Solución de problemas de routing Firepower Threat Defence

Contenido

Introducción

Este documento describe cómo Firepower Threat Defence (FTD) reenvía paquetes e implementa diversos conceptos de routing.

Prerequisites

Requirements

- Conocimiento básico de routing

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 41xx Threat Defense Versión 7.1.x
- Firepower Management Center (FMC) versión 7.1.x

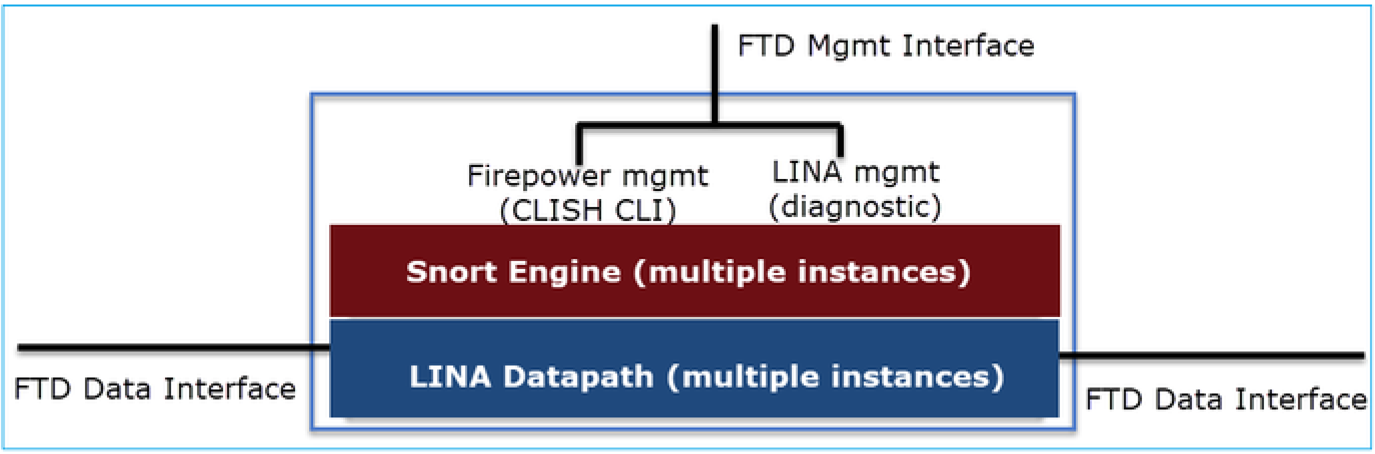
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Mecanismos de reenvío de paquetes FTD

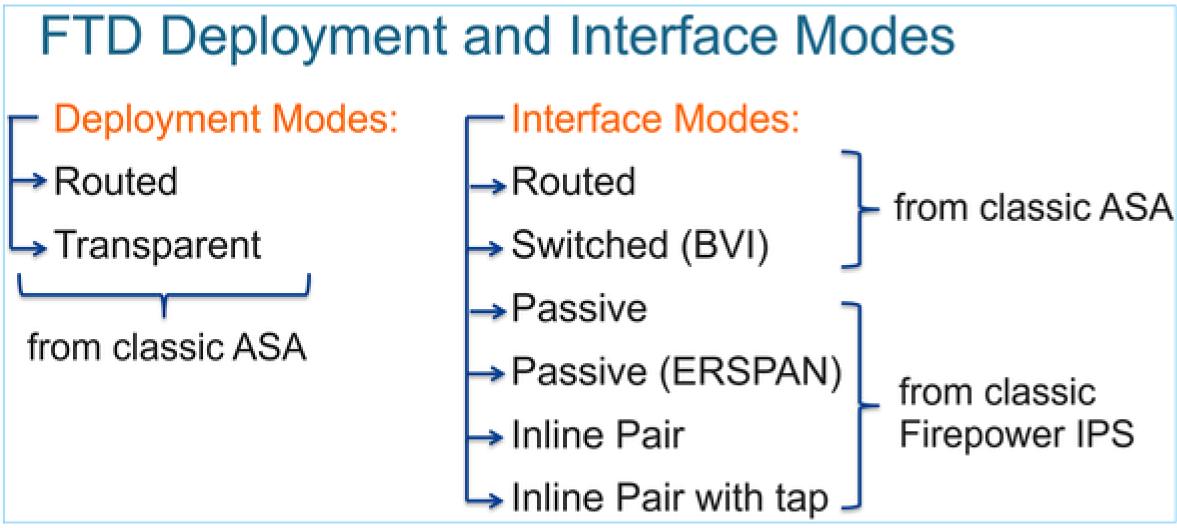
FTD es una imagen de software unificada que consta de 2 motores principales:

- Motor Datapath (LINA)
- Motor Snort

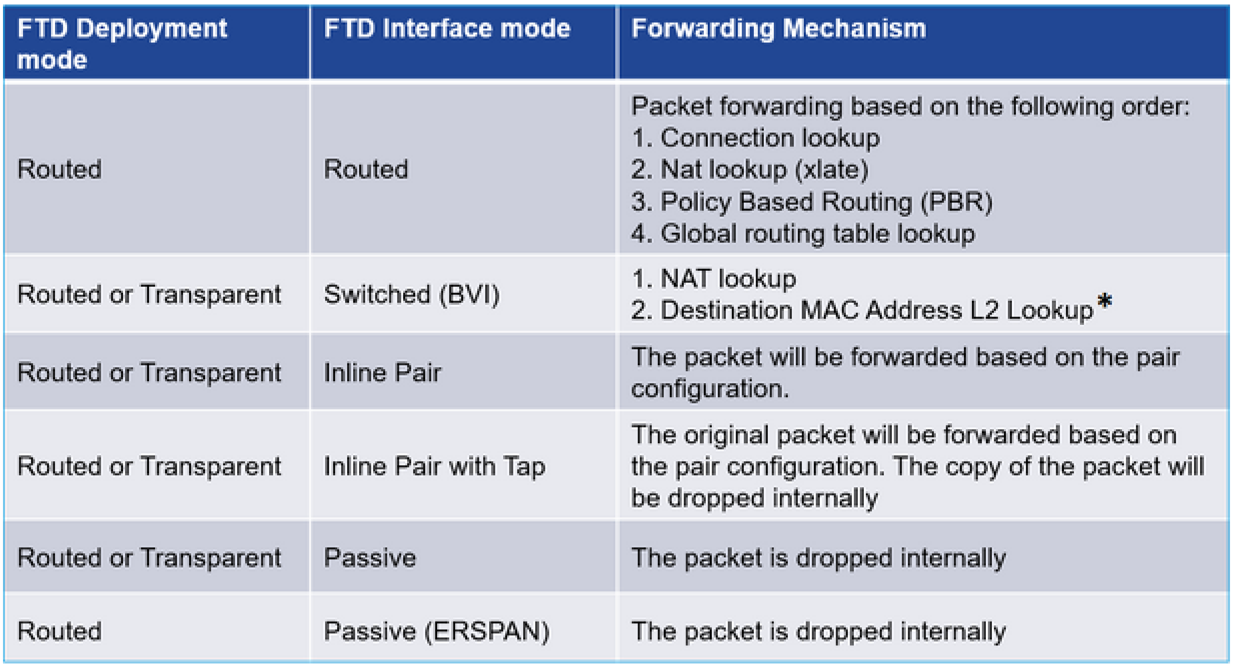


Datapath y Snort Engine son las partes principales del plano de datos del FTD.

El mecanismo de reenvío del plano de datos FTD depende del modo de interfaz. La siguiente imagen resume los diversos modos de interfaz junto con los modos de implementación FTD:

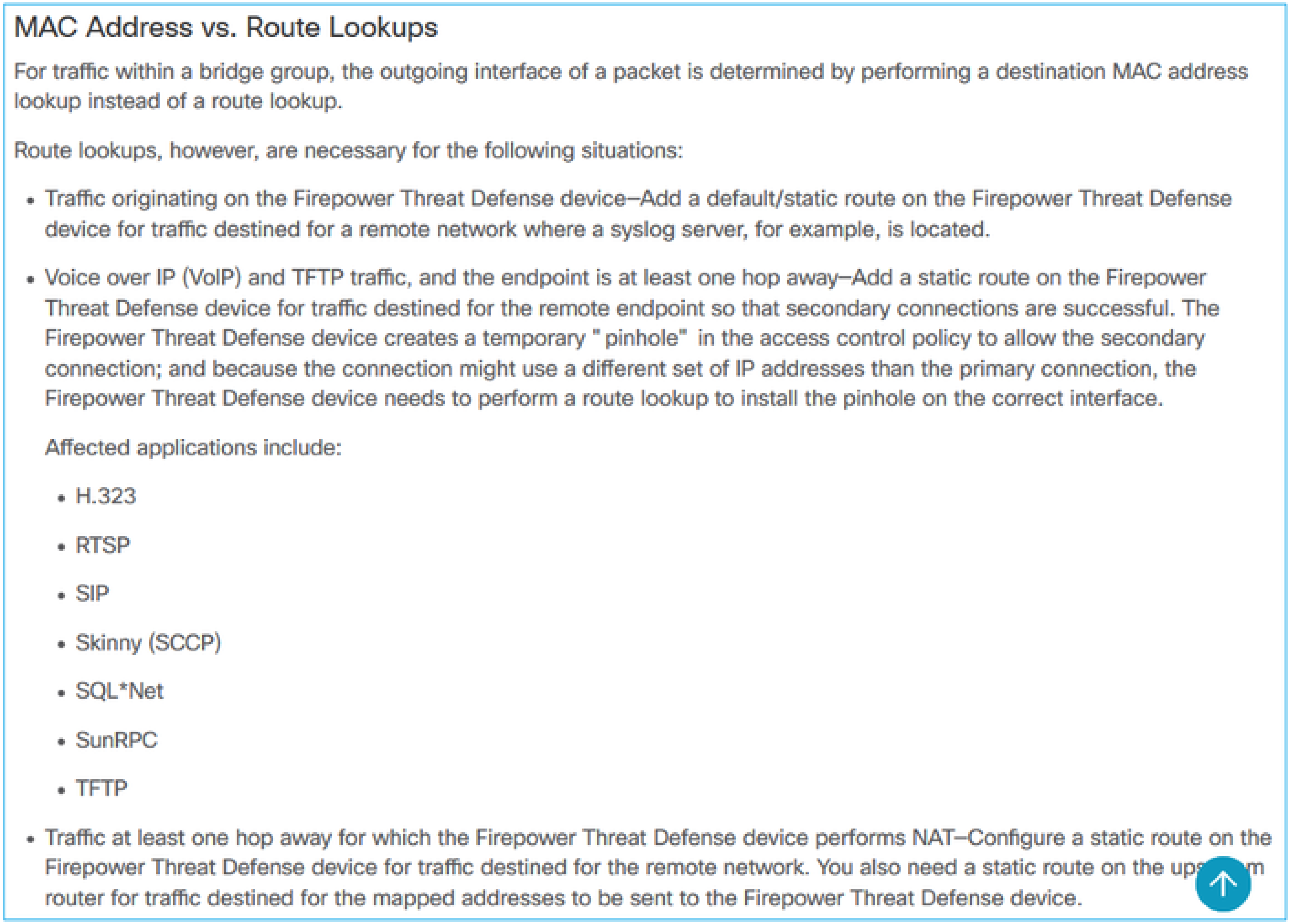


La tabla resume cómo el FTD reenvía paquetes en el plano de datos en función del modo de interfaz. Los mecanismos de reenvío se enumeran por orden de preferencia:



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

* Un FTD en modo Transparente realiza una búsqueda de ruta en algunas situaciones:



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:

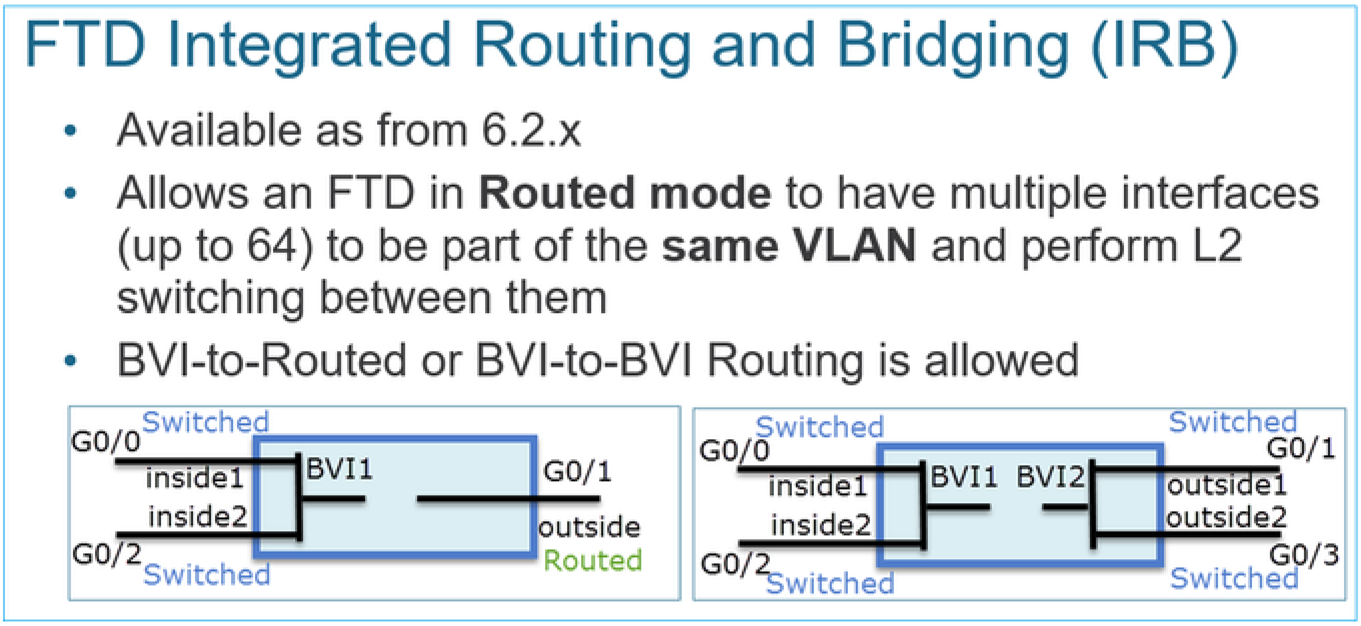
- Traffic originating on the Firepower Threat Defense device–Add a default/static route on the Firepower Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away–Add 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.

Consulte la guía del CSP para obtener más información.

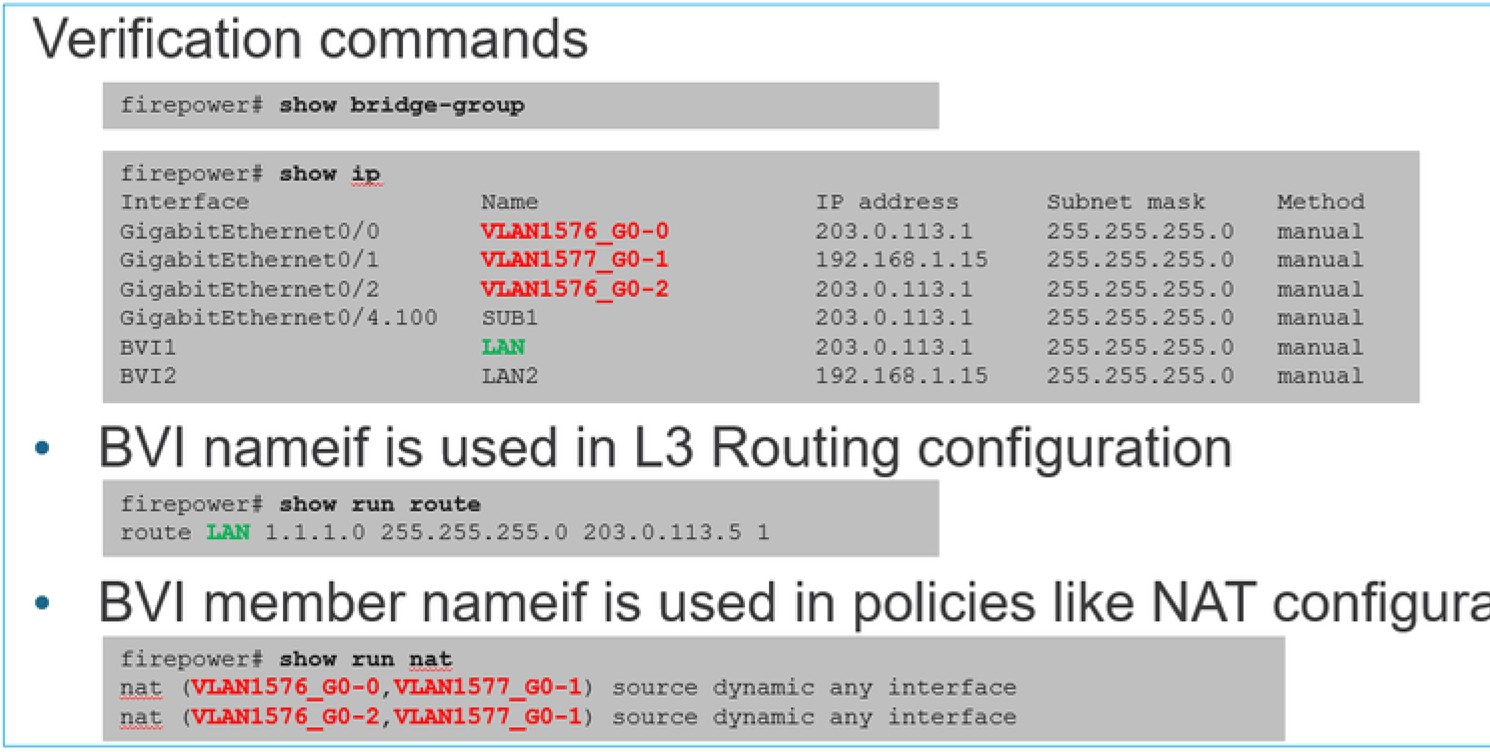
A partir de la versión 6.2.x, el FTD admite el routing y puente integrados (IRB):



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

Comandos de verificación BVI:



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 configura

```
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
```

Punto clave

Para interfaces enrutadas o BVI (IRB), el reenvío de paquetes se basa en este orden:

- Búsqueda de conexión
- Búsqueda de NAT (NAT de destino, también conocida como NAT-ONU)
- Routing basado en políticas (PBR)
- Búsqueda de tabla de routing global

¿Qué pasa con la NAT de origen?

La NAT de origen se verifica después de la búsqueda de ruteo global.

El resto de este documento se centra en el modo de interfaz ruteada.

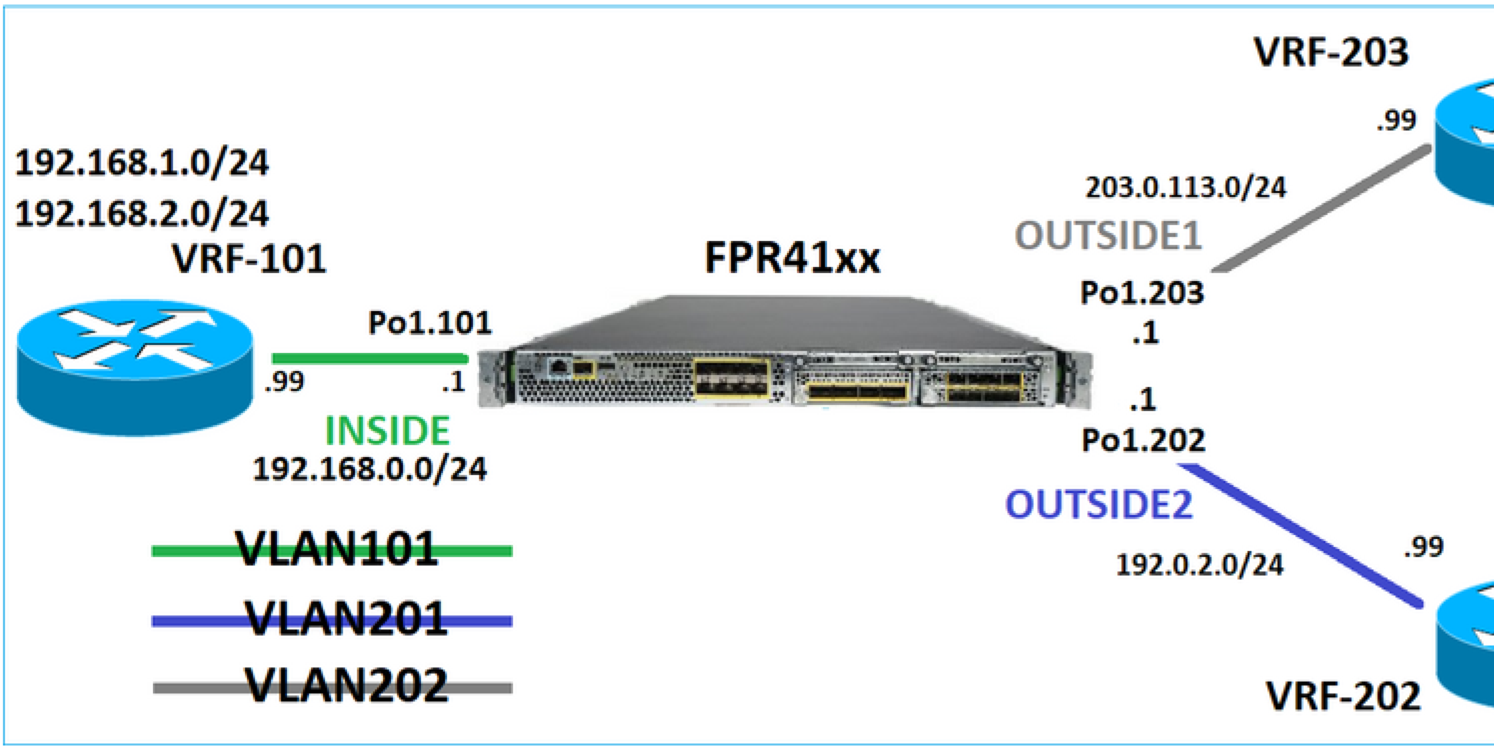
Comportamiento del enrutamiento del plano de datos (LINA)

En el modo de interfaz ruteada, FTD LINA reenvía los paquetes en 2 fases:

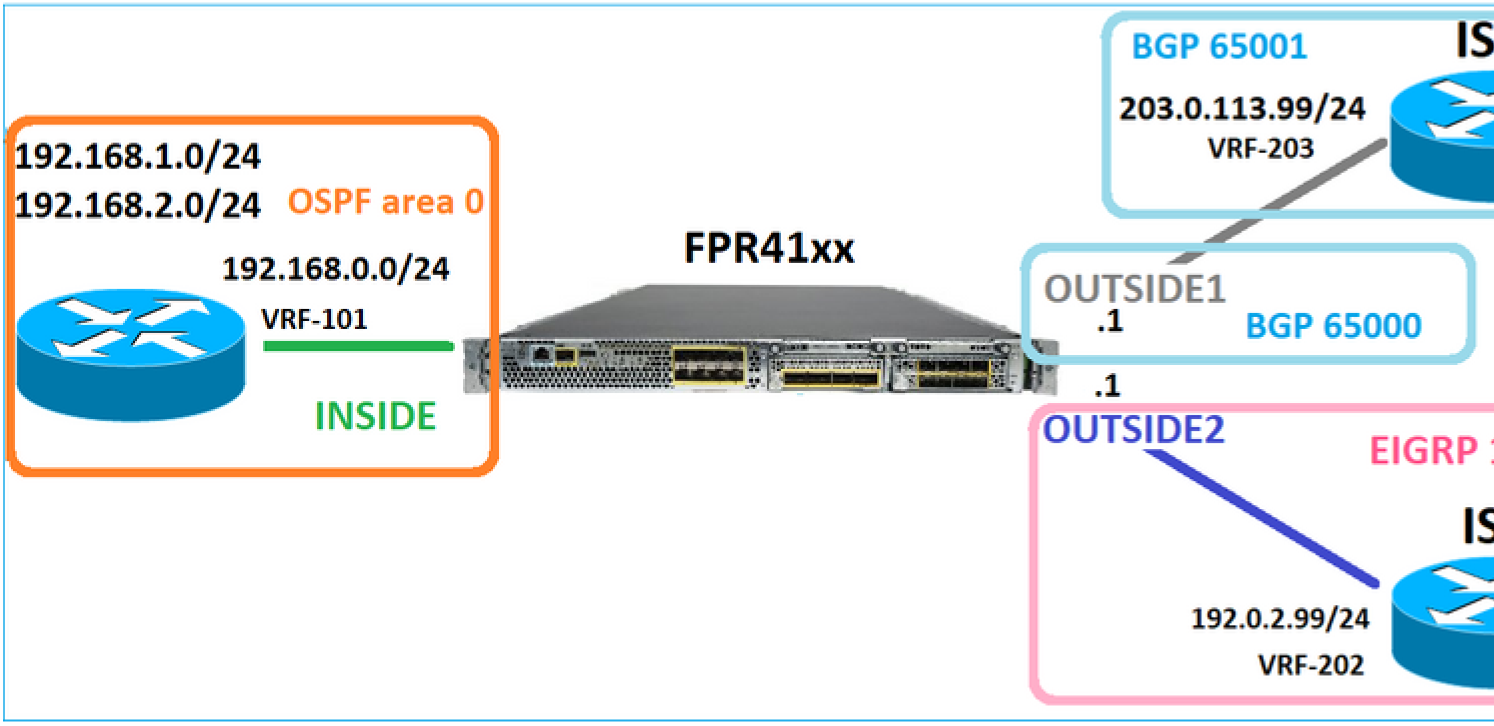
Fase 1: Determinación de la interfaz de salida

Fase 2: Selección del siguiente salto

Tenga en cuenta esta topología:



Y este diseño de routing:



La configuración de ruteo de FTD:

```
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
```

Base de información de routing (RIB) de FTD - Plano de control:

```
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
```

La tabla de enrutamiento de ruta de seguridad acelerada (ASP) de FTD correspondiente - Plano de datos:

```
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
```

Puntos clave

El FTD (de una manera similar a un Adaptive Security Appliance - ASA), primero determina la interfaz de salida (egreso) de un paquete (para eso, observa las entradas 'in' de la tabla de ruteo ASP). Luego, para la interfaz determinada, intenta encontrar el salto siguiente (para eso, observa las entradas 'out' de la tabla de ruteo ASP). Por ejemplo:

```
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
```

Finalmente, para el siguiente salto resuelto, LINA verifica la memoria caché ARP para una adyacencia válida.

La herramienta FTD packet-tracer confirma este proceso:

```
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
```

La tabla ARP de FTD tal como se ve en el plano de control:

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

Para forzar la resolución ARP:

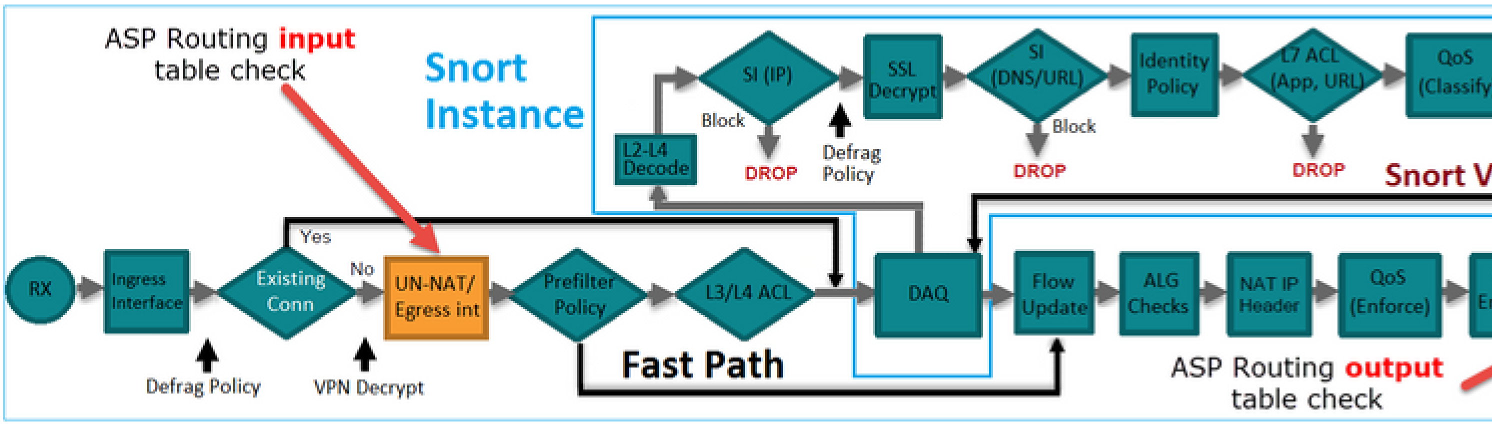
```
firepower# ping 192.168.0.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
firepower# show arp
INSIDE 192.168.0.99 4c4e.35fc.fcd8 45
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8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

La tabla ARP de FTD tal como se ve en el plano de datos:

```
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
```

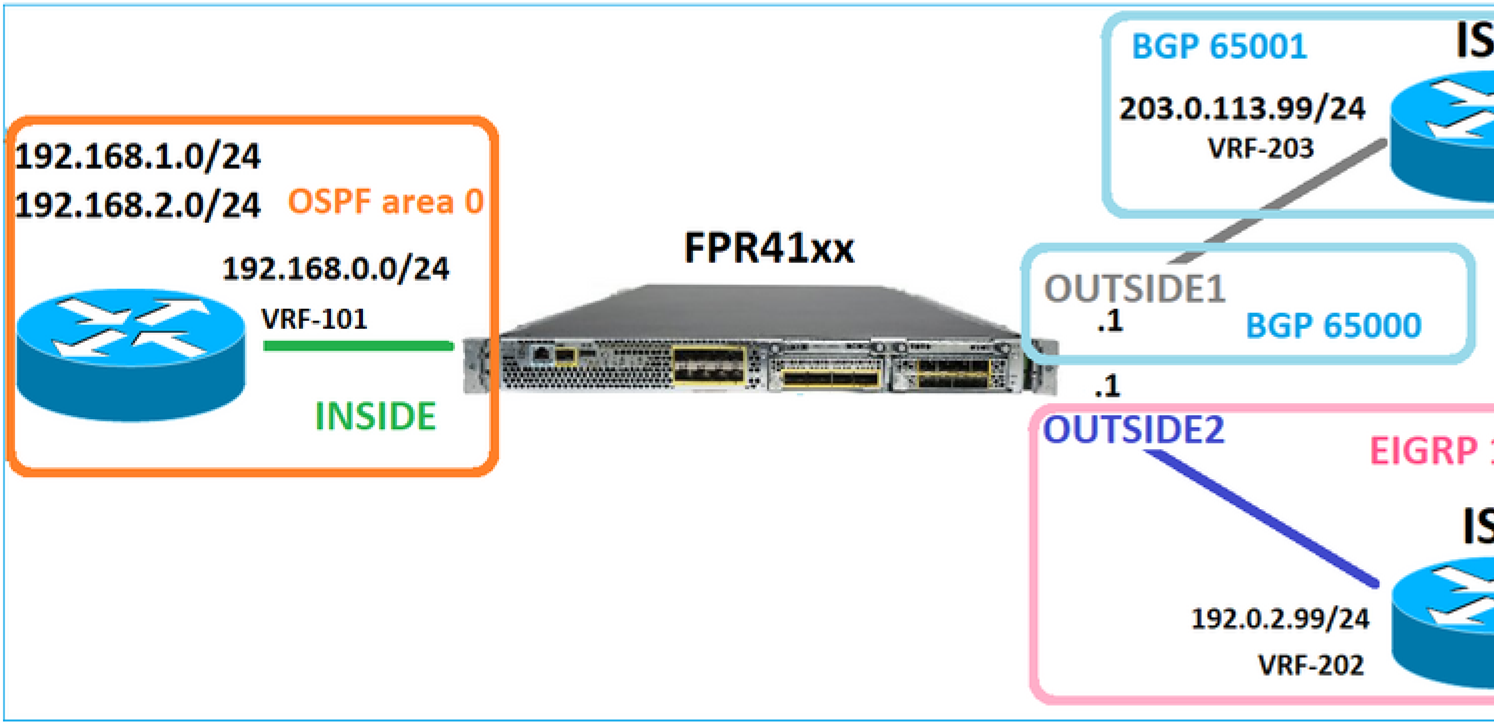
Orden de operaciones de FTD

La imagen muestra el orden de las operaciones y dónde se realizan las comprobaciones de enrutamiento ASP de entrada y salida:



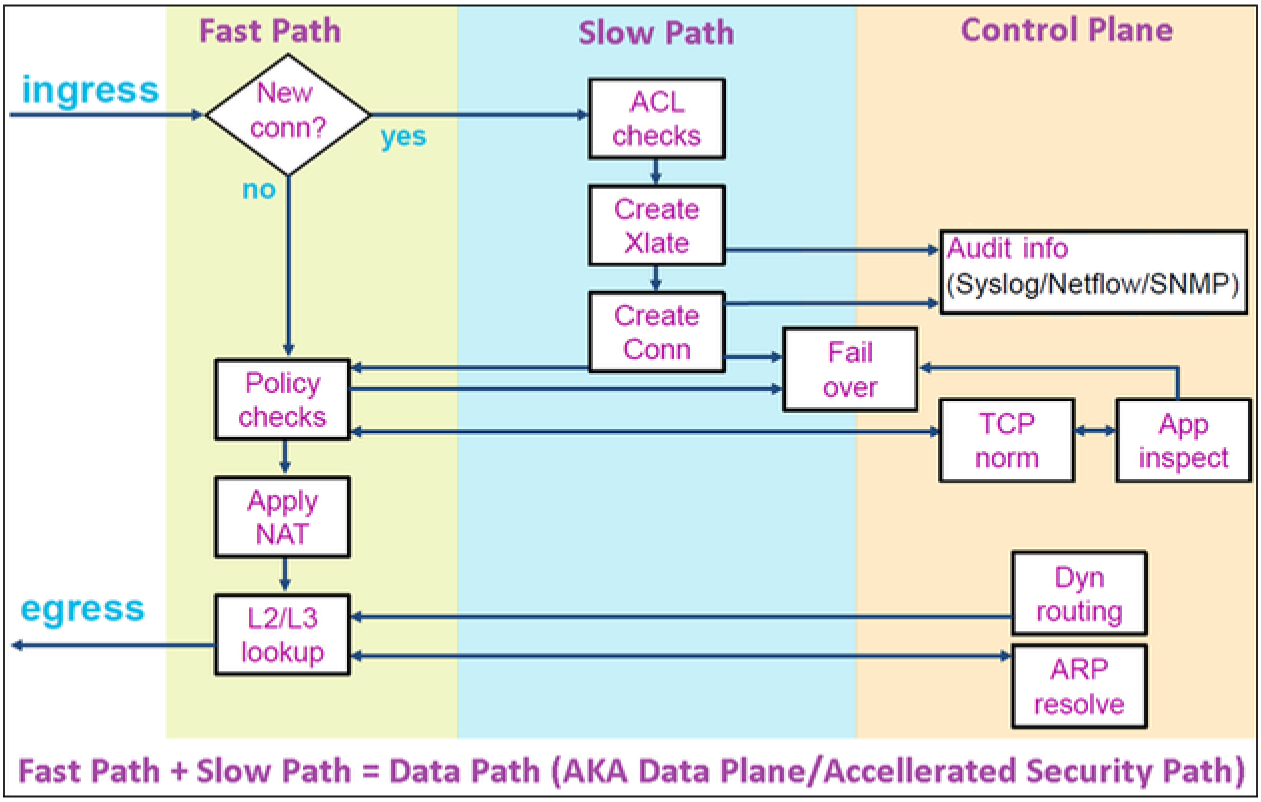
Configurar

Caso 1: reenvío basado en la búsqueda de conexiones



Como ya se ha mencionado, el componente principal del motor LINA de FTD es el proceso Datapath (instancias múltiples basadas en el número de núcleos de dispositivos). Además, la ruta de datos (también conocida como ruta de seguridad acelerada - ASP) consta de 2 rutas:

1. Ruta lenta = responsable del nuevo establecimiento de la conexión (rellena la ruta rápida).
2. Fast Path = Maneja paquetes que pertenecen a conexiones establecidas.



- Comandos como show route y show arp muestran el contenido del plano de control.
- Por otro lado, comandos como show asp table routing y show asp table arp muestran el contenido de ASP (Datapath) que es lo que realmente se aplica.

Habilite la captura con seguimiento en la interfaz FTD INSIDE:

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

Abra una sesión Telnet a través del FTD:

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

Las capturas de FTD muestran los paquetes desde el principio de la conexión (se captura el protocolo de enlace TCP de 3 vías):

```
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)
...
```

Seguimiento del primer paquete (TCP SYN). Este paquete pasa a través del trayecto lento LINA de FTD y se realiza una búsqueda de ruteo global en este caso:

```
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#
```

Rastrea otro paquete de ingreso desde el mismo flujo. El paquete que coincide con una conexión activa:

```
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#
```

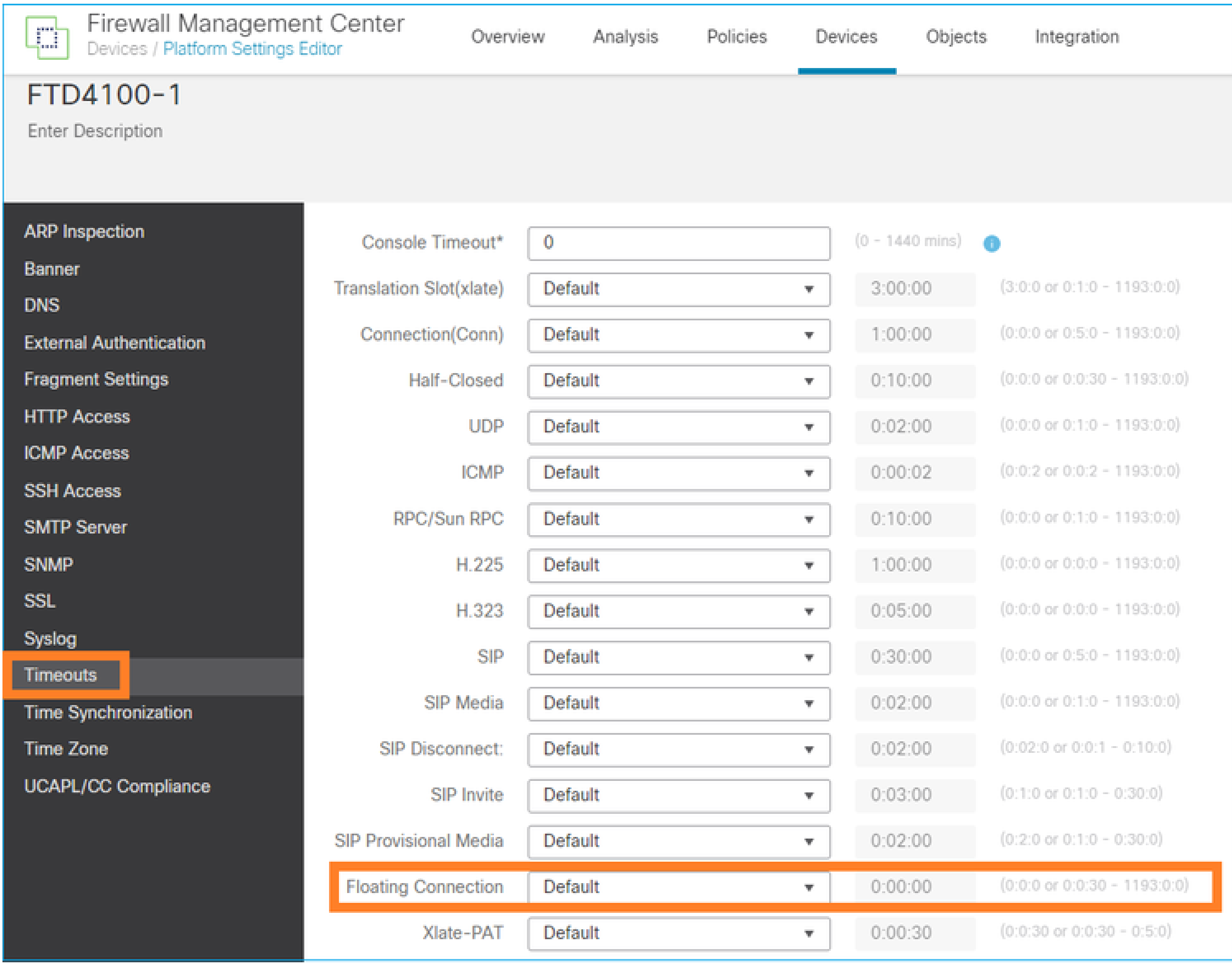
Límite de tiempo flotante

El problema

La inestabilidad de ruta temporal puede hacer que las conexiones UDP de larga duración (elefante) a través del FTD se establezcan a través de interfaces FTD diferentes a las deseadas.

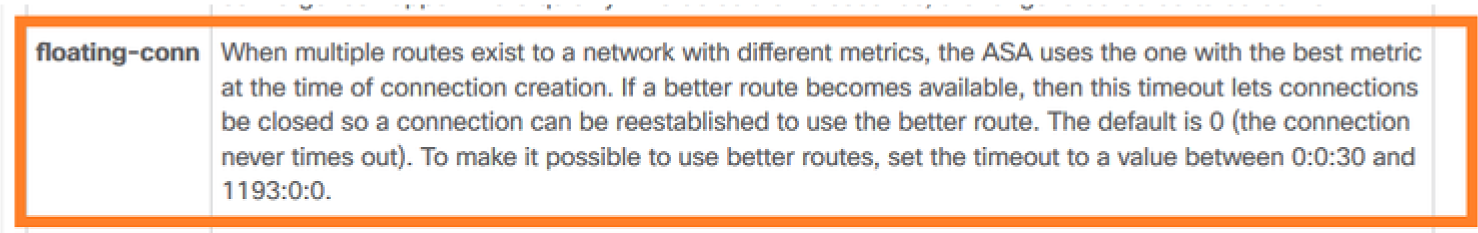
La solución

Para remediar esto, establezca el límite de tiempo flotante-conn en un valor diferente del valor predeterminado que está inhabilitado:



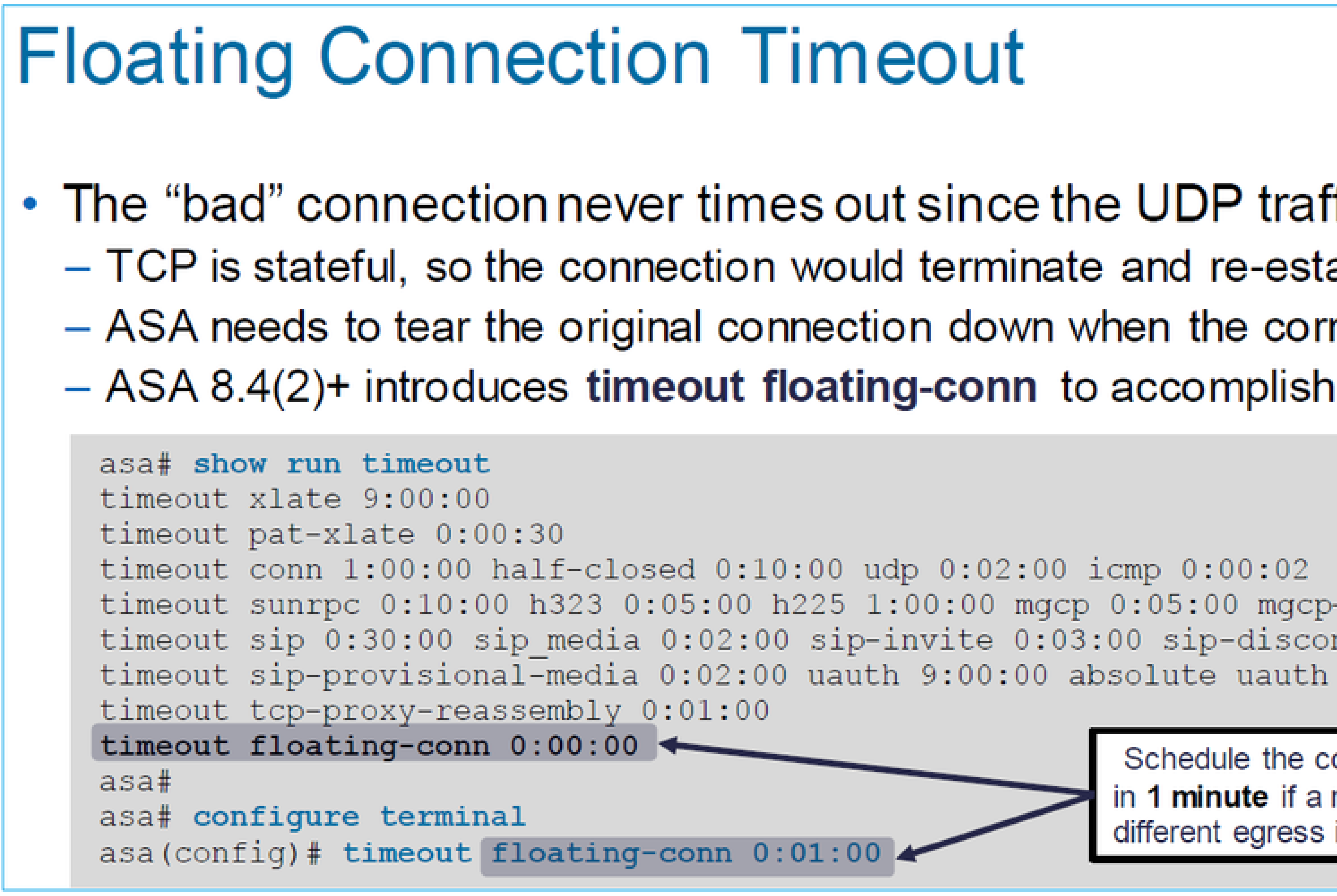
Console Timeout*	0	(0 - 1440 mins)	
Translation Slot(xlate)	Default	3:00:00	(3:0:0 or 0:1:0 - 1193:0:0)
Connection(Conn)	Default	1:00:00	(0:0:0 or 0:5:0 - 1193:0:0)
Half-Closed	Default	0:10:00	(0:0:0 or 0:0:30 - 1193:0:0)
UDP	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
ICMP	Default	0:00:02	(0:0:2 or 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)

Desde la Referencia de Comandos:



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.

Para obtener más información, consulte el caso práctico: Las conexiones UDP fallan tras la recarga desde la sesión de CiscoLive BRKSEC-3020:



Floating Connection Timeout

- The “bad” connection never times out since the UDP traf
  - TCP is stateful, so the connection would terminate and re-esta
  - ASA needs to tear the original connection down when the corr
  - ASA 8.4(2)+ introduces **timeout floating-conn** to accomplish

```
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-
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-discon
timeout sip-provisional-media 0:02:00 uauth 9:00:00 absolute uauth
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 co
in **1 minute** if a r
different egress i

Tiempo de espera de contención

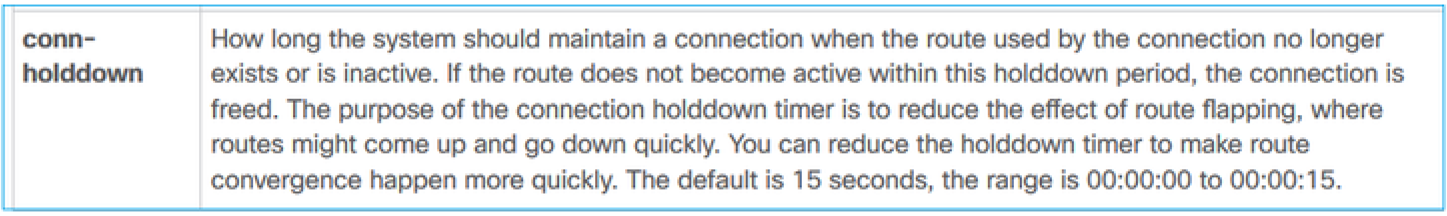
El problema

Una ruta deja de funcionar (se elimina), pero el tráfico coincide con una conexión establecida.

La solución

La función de retención de tiempo de espera fue agregada en ASA 9.6.2. La función está activada de forma predeterminada, pero actualmente (7.1.x) no es compatible con la interfaz de usuario de FMC o FlexConfig. Mejora relacionada: ENH: timeout conn-holddown no disponible para la configuración en FMC

En la guía CLI de ASA:



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
```

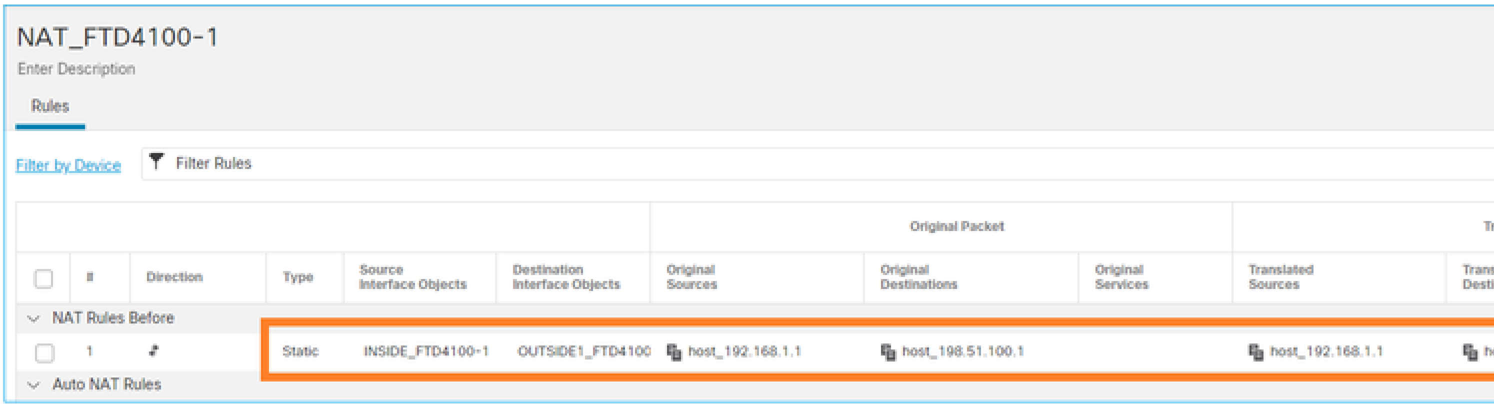
Caso 2: reenvío basado en la búsqueda de NAT

Requisito

Configure esta regla NAT:

- Tipo: Estático
- Interfaz de origen: INSIDE
- Interfaz de destino: OUTSIDE1
- Fuente original: 192.168.1.1
- Destino original: 198.51.100.1
- Fuente traducida: 192.168.1.1
- Destino traducido: 198.51.100.1

Solución



NAT_FTD4100-1

Enter Description

Rules

Filter by Device | Filter Rules

						Original Packet			Tr	
□	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Trans Desti
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	h
Auto NAT Rules										

La regla NAT implementada en la CLI de FTD:

```
firepower# show run nat
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100
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
```

Configurar 3 capturas:

```
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
```

Inicie una sesión telnet desde 192.168.1.1 hasta 198.51.100.1:

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

Los paquetes llegan al FTD, pero nada sale de las interfaces OUTSIDE1 ni OUTSIDE2:

```
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
```

Seguimiento del paquete TCP SYN. La Fase 3 (UN-NAT) muestra que NAT (UN-NAT específicamente) desvió el paquete a la interfaz OUTSIDE1 para la búsqueda de siguiente salto:

```
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) wi
2: 11:23:01.179632 802.1Q vlan#101 P0 192.168.1.1.38790 > 198.51.100.1.23: S 1174675193:1174675193(0) wi
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 4128
...
```

```
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_198.51.100
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
```

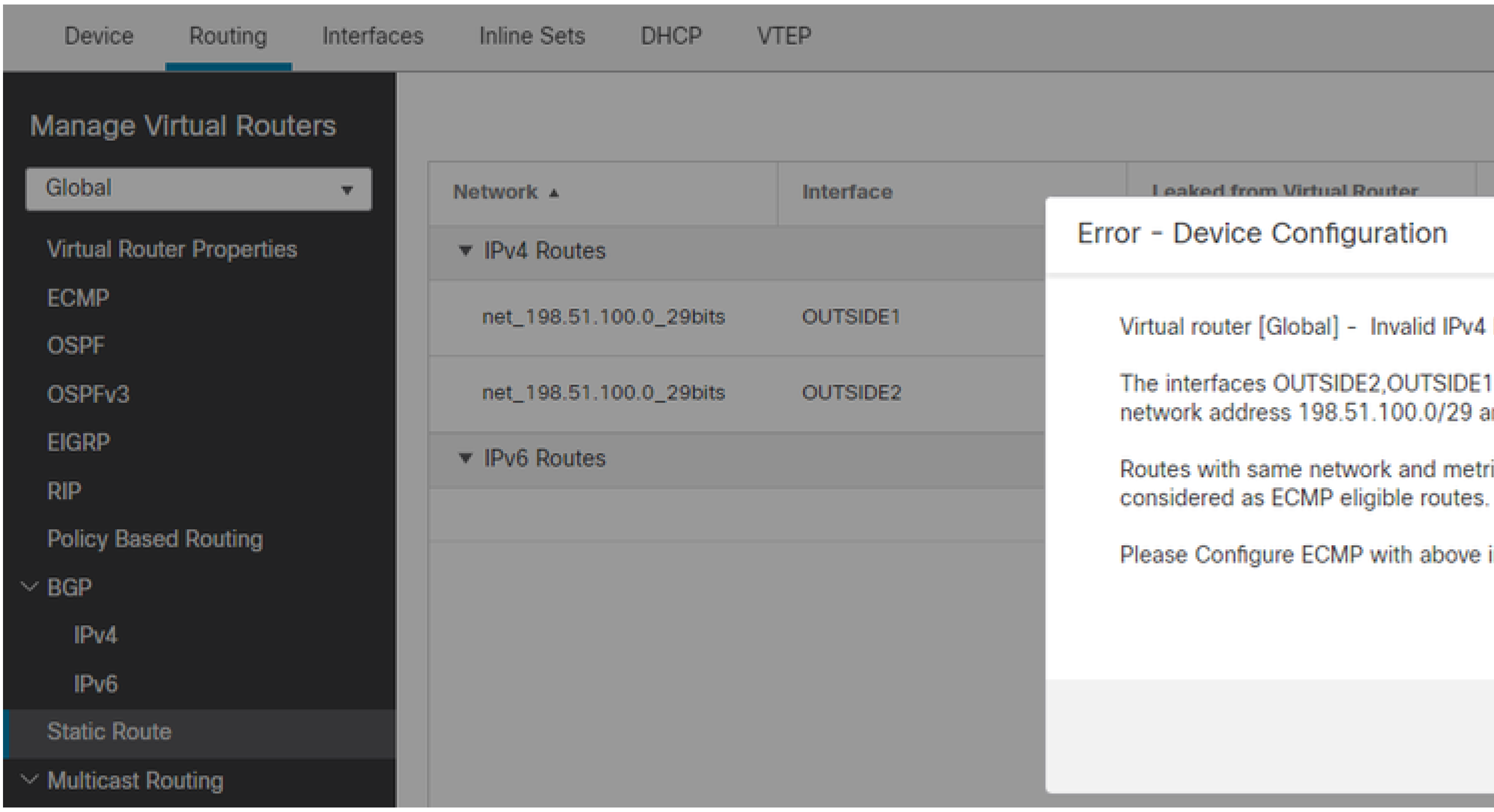
En este caso, SUBOPTIMAL-LOOKUP significa que la interfaz de salida determinada por el proceso NAT (OUTSIDE1) es diferente de la interfaz de salida especificada en la tabla de entrada ASP:

```
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
```

Una posible solución alternativa es agregar una ruta estática flotante en la interfaz OUTSIDE1:

```
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
```

Nota: Si intenta agregar una ruta estática con la misma métrica que la que ya existe, aparece este error:



Network ▲	Interface
net_198.51.100.0_29bits	OUTSIDE1
net_198.51.100.0_29bits	OUTSIDE2

Error - Device Configuration

Virtual router [Global] - Invalid IPv4

The interfaces OUTSIDE2,OUTSIDE1
network address 198.51.100.0/29 a

Routes with same network and metri
considered as ECMP eligible routes.

Please Configure ECMP with above i

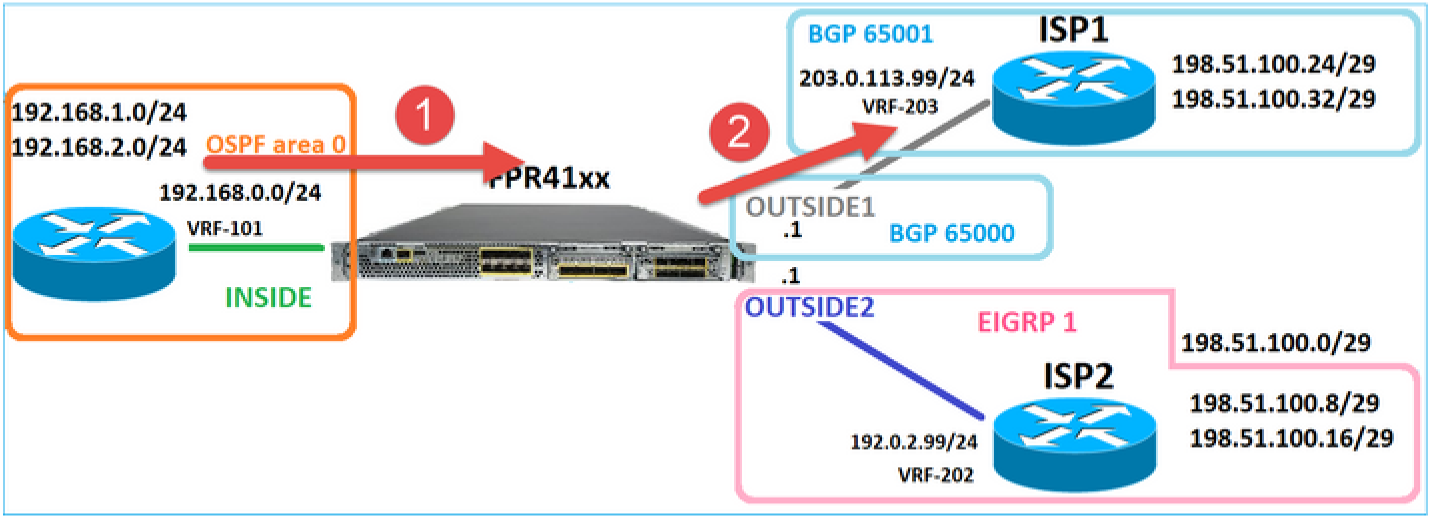
Nota: La ruta flotante con una métrica de distancia de 255 no está instalada en la tabla de routing.

Intente comunicarse vía Telnet que hay paquetes enviados a través del FTD:

```
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
```

El seguimiento de paquetes muestra que los paquetes se reenvían a la interfaz ISP1 (OUTSIDE1) en lugar de a ISP2 debido a la búsqueda de NAT:



```
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) wi
...

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_198.51.100
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
```

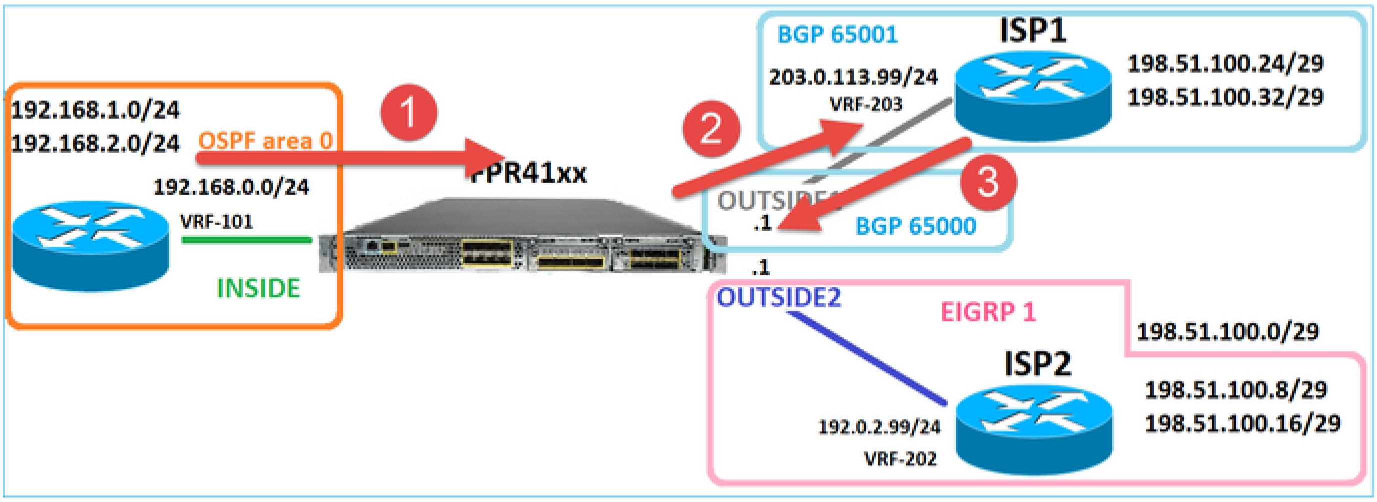
```
Action: allow
Time Taken: 723409 ns


1 packet shown
firepower#
```

Curiosamente, en este caso, hay paquetes que se muestran en INTERIOR y en ambas interfaces de salida:

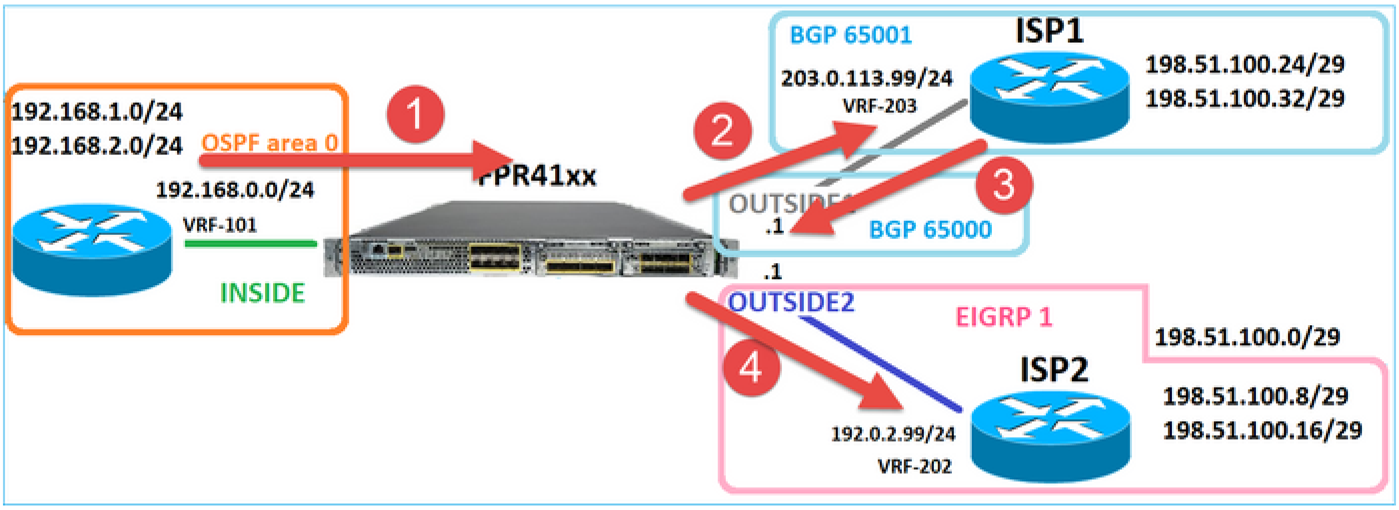
```
firepower# show capture CAPI

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
```

Los detalles del paquete incluyen la información de la dirección MAC, y un seguimiento de los paquetes en las interfaces OUTSIDE1 y OUTSIDE2 revela la trayectoria de los paquetes:

```
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 4128
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 4128
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 4128
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 4128
4 packets shown
```



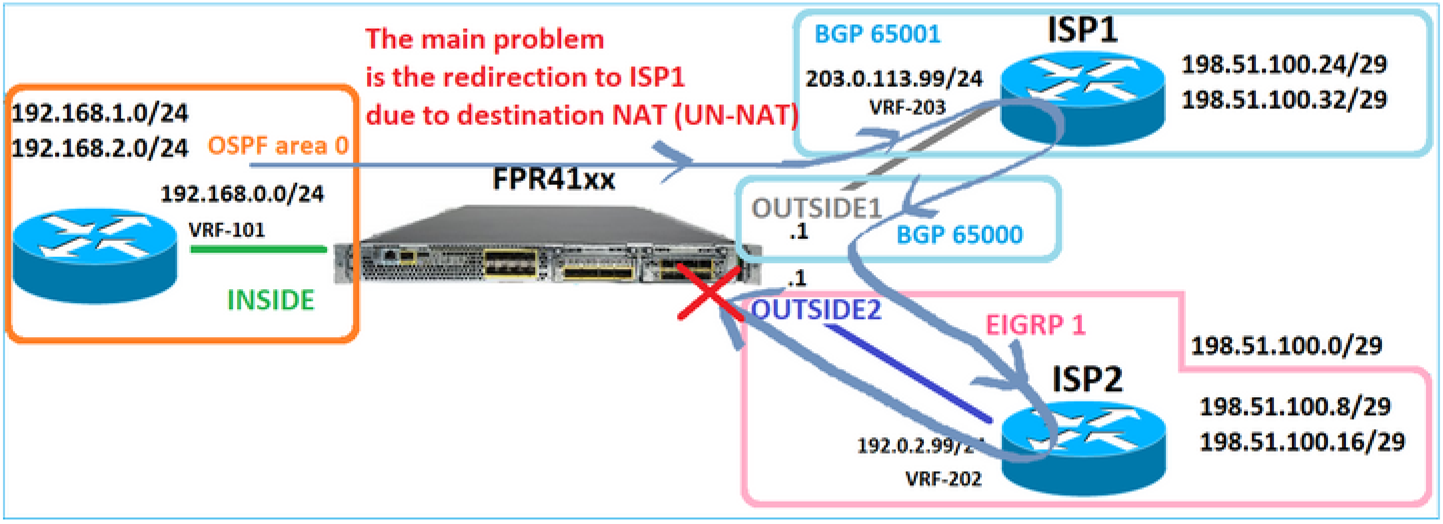
El seguimiento del paquete que devuelve muestra la redirección a la interfaz OUTSIDE2 debido a la búsqueda de la tabla de ruteo global:



```
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) wi
...

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#
```

El router ISP2 envía la respuesta (SYN/ACK), pero este paquete se redirige a ISP1 porque coincide con la conexión establecida. El FTD descarta el paquete debido a que no hay adyacencia L2 en la tabla de salida ASP:



```
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) ac
...

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
```

Caso 3: reenvío basado en routing basado en políticas (PBR)

Después de la búsqueda de flujo de conexión y la búsqueda de NAT de destino, PBR es el siguiente elemento que puede influir en la determinación de la interfaz de salida. PBR se documenta en: Routing basado en políticas

Para la configuración PBR en FMC, es importante tener en cuenta esta directriz:
FlexConfig se utilizó para configurar PBR en FMC para versiones de FTD anteriores a la 7.1. Puede seguir utilizando FlexConfig para configurar PBR en todas las versiones. Sin embargo, para una interfaz de ingreso, no puede configurar PBR mediante FlexConfig y la página Policy Based Routing de FMC.

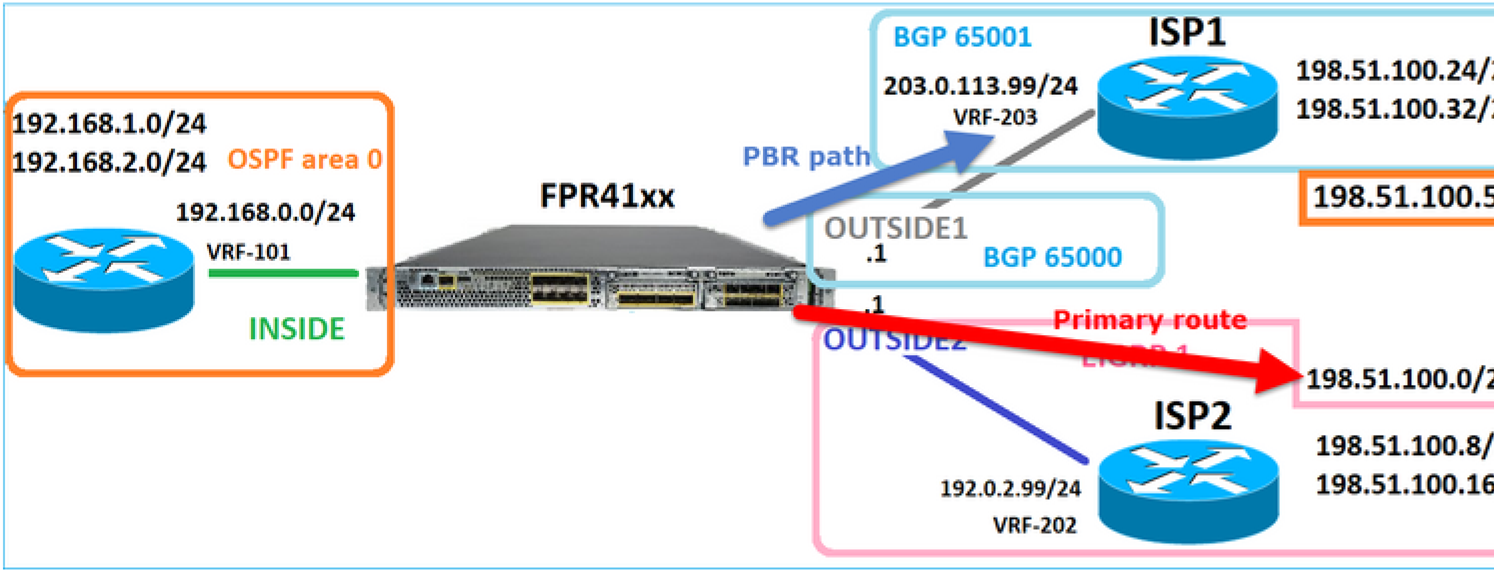
En este caso práctico, el FTD tiene una ruta hacia 198.51.100.0/24 que apunta hacia ISP2:

```
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
```

Requisito

Configure una política PBR con estas características:

- El tráfico de IP 192.168.2.0/24 destinado a 198.51.100.5 debe enviarse a ISP1 (salto siguiente 203.0.113.99) mientras que otros orígenes deben utilizar la interfaz OUTSIDE2.



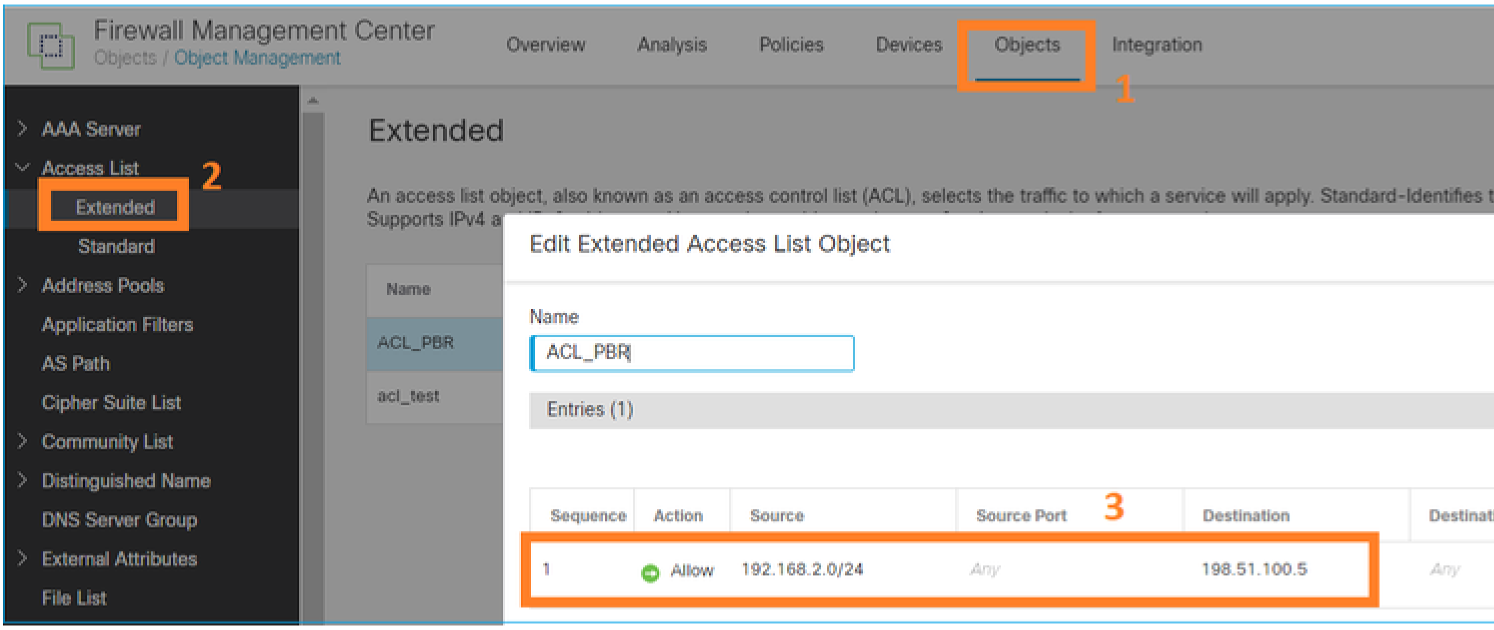
Solución

En las versiones anteriores a la 7.1, para configurar PBR:
1. Cree una ACL extendida que coincida con el tráfico interesante (por ejemplo, PBR_ACL).
2. Cree un route-map que coincida con la ACL creada en el Paso 1 y establezca el siguiente salto deseado.
3. Cree un objeto FlexConfig que habilite PBR en la interfaz de ingreso mediante el route map creado en el paso 2.

En las versiones posteriores a 7.1, puede configurar PBR usando la forma anterior a 7.1, o puede utilizar la nueva opción Policy Based Routing en la sección Device > Routing:
1. Cree una ACL extendida que coincida con el tráfico interesante (por ejemplo, PBR_ACL).
2. Agregue una política PBR y especifique:
a. El tráfico coincidente
b. La interfaz de ingreso
c. El salto siguiente

Configurar PBR (nueva forma)

Paso 1 - Definir una lista de acceso para el tráfico coincidente.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies t
Supports IPv4 a

Name
ACL_PBR
acl_test

Edit Extended Access List Object

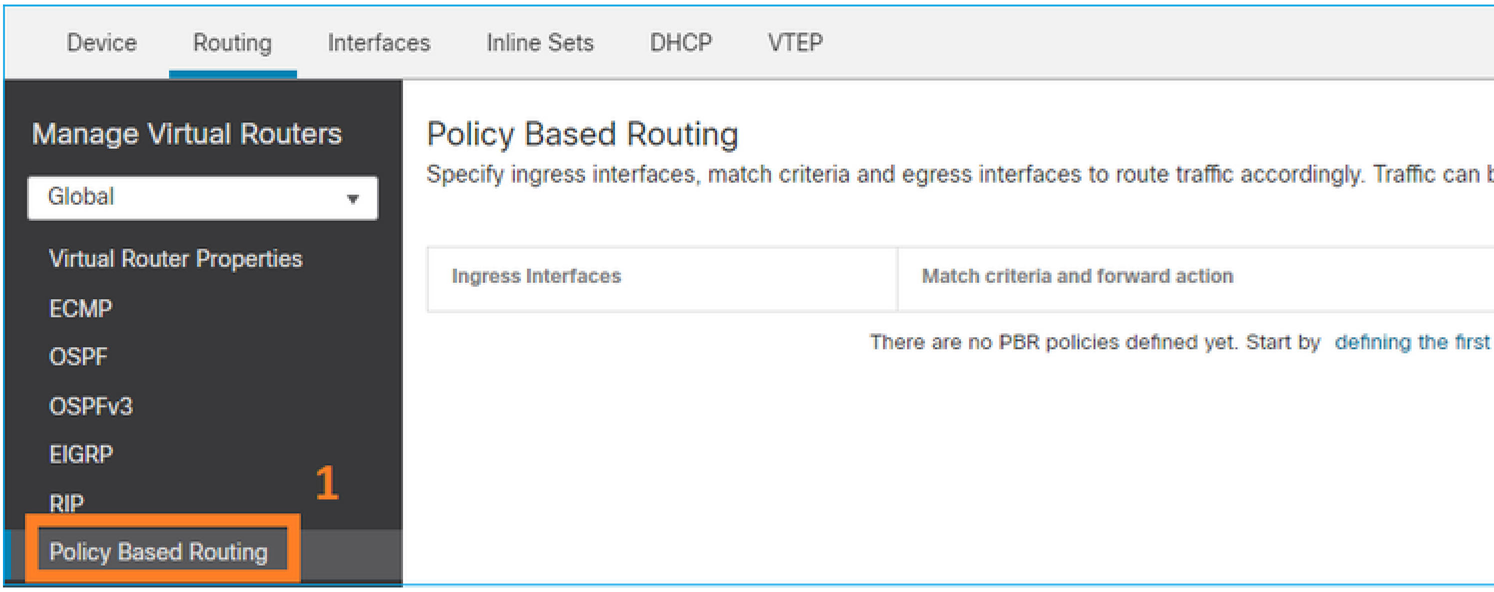
Name
ACL_PBR

Entries (1)

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

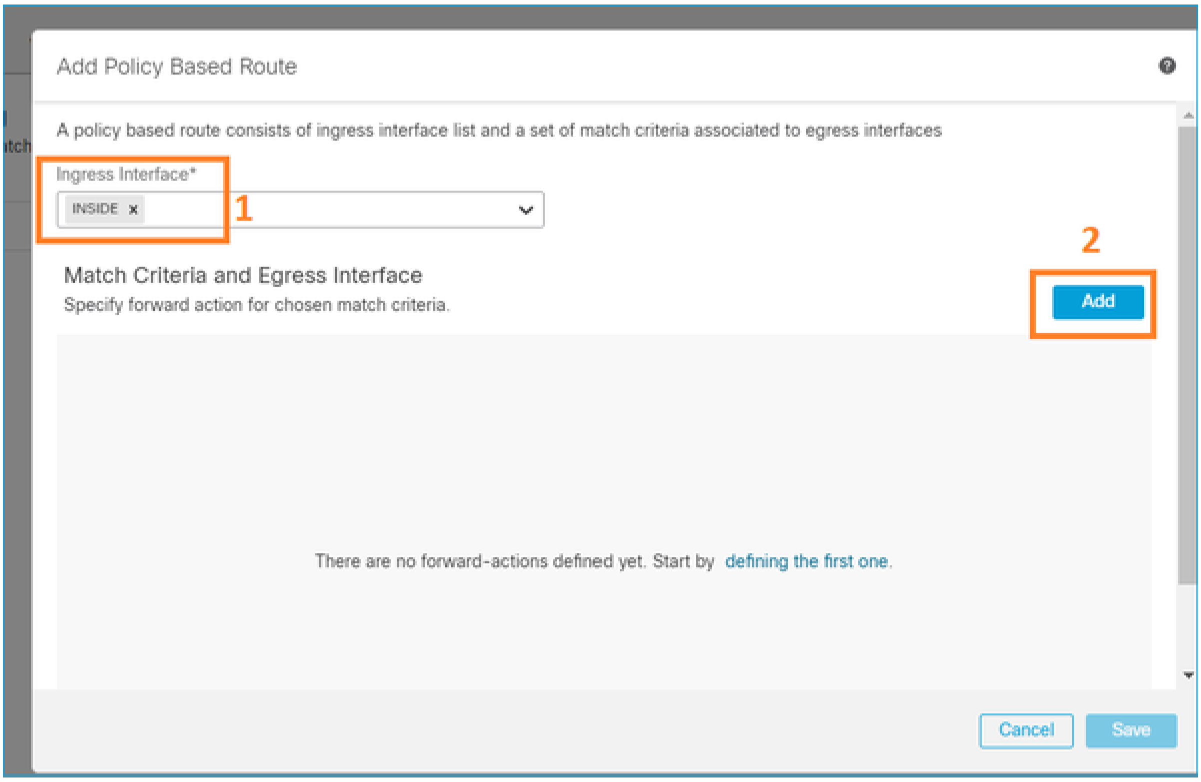
Paso 2 - Agregar una política PBR

Navegue hasta Devices > Device Management y edite el dispositivo FTD. Elija Routing > Policy Based Routing, y en la página Policy Based Routing, seleccione Agregar.



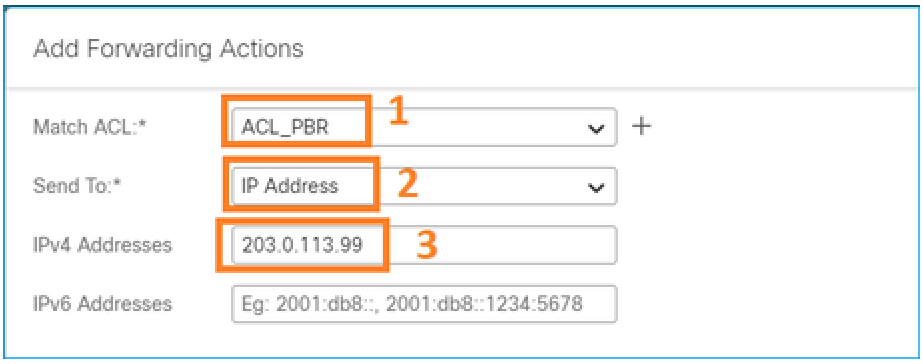
Device
Routing
Interfaces
Inline Sets
DHCP
VTEP
Manage Virtual Routers
Global
Virtual Router Properties
ECMP
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
1
Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can b
Ingress Interfaces
Match criteria and forward action
There are no PBR policies defined yet. Start by defining the first

Especifique la interfaz de ingreso:



Add Policy Based Route
A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces
Ingress Interface*
INSIDE ×
1
2
Match Criteria and Egress Interface
Specify forward action for chosen match criteria.
Add
There are no forward-actions defined yet. Start by defining the first one.
Cancel
Save

Especifique las acciones de reenvío:



Add Forwarding Actions

Match ACL:* ACL_PBR

Send To:* IP Address

IPv4 Addresses 203.0.113.99

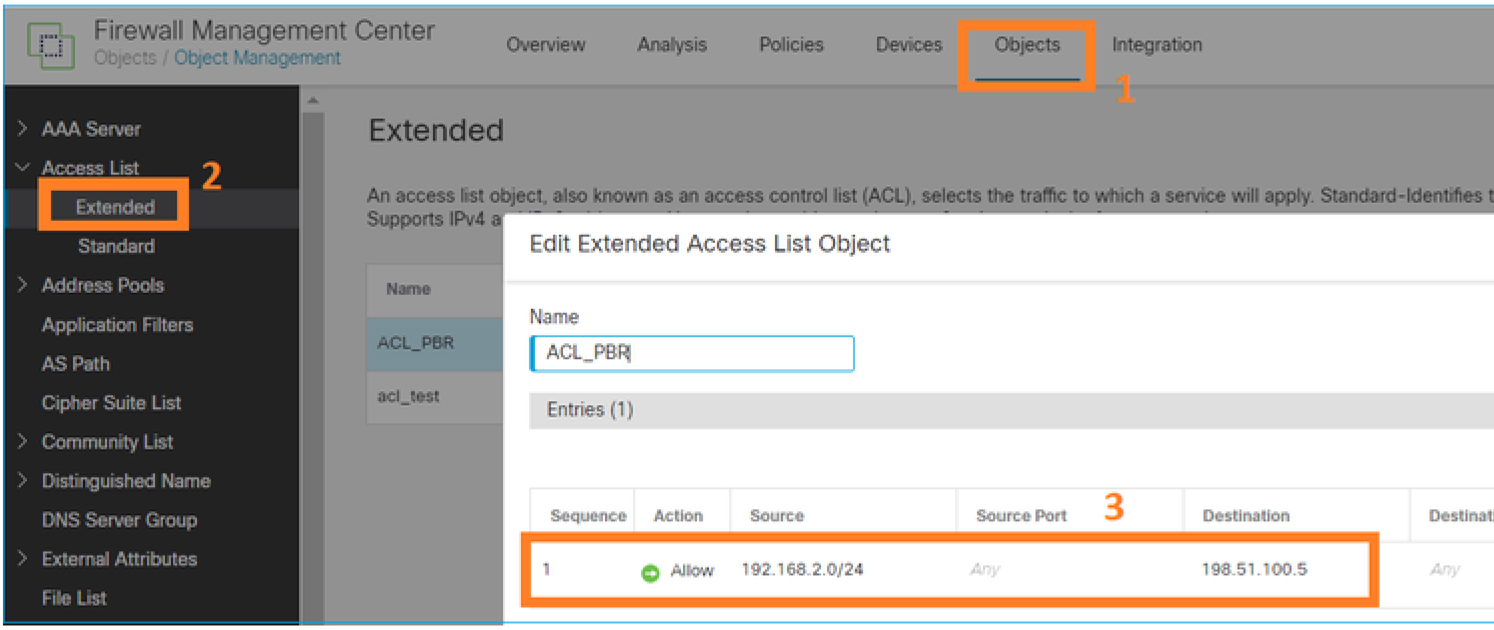
IPv6 Addresses Eg: 2001:db8::, 2001:db8::1234:5678

Guardar e implementar

> Nota: Si desea configurar varias interfaces de salida, debe establecer en el campo 'Enviar a' la opción 'Interfaces de salida' (disponible a partir de la versión 7.0+). Para más detalles, verifique: [Ejemplo de Configuración para Policy Based Routing]()

Configuración de PBR (modo heredado)

Paso 1 - Definir una lista de acceso para el tráfico coincidente.



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies t

Supports IPv4 a

Name
ACL_PBR
acl_test

Edit Extended Access List Object

Name

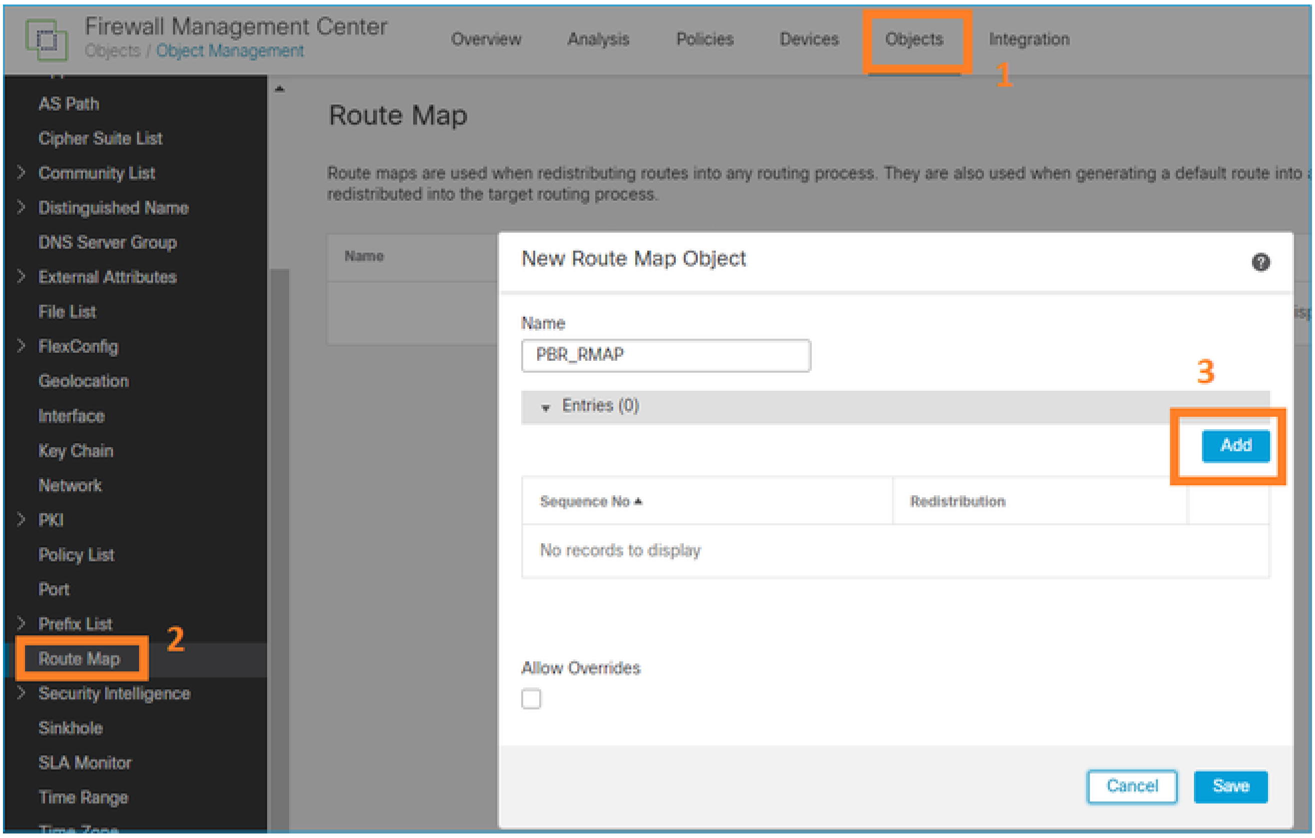
ACL_PBR

Entries (1)

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

Paso 2 - Defina un Route-Map que coincida con la ACL y establezca el Next Hop.

En primer lugar, defina la cláusula de correspondencia:

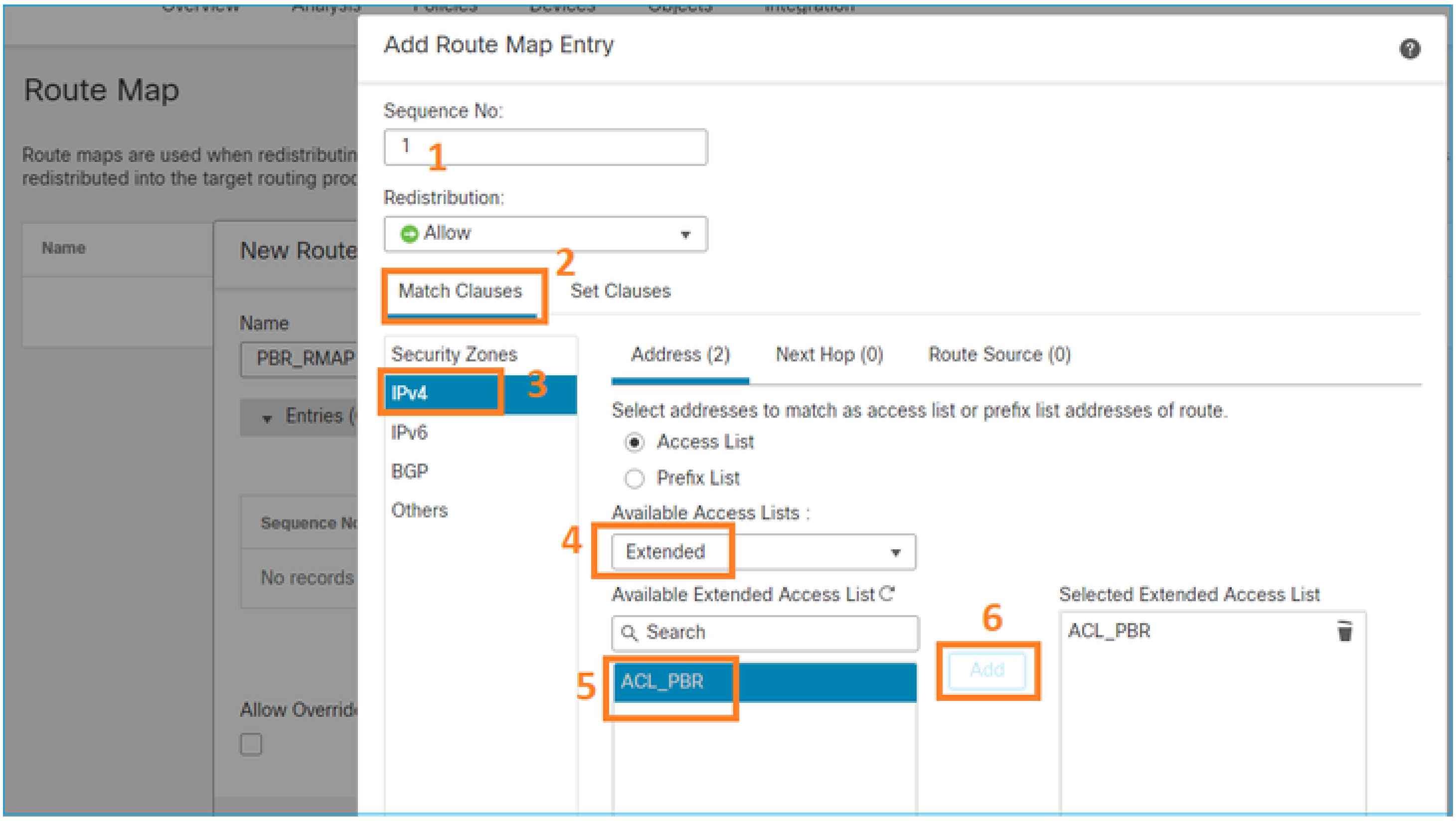


Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a redistributed into the target routing process.

Name: PBR_RMAP

Entries (0)

Allow Overrides ☐



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

Sequence No: 1

Redistribution: Allow

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

● Access List

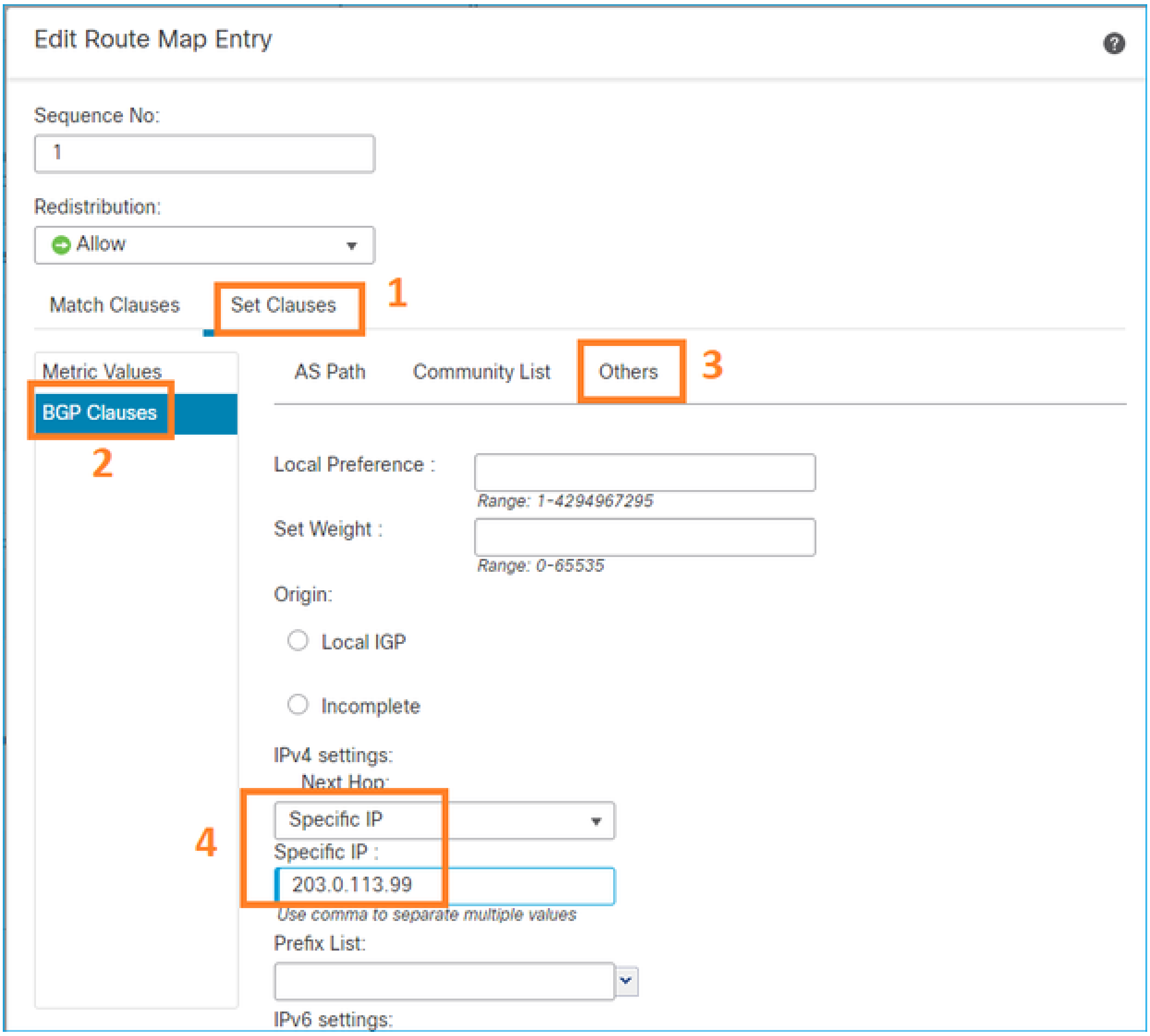
○ Prefix List

Available Access Lists : Extended

Available Extended Access List: ACL_PBR

Selected Extended Access List: ACL_PBR

Defina la cláusula de juego:



Edit Route Map Entry

Sequence No: 1

Redistribution: Allow

Match Clauses | Set Clauses

Metric Values | BGP Clauses

AS Path | Community List | Others

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

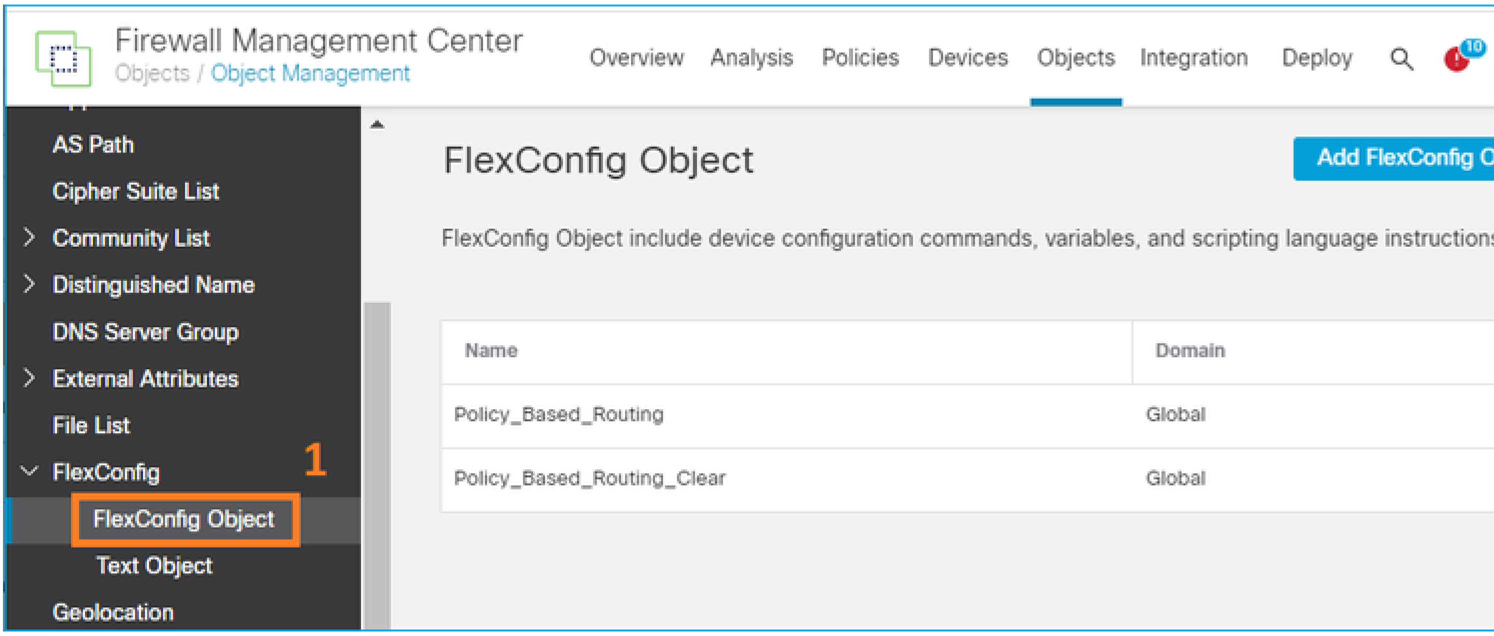
Prefix List:

IPv6 settings:

Agregar y guardar.

Paso 3: Configuración del objeto PBR de FlexConfig.

En primer lugar, copie (duplique) el objeto PBR existente:



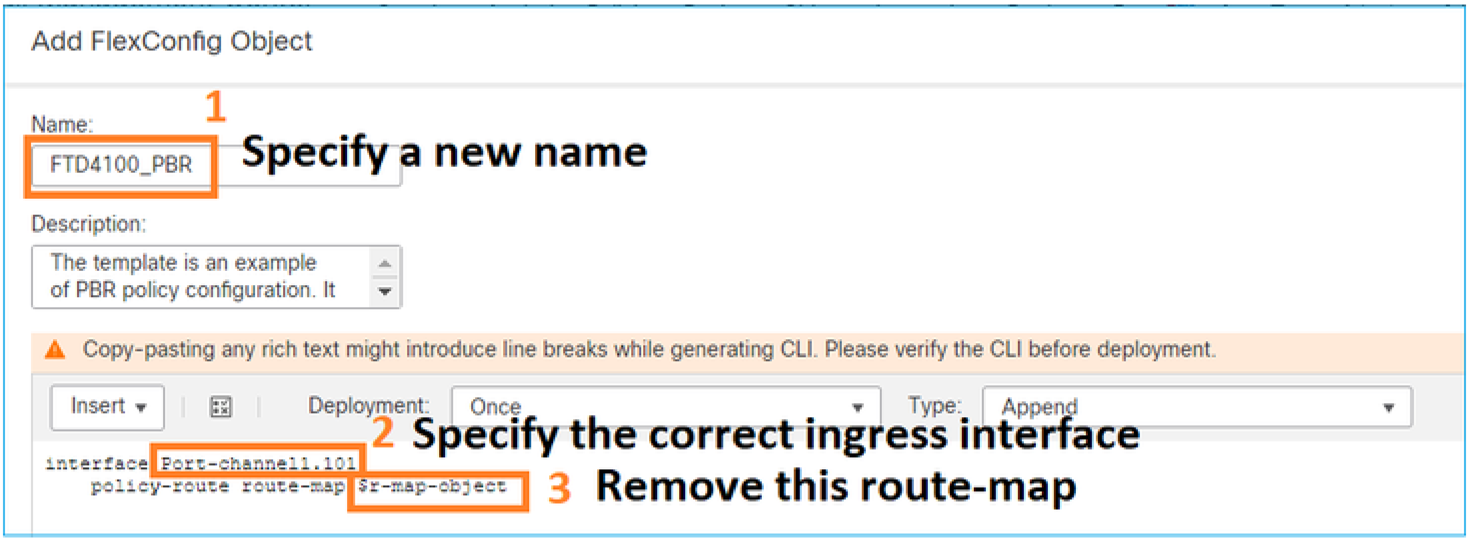
Firewall Management Center
Objects / Object Management

FlexConfig Object

FlexConfig Object include device configuration commands, variables, and scripting language instruction

Name	Domain
Policy_Based_Routing	Global
Policy_Based_Routing_Clear	Global

Especifique el nombre del objeto y elimine el objeto route-map predefinido:



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

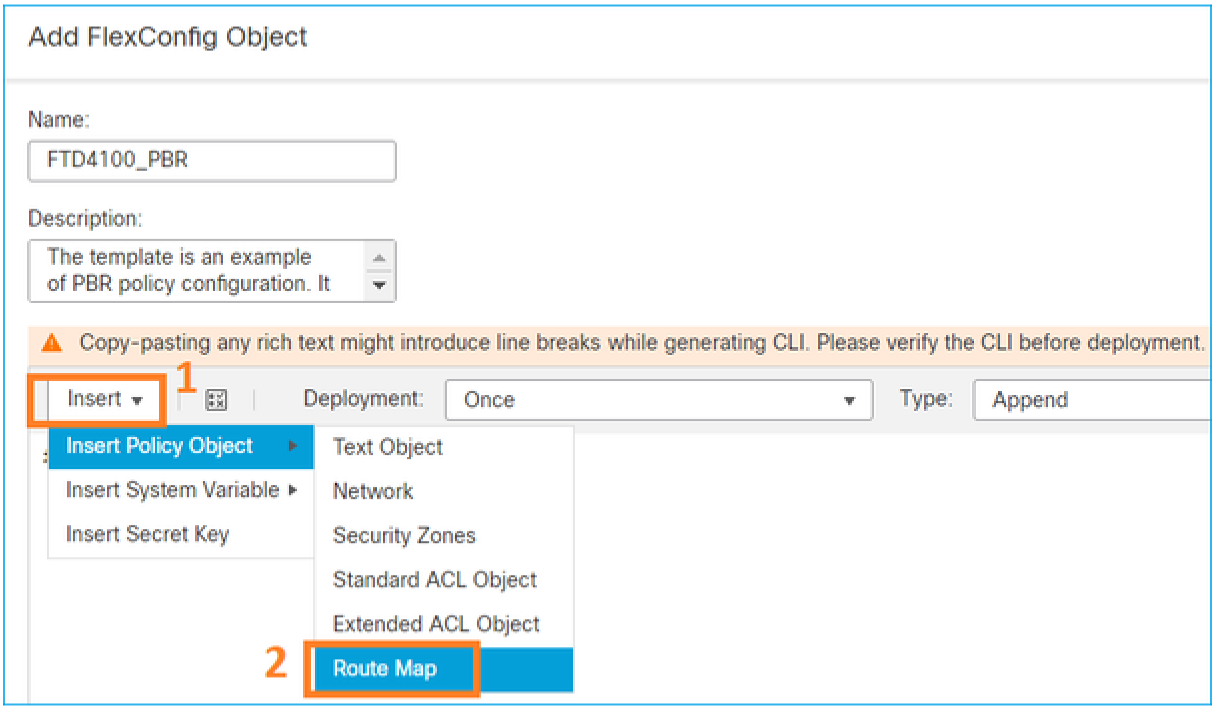
Type: Append

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

2 Specify the correct ingress interface

3 Remove this route-map

Especifique el nuevo route-map:



Add FlexConfig Object

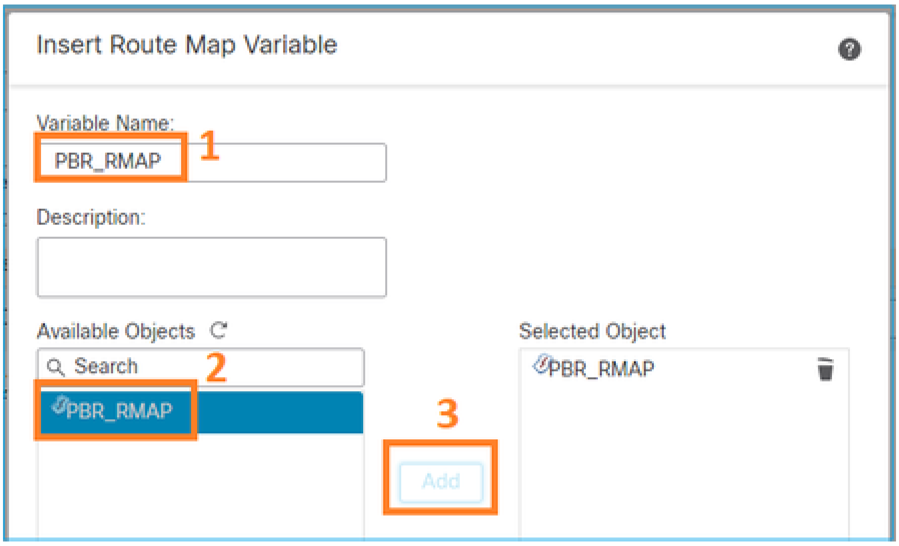
Name: FTD4100_PBR

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

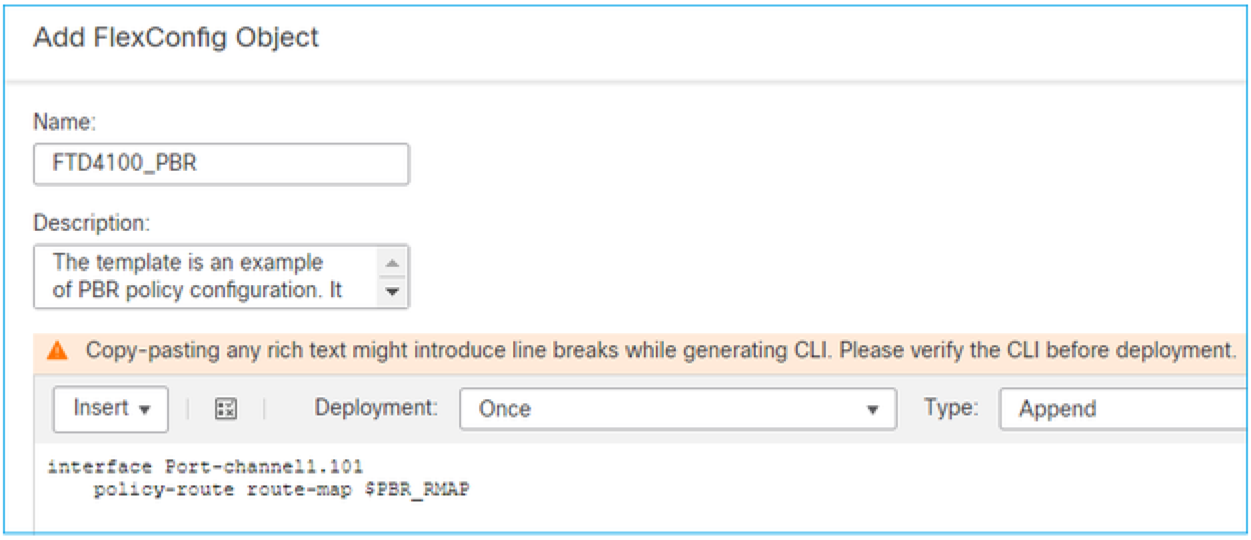
Variable Name: PBR_RMAP

Description:

Available Objects

Selected Object: PBR_RMAP

Este es el resultado final:



Add FlexConfig Object

Name:
FTD4100_PBR

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

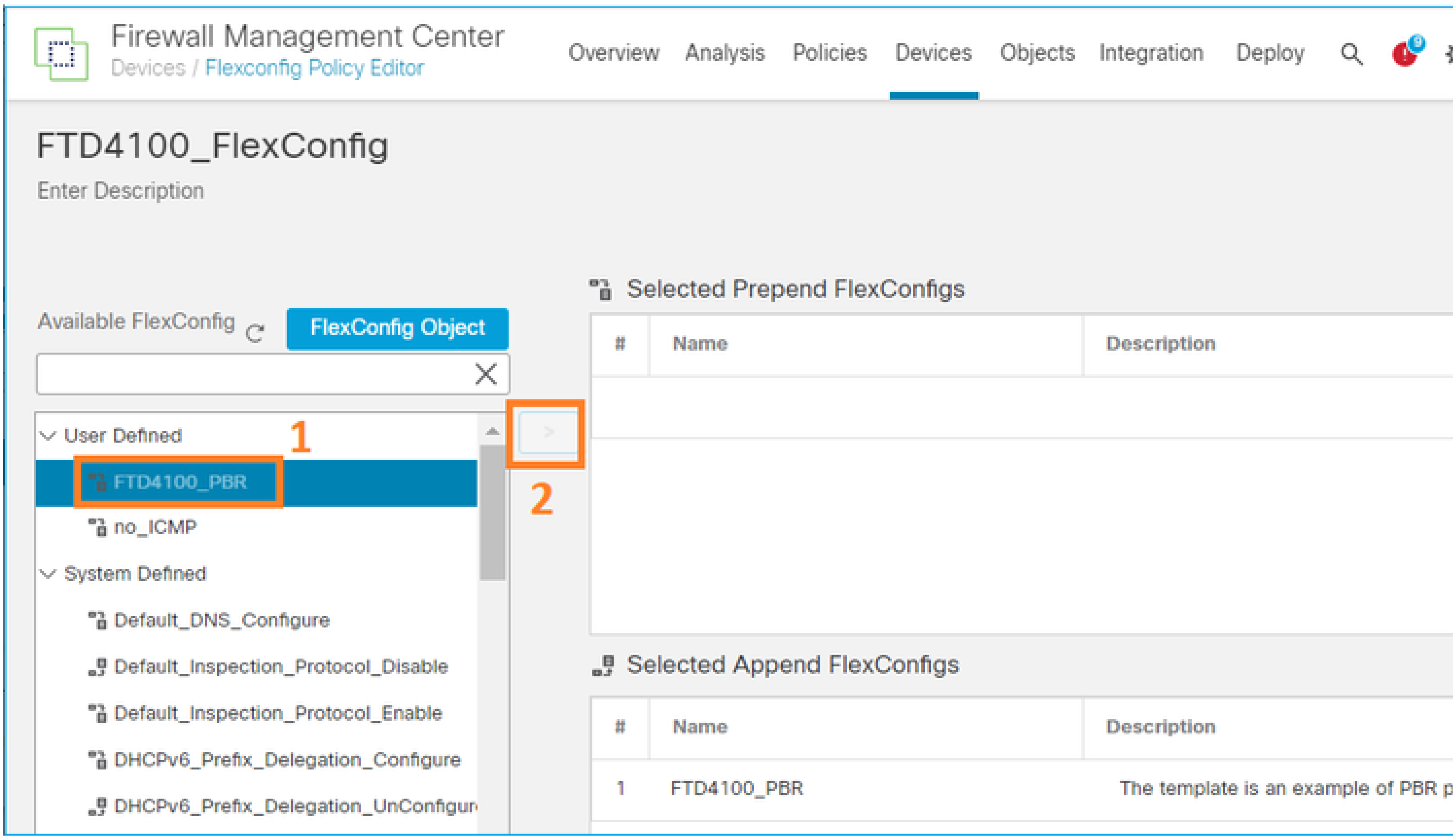
⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once

Type: Append

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

Paso 4: Agregar el objeto PBR a la directiva FlexConfig de FTD.



FTD4100_FlexConfig

Enter Description

Available FlexConfig

- User Defined
  - 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

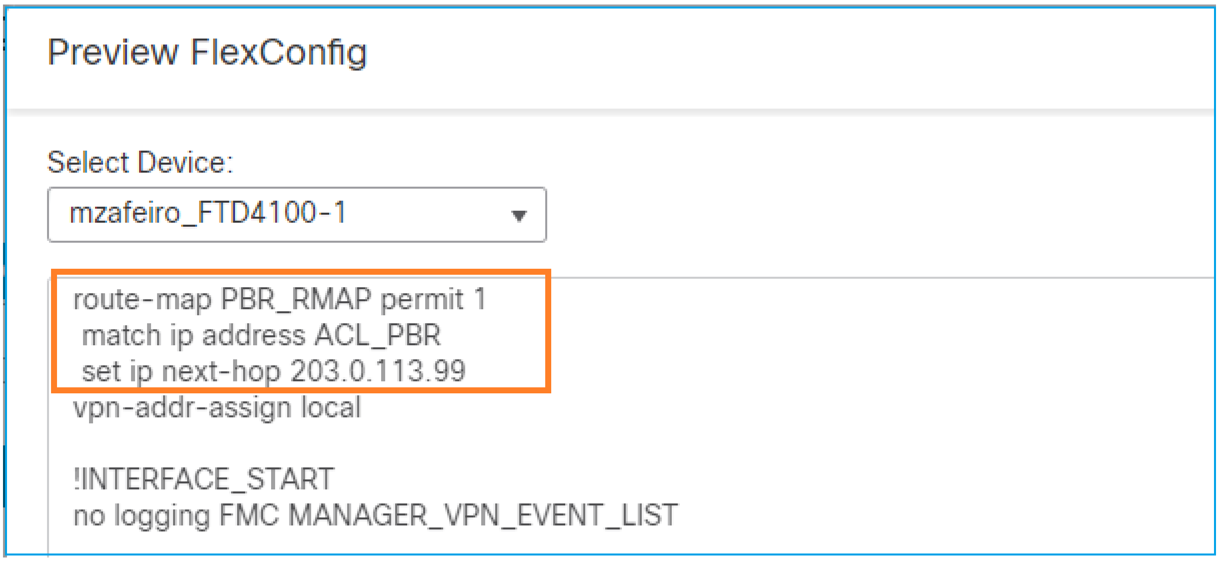
Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	FTD4100_PBR	The template is an example of PBR p

Guarde y seleccione Preview Config:

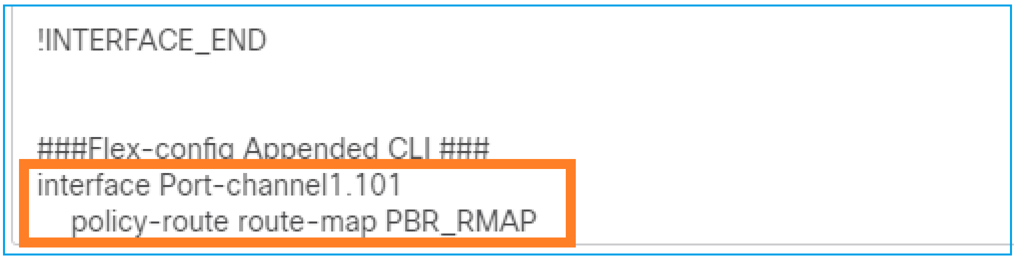


Preview FlexConfig

Select Device:

mzafeiro_FTD4100-1

```
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
```

Por último, implemente la política.

> Nota: PBR no se puede configurar mediante FlexConfig y la interfaz de usuario de FMC para la misma interfaz de entrada.

Para la configuración de PBR SLA, verifique este documento: Configure PBR con IP SLAs para DUAL ISP en FTD Managed by FMC

Verificación de PBR

Verificación de interfaz de ingreso:

```
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
```

Verificación del mapa de ruta:

```
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)
```

Verificación de ruta de política:

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

Packet-Tracer antes y después del cambio:

Sin PBR	Con 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:	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

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	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

Prueba con tráfico real

Configuración de la captura de paquetes con un seguimiento:

```
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
```

La captura muestra:

```
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
```

Seguimiento del paquete TCP SYN:

```
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
```

La tabla ASP PBR muestra los recuentos de visitas a la política:

```
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
```

Nota: El rastreador de paquetes también aumenta el contador de visitas.

Depuración PBR

Advertencia: En un entorno de producción, la depuración puede producir muchos mensajes.

Habilitar esta depuración:

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

Enviar tráfico real:

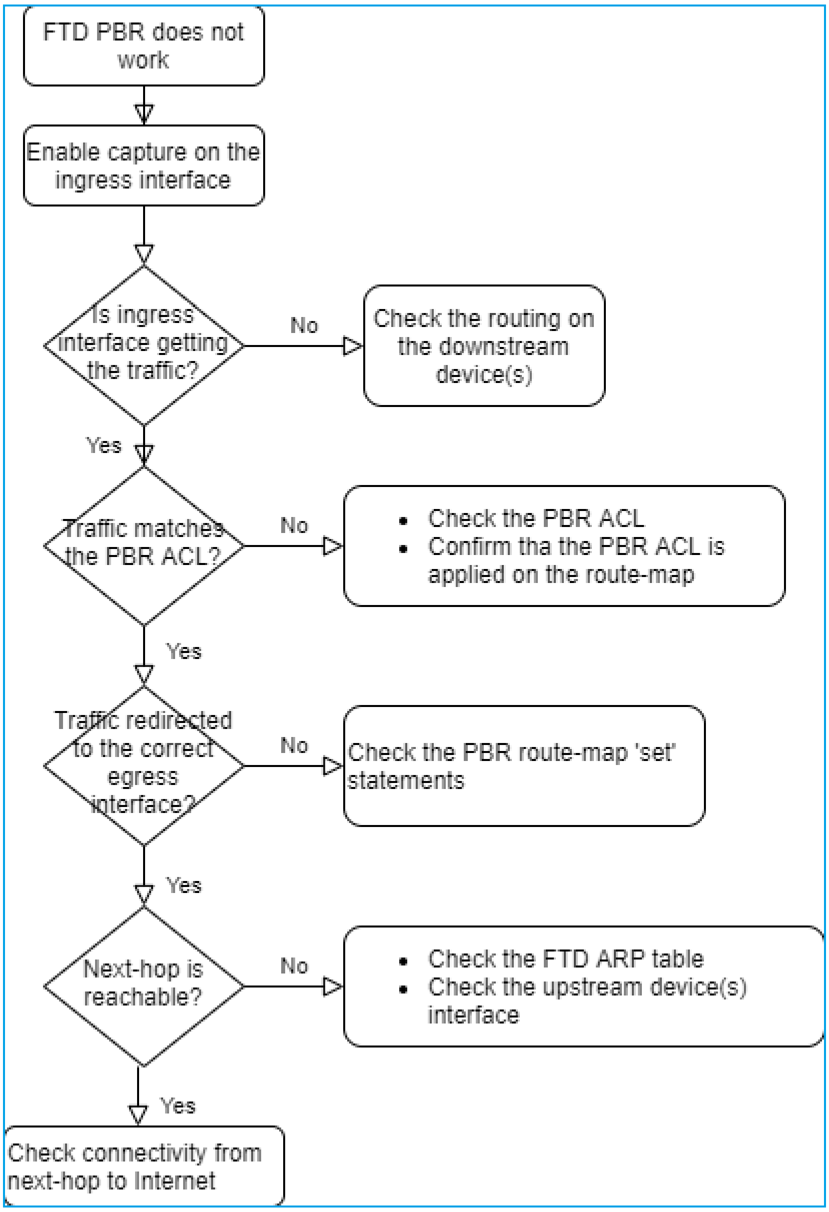
```
Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open
```

El comando debug muestra:

```
firepower#

pbr: policy based route lookup called for 192.168.2.1/37256 to 198.51.100.5/23 proto 6 sub_proto 0 recei
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
```

> Nota: Packet-tracer también genera una salida de depuración.

Este diagrama de flujo se puede utilizar para resolver problemas de PBR:


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

Resumen de comandos PBR

Para verificar la configuración:

```
show run route-map
show run interface
```

En caso de que el Monitor SLA también se utilice con PBR:

```
show run sla monitor
show run track
```

Para verificar la operación:

```
show route-map
packet-tracer
capture w/trace (for example, capture CAPI interface INSIDE trace match ip host 192.168.0.1 host 203.0.1
ASP drop capture (for example, capture ASP type asp-drop all)
show asp table classify domain pbr
show log
show arp
```

En caso de que el Monitor SLA también se utilice con PBR:

```
show sla monitor operational-state
show sla monitor configuration
show track
```

Para depurar PBR:

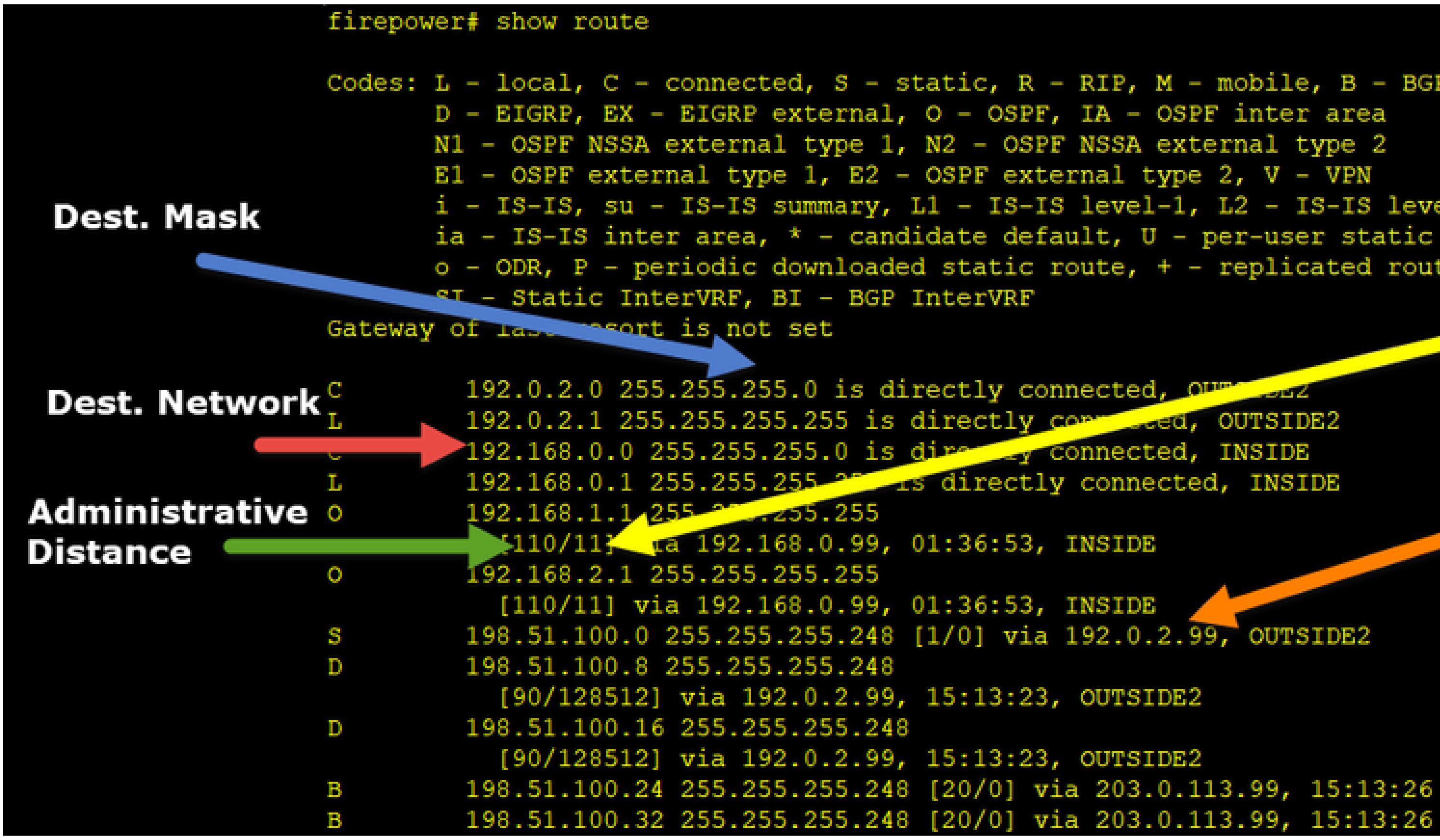
```
debug policy-route
show asp drop
```

Caso 4: reenvío basado en la búsqueda de routing global

Después de la búsqueda de conexión, la búsqueda NAT y PBR, el último elemento que se comprueba para determinar la interfaz de salida es la tabla de enrutamiento global.

Verificación de tabla de ruteo

Examinemos el resultado de una tabla de ruteo FTD:



```
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 leve
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route, + - replicated rout
       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
```

El objetivo principal del proceso de ruteo es encontrar el salto siguiente. La selección de la ruta se realiza en este orden:

1. El partido más largo gana
2. AD más bajo (entre diferentes orígenes de protocolo de routing)
3. Métrica más baja (en caso de que las rutas se aprendan de la misma fuente - protocolo de ruteo)

Cómo se rellena la tabla de routing:

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

- BGP (B)

- BGP InterVRF (BI)

- Estático (S)

- InterVRF estático (SI)

- Conectado (C)

- IP locales (L)

- VPN (V)

-Redistribución

-Predeterminado

Para ver el resumen de la tabla de ruteo utilice este comando:

<#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
```

Puede realizar un seguimiento de las actualizaciones de la tabla de ruteo con este comando:

<#root>

```
firepower#

debug ip routing



IP routing debugging is on
```

Por ejemplo, esto es lo que muestra la depuración cuando la ruta OSPF 192.168.1.0/24 se elimina de la tabla de ruteo global:

<#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_count
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
```

Cuando se vuelva a agregar:

<#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
```

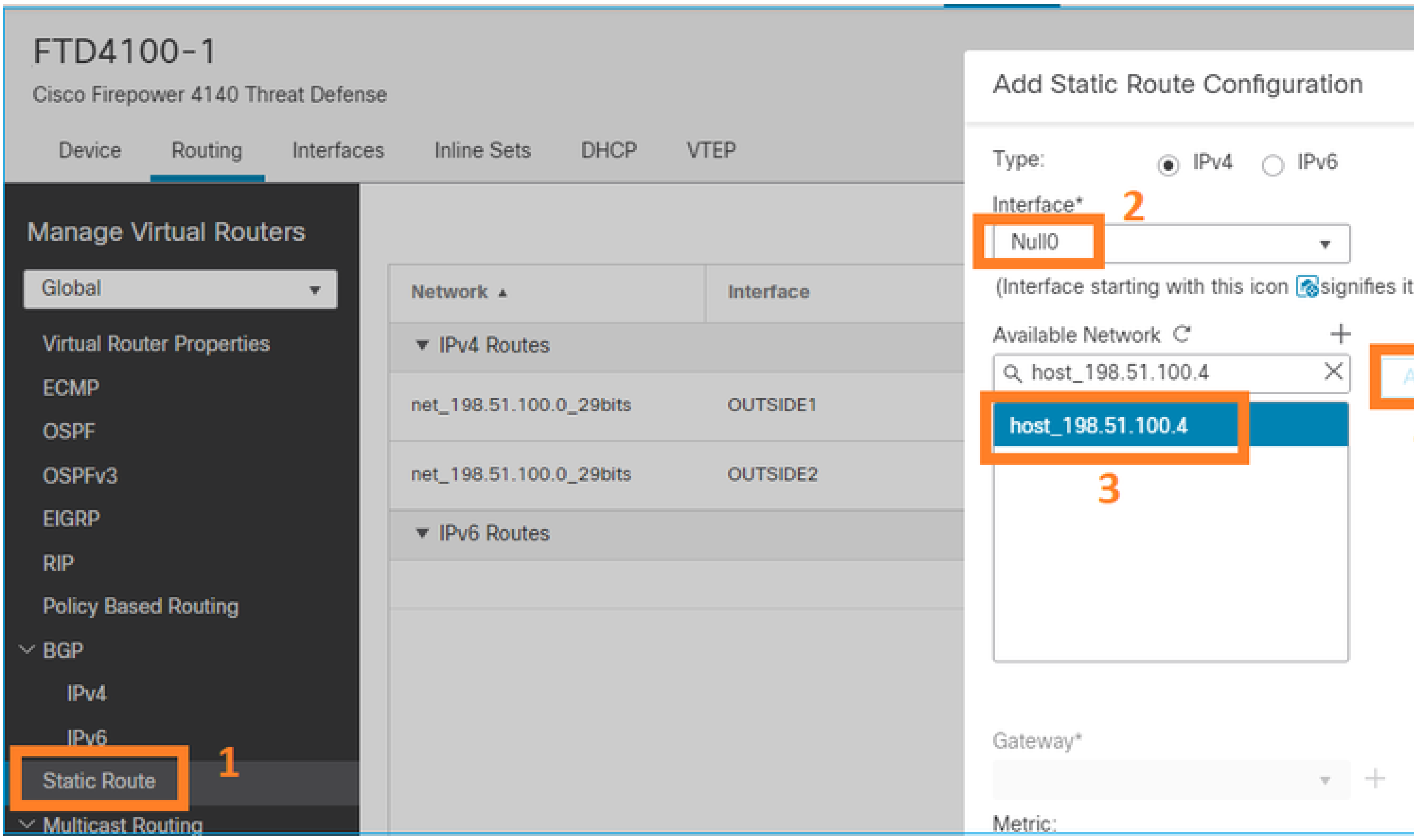
Interfaz Null0

La interfaz Null0 se puede utilizar para descartar tráfico no deseado. Esta caída tiene menos impacto en el rendimiento que la caída en el tráfico con una regla de política de control de acceso (ACL).

Requisito

Configure una ruta Null0 para el host 198.51.100.4/32.

Solución



Network ▲	Interface
net_198.51.100.0_29bits	OUTSIDE1
net_198.51.100.0_29bits	OUTSIDE2

Type: ● IPv4 ○ IPv6

Interface*: Null0

Available Network: host_198.51.100.4

host_198.51.100.4

Guardar e implementar.

Verificación:

<#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
```

Intente acceder al host remoto:

<#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)
```

Los registros de FTD muestran:

<#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
```

Las caídas ASP muestran:

<#root>

```
firepower#

show asp drop


Frame drop:
```

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

Ruta múltiple de igual coste (ECMP)

Zonas de tráfico

- La zona de tráfico ECMP permite a un usuario agrupar interfaces (denominada zona ECMP).
- Esto permite el ruteo ECMP así como el balanceo de carga del tráfico a través de múltiples interfaces.
- Cuando las interfaces se asocian con la zona de tráfico ECMP, el usuario puede crear rutas estáticas de igual coste a través de las interfaces. Las rutas estáticas de igual costo son rutas a la misma red de destino con el mismo valor de métrica.

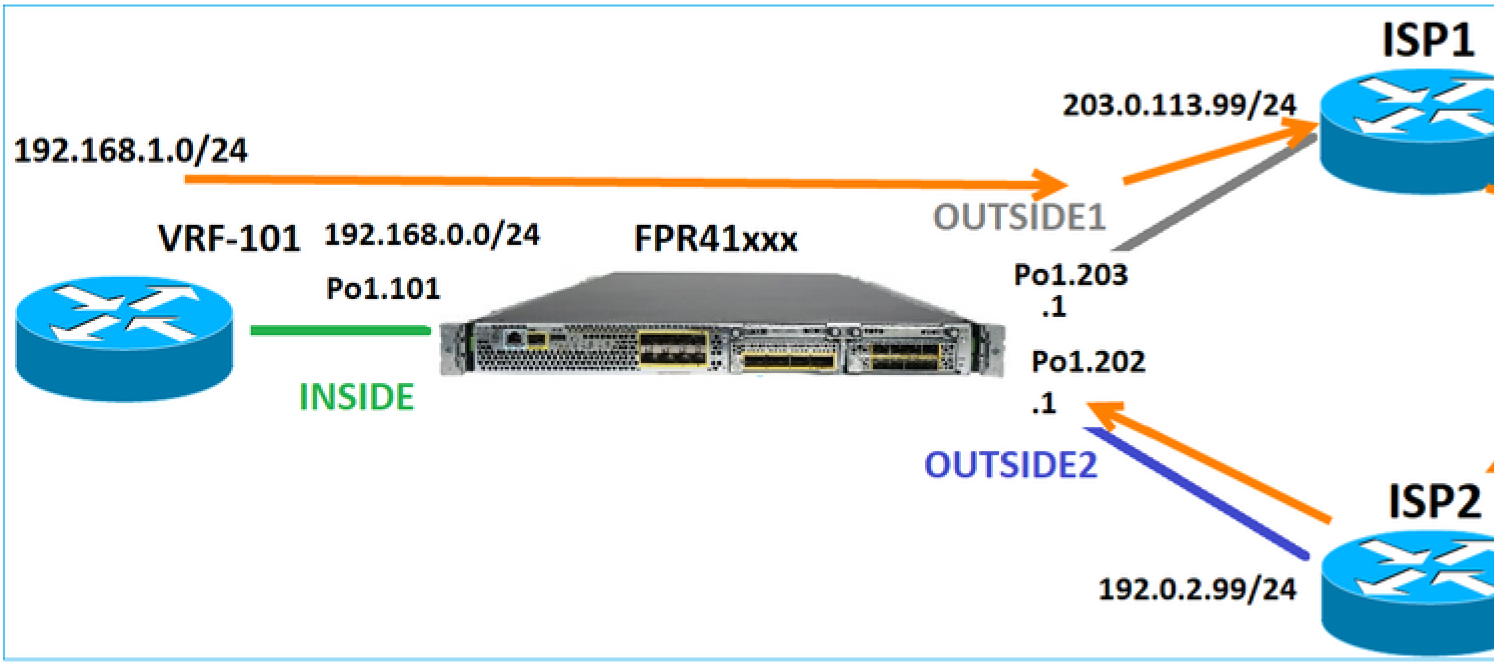
Antes de la versión 7.1, Firepower Threat Defence admitía el routing ECMP mediante políticas FlexConfig. A partir de la versión 7.1, puede agrupar interfaces en zonas de tráfico y configurar el enrutamiento ECMP en Firepower Management Center.

EMCP se documenta en: ECMP

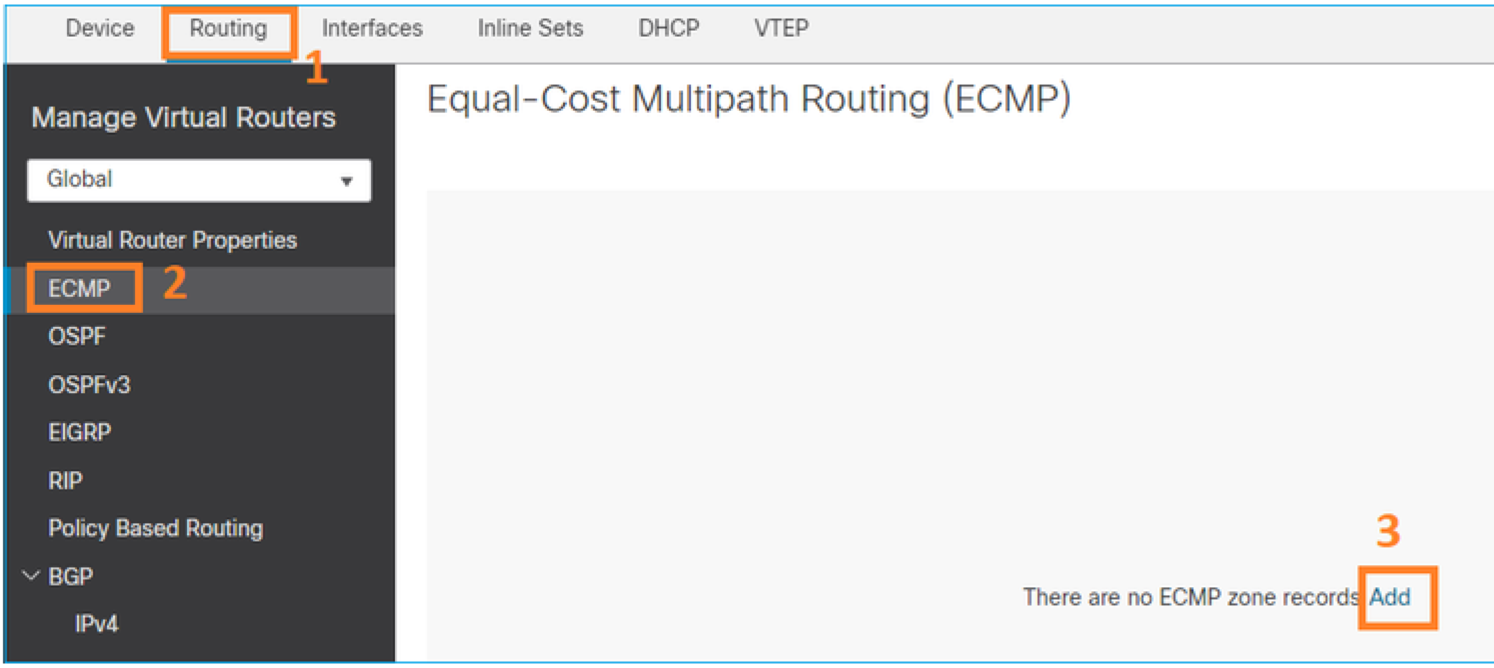
En este ejemplo, existe un ruteo asimétrico y el tráfico de retorno se descarta:

<#root>

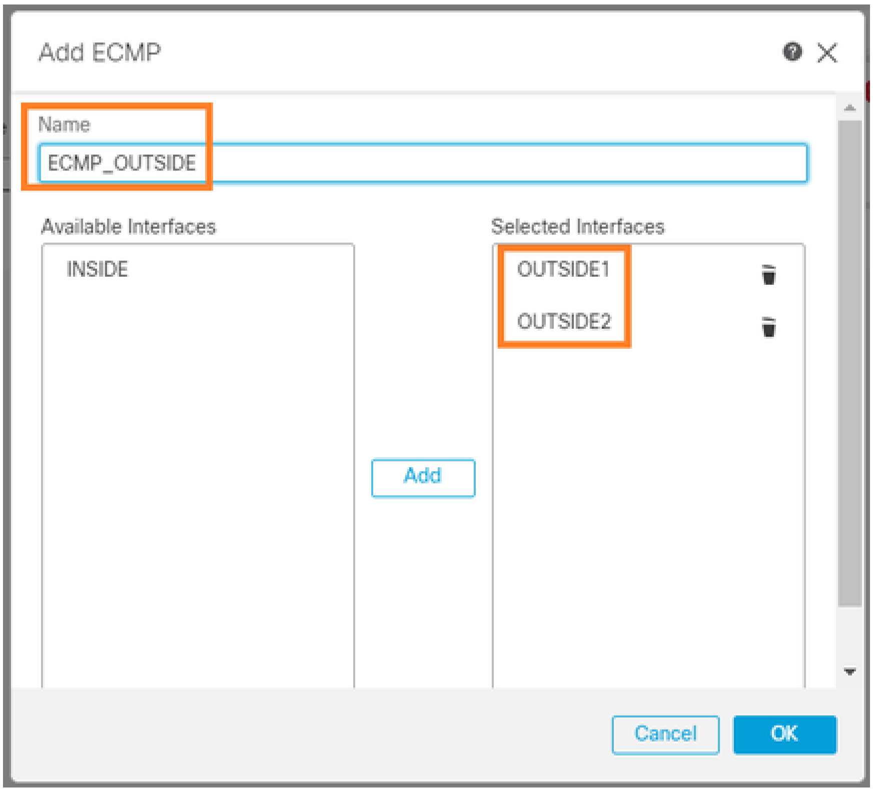
```
firepower#

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 OUTSIDE1:198.51.10


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 OUTSIDE
```



Configure ECMP desde la interfaz de usuario de FMC:



Agregue las 2 interfaces en el grupo ECMP:



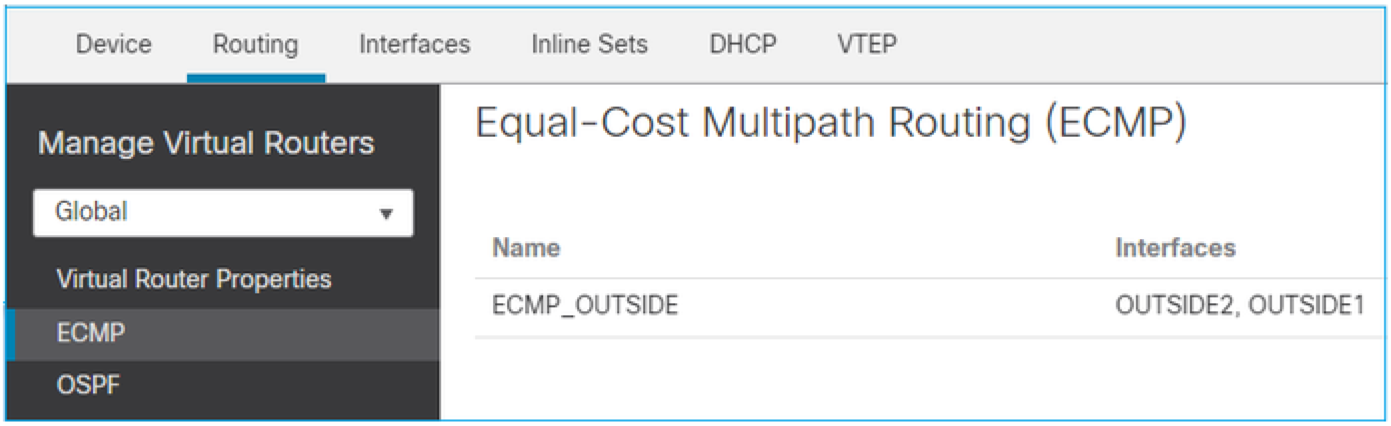
Add ECMP

Name: ECMP_OUTSIDE

Available Interfaces: INSIDE

Selected Interfaces: OUTSIDE1, OUTSIDE2

El resultado:



Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP_OUTSIDE	OUTSIDE2, OUTSIDE1

Guardar e implementar.

Verificación de zona ECMP:

<#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
```

Verificación de la interfaz:

<#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
```

Ahora, se permite el tráfico de retorno y la conexión es UP:

<#root>

```
Router1#
```

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


Trying 198.51.100.100 ... Open
```

La captura en la interfaz ISP1 muestra el tráfico de salida:

<#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
```

La captura en la interfaz ISP2 muestra el tráfico de retorno:

<#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
```

Plano de gestión de FTD

El FTD tiene 2 planos de gestión:

- Interfaz Management0: proporciona acceso al subsistema Firepower.
- Interfaz de diagnóstico LINA: proporciona acceso al subsistema LINA del FTD

Para configurar y verificar la interfaz Management0, utilice los comandos configure network y show network respectivamente.

Por otro lado, las interfaces LINA proporcionan acceso a la propia LINA. Las entradas de la interfaz FTD en la RIB FTD se pueden ver como rutas locales:

<#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
```

De manera similar, se pueden ver como entradas de identidad en la tabla de ruteo ASP:

<#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
```

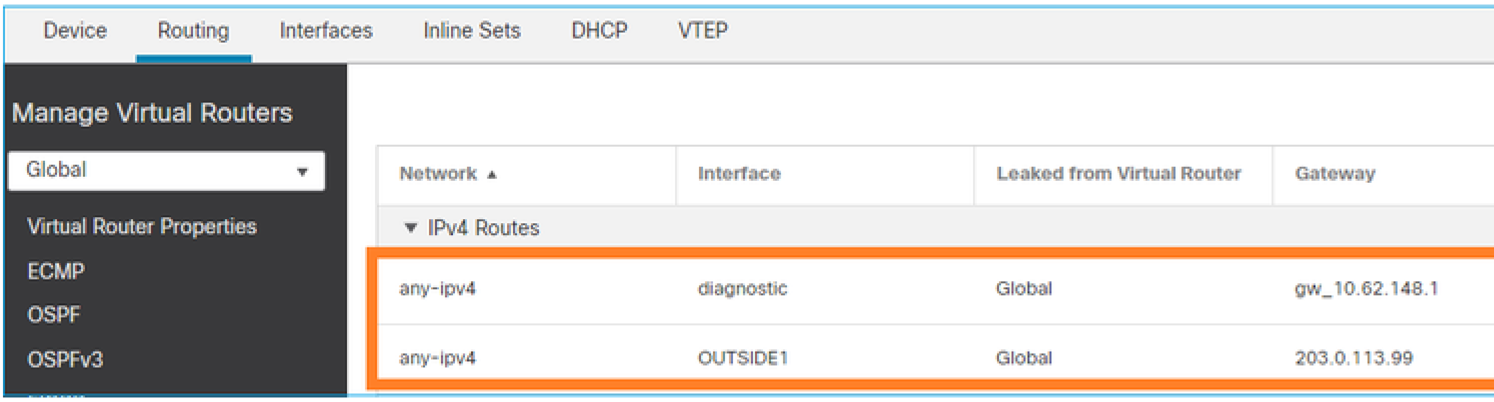
Punto principal

Cuando un paquete llega a FTD y la IP de destino coincide con una de las IP de identidad, el FTD sabe que tiene que consumir el paquete.

Routing de interfaz de diagnóstico de LINA FTD

FTD (como un ASA que ejecuta código posterior a 9.5) mantiene una tabla de ruteo similar a VRF para cualquier interfaz que esté configurada como solo administración. Un ejemplo de dicha interfaz es la interfaz de diagnóstico.

Mientras que FMC no le permite (sin ECMP) configurar 2 rutas predeterminadas en 2 interfaces diferentes con la misma métrica, puede configurar 1 ruta predeterminada en una interfaz de datos FTD y otra ruta predeterminada en la interfaz de diagnóstico:



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

El tráfico del plano de datos utiliza el gateway predeterminado de la tabla global, mientras que el tráfico del plano de administración utiliza el GW predeterminado de diagnóstico:

<#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
```

El gateway de la tabla de ruteo global:

<#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
```

Cuando envía tráfico desde el FTD (tráfico desde el dispositivo), la interfaz de salida se selecciona en función de:

1. Tabla de ruteo global
2. Tabla de ruteo de solo administración

Puede sobrescribir la selección de interfaz de salida si especifica manualmente la interfaz de salida.

Intente hacer ping en la puerta de enlace de la interfaz de diagnóstico. Si no especifica la interfaz de origen, el ping falla porque FTD utiliza primero la tabla de ruteo global que, en este caso, contiene una ruta predeterminada. Si no hay ninguna ruta en la tabla global, el FTD realiza una búsqueda de rutas en la tabla de ruteo de sólo administración:

<#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
```

Lo mismo se aplica si intenta copiar un archivo desde la CLI de LINA con el comando copy.

Detección de reenvío bidireccional (BFD)

El soporte BFD fue agregado en la versión clásica ASA 9.6 y solamente para el protocolo BGP: Bidirectional Forwarding Detection Routing

En FTD:

- Se admiten los protocolos BGP IPv4 y BGP IPv6 (software 6.4).
- Los protocolos OSPFv2, OSPFv3 y EIGRP no son compatibles.
- No se admite BFD para rutas estáticas.

Routers virtuales (VRF)

El soporte VRF fue agregado en la versión 6.6. Para obtener más detalles, consulte este documento: Ejemplos de Configuración de Routers Virtuales

Información Relacionada

- Rutas FTD estáticas y predeterminadas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).