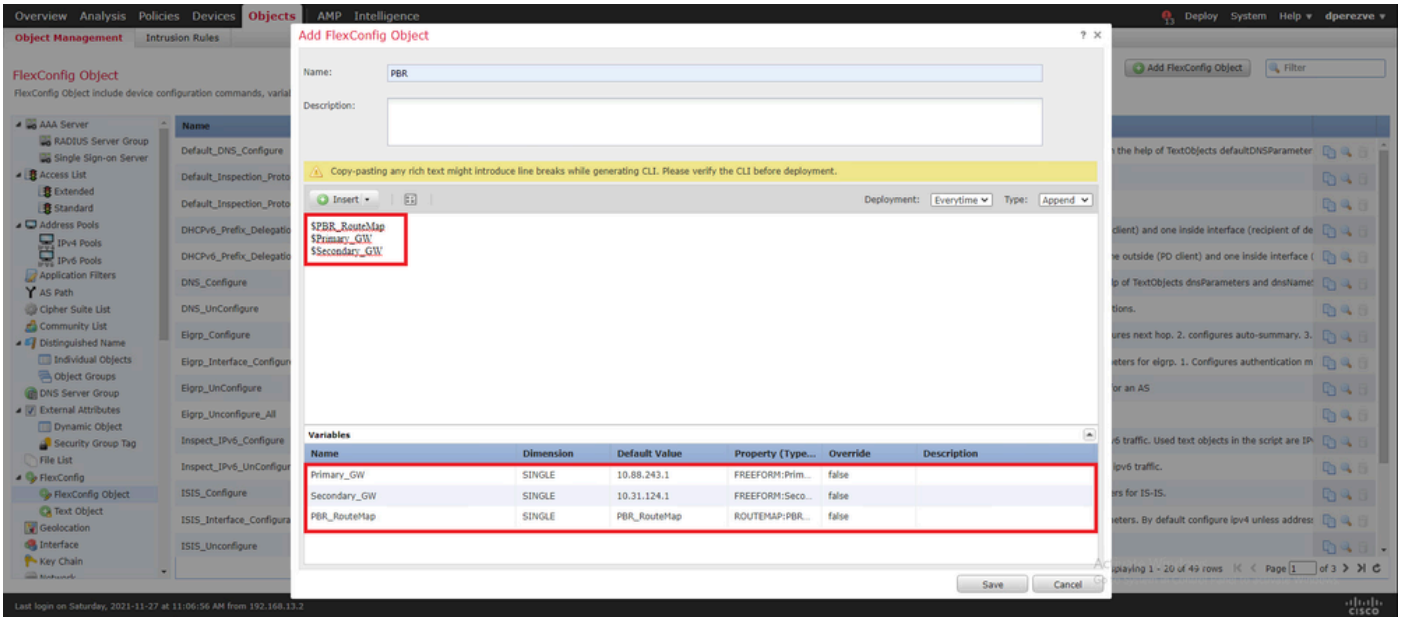


In the **Insert Text Object Variable** window assign a name for the variable and select the text object that represents the primary Gateway defined in Step 3.

Click **Save** button in order to add it to the FlexConfig object.



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

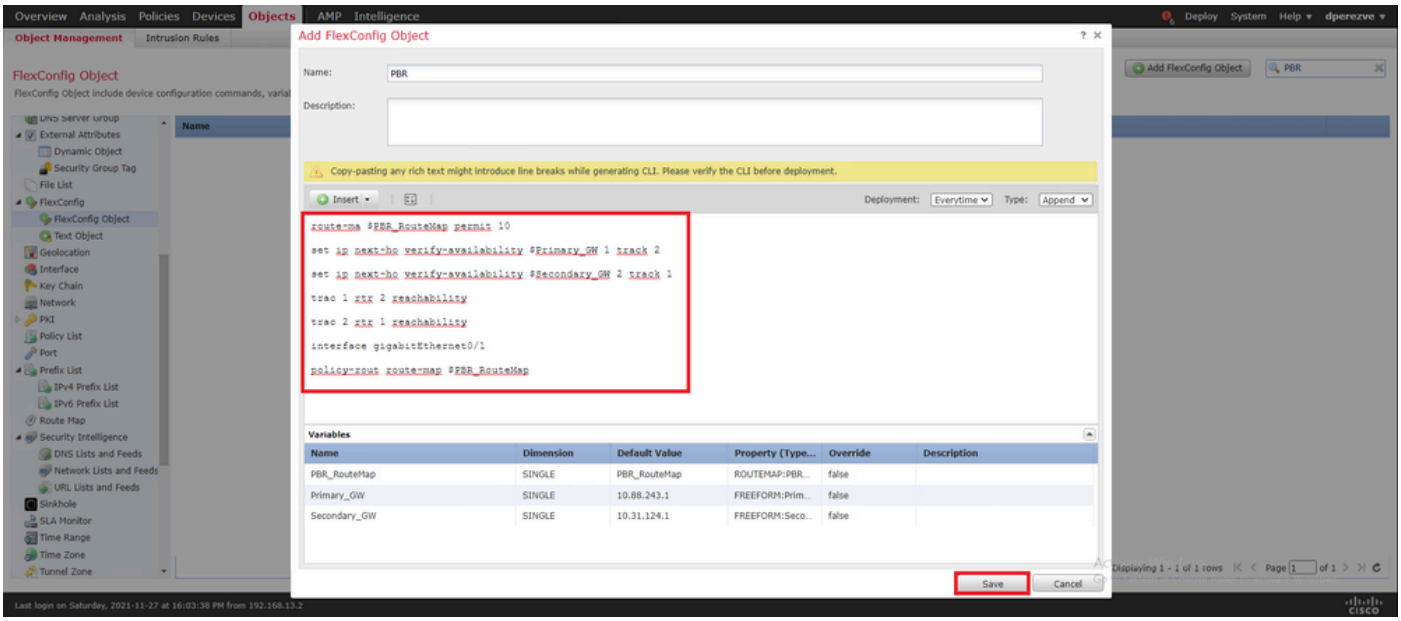


The syntax for the PBR configuration must be the same as in Cisco ASA. The sequence number for the route map must match the one configured in Step 2 (10 in this case) as well as the SLA IDs.

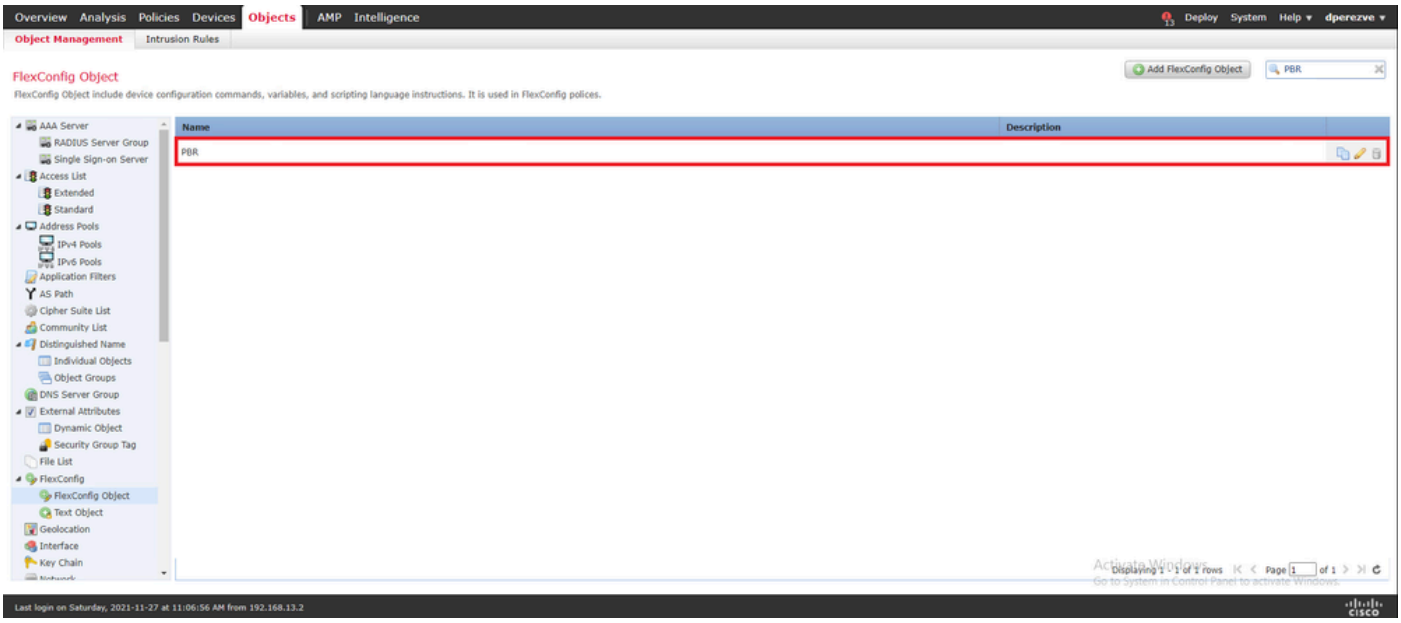
To configure PBR to check availability for the next hop, the **set ip next-hop verify-availability** command must be used.

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

Click **Save** when configuration is completed.



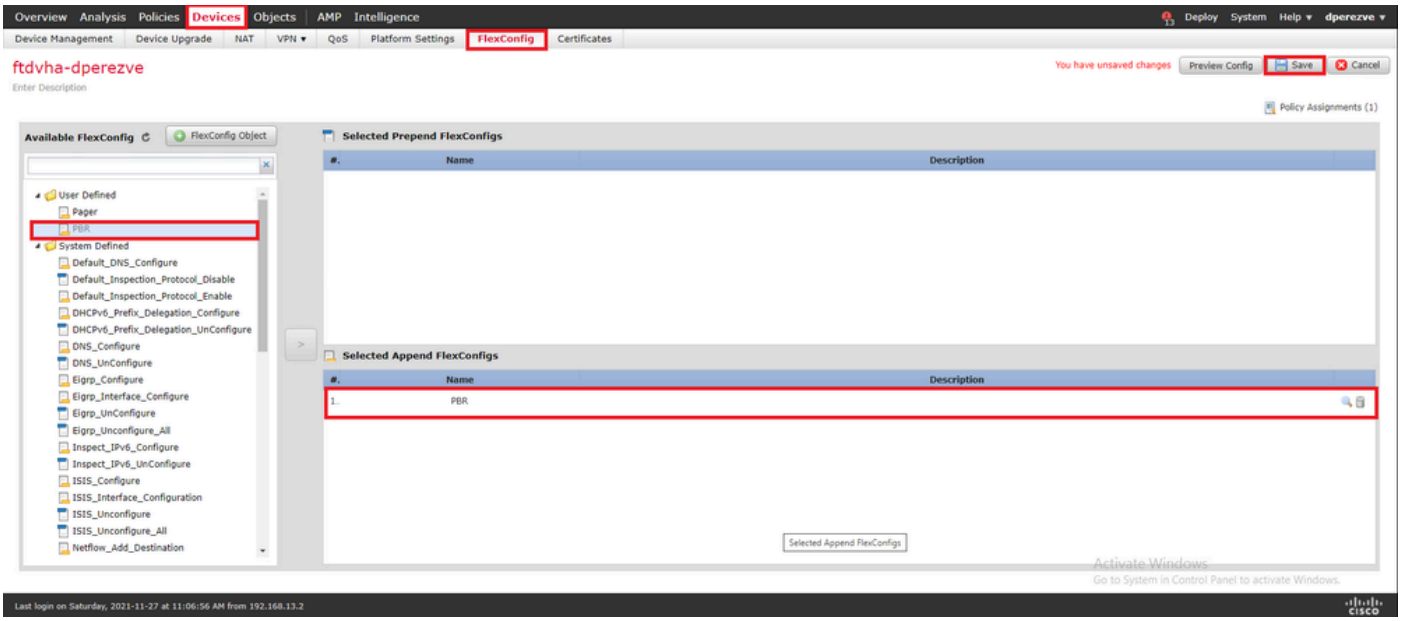
The FlexConfig object must be added to the list.



Step 6. Assign PBR FlexConfig Object to FlexConfig Policy

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

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



Verify

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

```
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
```

Because connectivity to primary Gateway is up, traffic from internal subnet (VLAN2813) must be

forwarded through the primary ISP circuit.

```
firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed

Phase: 1
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map PBR_RouteMap permit 10
 match ip address PBR_ACL
 set ip next-hop verify-availability 10.88.243.1 1 track 2
 set ip next-hop verify-availability 10.31.124.1 2 track 1
Additional Information:
 Matched route-map PBR_RouteMap, sequence 10, permit
 Found next-hop 10.88.243.1 using egress ifc VLAN230

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log
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
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
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
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
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 rul


Result:
input-interface: VLAN2813(vrfid:0)
input-status: up
input-line-status: up
output-interface: VLAN230(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

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

```
firepower# show route-map
route-map PBR_RouteMap, permit, sequence 10
  Match clauses:
    ip address (access-lists): PBR_ACL

  Set clauses:
    ip next-hop verify-availability 10.88.243.1 1 track 2  [down]
    ip next-hop verify-availability 10.31.124.1 2 track 1  [up]

firepower# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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
```

Informational message 622001 is generated everytime FTD either adds or removes a tracked route from routing table.

```
firepower# show logg | i 622001
%FTD-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.31.124.1, distance 2, table default, on interf
```

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

```
firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed

Phase: 1
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map PBR_RouteMap permit 10
 match ip address PBR_ACL
 set ip next-hop verify-availability 10.88.243.1 1 track 2
 set ip next-hop verify-availability 10.31.124.1 2 track 1
Additional Information:
 Matched route-map PBR_RouteMap, sequence 10, permit
 Found next-hop 10.31.124.1 using egress ifc VLAN232

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log
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
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
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
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
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
```

Troubleshoot

In order to validate which PBR entry is enforced in **interesting traffic** , run command **debug policy-route**.

```
firepower# debug policy-route
debug policy-route  enabled at level 1
firepower# pbr: policy based route lookup called for 192.168.13.5/45951 to 208.67.220.220/53 proto 17 s
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
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
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
```