排除Firepower威胁防御路由故障

目录

简介

本文档介绍Firepower威胁防御(FTD)如何转发数据包和实施各种路由概念。

先决条件

要求

- 基本的路由知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower 41xx威胁防御版本7.1.x
- Firepower管理中心(FMC)版本7.1.x

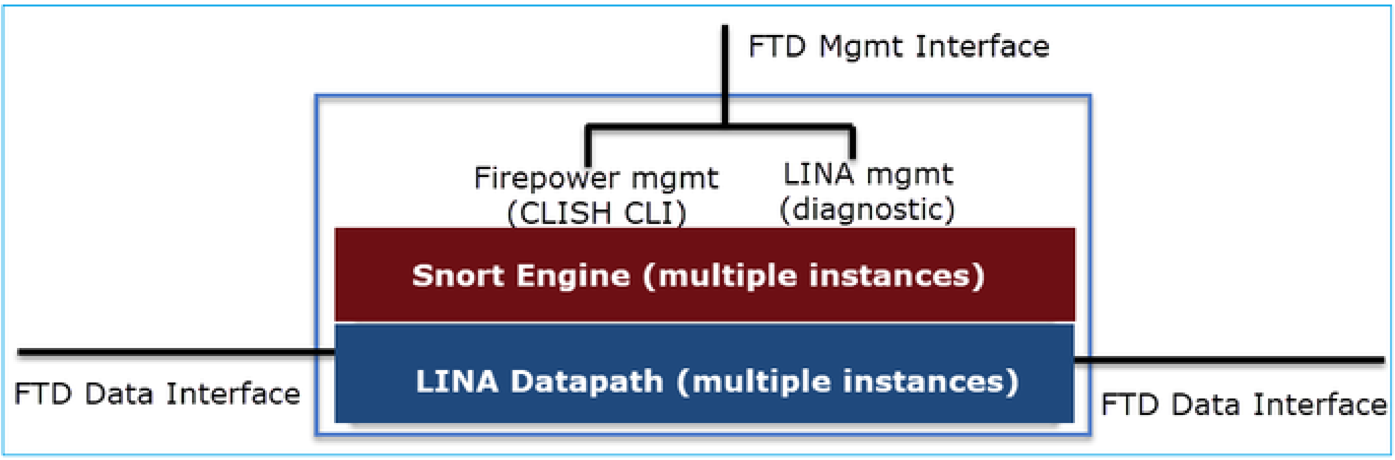
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FTD数据包转发机制

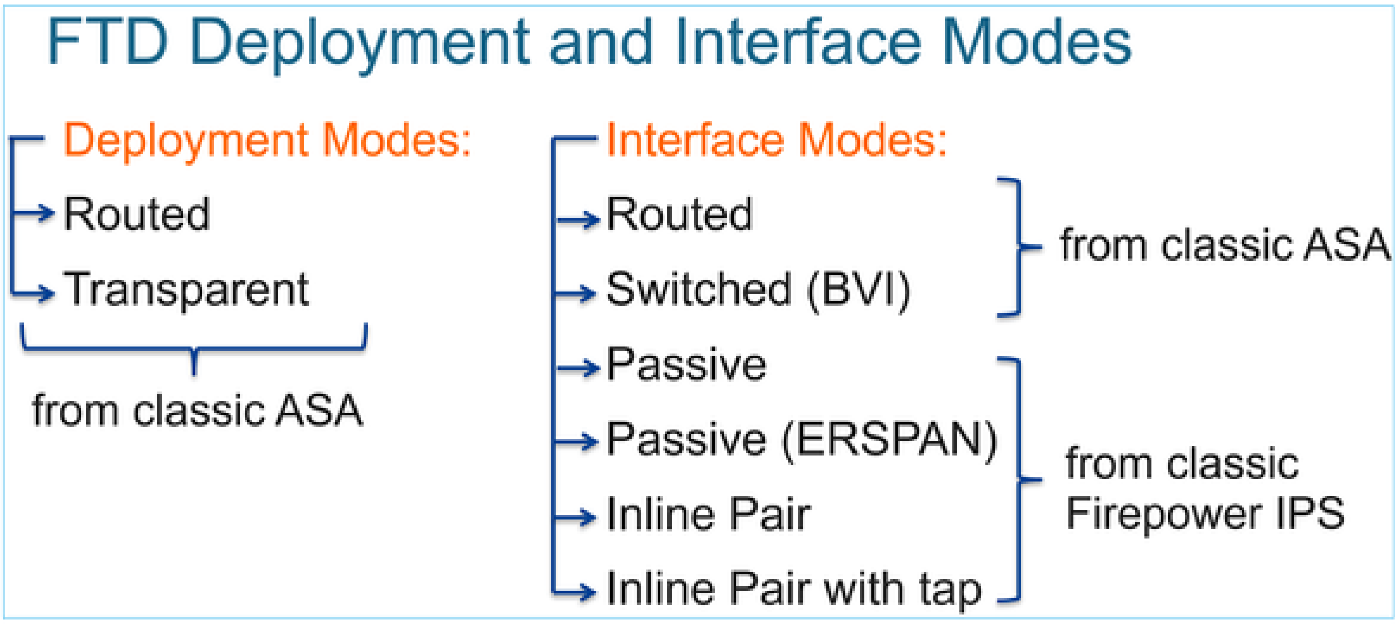
FTD 是由两个主要引擎组成的统一软件映像：

- 数据路径引擎(LINA)
- Snort 引擎

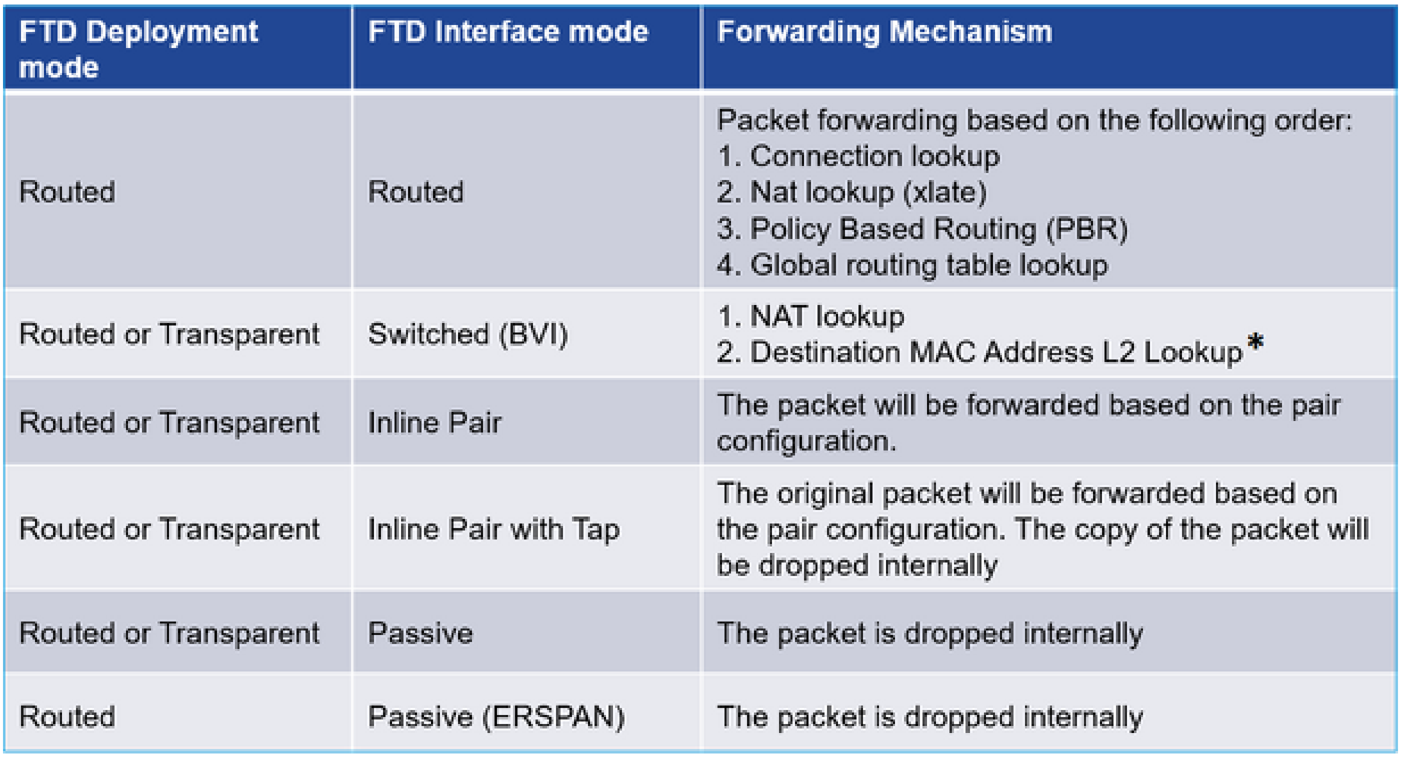


数据路径和Snort引擎是FTD数据平面的主要部分。

FTD数据平面转发机制取决于接口模式。下图总结了各种接口模式以及FTD部署模式：

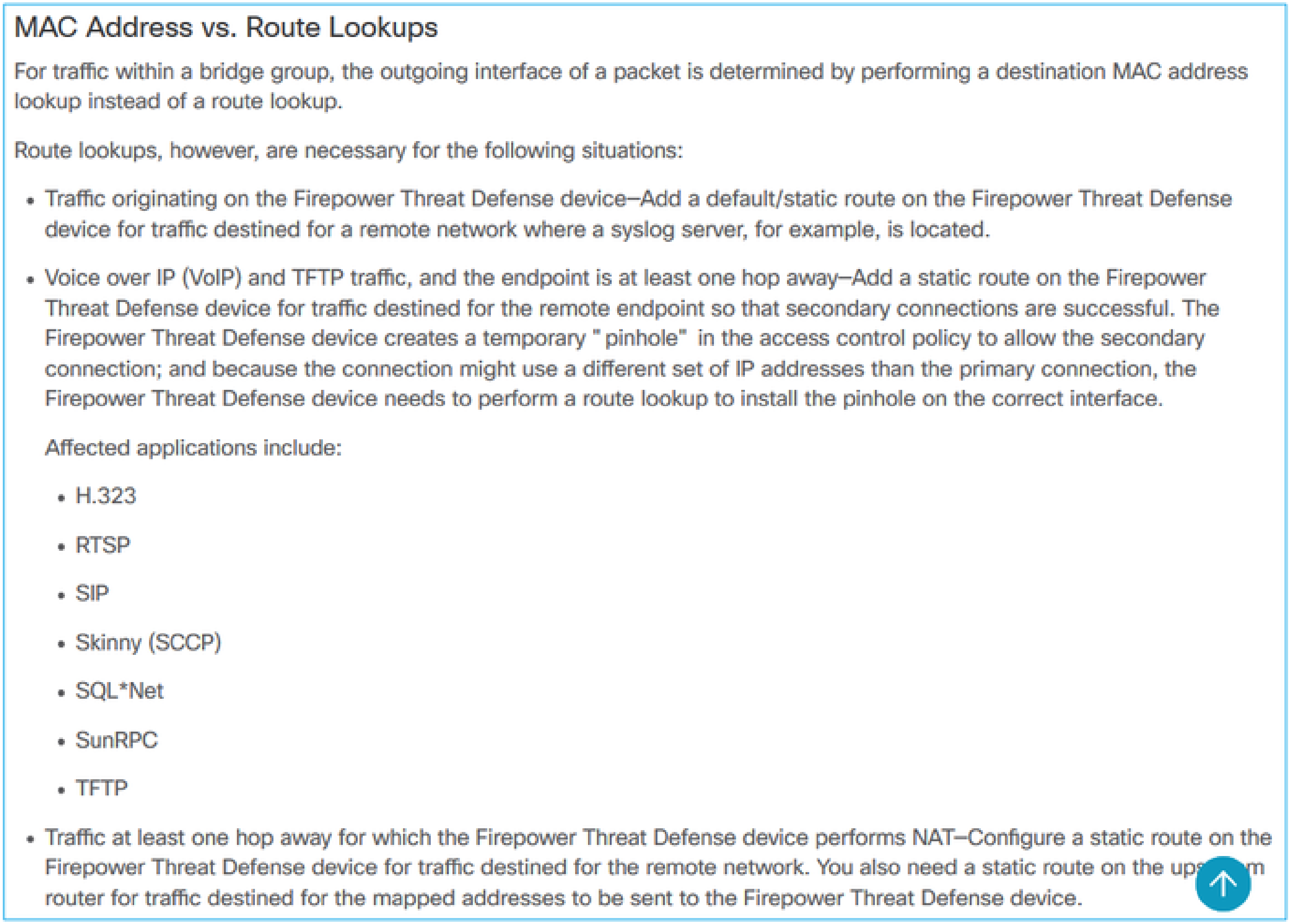


下表总结了FTD如何根据接口模式在数据平面中转发数据包。转发机制按优先顺序列出：



FTD Deployment mode	FTD Interface mode	Forwarding Mechanism
Routed	Routed	Packet forwarding based on the following order: 1. Connection lookup 2. Nat lookup (xlate) 3. Policy Based Routing (PBR) 4. Global routing table lookup
Routed or Transparent	Switched (BVI)	1. NAT lookup 2. Destination MAC Address L2 Lookup*
Routed or Transparent	Inline Pair	The packet will be forwarded based on the pair configuration.
Routed or Transparent	Inline Pair with Tap	The original packet will be forwarded based on the pair configuration. The copy of the packet will be dropped internally
Routed or Transparent	Passive	The packet is dropped internally
Routed	Passive (ERSPAN)	The packet is dropped internally

*透明模式下的FTD在某些情况下执行路由查找：



MAC Address vs. Route Lookups

For traffic within a bridge group, the outgoing interface of a packet is determined by performing a destination MAC address lookup instead of a route lookup.

Route lookups, however, are necessary for the following situations:

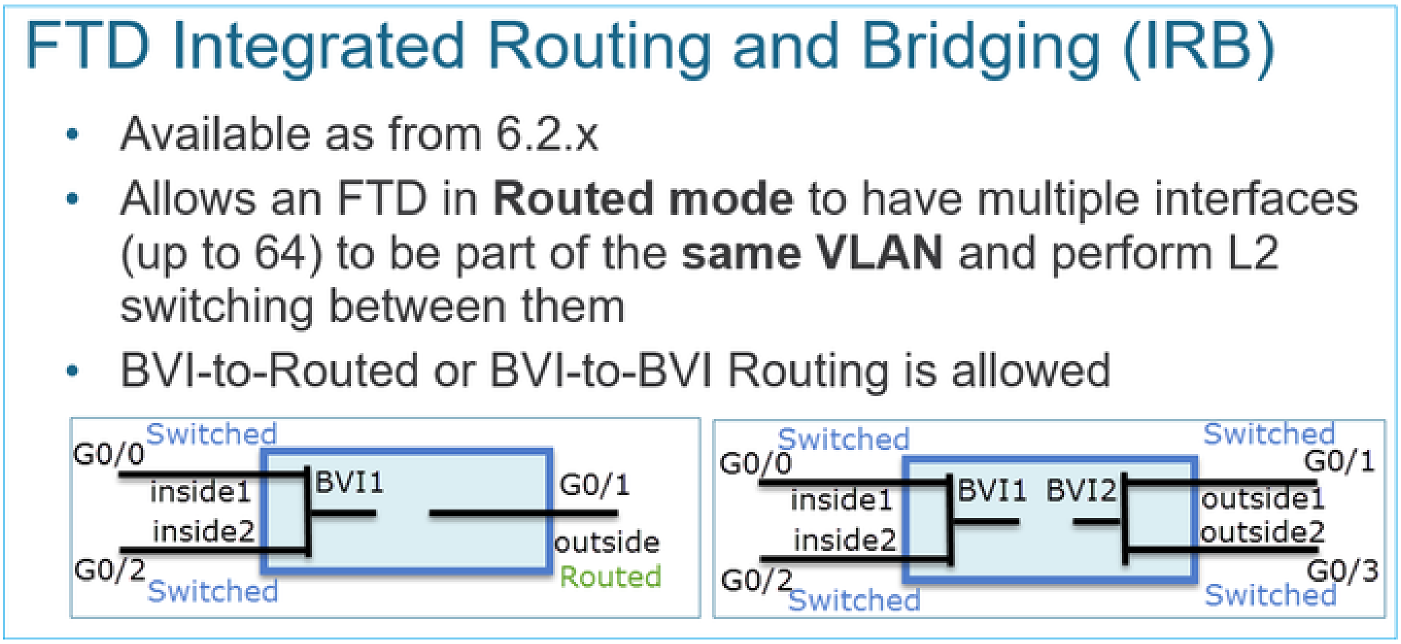
- Traffic originating on the Firepower Threat Defense device–Add a default/static route on the Firepower Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away–Add a static route on the Firepower Threat Defense device for traffic destined for the remote endpoint so that secondary connections are successful. The Firepower Threat Defense device creates a temporary "pinhole" in the access control policy to allow the secondary connection; and because the connection might use a different set of IP addresses than the primary connection, the Firepower Threat Defense device needs to perform a route lookup to install the pinhole on the correct interface.

  Affected applications include:

  - H.323
  - RTSP
  - SIP
  - Skinny (SCCP)
  - SQL*Net
  - SunRPC
  - TFTP
- Traffic at least one hop away for which the Firepower Threat Defense device performs NAT–Configure a static route on the Firepower Threat Defense device for traffic destined for the remote network. You also need a static route on the upstream router for traffic destined for the mapped addresses to be sent to the Firepower Threat Defense device.

有关详细信息，请查看FMC指南。

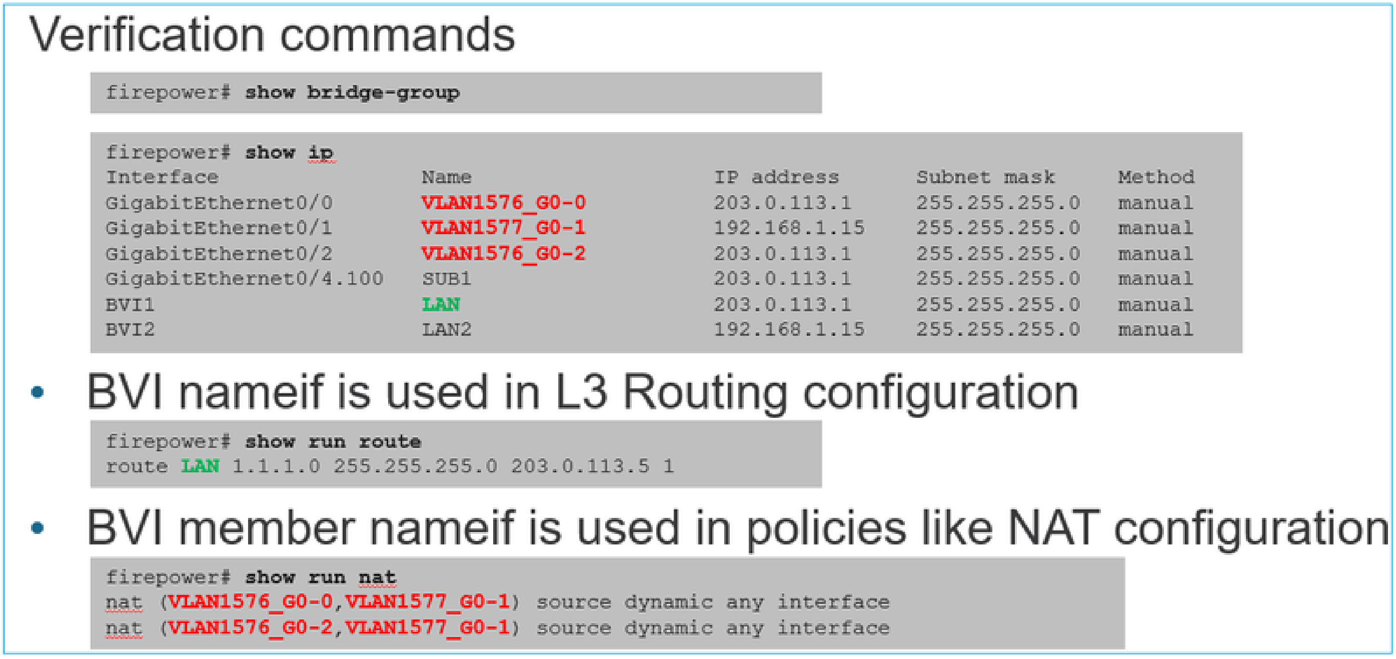
从6.2.x版本开始，FTD支持集成路由和桥接(IRB):



FTD Integrated Routing and Bridging (IRB)

- Available as from 6.2.x
- Allows an FTD in **Routed mode** to have multiple interfaces (up to 64) to be part of the **same VLAN** and perform L2 switching between them
- BVI-to-Routed or BVI-to-BVI Routing is allowed

BVI验证命令：



Verification commands

```
firepower# show bridge-group
```

```
firepower# show ip
Interface                 Name              IP address      Subnet mask     Method
GigabitEthernet0/0        VLAN1576_G0-0     203.0.113.1     255.255.255.0   manual
GigabitEthernet0/1        VLAN1577_G0-1     192.168.1.15    255.255.255.0   manual
GigabitEthernet0/2        VLAN1576_G0-2     203.0.113.1     255.255.255.0   manual
GigabitEthernet0/4.100    SUB1              203.0.113.1     255.255.255.0   manual
BVI1                      LAN               203.0.113.1     255.255.255.0   manual
BVI2                      LAN2              192.168.1.15    255.255.255.0   manual
```

- BVI nameif is used in L3 Routing configuration

```
firepower# show run route
route LAN 1.1.1.0 255.255.255.0 203.0.113.5 1
```

- BVI member nameif is used in policies like NAT configuration

```
firepower# show run nat
nat (VLAN1576_G0-0,VLAN1577_G0-1) source dynamic any interface
nat (VLAN1576_G0-2,VLAN1577_G0-1) source dynamic any interface
```

要点

对于路由接口或BVI(IRB)，数据包转发基于以下顺序：

- 连接查找
- NAT查找（目标NAT，也称为UN-NAT）
- 基于策略的路由 (PBR)
- 全局路由表查找

源NAT是什么？

在全局路由查找之后检查源NAT。

本文档的其余部分将重点介绍路由接口模式。

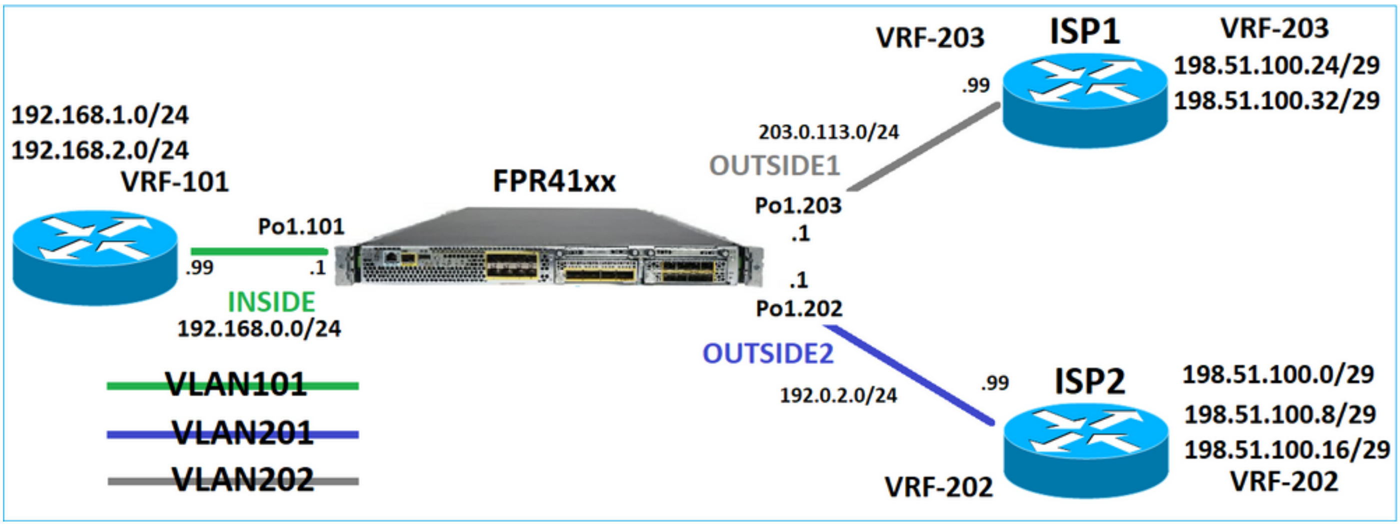
数据平面(LINA)路由行为

在路由接口模式下，FTD LINA分两个阶段转发数据包：

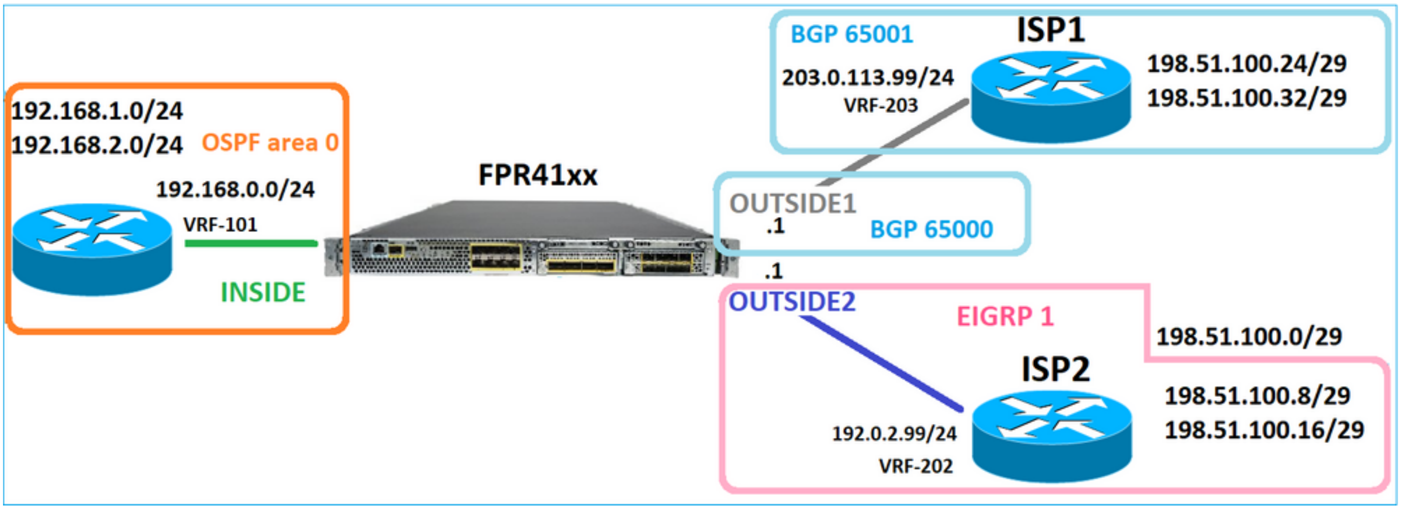
第1阶段 — 出口接口确定

第2阶段 — 下一跳选择

请思考以下拓扑：



此路由设计：



FTD路由配置：

```
firepower# show run router
router ospf 1
network 192.168.0.0 255.255.255.0 area 0
log-adj-changes
```

```
!
router bgp 65000
bgp log-neighbor-changes
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 203.0.113.99 remote-as 65001
neighbor 203.0.113.99 ebgp-multihop 255
neighbor 203.0.113.99 transport path-mtu-discovery disable
neighbor 203.0.113.99 activate
no auto-summary
no synchronization
exit-address-family
!
router eigrp 1
no default-information in
no default-information out
no eigrp log-neighbor-warnings
no eigrp log-neighbor-changes
network 192.0.2.0 255.255.255.0
!
firepower# show run route
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
```

FTD路由信息库(RIB) — 控制平面：

```
firepower# show route | begin Gate
Gateway of last resort is not set

C 192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C 192.168.0.0 255.255.255.0 is directly connected, INSIDE
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
O 192.168.1.1 255.255.255.255
[110/11] via 192.168.0.99, 01:11:25, INSIDE
O 192.168.2.1 255.255.255.255
[110/11] via 192.168.0.99, 01:11:15, INSIDE
S 198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D 198.51.100.8 255.255.255.248
[90/130816] via 192.0.2.99, 01:08:11, OUTSIDE2
D 198.51.100.16 255.255.255.248
[90/130816] via 192.0.2.99, 01:08:04, OUTSIDE2
B 198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 00:28:29
B 198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 00:28:16
C 203.0.113.0 255.255.255.0 is directly connected, OUTSIDE1
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

相应的FTD加速安全路径(ASP)路由表 — 数据平面：

```
firepower# show asp table routing
route table timestamp: 91
in 169.254.1.1 255.255.255.255 identity
in 192.168.0.1 255.255.255.255 identity
in 192.0.2.1 255.255.255.255 identity
in 192.168.1.1 255.255.255.255 via 192.168.0.99, INSIDE
in 192.168.2.1 255.255.255.255 via 192.168.0.99, INSIDE
in 203.0.113.1 255.255.255.255 identity
in 169.254.1.0 255.255.255.248 nlp_int_tap
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
in 198.51.100.24 255.255.255.248 via 203.0.113.99 (unresolved, timestamp: 89)
in 198.51.100.32 255.255.255.248 via 203.0.113.99 (unresolved, timestamp: 90)
in 192.168.0.0 255.255.255.0 INSIDE
in 192.0.2.0 255.255.255.0 OUTSIDE2
in 203.0.113.0 255.255.255.0 OUTSIDE1
in ff02::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff00:1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fe80::200:ff:fe01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out 255.255.255.255 255.255.255.255 OUTSIDE1
out 203.0.113.1 255.255.255.255 OUTSIDE1
out 203.0.113.0 255.255.255.0 OUTSIDE1
out 224.0.0.0 240.0.0.0 OUTSIDE1
out 255.255.255.255 255.255.255.255 OUTSIDE2
out 192.0.2.1 255.255.255.255 OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 192.0.2.0 255.255.255.0 OUTSIDE2
out 224.0.0.0 240.0.0.0 OUTSIDE2
out 255.255.255.255 255.255.255.255 INSIDE
out 192.168.0.1 255.255.255.255 INSIDE
out 192.168.1.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.2.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.0.0 255.255.255.0 INSIDE
out 224.0.0.0 240.0.0.0 INSIDE
out 255.255.255.255 255.255.255.255 cmi_mgmt_int_tap
out 224.0.0.0 240.0.0.0 cmi_mgmt_int_tap
out 255.255.255.255 255.255.255.255 ha_ctl_nlp_int_tap
out 224.0.0.0 240.0.0.0 ha_ctl_nlp_int_tap
out 255.255.255.255 255.255.255.255 ccl_ha_nlp_int_tap
out 224.0.0.0 240.0.0.0 ccl_ha_nlp_int_tap
out 255.255.255.255 255.255.255.255 nlp_int_tap
out 169.254.1.1 255.255.255.255 nlp_int_tap
out 169.254.1.0 255.255.255.248 nlp_int_tap
out 224.0.0.0 240.0.0.0 nlp_int_tap
out fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap
out fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out fe80:: ffc0:: nlp_int_tap
out ff00:: ff00:: nlp_int_tap
out 0.0.0.0 0.0.0.0 via 0.0.0.0, identity
out :: :: via 0.0.0.0, identity
```

要点

FTD（以类似于自适应安全设备 — ASA的方式）首先确定数据包的出口（出口）接口（为此，它会查看ASP路由表的“in”条目）。然后，对于确定的接口，它会尝试查找下一跳（为此，它会查看ASP路由表的“out”条目）。例如：

```
firepower# show asp table routing | include in.*198.51.100.0
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
firepower#
firepower# show asp table routing | include out.*OUTSIDE2
out 255.255.255.255 255.255.255.255 OUTSIDE2
out 192.0.2.1 255.255.255.255 OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 192.0.2.0 255.255.255.0 OUTSIDE2
out 224.0.0.0 240.0.0.0 OUTSIDE2
```

最后，对于已解析的下一跳，LINA会检查ARP缓存中的有效邻接关系。

FTD Packet Tracer工具确认此过程：

```
firepower# packet-tracer input INSIDE icmp 192.168.1.1 8 0 198.51.100.1

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 7582 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8474 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 5017 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 5017 ns
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:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 5017 ns
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 5017 ns
Config:
Additional Information:

Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Elapsed time: 57534 ns
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
Additional Information:

Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Elapsed time: 3122 ns
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 29882 ns
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
```

```
Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20962 ns
Config:
Additional Information:
New flow created with id 178, packet dispatched to next module

Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 20070 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Elapsed time: 870592 ns
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Phase: 14
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 6244 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 5 reference 1

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 1046760 ns
```

FTD ARP表，如控制平面所示：

```
firepower# show arp
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8 3051
OUTSIDE2 192.0.2.99 4c4e.35fc.fcd8 5171
```

要强制ARP解析，请执行以下操作：

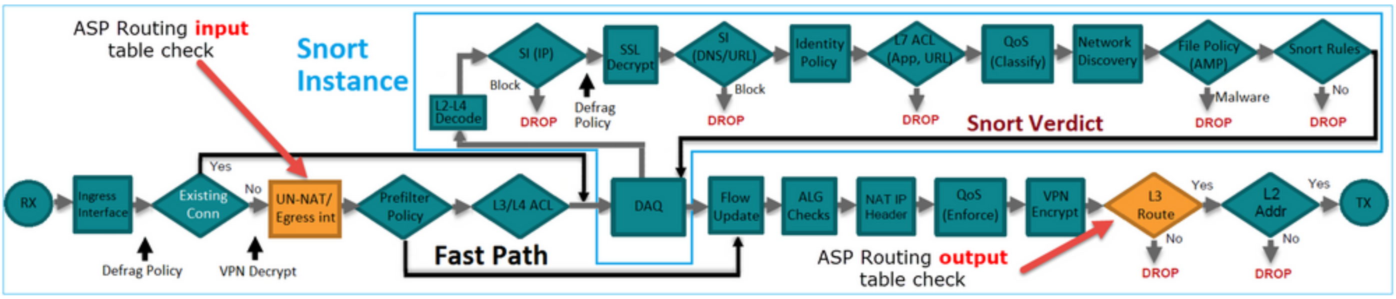
```
firepower# ping 192.168.0.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
firepower# show arp
INSIDE 192.168.0.99 4c4e.35fc.fcd8 45
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8 32
OUTSIDE2 192.0.2.99 4c4e.35fc.fcd8 1
```

FTD ARP表，如数据平面所示：

```
firepower# show asp table arp

Context: single_vf, Interface: OUTSIDE1
203.0.113.99 Active 4c4e.35fc.fcd8 hits 2 reference 1

Context: single_vf, Interface: OUTSIDE2
192.0.2.99 Active 4c4e.35fc.fcd8 hits 5 reference 0

Context: single_vf, Interface: INSIDE
192.168.0.99 Active 4c4e.35fc.fcd8 hits 5 reference 0

Context: single_vf, Interface: identity
:: Active 0000.0000.0000 hits 0 reference 0
0.0.0.0 Active 0000.0000.0000 hits 848 reference 0

Last clearing of hits counters: Never
```

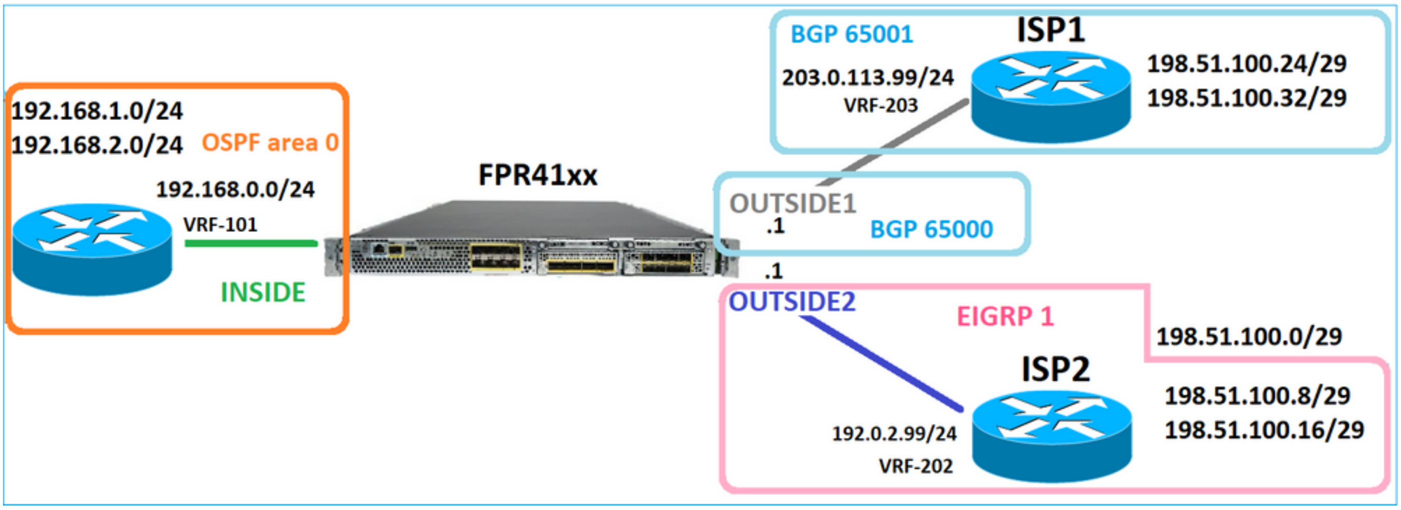
FTD操作顺序

该图显示了操作的顺序以及输入和输出ASP路由检查的完成位置：



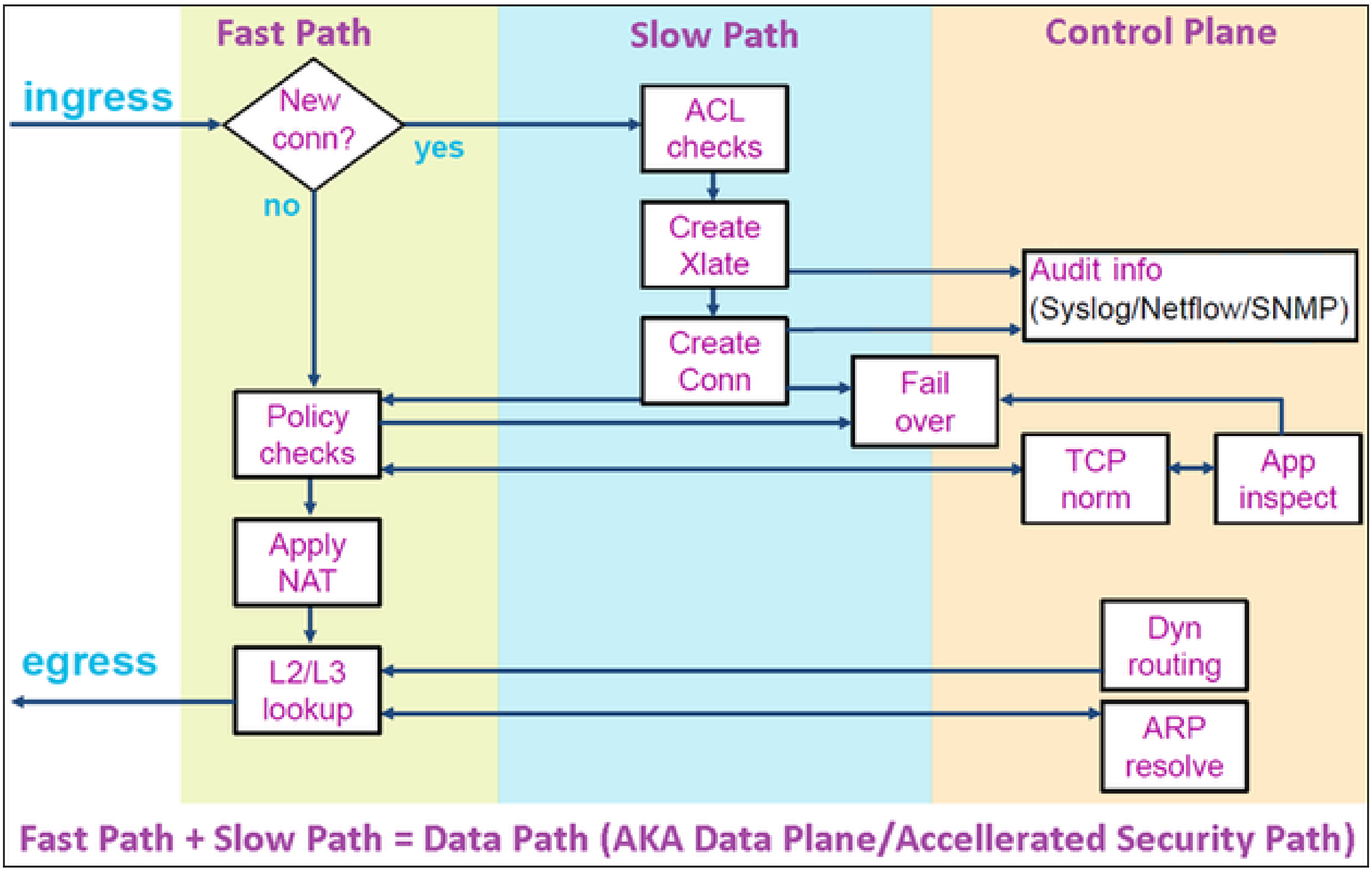
配置

案例1 — 基于连接查找的转发



如前所述，FTD LINA引擎的主要组件是数据路径进程（基于设备核心数量的多个实例）。此外，数据路径（也称为加速安全路径 — ASP）包括2条路径：

1. Slow Path =负责建立新连接（它填充快速路径）。
2. 快速路径=处理属于已建立连接的数据包。



- show route和show arp等命令显示控制平面的内容。
- 另一方面，show asp table routing和show asp table arp等命令显示ASP(Datapath)的内容，即实际应用的内容。

在FTD INSIDE接口上启用带跟踪的捕获：

```
firepower# capture CAPI trace detail interface INSIDE match ip host 192.168.1.1 host 198.51.100.1
```

通过FTD打开Telnet会话：

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ... Open
```

FTD捕获显示从连接开始的数据包（捕获TCP三次握手）：

```
firepower# show capture CAPI

26 packets captured
```

```
1: 10:50:38.407190 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: S 1306692135:1306692135(0) wi
2: 10:50:38.408929 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: S 1412677784:1412677784(0) ac
3: 10:50:38.409265 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128
4: 10:50:38.409433 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692136:1306692154(18) a
5: 10:50:38.409845 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128
6: 10:50:38.410135 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: . ack 1306692154 win 4110
7: 10:50:38.411355 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: P 1412677785:1412677797(12) a
8: 10:50:38.413049 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692154:1306692157(3) ac
9: 10:50:38.413140 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: P 1306692157:1306692166(9) ac
10: 10:50:38.414071 802.1Q vlan#101 P0 198.51.100.1.23 > 192.168.1.1.57734: . 1412677797:1412678322(525)
...
```

跟踪第一个数据包(TCP SYN)。此数据包通过FTD LINA慢路径，并且在此情况下会执行全局路由查找：

```
firepower# show capture CAPI packet-number 1 trace

26 packets captured

   1: 10:50:38.407190 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: S 1306692135:1306692135(0)
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 4683 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x1505f1d17940, priority=13, domain=capture, deny=false
hits=1783, user_data=0x1505f2096910, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 4683 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x1502a7ba4d40, priority=1, domain=permit, deny=false
hits=28, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 5798 ns
Config:
Additional Information:
```

```
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 3010 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
Forward Flow based lookup yields rule:
in id=0x1505f1e2e980, priority=12, domain=permit, deny=false
hits=4, user_data=0x15024a56b940, 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, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any,, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 3010 ns
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=0x1505f1f18bc0, priority=7, domain=conn-set, deny=false
hits=4, user_data=0x1505f1f13f70, 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=INSIDE(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 3010 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x15052e96b150, priority=0, domain=nat-per-session, deny=false
hits=125, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
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: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 3010 ns
Config:
Additional Information:
```

```
Forward Flow based lookup yields rule:
in id=0x1502a7bacde0, priority=0, domain=inspect-ip-options, deny=true
hits=19, 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=INSIDE(vrfid:0), output_ifc=any

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 52182 ns
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x15052e96b150, priority=0, domain=nat-per-session, deny=false
hits=127, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
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: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 892 ns
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x1502a7f9b460, priority=0, domain=inspect-ip-options, deny=true
hits=38, 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=OUTSIDE2(vrfid:0), output_ifc=any

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 25422 ns
Config:
Additional Information:
New flow created with id 244, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
```

```
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 36126 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Elapsed time: 564636 ns
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 182318660
Session: new snort session
AppID: service unknown (0), application unknown (0)
Snort id 28, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 7136 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 10 reference 1

Phase: 15
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 5352 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
out id=0x150521389870, priority=13, domain=capture, deny=false
hits=1788, user_data=0x1505f1d2b630, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=OUTSIDE2, output_ifc=any
```

```
Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 721180 ns

1 packet shown
firepower#
```

跟踪来自同一流的另一个入口数据包。与活动连接匹配的数据包：

```
firepower# show capture CAPI packet-number 3 trace

33 packets captured

3: 10:50:38.409265 802.1Q vlan#101 P0 192.168.1.1.57734 > 198.51.100.1.23: . ack 1412677785 win 4128
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2676 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x1505f1d17940, priority=13, domain=capture, deny=false
hits=105083, user_data=0x1505f2096910, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 2676 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x1502a7ba4d40, priority=1, domain=permit, deny=false
hits=45, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=INSIDE, output_ifc=any

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
```

```
Found flow with id 2552, using existing flow
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_snort
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_snort
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 16502 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Elapsed time: 12934 ns
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 1306692136, ack 1412677785
AppID: service unknown (0), application unknown (0)
Snort id 19, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 36126 ns

1 packet shown
firepower#
```

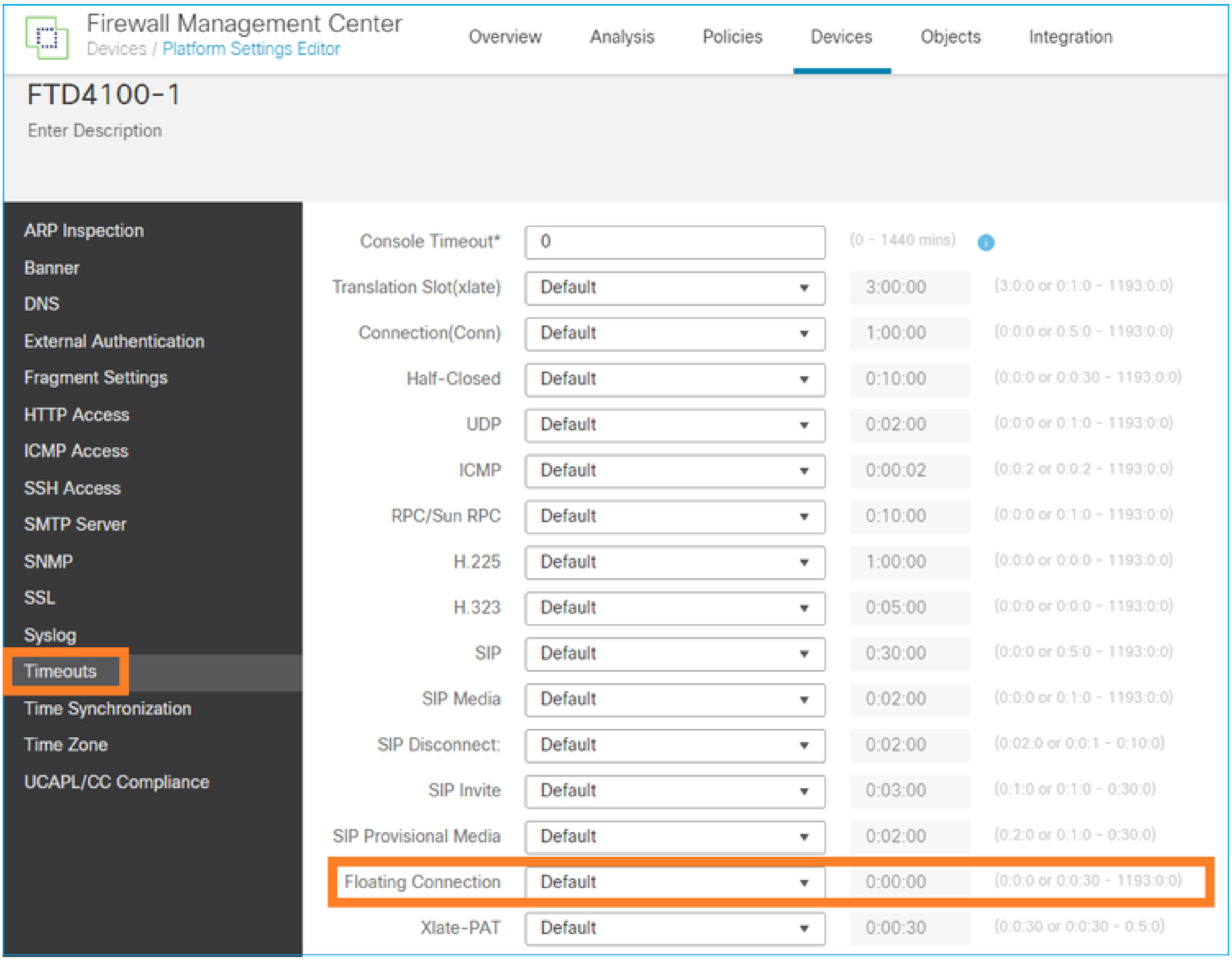
浮动超时

问题

临时路由不稳定可能导致通过FTD建立的长期（大象）UDP连接通过不同的FTD接口建立，而不是期望的。

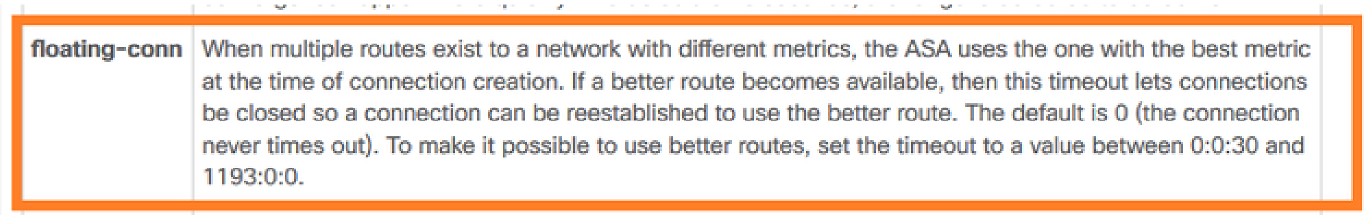
解决方案

要对此进行补救，请将timeout floating-conn设置为一个不同于默认值的值，默认值为禁用：



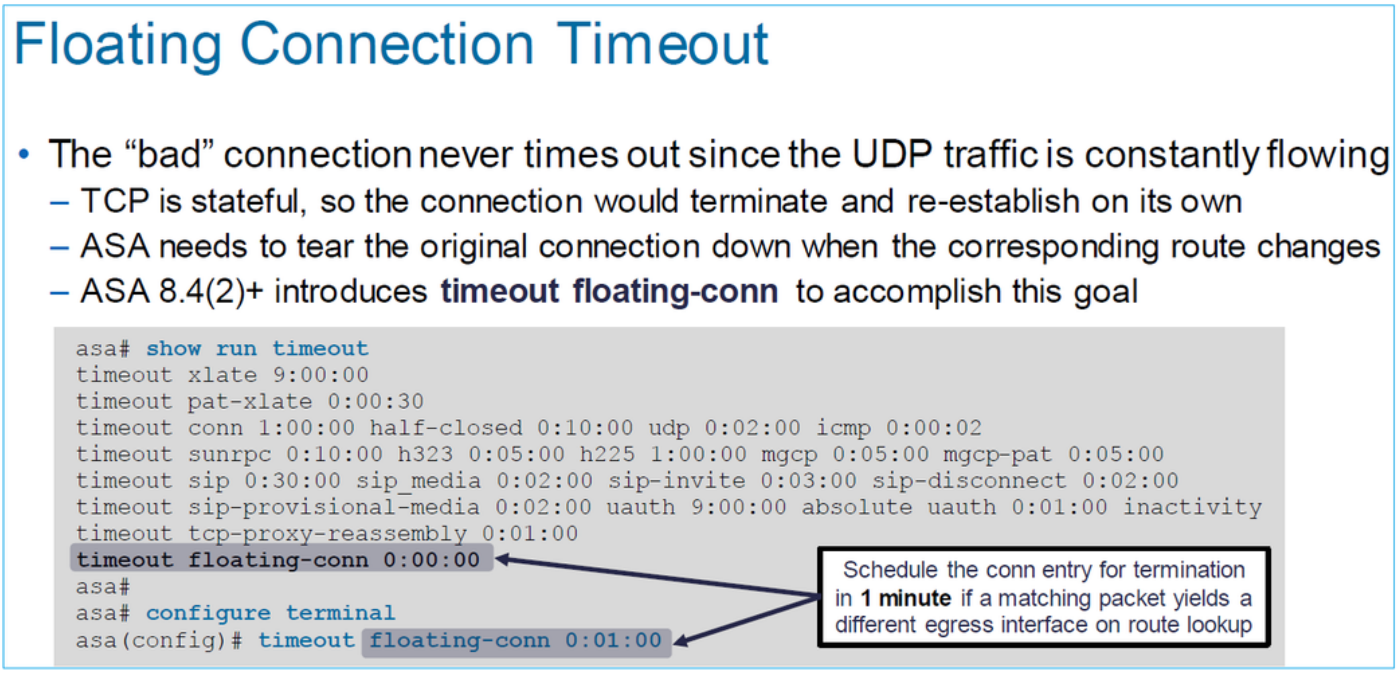
Console Timeout*	0	(0 - 1440 mins)	
Translation Slot(xlate)	Default	3:00:00	(3:0:0 or 0:1:0 - 1193:0:0)
Connection(Conn)	Default	1:00:00	(0:0:0 or 0:5:0 - 1193:0:0)
Half-Closed	Default	0:10:00	(0:0:0 or 0:0:30 - 1193:0:0)
UDP	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
ICMP	Default	0:00:02	(0:0:2 or 0:0:2 - 1193:0:0)
RPC/Sun RPC	Default	0:10:00	(0:0:0 or 0:1:0 - 1193:0:0)
H.225	Default	1:00:00	(0:0:0 or 0:0:0 - 1193:0:0)
H.323	Default	0:05:00	(0:0:0 or 0:0:0 - 1193:0:0)
SIP	Default	0:30:00	(0:0:0 or 0:5:0 - 1193:0:0)
SIP Media	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
SIP Disconnect:	Default	0:02:00	(0:02:0 or 0:0:1 - 0:10:0)
SIP Invite	Default	0:03:00	(0:1:0 or 0:1:0 - 0:30:0)
SIP Provisional Media	Default	0:02:00	(0:2:0 or 0:1:0 - 0:30:0)
Floating Connection	Default	0:00:00	(0:0:0 or 0:0:30 - 1193:0:0)
Xlate-PAT	Default	0:00:30	(0:0:30 or 0:0:30 - 0:5:0)

在Command Reference（命令参考）中：



floating-conn	When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0.

有关详细信息，请参阅案例研究：从CiscoLive BRKSEC-3020会话重新加载后UDP连接失败：



Floating Connection Timeout

- The “bad” connection never times out since the UDP traffic is constantly flowing
  - TCP is stateful, so the connection would terminate and re-establish on its own
  - ASA needs to tear the original connection down when the corresponding route changes
  - ASA 8.4(2)+ introduces **timeout floating-conn** to accomplish this goal

```
asa# show run timeout
timeout xlate 9:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 9:00:00 absolute uauth 0:01:00 inactivity
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
asa#
asa# configure terminal
asa(config)# timeout floating-conn 0:01:00
```

Schedule the conn entry for termination in **1 minute** if a matching packet yields a different egress interface on route lookup

连接抑制超时

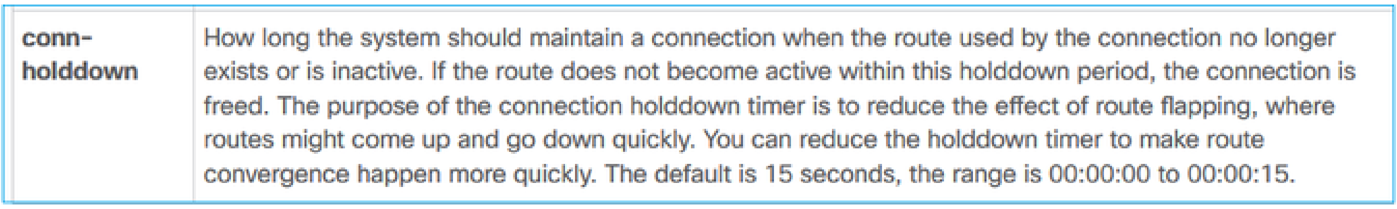
问题

路由断开（被删除），但流量与已建立的连接匹配。

解决方案

ASA 9.6.2上添加了超时连接抑制功能。该功能默认启用，但目前(7.1.x)不受FMC UI或FlexConfig支持。相关增强：增强版：超时连接抑制不可用于FMC中的配置

从ASA CLI指南：



conn-holddown	How long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. The purpose of the connection holddown timer is to reduce the effect of route flapping, where routes might come up and go down quickly. You can reduce the holddown timer to make route convergence happen more quickly. The default is 15 seconds, the range is 00:00:00 to 00:00:15.

```
firepower# show run all timeout
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
```

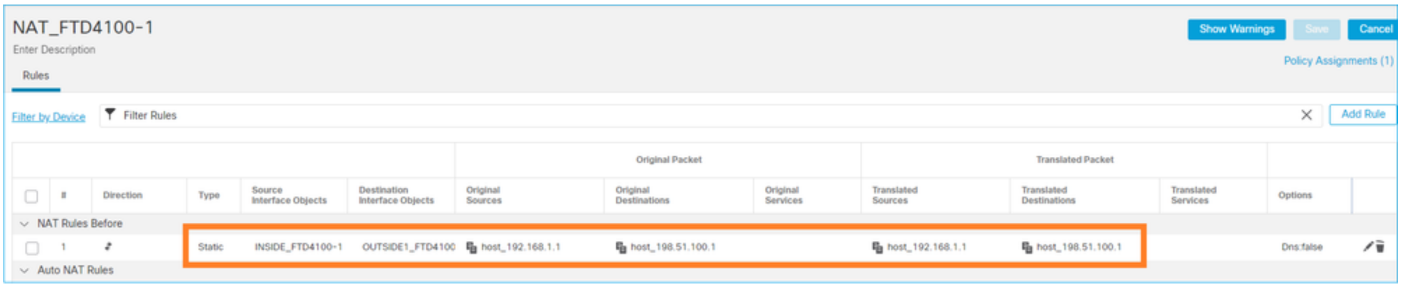
案例2 — 基于NAT查找的转发

要求

配置此NAT规则：

- 类型：静态
- 源接口：INSIDE
- 目标接口：OUTSIDE1
- 原始源：192.168.1.1
- 原始目的地：198.51.100.1
- 转换后的源：192.168.1.1
- 转换后的目的地：198.51.100.1

解决方案



NAT_FTD4100-1

Enter Description

Rules

Filter by Device | Filter Rules | Add Rule

						Original Packet			Translated Packet			
□	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before												
□	1	⇄	Static	INSIDE_FTD4100-1	OUTSIDE1_FTD4100	host_192.168.1.1	host_198.51.100.1		host_192.168.1.1	host_198.51.100.1		Dns:false
Auto NAT Rules												

在FTD CLI上部署的NAT规则：

```
firepower# show run nat
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.10
firepower# show nat
Manual NAT Policies (Section 1)
1 (INSIDE) to (OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51
translate_hits = 0, untranslate_hits = 0
```

配置3个捕获：

```
firepower# capture CAPI trace detail interface INSIDE match ip host 192.168.1.1 host 198.51.100.1
firepower# capture CAPO1 interface OUTSIDE1 match ip host 192.168.1.1 any
firepower# capture CAPO2 interface OUTSIDE2 match ip host 192.168.1.1 any
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 0 bytes]
match ip host 192.168.1.1 host 198.51.100.1
capture CAPO1 type raw-data interface OUTSIDE1 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
capture CAPO2 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
```

```
match ip host 192.168.1.1 any
```

启动从192.168.1.1到198.51.100.1的telnet会话：

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

数据包到达FTD，但没有数据包离开OUTSIDE1和OUTSIDE2接口：

```
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 156 bytes]
match ip host 192.168.1.1 host 198.51.100.1
capture CAPO1 type raw-data interface OUTSIDE1 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
capture CAPO2 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
```

跟踪TCP SYN数据包。第3阶段(UN-NAT)显示NAT（尤其是UN-NAT）将数据包转移到OUTSIDE1接口进行下一跳查找：

```
firepower# show capture CAPI
2 packets captured
1: 11:22:59.179678 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) w
2: 11:23:01.179632 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) w
2 packets shown
firepower#
```

```
firepower# show capture CAPI packet-number 1 trace detail

2 packets captured

1: 11:22:59.179678 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S [tcp sum ok] 1174675193:1174675193(0) win 412
...

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 6244 ns
Config:
```

```
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.10
Additional Information:
NAT divert to egress interface OUTSIDE1(vrfid:0)
Untranslate 198.51.100.1/23 to 198.51.100.1/23

...
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 25422 ns
Config:
Additional Information:
New flow created with id 2614, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat


Phase: 15
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 8028 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 16
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 777375 ns
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame 0x00005577204a7287 flow (NA)/NA


1 packet shown
```

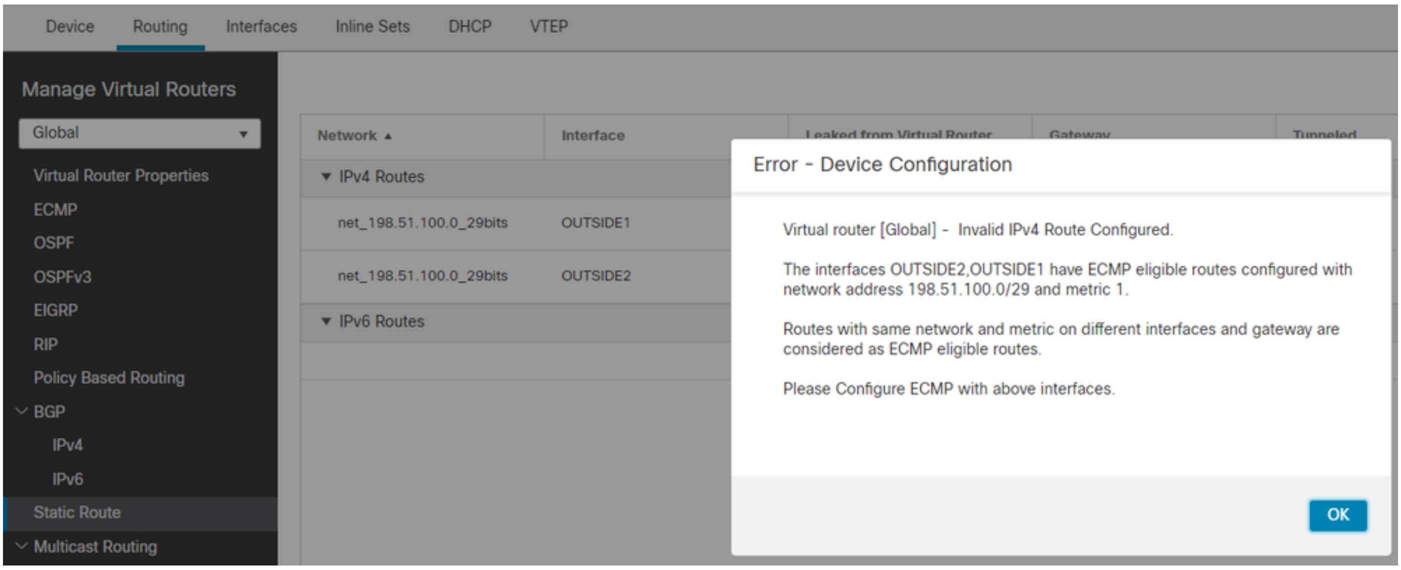
在这种情况下，SUBOPTIMAL-LOOKUP意味着NAT进程(OUTSIDE1)确定的出口接口不同于ASP输入表中指定的出口接口：

```
firepower# show asp table routing | include 198.51.100.0
in 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
```

一种可能的解决方法是在OUTSIDE1接口上添加浮动静态路由：

```
firepower# show run route
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
route OUTSIDE1 198.51.100.0 255.255.255.248 203.0.113.99 200
```

注意：如果您尝试添加的静态路由度量与已经存在的静态路由度量相同，则会出现以下错误：



Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled
IPv4 Routes				
net_198.51.100.0_29bits	OUTSIDE1			
net_198.51.100.0_29bits	OUTSIDE2			
IPv6 Routes				

Error - Device Configuration

Virtual router [Global] - Invalid IPv4 Route Configured.

The interfaces OUTSIDE2,OUTSIDE1 have ECMP eligible routes configured with network address 198.51.100.0/29 and metric 1.

Routes with same network and metric on different interfaces and gateway are considered as ECMP eligible routes.

Please Configure ECMP with above interfaces.

注意：路由表中未安装距离度量为255的浮动路由。

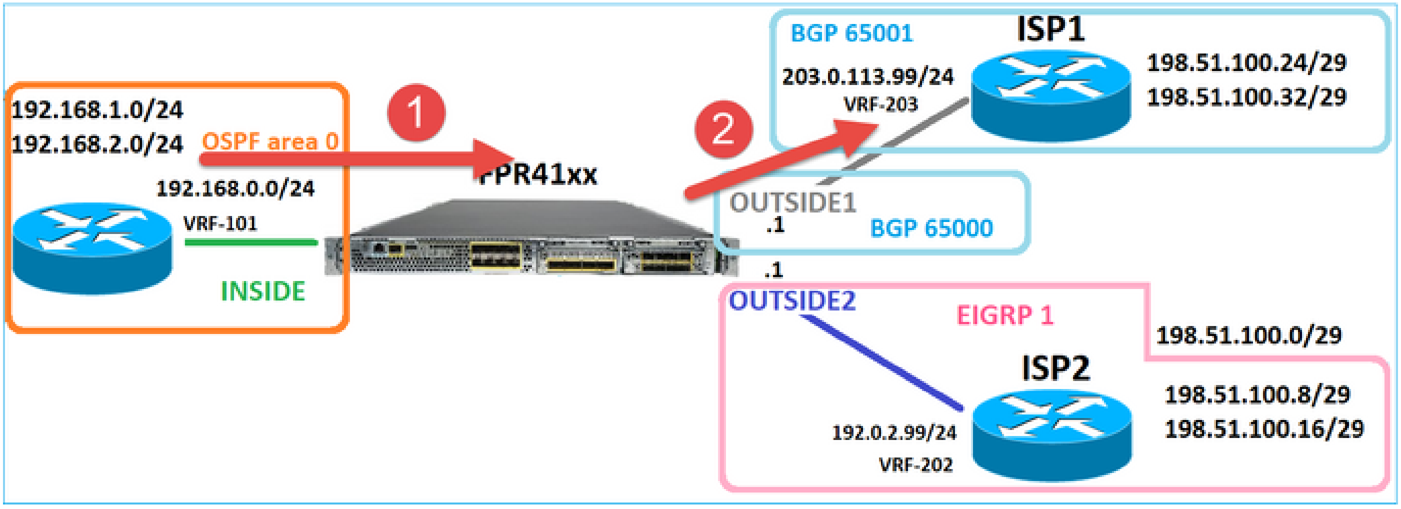
尝试Telnet以确认存在通过FTD发送的数据包：

```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

```
firepower# show capture
capture CAPI type raw-data trace detail interface INSIDE [Capturing - 156 bytes]
```

```
match ip host 192.168.1.1 host 198.51.100.1
capture CAPO1 type raw-data interface OUTSIDE1 [Capturing - 312 bytes]
match ip host 192.168.1.1 any
capture CAPO2 type raw-data interface OUTSIDE2 [Capturing - 386 bytes]
match ip host 192.168.1.1 any
```

数据包跟踪显示由于NAT查找，数据包被转发到ISP1(OUTSIDE1)接口而不是ISP2:



```
firepower# show capture CAPI packet-number 1 trace

2 packets captured

1: 09:03:02.773962 802.1Q vlan#101 P0 192.168.1.1.16774 > 198.51.100.1.23: S 2910053251:2910053251(0) w
...

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 4460 ns
Config:
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.10
Additional Information:
NAT divert to egress interface OUTSIDE1(vrfid:0)
Untranslate 198.51.100.1/23 to 198.51.100.1/23

...

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 29436 ns
Config:
Additional Information:
New flow created with id 2658, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_snort
```

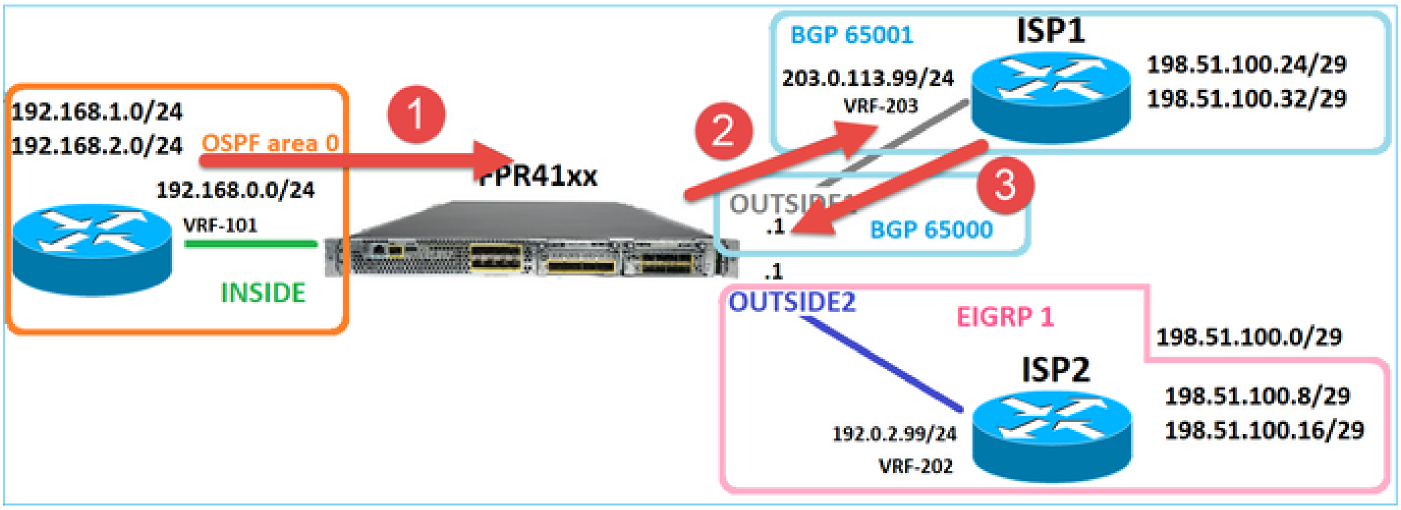
```
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 15
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 5798 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 16
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 446 ns
Config:
Additional Information:
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Phase: 17
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1(vrfid:0)

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 106 reference 2
...

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 723409 ns


1 packet shown
firepower#
```

有趣的是，在这种情况下，INSIDE接口和两个出口接口上均显示了数据包：

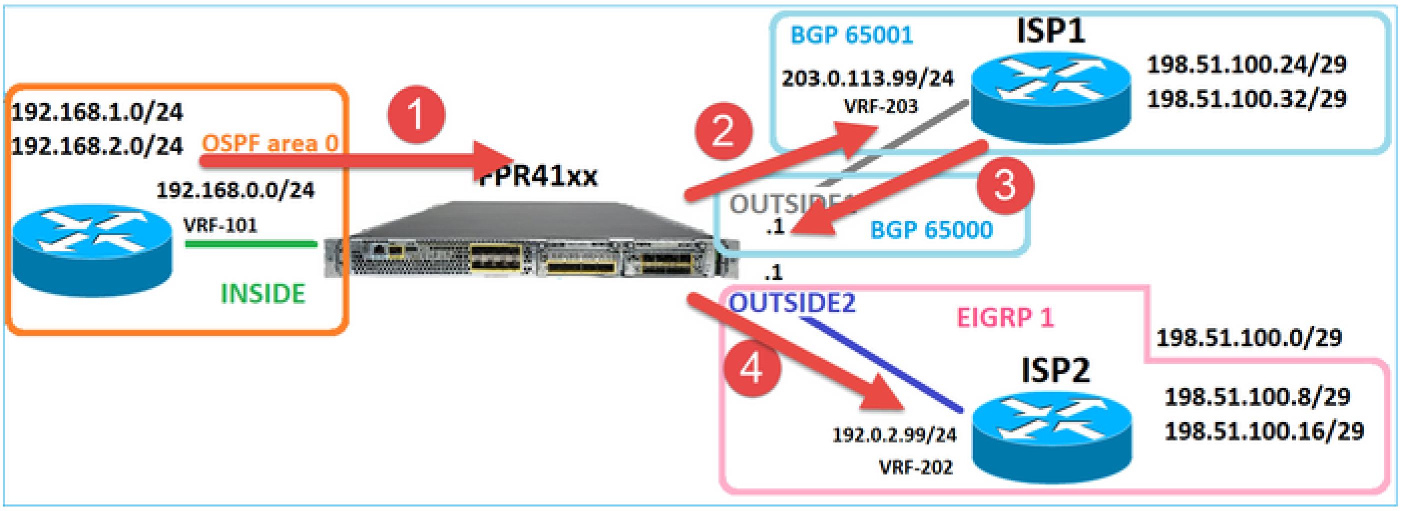
```
firepower# show capture CAPI

2 packets captured

1: 09:03:02.773962 802.1Q vlan#101 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) wi
2: 09:03:05.176565 802.1Q vlan#101 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) wi
2 packets shown
firepower# show capture CAPO1

4 packets captured

1: 09:03:02.774358 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) wi
2: 09:03:02.774557 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) wi
3: 09:03:05.176702 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) wi
4: 09:03:05.176870 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) wi
4 packets shown
firepower# show capture CAPO2

5 packets captured

1: 09:03:02.774679 802.1Q vlan#202 P0 192.168.1.1.32134 > 198.51.100.1.23: S 194652172:194652172(0) win
2: 09:03:02.775457 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) ac
3: 09:03:05.176931 802.1Q vlan#202 P0 192.168.1.1.32134 > 198.51.100.1.23: S 194652172:194652172(0) win
4: 09:03:05.177282 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: . ack 194652173 win 4128
5: 09:03:05.180517 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) ac
```

数据包详细信息包括MAC地址信息，对OUTSIDE1和OUTSIDE2接口上的数据包进行跟踪可显示数据包的路径：

```
firepower# show capture CAPO1 detail

4 packets captured

1: 09:03:02.774358 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 412
2: 09:03:02.774557 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 412
3: 09:03:05.176702 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 412
4: 09:03:05.176870 4c4e.35fc.fcd8 00be.75f6.1dae 0x8100 Length: 62
802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S [tcp sum ok] 3249840142:3249840142(0) win 412
4 packets shown
```



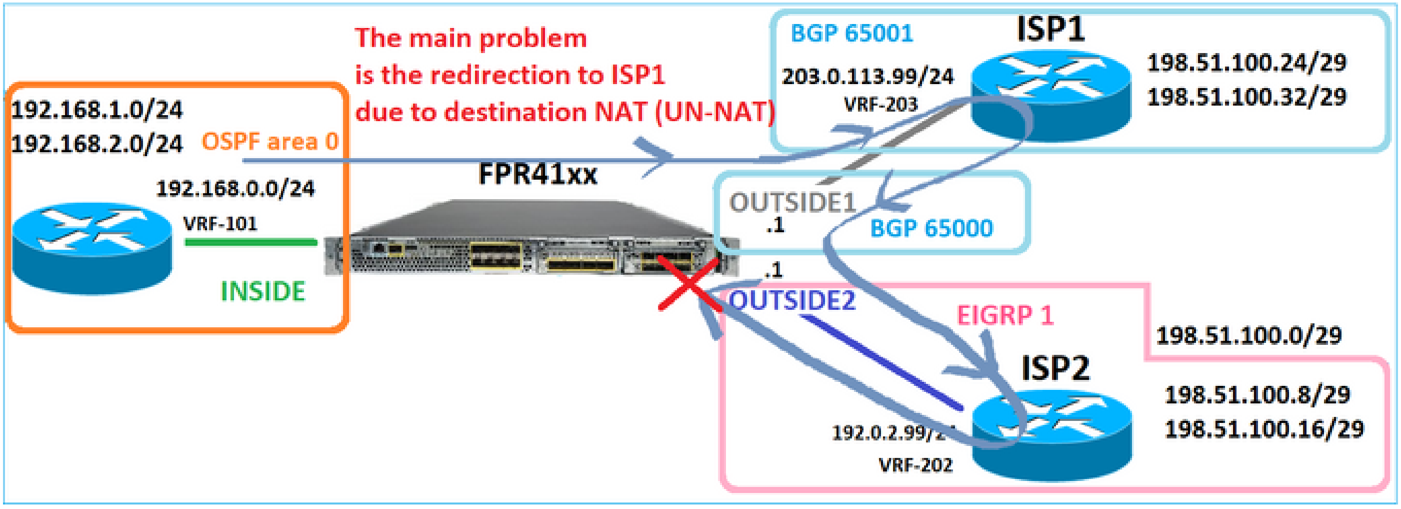
返回的数据包的跟踪显示由于全局路由表查找而重定向到OUTSIDE2接口：



```
firepower# show capture CAP01 packet-number 2 trace

4 packets captured

2: 09:03:02.774557 802.1Q vlan#203 P0 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
...

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 7136 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

...

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 12488 ns
Config:
```

```
Additional Information:
New flow created with id 13156, packet dispatched to next module

...

Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 3568 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1

...

Result:
input-interface: OUTSIDE1(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 111946 ns


1 packet shown
firepower#
```

ISP2路由器发送应答(SYN/ACK)，但此数据包被重定向到ISP1，因为它与已建立的连接匹配。由于ASP输出表中没有L2邻接关系，数据包被FTD丢弃：



```
firepower# show capture CAPO2 packet-number 2 trace

5 packets captured

2: 09:03:02.775457 802.1Q vlan#202 P0 198.51.100.1.23 > 192.168.1.1.32134: S 4075003210:4075003210(0) a
...

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
Found flow with id 13156, using existing flow

...

Phase: 7
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
Input route lookup returned ifc INSIDE is not same as existing ifc OUTSIDE1

Result:
input-interface: OUTSIDE2(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 52628 ns
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame 0x00005577204a7287 flow (NA)/NA
```

案例3 — 基于策略路由(PBR)的转发

在连接流查找和目标NAT查找之后，PBR是可能影响出口接口确定的下一项。PBR的文档记录在 :Policy Based Routing

对于FMC上的PBR配置，请务必注意以下指南：
FlexConfig用于在FMC中为早于7.1的FTD版本配置PBR。您仍然可以使用FlexConfig在所有版本中配置PBR。但是，对于入口接口，不能同时使用FlexConfig和FMC的基于策略的路由页面配置PBR。

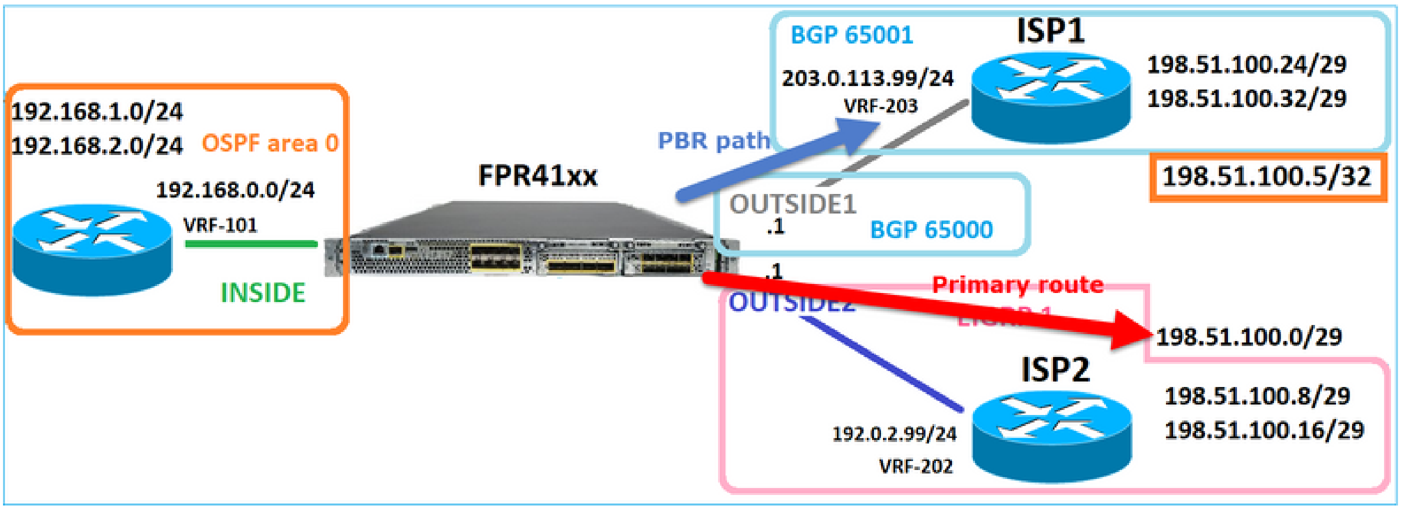
在本案例研究中，FTD有一条指向198.51.100.0/24的路由，该路由指向ISP2:

```
firepower# show route | begin Gate
Gateway of last resort is not set

C 192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C 192.168.0.0 255.255.255.0 is directly connected, INSIDE
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
O 192.168.1.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, INSIDE
O 192.168.2.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, INSIDE
S 198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D 198.51.100.8 255.255.255.248
[90/130816] via 192.0.2.99, 5d01h, OUTSIDE2
D 198.51.100.16 255.255.255.248
[90/130816] via 192.0.2.99, 5d01h, OUTSIDE2
B 198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 5d00h
B 198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 5d00h
C 203.0.113.0 255.255.255.0 is directly connected, OUTSIDE1
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

要求

使用以下特征配置PBR策略：

- 从IP 192.168.2.0/24发往198.51.100.5的流量必须发送到ISP1（下一跳203.0.113.99），而其他源必须使用OUTSIDE2接口。



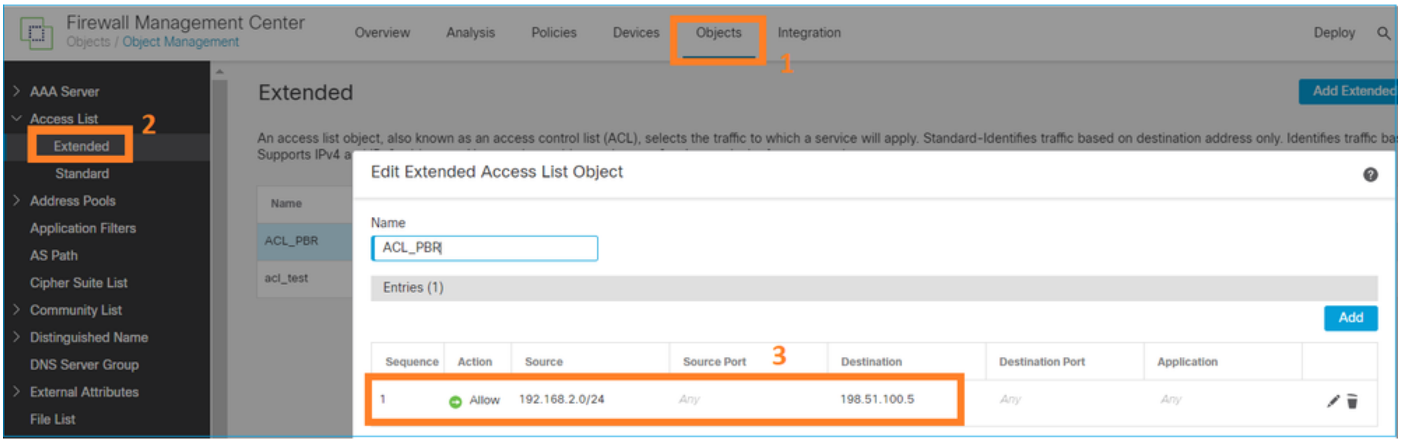
解决方案

在7.1之前的版本中，要配置PBR，请执行以下操作：
1.创建匹配相关流量（例如PBR_ACL）的扩展ACL。
2.创建与步骤1中创建的ACL匹配的路由映射，并设置所需的下一跳。
3.使用步骤2中创建的路由映射创建在入口接口上启用PBR的FlexConfig对象。

在7.1之后的版本中，您可以使用7.1之前版本的方式配置PBR，也可以在Device > Routing部分下使用新的基于策略的路由选项：
1.创建匹配相关流量（例如PBR_ACL）的扩展ACL。
2.添加PBR策略并指定：
a.匹配的流量
b.入口接口
c.下一跳

配置PBR（新方式）

第1步 — 为匹配流量定义访问列表。



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 ba
Supports IPv4 a

Edit Extended Access List Object

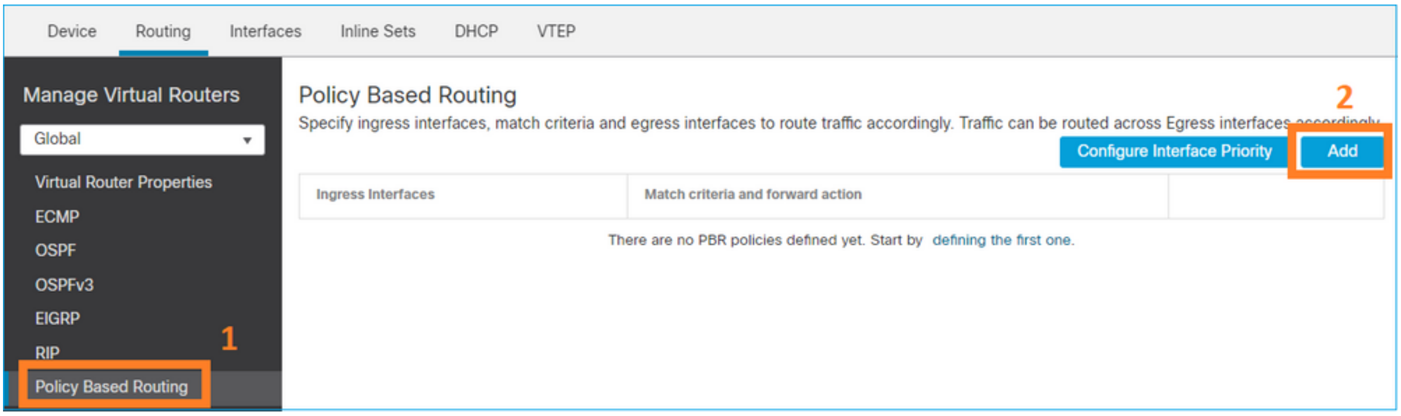
Name
ACL_PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	192.168.2.0/24	Any	198.51.100.5	Any	Any

第2步 — 添加PBR策略

导航到Devices > Device Management，然后编辑FTD设备。选择Routing > Policy Based Routing，然后在Policy Based Routing页面中选择Add。

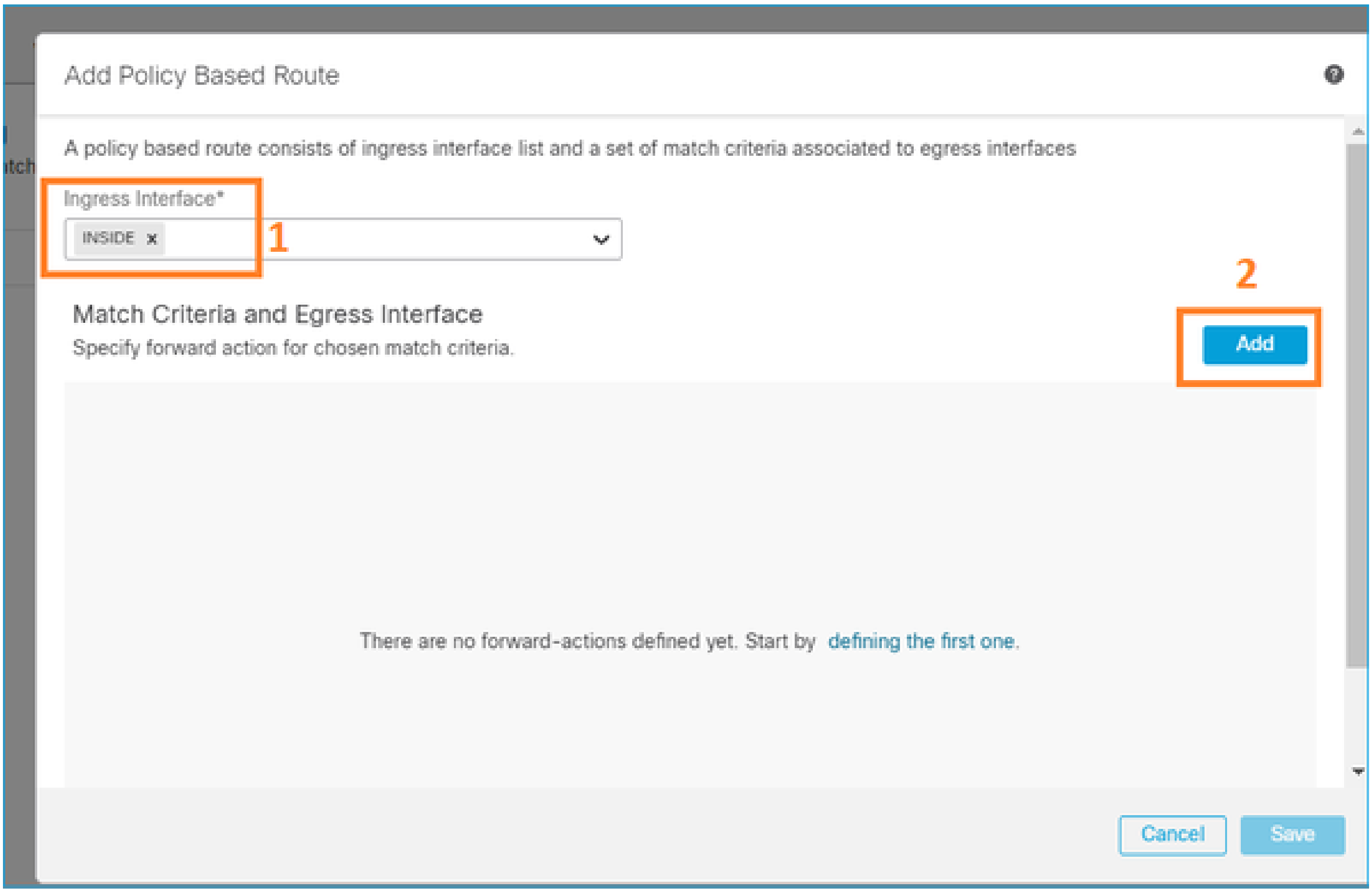


Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly.

There are no PBR policies defined yet. Start by defining the first one.

指定入口接口：



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

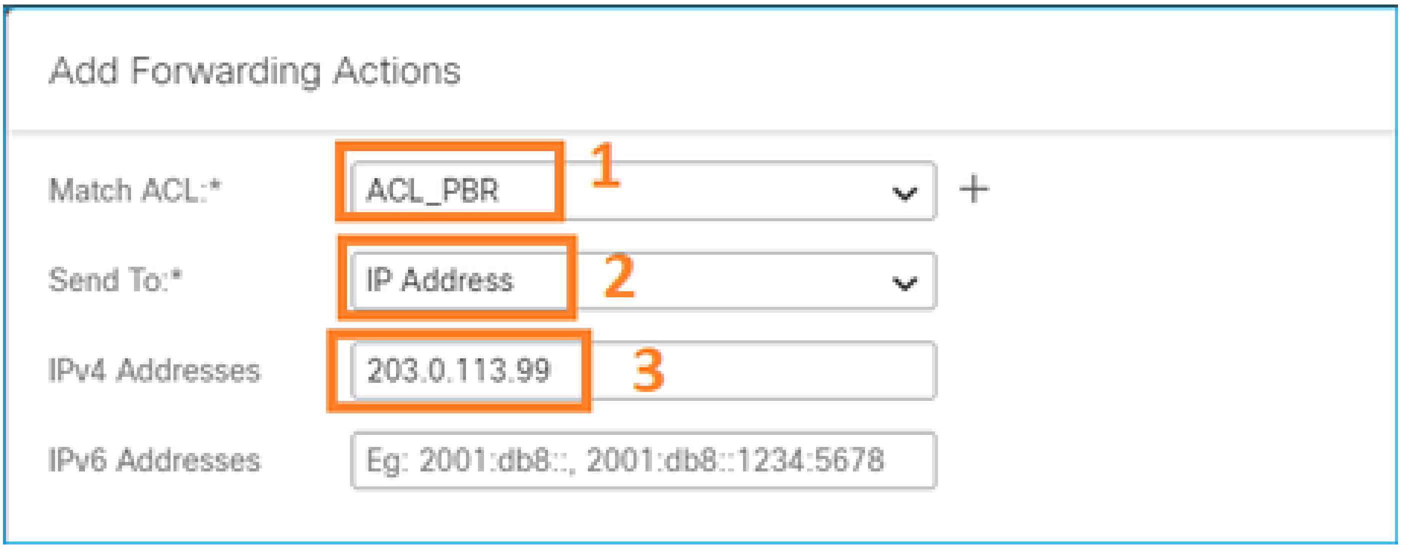
Ingress Interface*: INSIDE

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

There are no forward-actions defined yet. Start by defining the first one.

指定转发操作：



Add Forwarding Actions

Match ACL:* ACL_PBR

Send To:* IP Address

IPv4 Addresses 203.0.113.99

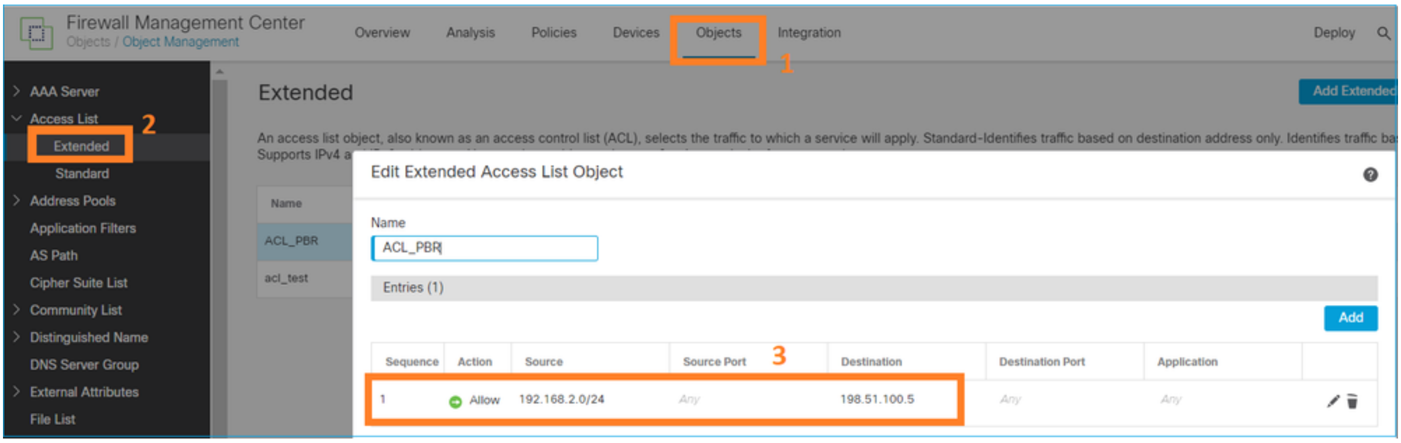
IPv6 Addresses Eg: 2001:db8::, 2001:db8::1234:5678

保存和部署

注意：如果要配置多个出口接口，必须在“发送至”字段中设置“出口接口”选项（从版本7.0+开始提供）。有关更多详细信息，请参[阅：基于策略的路由配置示例](#)

配置PBR（传统方式）

第1步 — 为匹配流量定义访问列表。



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 ba
Supports IPv4 a

Edit Extended Access List Object

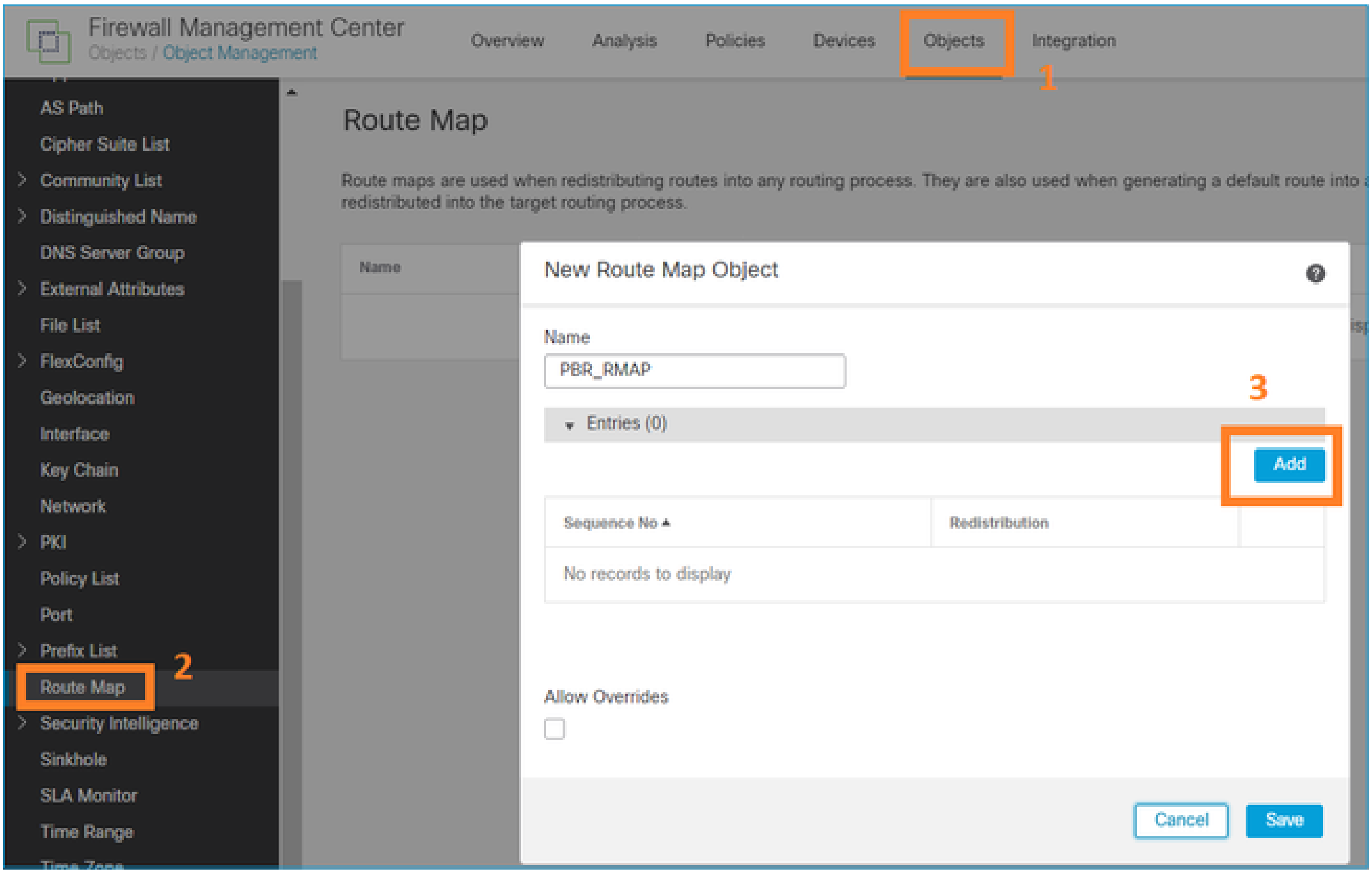
Name: ACL_PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	192.168.2.0/24	Any	198.51.100.5	Any	Any

第2步 — 定义与ACL匹配的路由映射并设置下一跳。

首先，定义Match子句：

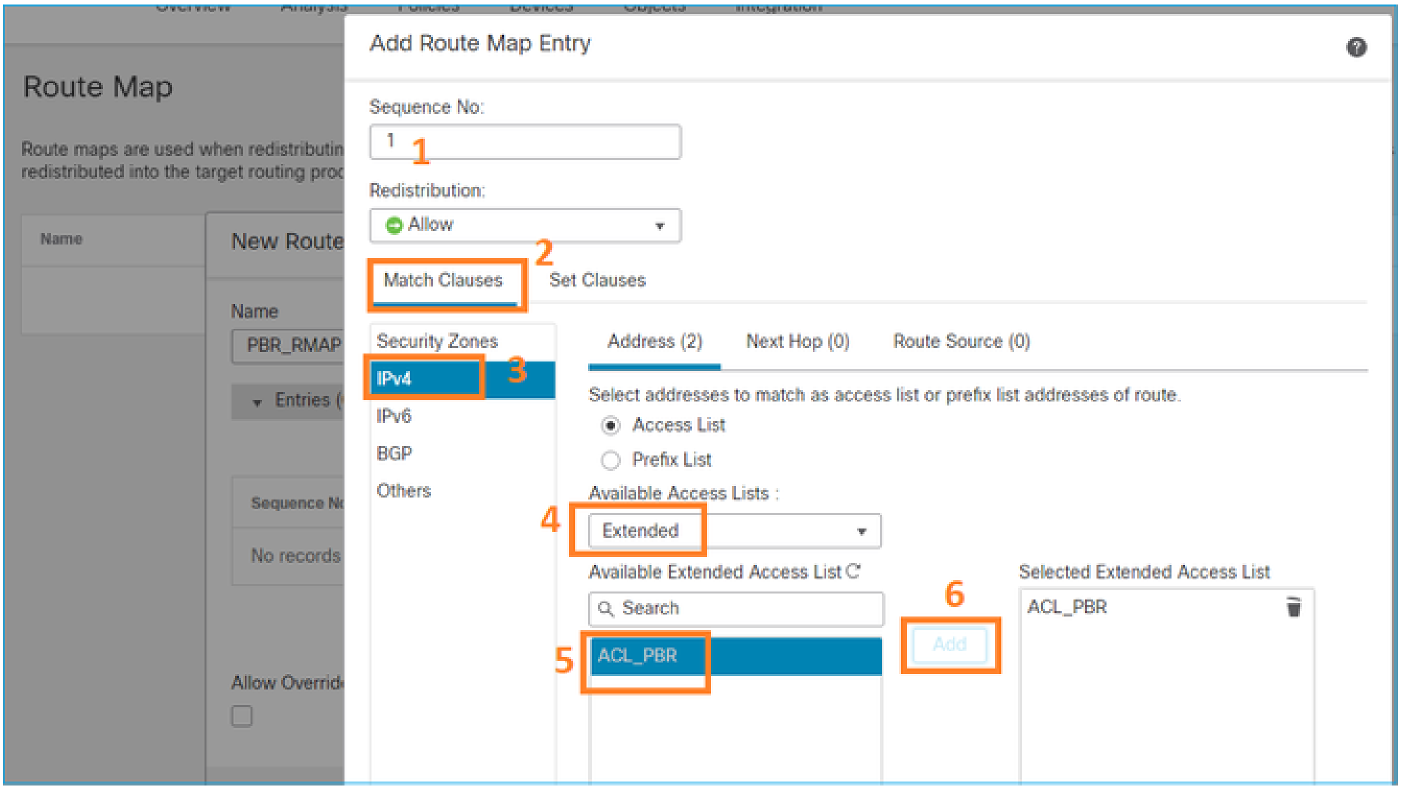


Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a redistributed into the target routing process.

Name: PBR_RMAP

Entries (0)

Allow Overrides □



Route maps are used when redistributin redistributed into the target routing proc

Name: PBR_RMAP

Sequence No: 1

Redistribution: Allow

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

● Access List

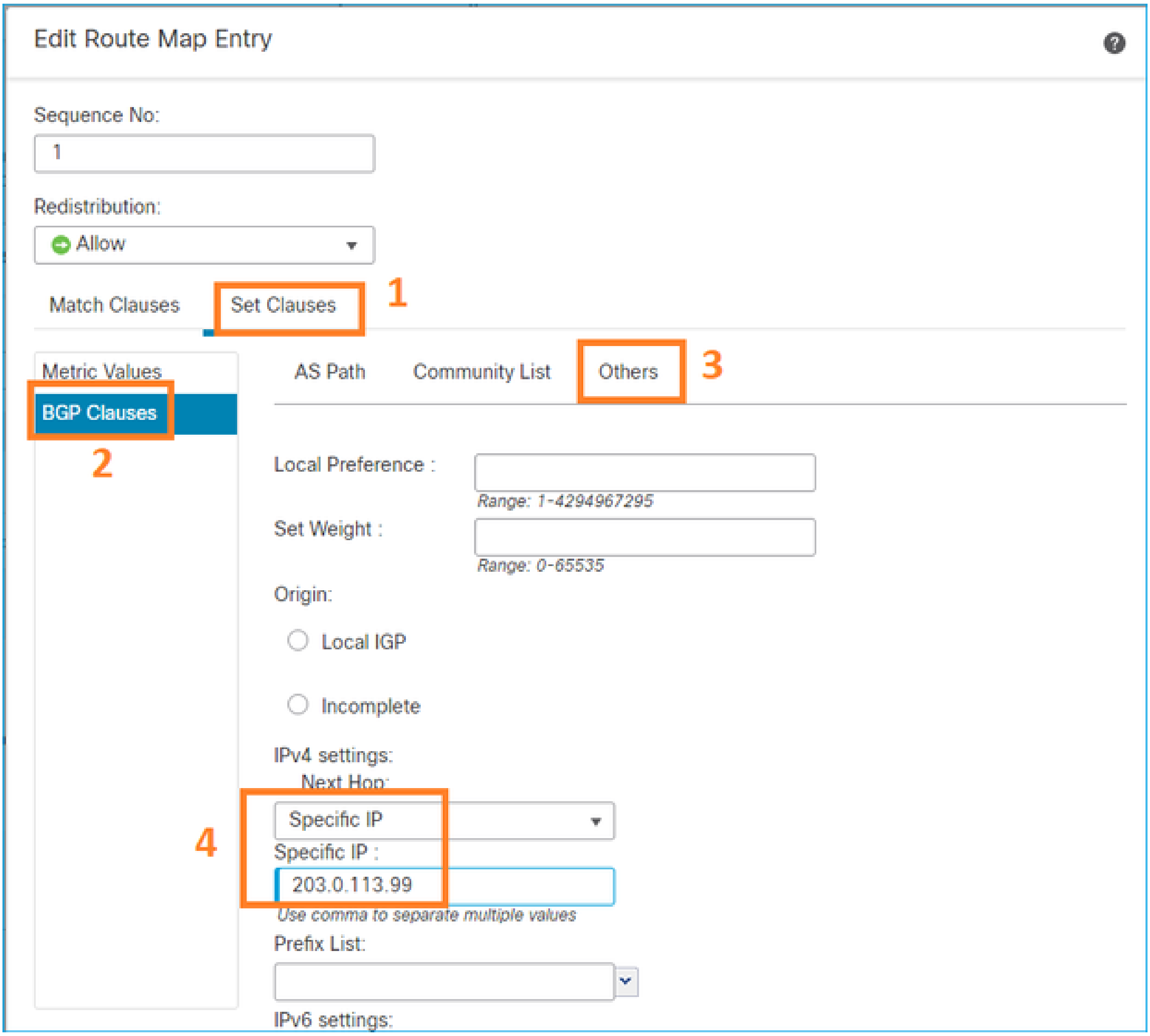
○ Prefix List

Available Access Lists : Extended

Available Extended Access List: ACL_PBR

Selected Extended Access List: ACL_PBR

定义Set子句：



Sequence No: 1

Redistribution: Allow

Local Preference :
Range: 1-4294967295

Set Weight :
Range: 0-65535

Origin:

○ Local IGP

○ Incomplete

IPv4 settings:
Next Hop:
Specific IP
Specific IP : 203.0.113.99
Use comma to separate multiple values

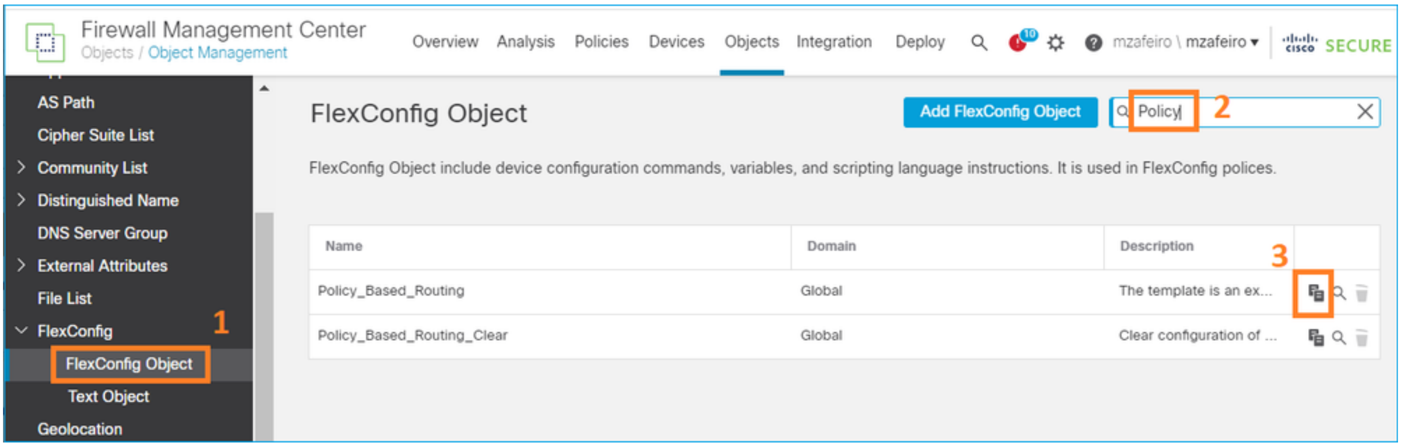
Prefix List:

IPv6 settings:

添加并保存。

第3步 — 配置FlexConfig PBR对象。

首先，复制（复制）现有PBR对象：



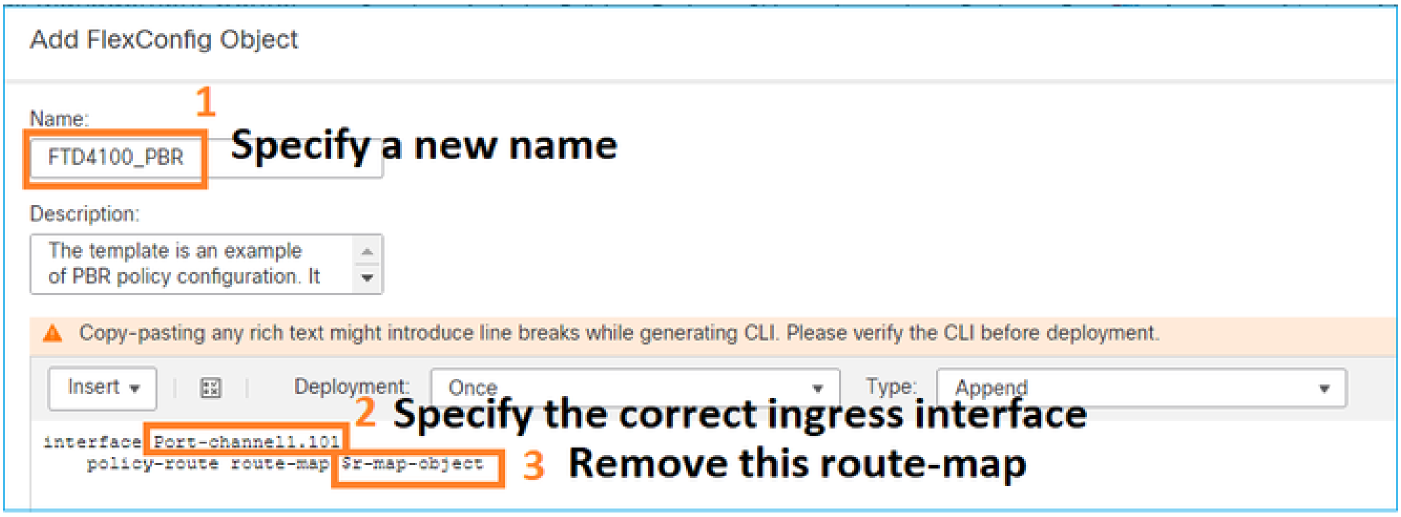
FlexConfig Object

Search: Policy

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

Name	Domain	Description
Policy_Based_Routing	Global	The template is an ex...
Policy_Based_Routing_Clear	Global	Clear configuration of ...

指定Object名称并删除预定义的路由映射对象：



Add FlexConfig Object

Name: FTD4100_PBR

1 Specify a new name

Description: The template is an example of PBR policy configuration. It

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

Deployment: Once

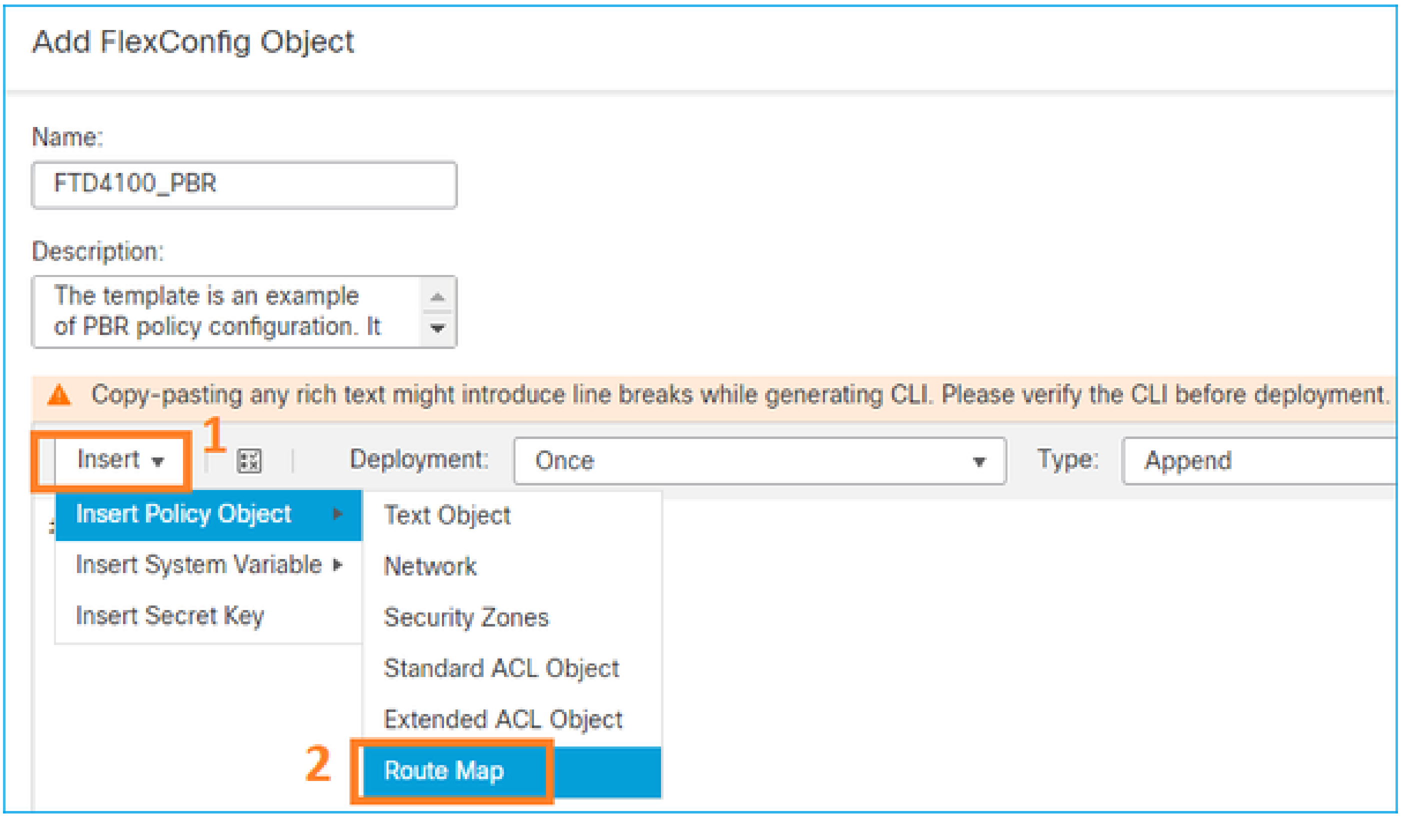
Type: Append

```
interface Port-channel1.101
    policy-route route-map $r-map-object
```

2 Specify the correct ingress interface

3 Remove this route-map

指定新的路由映射：



Add FlexConfig Object

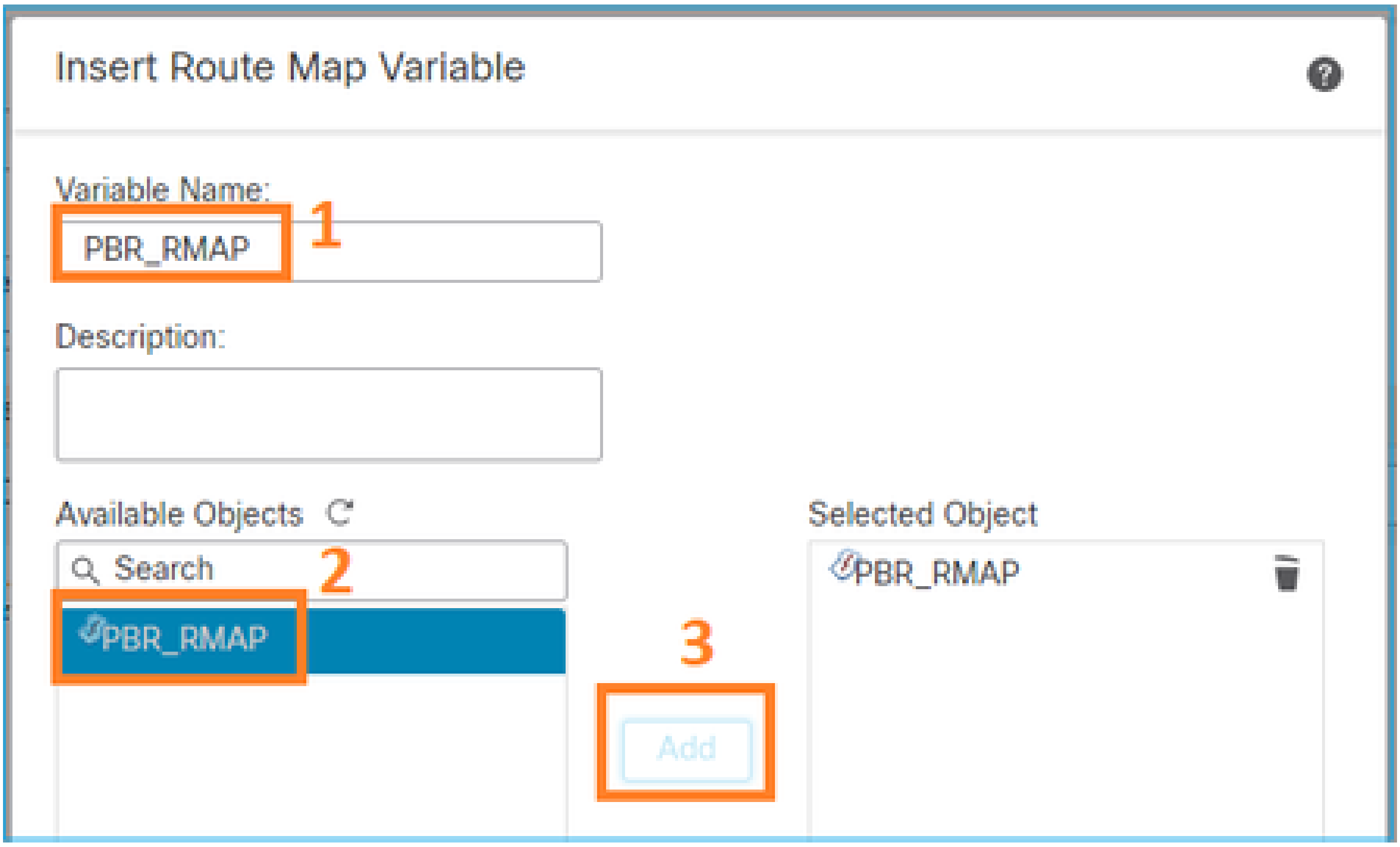
Name: FTD4100_PBR

Description: The template is an example of PBR policy configuration. It

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

Deployment: Once

Type: Append


Insert Route Map Variable

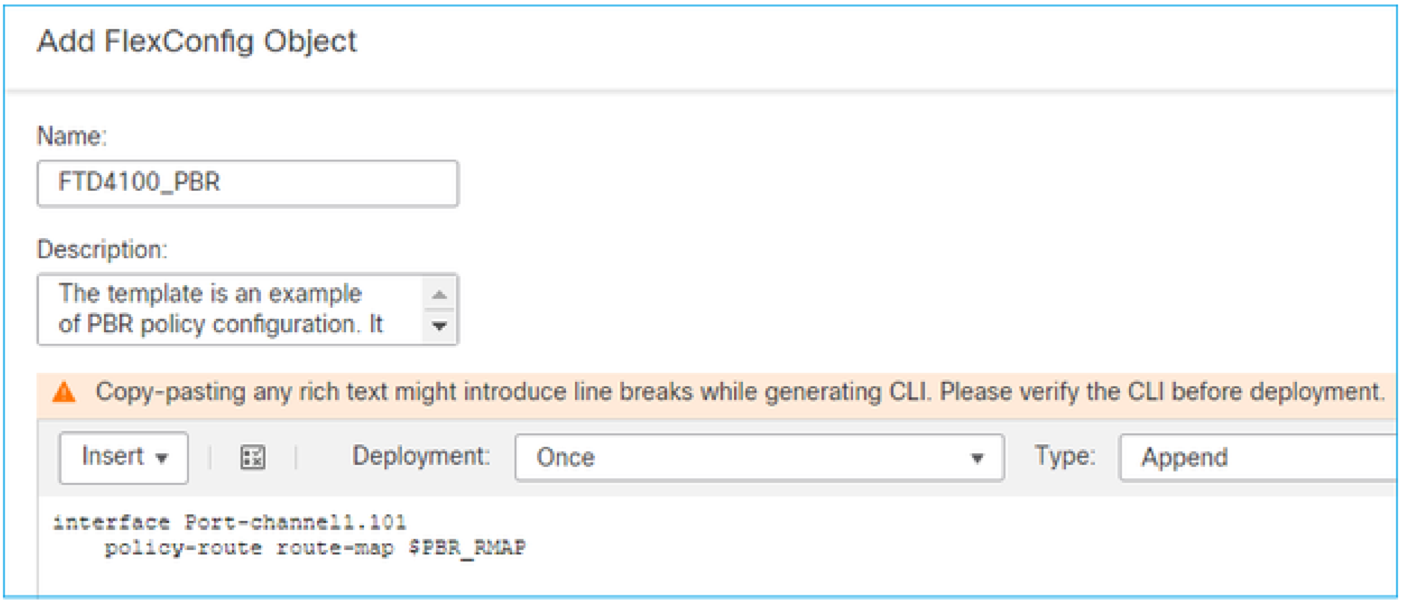
Variable Name: PBR_RMAP

Description:

Available Objects: PBR_RMAP

Selected Object: PBR_RMAP

这就是最终结果：


Add FlexConfig Object

Name: FTD4100_PBR

Description: The template is an example of PBR policy configuration. It

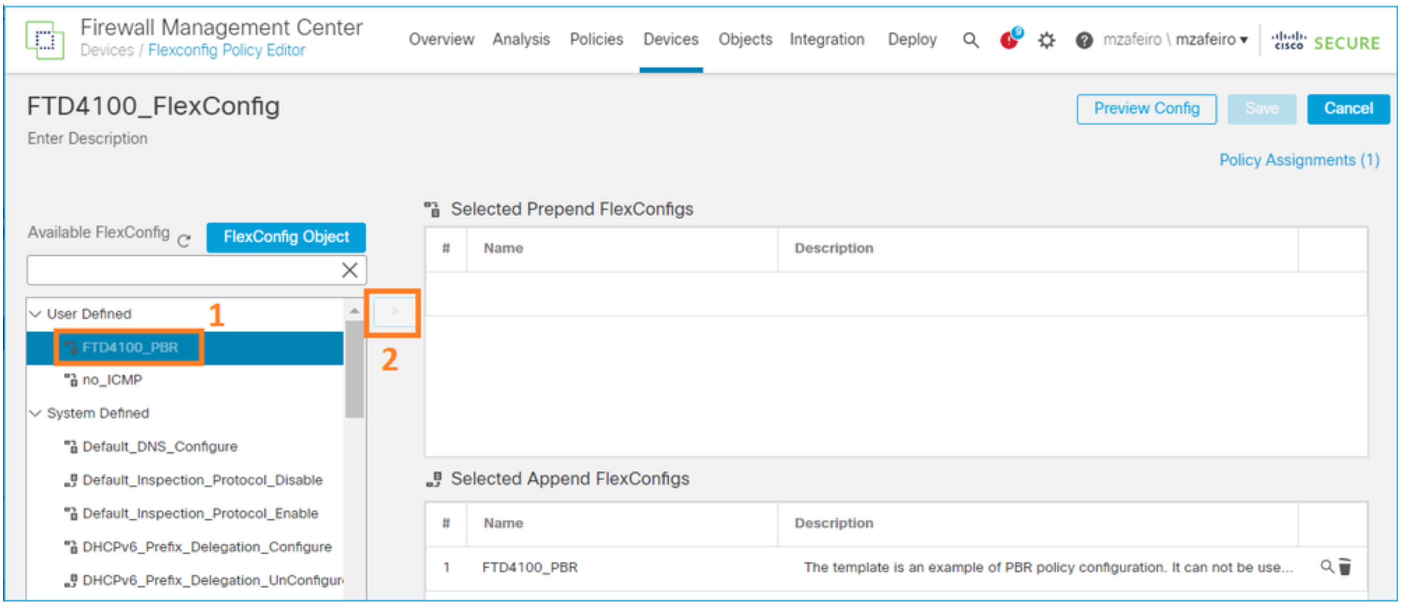
Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once

Type: Append

```
interface Port-channel1.101
    policy-route route-map $PBR_RMAP
```

第4步 — 将PBR对象添加到FTD FlexConfig策略。


Firewall Management Center
Devices / Flexconfig Policy Editor
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
mzafeiro \ mzafeiro
SECURE
Preview Config
Save
Cancel
Policy Assignments (1)
Available FlexConfig
FlexConfig Object
User Defined
1
FTD4100_PBR
no_ICMP
System Defined
Default_DNS_Configure
Default_Inspection_Protocol_Disable
Default_Inspection_Protocol_Enable
DHCPv6_Prefix_Delegation_Configure
DHCPv6_Prefix_Delegation_UnConfigur
2
Selected Prepend FlexConfigs
Selected Append FlexConfigs

FTD4100_FlexConfig

Enter Description

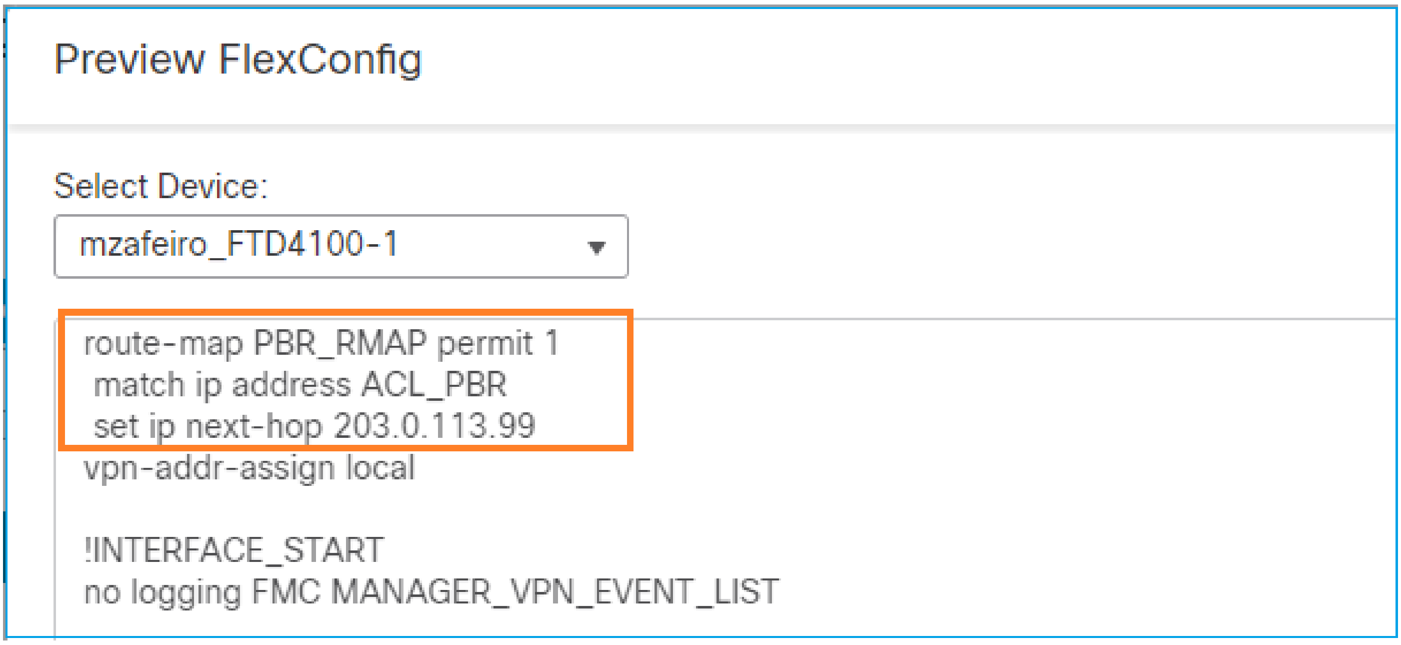
Selected Prepend FlexConfigs

#	Name	Description

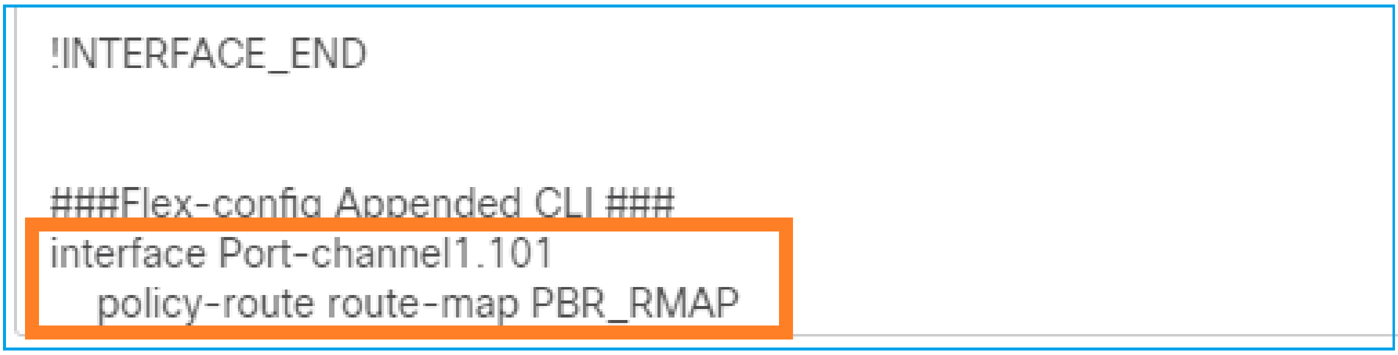
Selected Append FlexConfigs

#	Name	Description
1	FTD4100_PBR	The template is an example of PBR policy configuration. It can not be use...

保存并选择预览配置：



```
route-map PBR_RMAP permit 1
 match ip address ACL_PBR
 set ip next-hop 203.0.113.99
vpn-addr-assign local

!INTERFACE_START
no logging FMC MANAGER_VPN_EVENT_LIST
```



```
!INTERFACE_END


###Flex-config Appended CLI ###
interface Port-channel1.101
    policy-route route-map PBR_RMAP
```

最后，部署策略。

注意：不能使用FlexConfig和FMC UI为同一入口接口配置PBR。

对于PBR SLA配置，请查阅本文档：在FMC管理的FTD上为DUAL ISP配置PBR的IP SLA

PBR验证

入口接口验证：

```
firepower# show run interface Po1.101
!
interface Port-channel1.101
vlan 101
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.0.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1649228271478
ospf authentication null
```

路由映射验证：

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1649228271478 permit 5
 match ip address ACL_PBR
 set ip next-hop 203.0.113.99
```

```
firepower# show route-map
route-map FMC_GENERATED_PBR_1649228271478, permit, sequence 5
Match clauses:
ip address (access-lists): ACL_PBR

Set clauses:
adaptive-interface cost OUTSIDE1 (0)
```

策略路由验证：

```
firepower# show policy-route
Interface Route map
Port-channel1.101 FMC_GENERATED_PBR_1649228271478
```

更改前后Packet Tracer:

无PBR	使用PBR

```
firepower# packet-tracer input INSIDE tcp 192.168.2.100 1111 198.51.100.5 23

....

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 11596 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)

...

Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 6244 ns
Config:
Additional Information:
Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0)


Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1


Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 272058 ns
```

```
firepower# packet-tracer i

...
Phase: 3
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-h
Result: ALLOW
Elapsed time: 39694 ns
Config:
Additional Information:
Input route lookup returne

Phase: 4
Type: ECMP load balancing
Subtype:
Result: ALLOW
Elapsed time: 2230 ns
Config:
Additional Information:
ECMP load balancing
Found next-hop 203.0.113.9

Phase: 5
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 446 ns
Config:
route-map FMC_GENERATED_PB
match ip address ACL_PBR
set adaptive-interface cos
Additional Information:
Matched route-map FMC_GENE
Found next-hop 203.0.113.9

...

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop I
Result: ALLOW
Elapsed time: 5352 ns
Config:
Additional Information:
Found adjacency entry for
Adjacency :Active
MAC address 4c4e.35fc.fcd8

Result:
input-interface: INSIDE(vr
input-status: up
input-line-status: up
output-interface: OUTSIDE1
output-status: up
output-line-status: up
Action: allow
Time Taken: 825100 ns
```

使用实际流量进行测试

使用跟踪配置数据包捕获：

```
firepower# capture CAPI trace interface INSIDE match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAPO1 trace interface OUTSIDE1 match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAPO2 trace interface OUTSIDE2 match ip host 192.168.2.1 host 198.51.100.5
```

```
Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open
```

捕获显示：

```
firepower# show capture
capture CAPI type raw-data trace interface INSIDE [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAPO1 type raw-data trace interface OUTSIDE1 [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAPO2 type raw-data trace interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.2.1 host 198.51.100.5
```

TCP SYN数据包的跟踪：

```
firepower# show capture CAPI packet-number 1 trace

44 packets captured

1: 13:26:38.485585 802.1Q vlan#101 P0 192.168.2.1.49032 > 198.51.100.5.23: S 571152066:571152066(0) win
...

Phase: 3
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Elapsed time: 13826 ns
Config:
Additional Information:
Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Phase: 4
Type: ECMP load balancing
Subtype:
Result: ALLOW
Elapsed time: 1784 ns
Config:
Additional Information:
ECMP load balancing
```

```
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1(vrfid:0)

Phase: 5
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 446 ns
Config:
route-map FMC_GENERATED_PBR_1649228271478 permit 5
match ip address ACL_PBR
set adaptive-interface cost OUTSIDE1
Additional Information:
Matched route-map FMC_GENERATED_PBR_1649228271478, sequence 5, permit
Found next-hop 203.0.113.99 using egress ifc OUTSIDE1

...

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 4906 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 348 reference 2

...

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 222106 ns
```

ASP PBR表显示策略命中计数：

```
firepower# show asp table classify domain pbr

Input Table
in id=0x1505f26d3420, priority=2147483642, domain=pbr, deny=false
hits=7, user_data=0x1505f26e7590, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.2.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=198.51.100.5, mask=255.255.255.255, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=INSIDE(vrfid:0), output_ifc=any

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

注意：Packet Tracer还会增加命中计数器。

PBR调试

警告：在生产环境中，调试会产生大量消息。

启用此调试：

```
firepower# debug policy-route
debug policy-route enabled at level 1
```

发送实际流量：

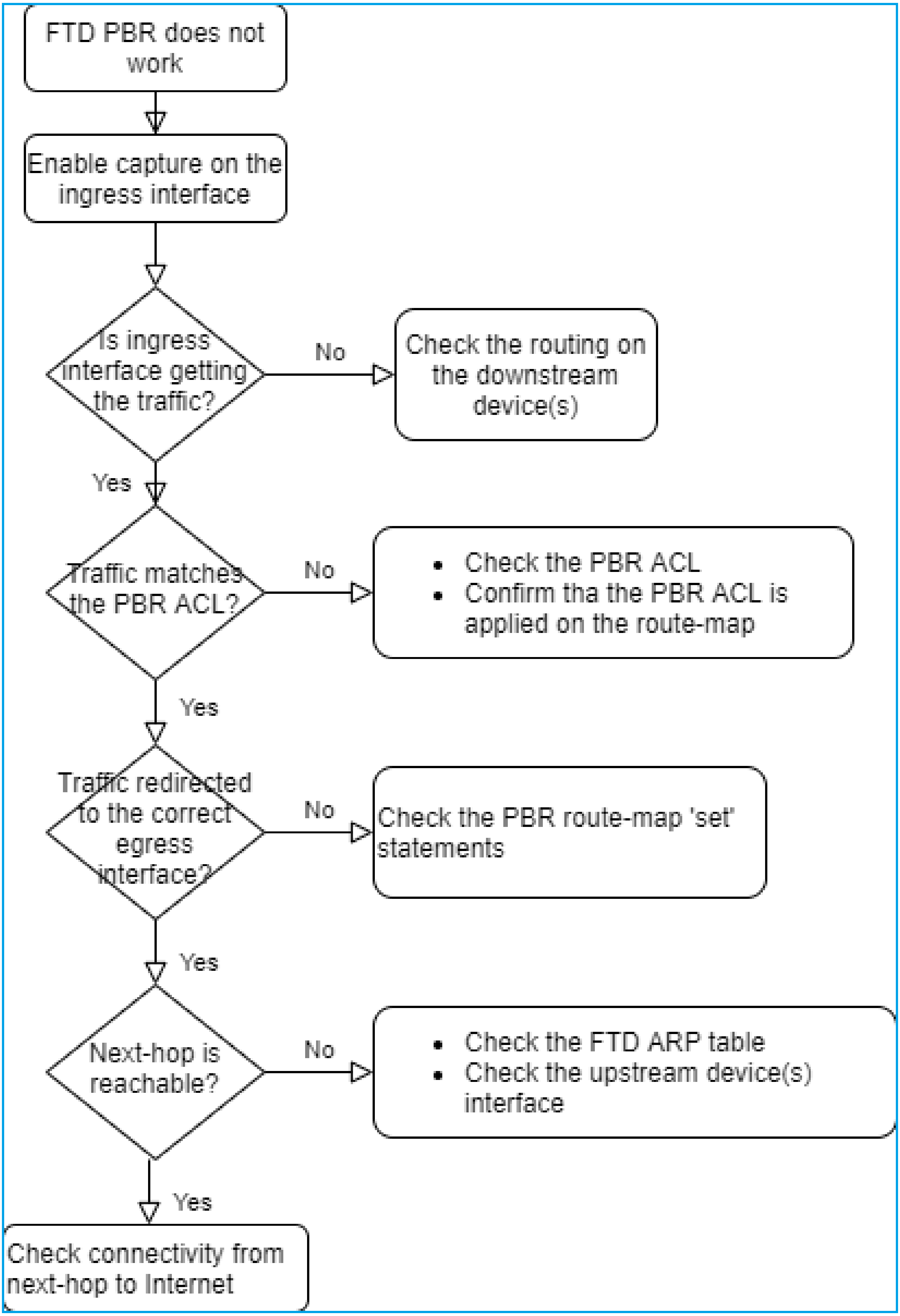
```
Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open
```

调试显示：

```
firepower#

pbr: policy based route lookup called for 192.168.2.1/37256 to 198.51.100.5/23 proto 6 sub_proto 0 rece
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1649228271478, sequence 5, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = OUTSIDE1 : next_hop = 203.0.113.99
```

注意：Packet Tracer还会生成调试输出。

此流程图可用于对PBR进行故障排除：


FTD PBR does not work
Enable capture on the ingress interface
Is ingress interface getting the traffic?
No
Check the routing on the downstream device(s)
Yes
Traffic matches the PBR ACL?
No
Check the PBR ACL
Confirm tha the PBR ACL is applied on the route-map
Yes
Traffic redirected to the correct egress interface?
No
Check the PBR route-map 'set' statements
Yes
Next-hop is reachable?
No
Check the FTD ARP table
Check the upstream device(s) interface
Yes
Check connectivity from next-hop to Internet

PBR命令摘要

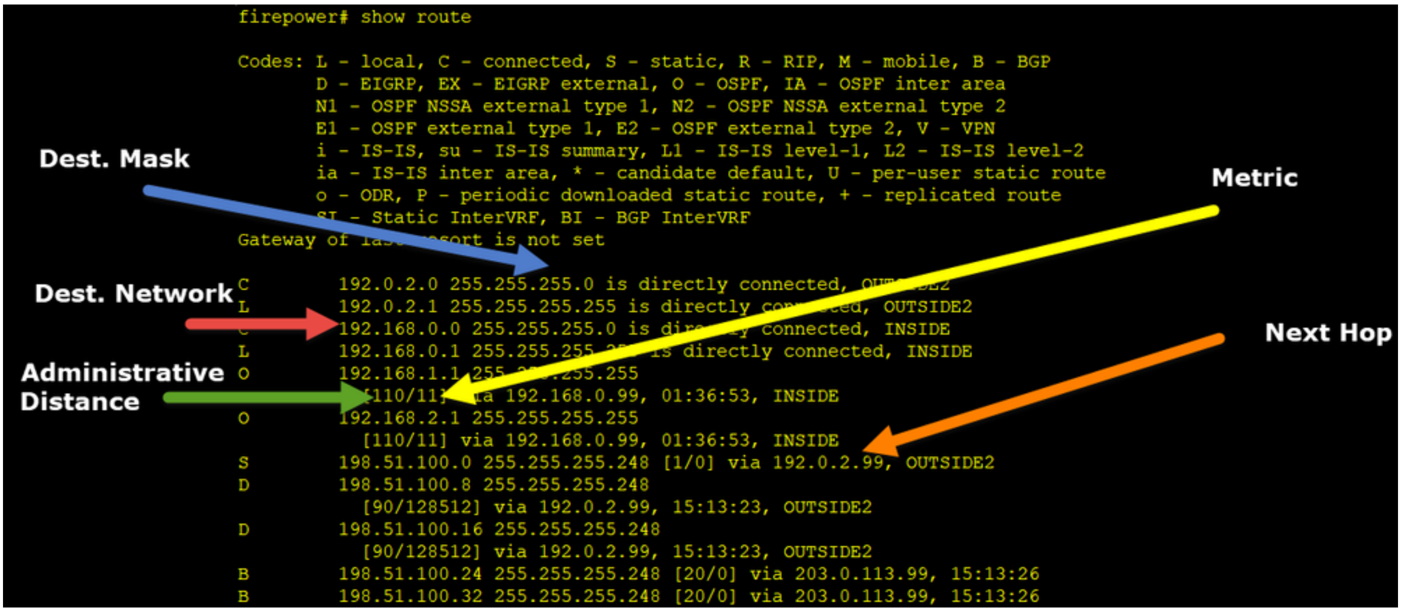
```
show asp drop
```

案例4 — 基于全局路由查找的转发

在连接查找、NAT查找和PBR之后，最后检查以确定出口接口的项目是全局路由表。

路由表验证

让我们检查FTD路由表输出：



```
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, BI - BGP InterVRF
Gateway of last resort is not set

C        192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L        192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C        192.168.0.0 255.255.255.0 is directly connected, INSIDE
L        192.168.0.1 255.255.255.255 is directly connected, INSIDE
O        192.168.1.1 255.255.255.255
           [110/11] via 192.168.0.99, 01:36:53, INSIDE
O        192.168.2.1 255.255.255.255
           [110/11] via 192.168.0.99, 01:36:53, INSIDE
S        198.51.100.0 255.255.255.248 [1/0] via 192.0.2.99, OUTSIDE2
D        198.51.100.8 255.255.255.248
           [90/128512] via 192.0.2.99, 15:13:23, OUTSIDE2
D        198.51.100.16 255.255.255.248
           [90/128512] via 192.0.2.99, 15:13:23, OUTSIDE2
B        198.51.100.24 255.255.255.248 [20/0] via 203.0.113.99, 15:13:26
B        198.51.100.32 255.255.255.248 [20/0] via 203.0.113.99, 15:13:26
```

路由过程的主要目标是查找下一跳。路由选择顺序如下：

1. 最长匹配成功次数
2. 最低AD（在不同的路由协议源之间）
3. 最低度量（如果路由是从同一源 — 路由协议获知）

路由表的填充方式：

- IGP(R、D、EX、O、IA、N1、N2、E1、E2、i、su、L1、L2、ia、o)

- BGP(B)

- BGP InterVRF(BI)

— 静态（秒）

— 静态InterVRF(SI)

— 已连接(C)

— 本地IP(L)

- VPN(V)

— 重分发

-默认

要查看路由表摘要，请使用以下命令：

<#root>

```
firepower#

show route summary



IP routing table maximum-paths is 8
Route Source   Networks Subnets Replicates Overhead Memory (bytes)
connected      0        8       0          704      2368
static         0        1       0          88       296
ospf 1         0        2       0          176      600
Intra-area: 2 Inter-area: 0 External-1: 0 External-2: 0
NSSA External-1: 0 NSSA External-2: 0
bgp 65000      0        2       0          176      592
External: 2 Internal: 0 Local: 0
eigrp 1        0        2       0          216      592
internal       7                                    3112

Total          7        15      0          1360     7560
```

您可以使用以下命令跟踪路由表更新：

<#root>

```
firepower#

debug ip routing


IP routing debugging is on
```

例如，从全局路由表中删除OSPF路由192.168.1.0/24时，调试将显示以下内容：

<#root>

```
firepower#

RT: ip_route_delete 192.168.1.0 255.255.255.0 via 192.0.2.99, INSIDE


ha_cluster_synced 0 routetype 0
RT: del 192.168.1.0 via 192.0.2.99, ospf metric [110/11]NP-route: Delete-Output 192.168.1.0/24 hop_coun
RT: delete network route to 192.168.1.0 255.255.255.0NP-route: Delete-Output 192.168.1.0/24 hop_count:1
```

```
NP-route: Delete-Input 192.168.1.0/24 hop_count:1 Distance:110 Flags:0X0 , via 0.0.0.0, INSIDE
```

当添加回时：

<#root>

```
firepower#
RT: NP-route: Add-Output 192.168.1.0/24 hop_count:1 , via 192.0.2.99, INSIDE

NP-route: Add-Input 192.168.1.0/24 hop_count:1 Distance:110 Flags:0X0 , via 192.0.2.99, INSIDE
```

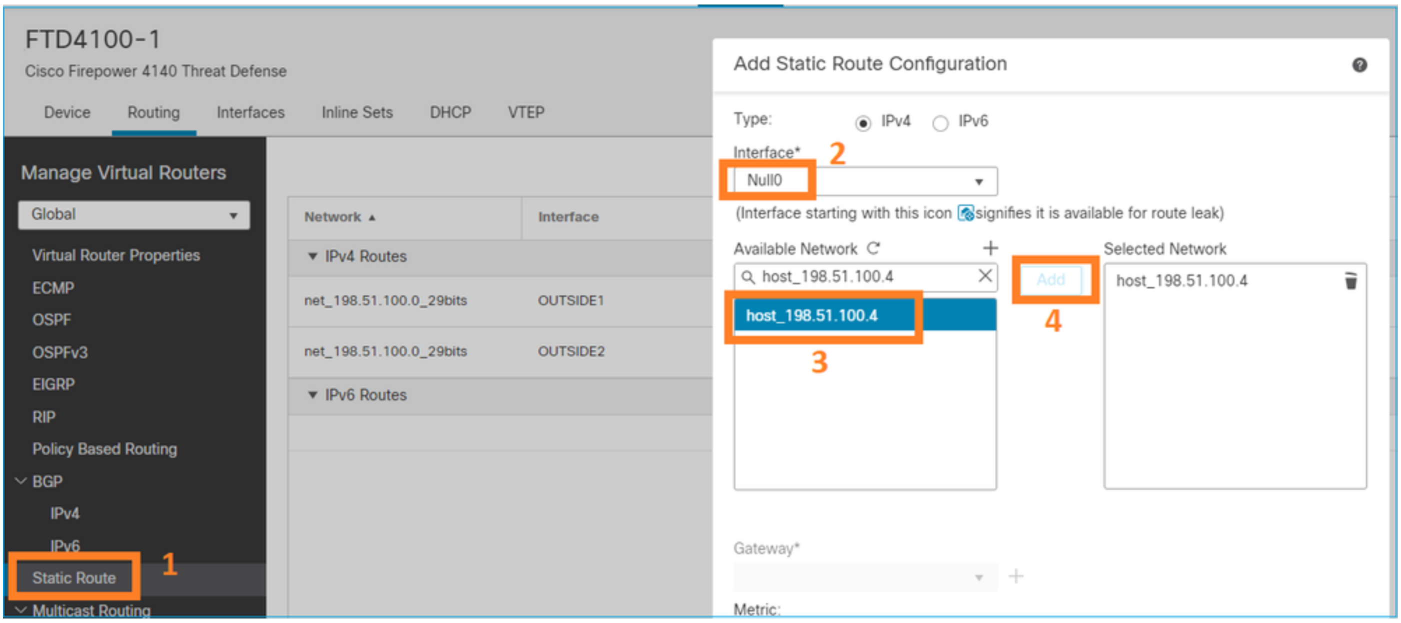
Null0接口

Null0接口可用于丢弃不需要的流量。此丢弃对性能的影响小于具有访问控制策略(ACL)规则的流量丢弃。

要求

为198.51.100.4/32主机配置Null0路由。

解决方案



Network ▲	Interface
▼ IPv4 Routes	
net_198.51.100.0_29bits	OUTSIDE1
net_198.51.100.0_29bits	OUTSIDE2
▼ IPv6 Routes	

Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* Null0

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

Available Network: host_198.51.100.4

Selected Network: host_198.51.100.4

Gateway*

Metric:

保存并部署。

验证：

<#root>

```
firepower#

show run route


route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
route OUTSIDE1 198.51.100.0 255.255.255.248 203.0.113.99 200

route Null0 198.51.100.4 255.255.255.255 1
```

```
<#root>

firepower#

show route | include 198.51.100.4


S 198.51.100.4 255.255.255.255 [1/0] is directly connected, Null0
```

尝试访问远程主机：

```
<#root>

Router1#

ping vrf VRF-101 198.51.100.4


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.4, timeout is 2 seconds:

.....


Success rate is 0 percent (0/5)
```

FTD日志显示：

```
<#root>

firepower#

show log | include 198.51.100.4


Apr 12 2022 12:35:28:

%FTD-6-110002: Failed to locate egress interface for ICMP from INSIDE:192.168.0.99/0 to 198.51.100.4/0
```

ASP丢弃显示：

```
<#root>

firepower#

show asp drop


Frame drop:

No route to host (no-route)                1920
```

等价多路径(ECMP)

流量区域

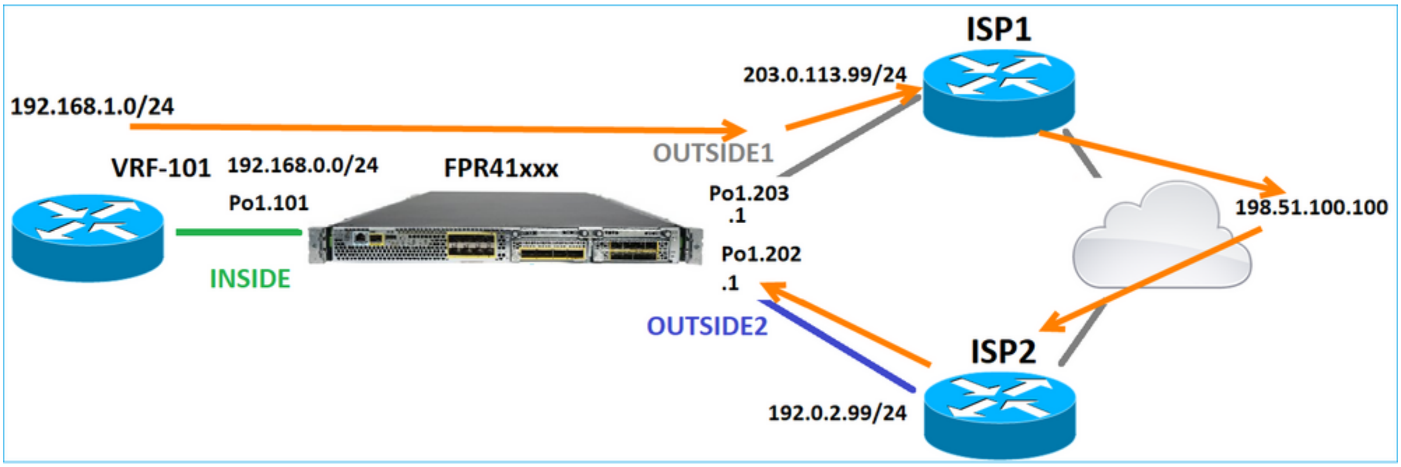
- ECMP Traffic Zone允许用户将接口组合在一起（称为ECMP Zone）。
- 这允许ECMP路由和跨多个接口流量的负载均衡。
- 当接口与ECMP Traffic Zone关联时，用户可以跨接口创建等价静态路由。等价静态路由是指通往具有相同度量值的同一目的网络的路由。

在版本7.1之前，Firepower威胁防御支持通过FlexConfig策略的ECMP路由。从7.1版开始，您可以将接口分组到流量区域，并在Firepower管理中心中配置ECMP路由。

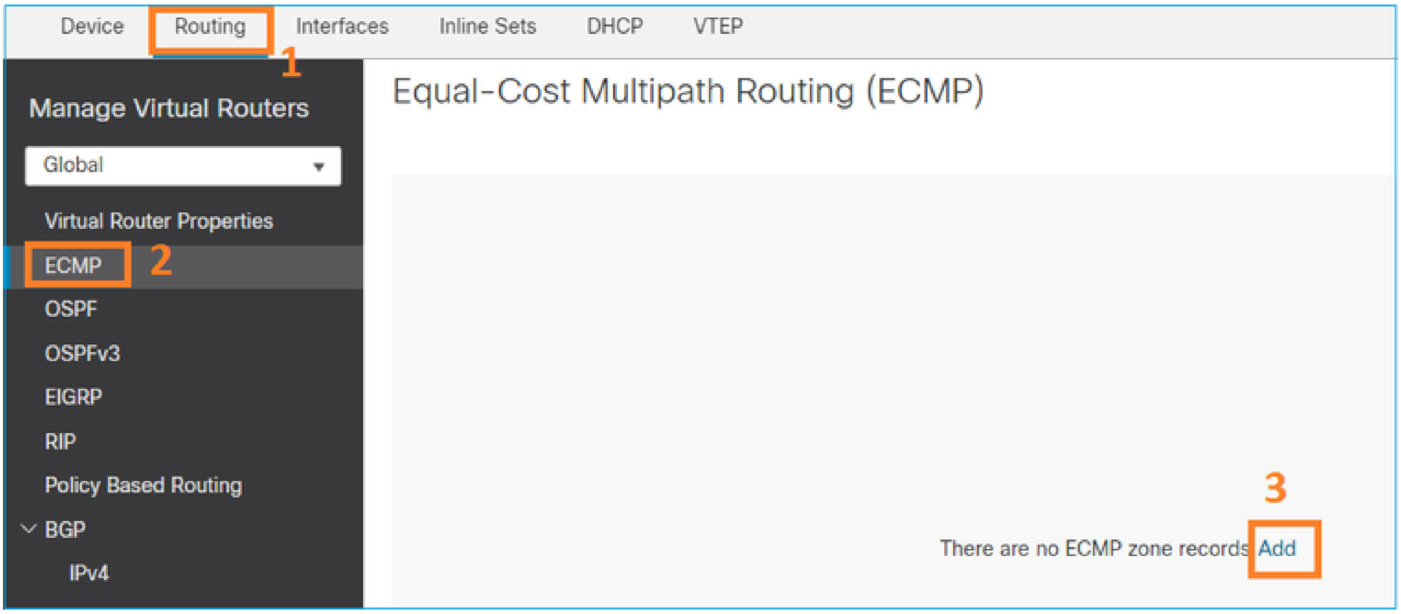
EMCP的文档如下

在本示例中，存在非对称路由，且会丢弃返回流量：

```
<#root>

firepower#

show log


Apr 13 2022 07:20:48: %FTD-6-302013:

B

uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE1:198.51.100


Apr 13 2022 07:20:48: %FTD-6-106015:

Deny TCP (no connection) from 198.51.100.100/23 to 192.168.1.1/23943 flags SYN ACK on interface OUTSIDE2
```



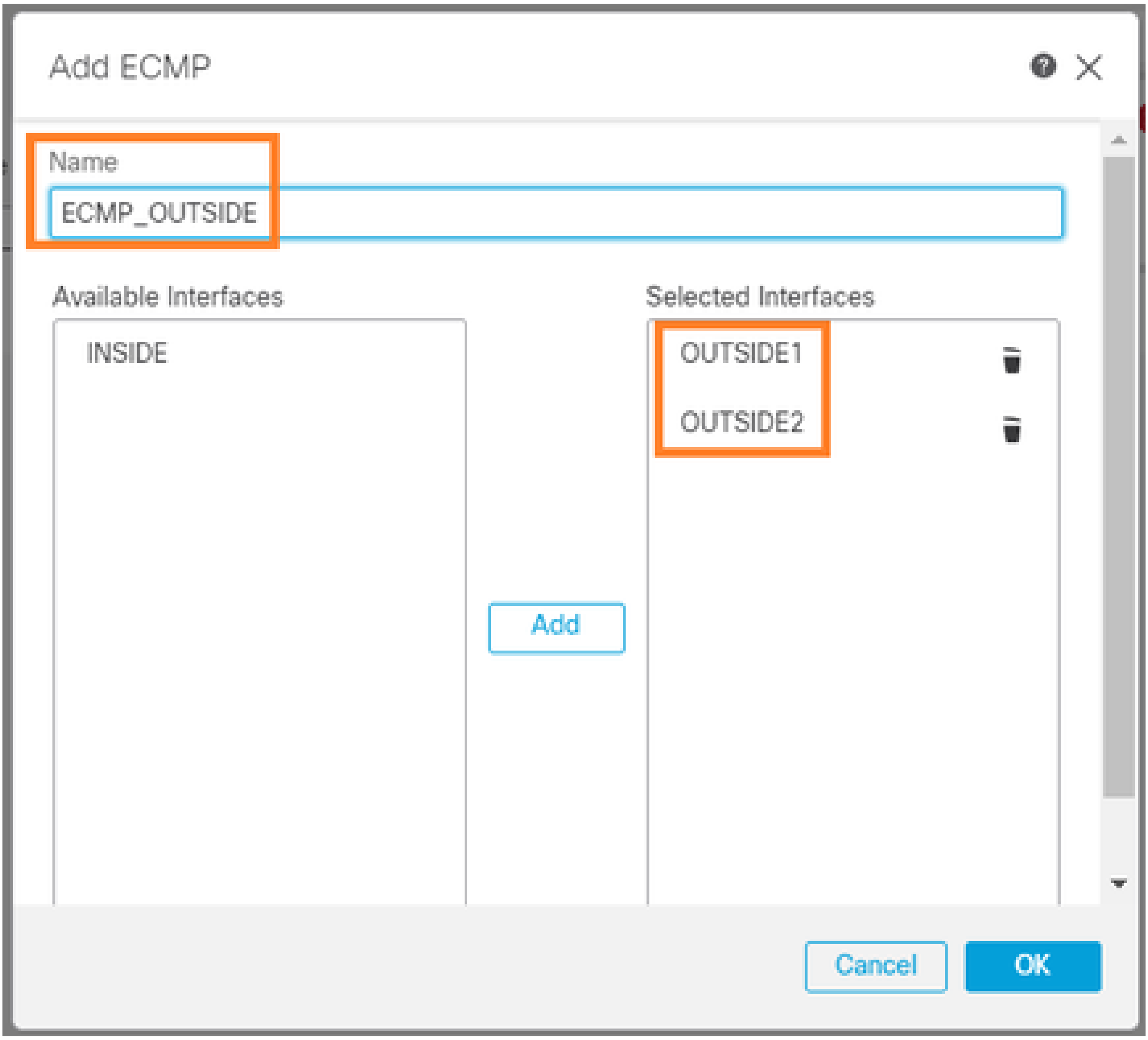
从FMC UI配置ECMP:



Equal-Cost Multipath Routing (ECMP)

There are no ECMP zone records

在ECMP组中添加2个接口：

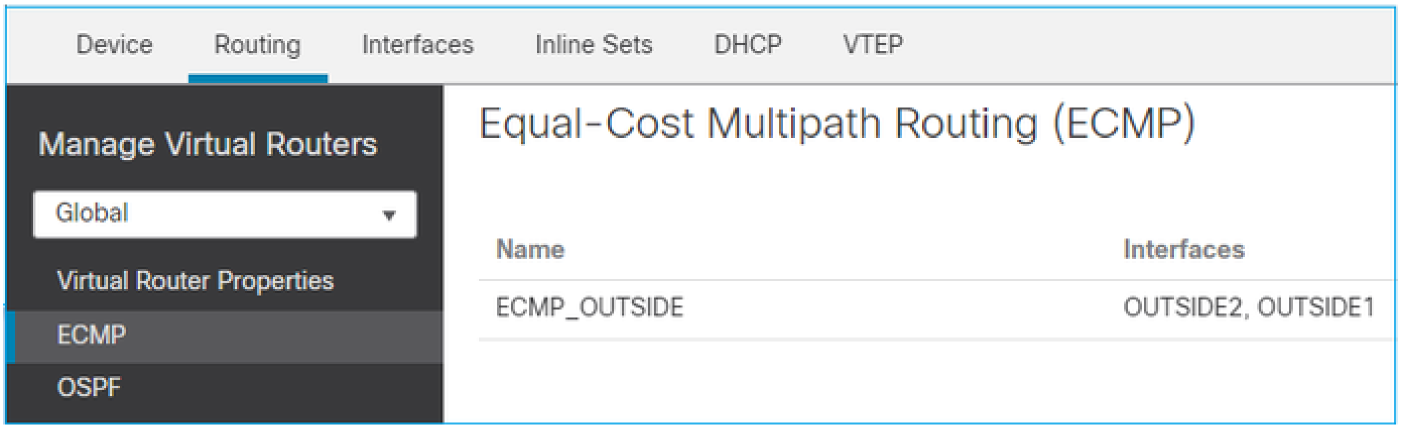


Name: ECMP_OUTSIDE

Available Interfaces: INSIDE

Selected Interfaces: OUTSIDE1, OUTSIDE2

结果：



Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP_OUTSIDE	OUTSIDE2, OUTSIDE1

保存并部署。

ECMP区域验证：

<#root>

```
firepower#

show run zone


zone ECMP_OUTSIDE ecmp

firepower#

show zone


Zone: ECMP_OUTSIDE ecmp


Security-level: 0


Zone member(s): 2


OUTSIDE1 Port-channel1.203


OUTSIDE2 Port-channel1.202
```

接口验证：

<#root>

```
firepower#

show run int po1.202


!
interface Port-channel1.202
vlan 202
nameif OUTSIDE2
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

zone-member ECMP_OUTSIDE


ip address 192.0.2.1 255.255.255.0

firepower#

show run int po1.203
```

```
!
interface Port-channel1.203
vlan 203
nameif OUTSIDE1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
```

zone-member ECMP_OUTSIDE

```
ip address 203.0.113.1 255.255.255.0
```

现在，允许返回流量，并且连接为UP:

<#root>

```
Router1#
```

telnet 198.51.100.100 /vrf VRF-101 /source-interface lo1

Trying 198.51.100.100 ... Open

ISP1接口上的捕获显示出口流量：

<#root>

```
firepower#
```

show capture CAP1

```
5 packets captured

1: 10:03:52.620115 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: S 1782458734:1782458734(0)
2: 10:03:52.621992 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
3: 10:03:52.622114 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
4: 10:03:52.622465 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: P 1782458735:1782458753(18
5: 10:03:52.622556 802.1Q vlan#203 P0 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
```

ISP2接口上的捕获显示返回流量：

<#root>

```
firepower#
```

show capture CAP2

```
6 packets captured

1: 10:03:52.621305 802.1Q vlan#202 P0 198.51.100.100.23 > 192.168.1.1.56199:

S

 2000807245:2000807245(0)

ack

 1782458735 win 64240 <mss 1460>
3: 10:03:52.623808 802.1Q vlan#202 P0 198.51.100.100.23 > 192.168.1.1.56199: . ack 1782458753 win 64222
```

FTD管理平面

FTD有2个管理平面：

- Management0接口 — 提供对Firepower子系统的访问
- LINA诊断接口 — 提供对FTD LINA子系统的访问

要配置和验证Management0接口，请分别使用configure network和show network命令。

另一方面，LINA接口提供对LINA本身的访问。FTD RIB中的FTD接口条目可视为本地路由：

<#root>

```
firepower#

show route | include L


Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

同样，它们可以视为ASP路由表中的身份条目：

<#root>

```
firepower#

show asp table routing | include identity


in 169.254.1.1 255.255.255.255 identity
in

192.0.2.1 255.255.255.255 identity
```

```
in

203.0.113.1 255.255.255.255 identity


in

192.168.0.1 255.255.255.255 identity


in ff02::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in ff02::1:ff00:1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fe80::200:ff:fe01:3 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
in fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff identity
out 0.0.0.0 0.0.0.0 via 0.0.0.0, identity
out :: :: via 0.0.0.0, identity
```

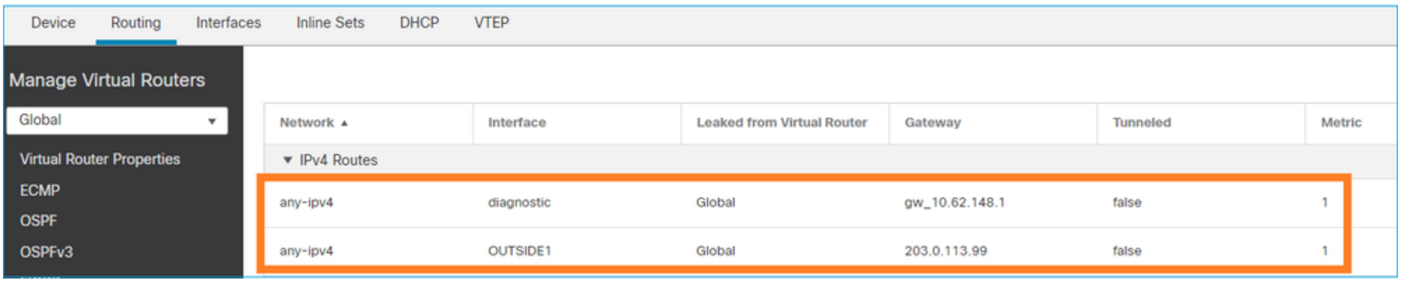
要点

当数据包到达FTD，并且目标IP与某个身份IP匹配时，FTD知道它必须使用该数据包。

FTD LINA诊断接口路由

FTD（与运行9.5后代码的ASA类似）为配置为仅管理的任意接口维护类似VRF的路由表。诊断接口便属于此类接口。

虽然FMC不允许您（不带ECMP）使用相同的度量在两个不同的接口上配置2条默认路由，但您可以在FTD数据接口上配置1条默认路由，并在诊断接口上配置另一条默认路由：



Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
any-ipv4	diagnostic	Global	gw_10.62.148.1	false	1
any-ipv4	OUTSIDE1	Global	203.0.113.99	false	1

数据平面流量使用全局表默认网关，而管理平面流量使用诊断默认GW:

<#root>

```
firepower#

show route management-only



Routing Table: mgmt-only


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, BI - BGP InterVRF

Gateway of last resort is 10.62.148.1 to network 0.0.0.0



S* 0.0.0.0 0.0.0.0 [1/0] via 10.62.148.1, diagnostic
```

全局路由表网关：

```
<#root>

firepower#

show route | include S\*|Gateway


Gateway of last resort is 203.0.113.99 to network 0.0.0.0


S* 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.99, OUTSIDE1
```

当您从FTD发送流量（来自设备的流量）时，会根据以下条件选择出口接口：

1. 全局路由表
2. 仅管理路由表

如果手动指定出口接口，可以覆盖出口接口选择。

尝试ping诊断接口网关。如果不指定源接口，ping会失败，因为FTD首先使用全局路由表，在本例中，全局路由表包含默认路由。如果全局表中没有路由，则FTD对仅管理路由表执行路由查找：

```
<#root>

firepower#

ping 10.62.148.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.62.148.1, timeout is 2 seconds:

?????


Success rate is 0 percent (0/5)
firepower#

show capture CAP1 | include 10.62.148.1
```

```
1: 10:31:22.970607 802.1Q vlan#203 P0

203.0.113.1 > 10.62.148.1 icmp: echo request


2: 10:31:22.971431 802.1Q vlan#203 P0

10.1.1.2 > 203.0.113.1 icmp: host 10.62.148.1 unreachable
```

<#root>

```
firepower#

ping diagnostic 10.62.148.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.62.148.1, timeout is 2 seconds:

!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

如果您尝试使用copy命令从LINA CLI复制文件，同样适用。

双向转发检测(BFD)

已在传统ASA 9.6版上添加了BFD支持，并且仅针对BGP协议：双向转发检测路由

在FTD上：

- 支持BGP IPv4和BGP IPv6协议（软件6.4）。
- 不支持OSPFv2、OSPFv3和EIGRP协议。
- 不支持静态路由的BFD。

虚拟路由器(VRF)

6.6版本中添加了VRF支持。有关详细信息，请查看本文档：虚拟路由器配置示例

相关信息

- FTD静态路由和默认路由

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。