Solucionar problemas de roteamento do Firepower Threat Defense

Contents

Introdução

Este documento descreve como o Firepower Threat Defense (FTD) encaminha pacotes e implementa vários conceitos de roteamento.

Pré-requisitos

Requisitos

- Conhecimento básico de roteamento

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Defesa contra ameaças do Cisco Firepower 41xx versão 7.1.x
- Firepower Management Center (FMC) versão 7.1.x

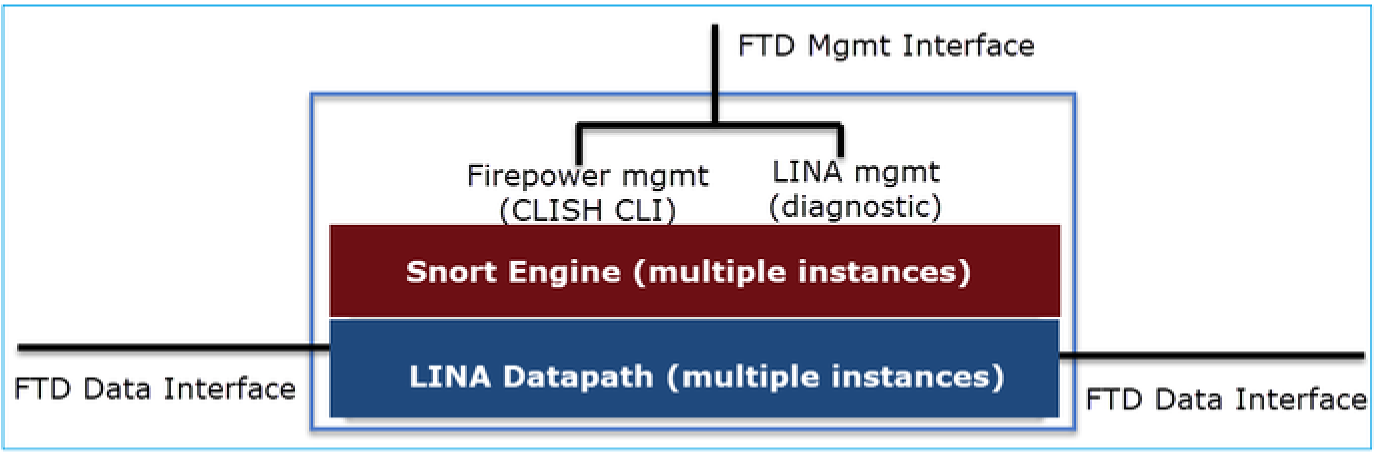
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Mecanismos de encaminhamento de pacotes FTD

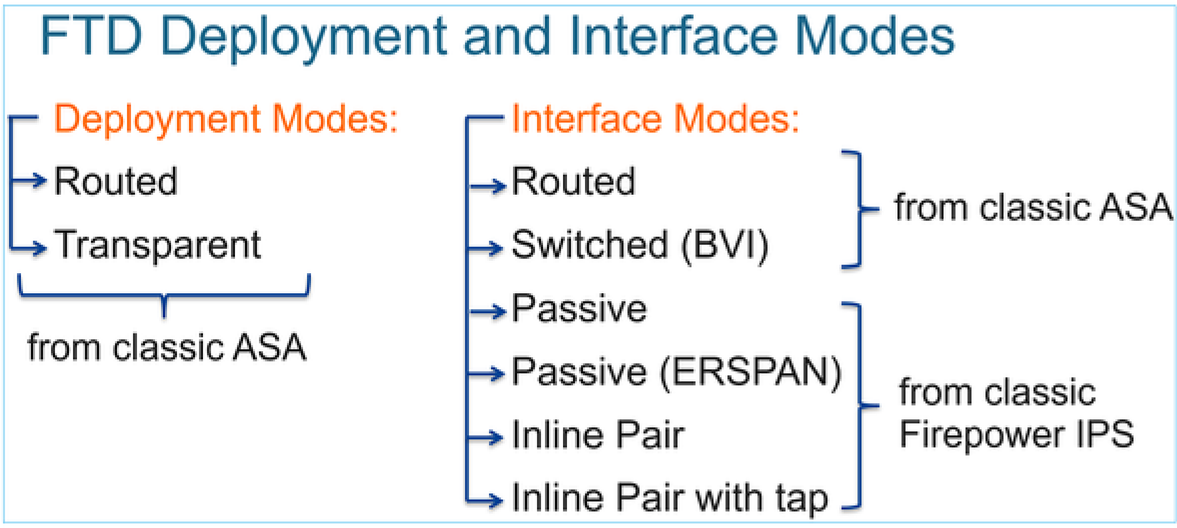
O FTD é uma imagem de software unificada que consiste em dois mecanismos principais:

- Mecanismo de caminho de dados (LINA)
- Mecanismo Snort

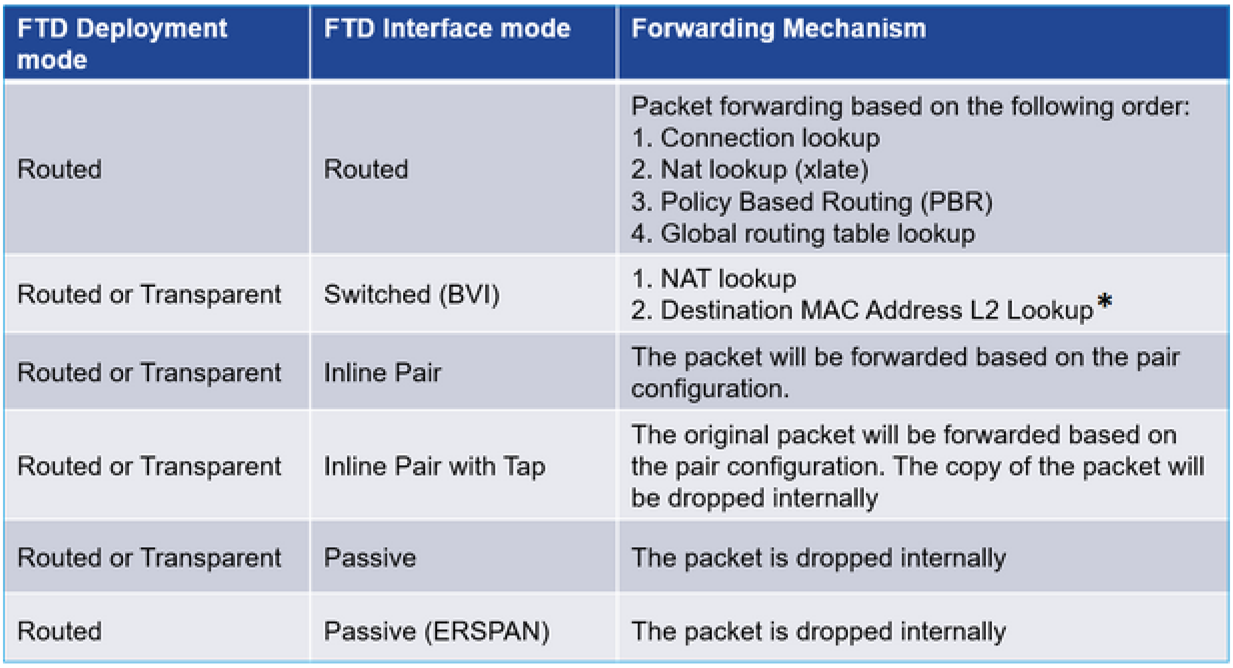


O Datapath e o Snort Engine são as partes principais do Plano de Dados do FTD.

O mecanismo de encaminhamento do plano de dados FTD depende do modo da interface. A imagem a seguir resume os vários modos de interface juntamente com os modos de implantação do FTD:

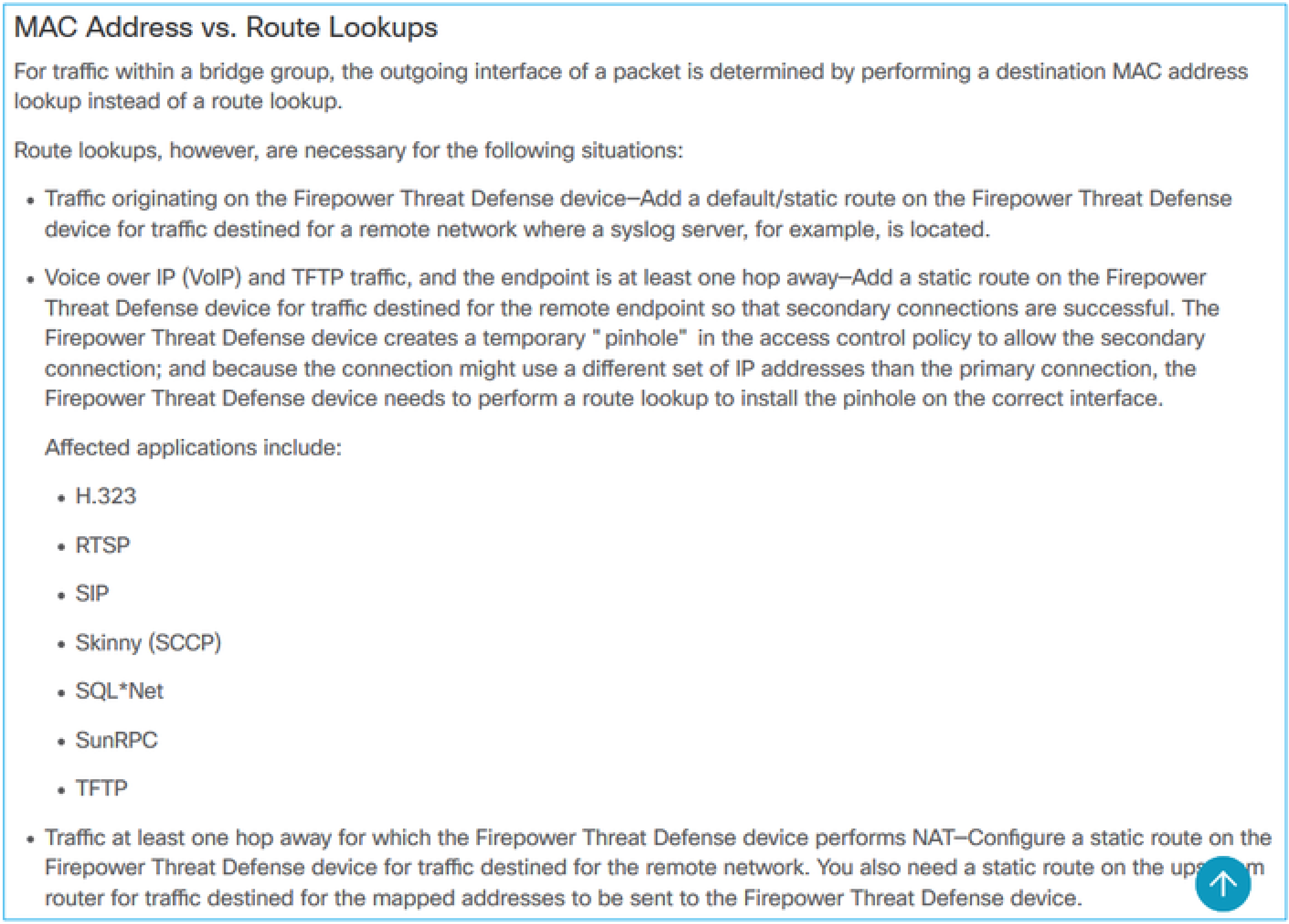


A tabela resume como o FTD encaminha pacotes no plano de dados com base no modo de interface. Os mecanismos de encaminhamento são listados em ordem de preferência:



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

* Um FTD no modo Transparente executa uma Pesquisa de Rota em algumas situações:



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:

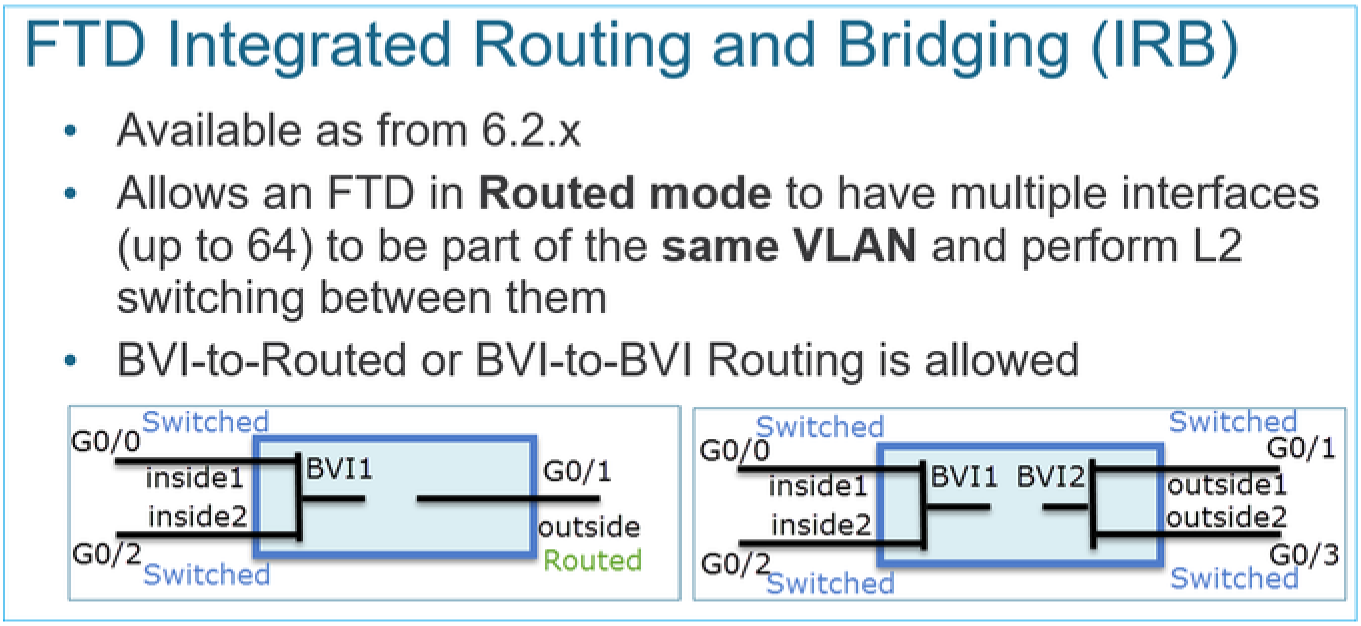
- Traffic originating on the Firepower Threat Defense device–Add a default/static route on the Firepower Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away–Add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

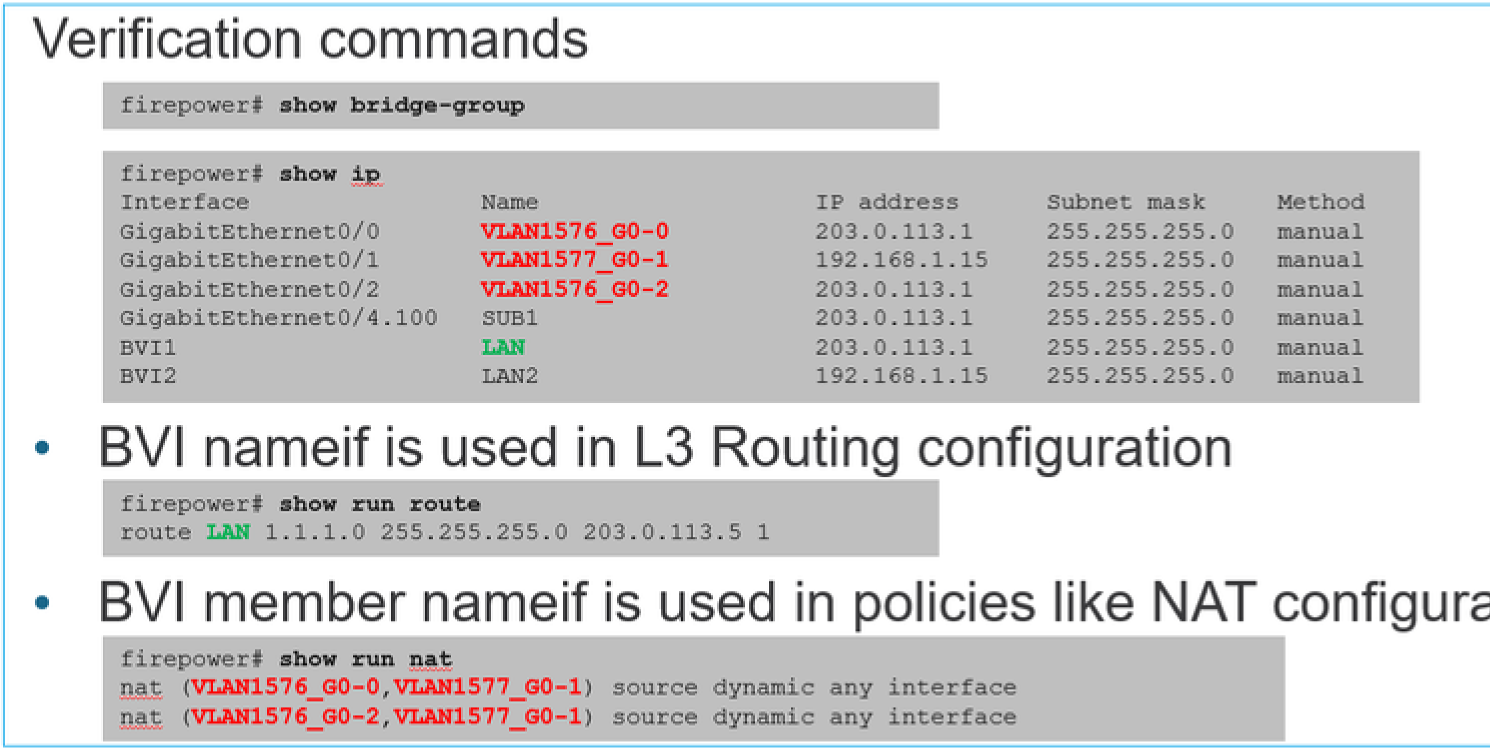
A partir da versão 6.2.x, o FTD suporta Integrated Routing and Bridging (IRB):



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 verificação 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
```

Ponto-chave

Para interfaces roteadas ou BVIs (IRB), o encaminhamento de pacotes é baseado nesta ordem:

- Pesquisa de conexão
- Consulta de NAT (NAT de destino, também conhecido como UN-NAT)
- Roteamento baseado em políticas (PBR)
- Pesquisa de tabela de roteamento global

E o NAT de origem?

O NAT de origem é verificado após a pesquisa de roteamento global.

O restante deste documento se concentra no modo de interface Roteada.

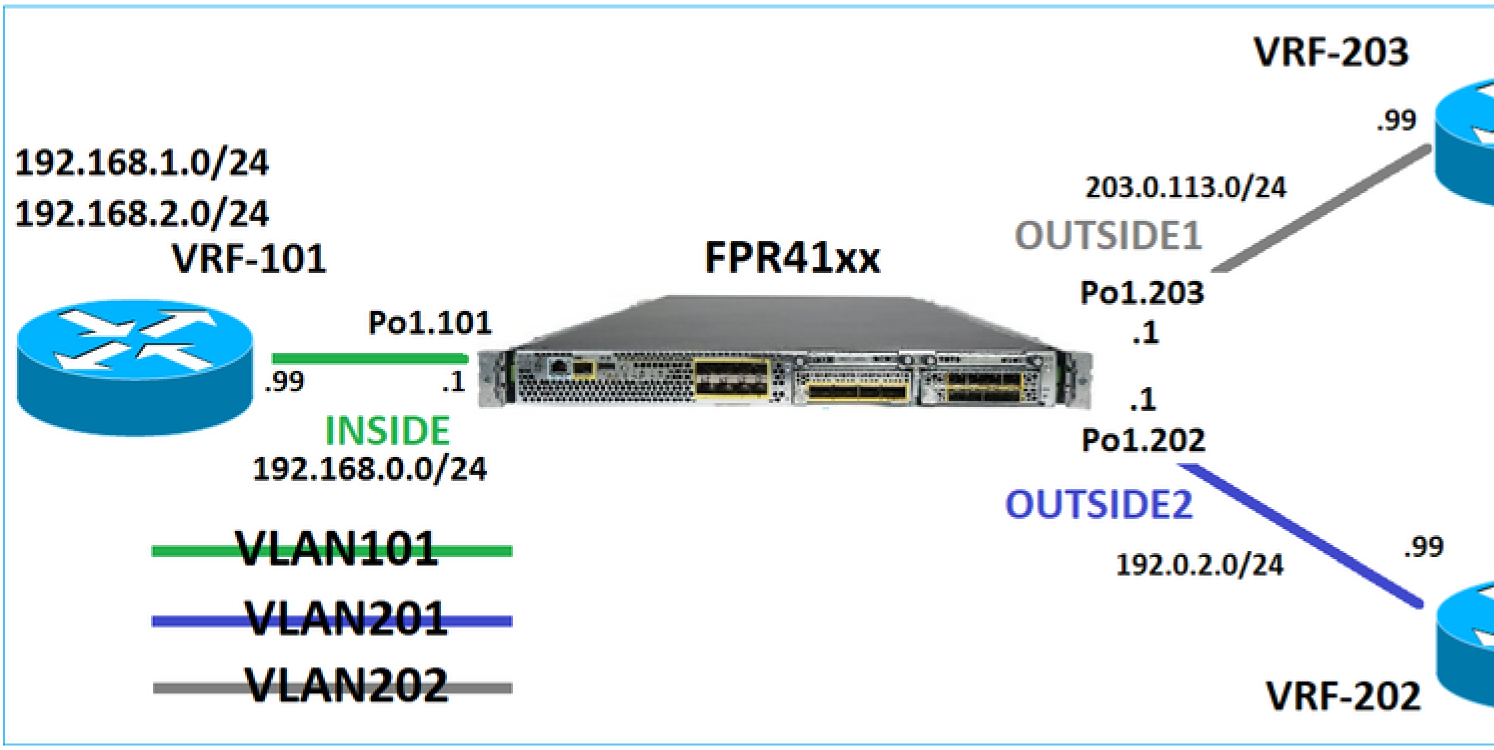
Comportamento de roteamento de plano de dados (LINA)

No modo de interface roteada, o FTD LINA encaminha os pacotes em 2 fases:

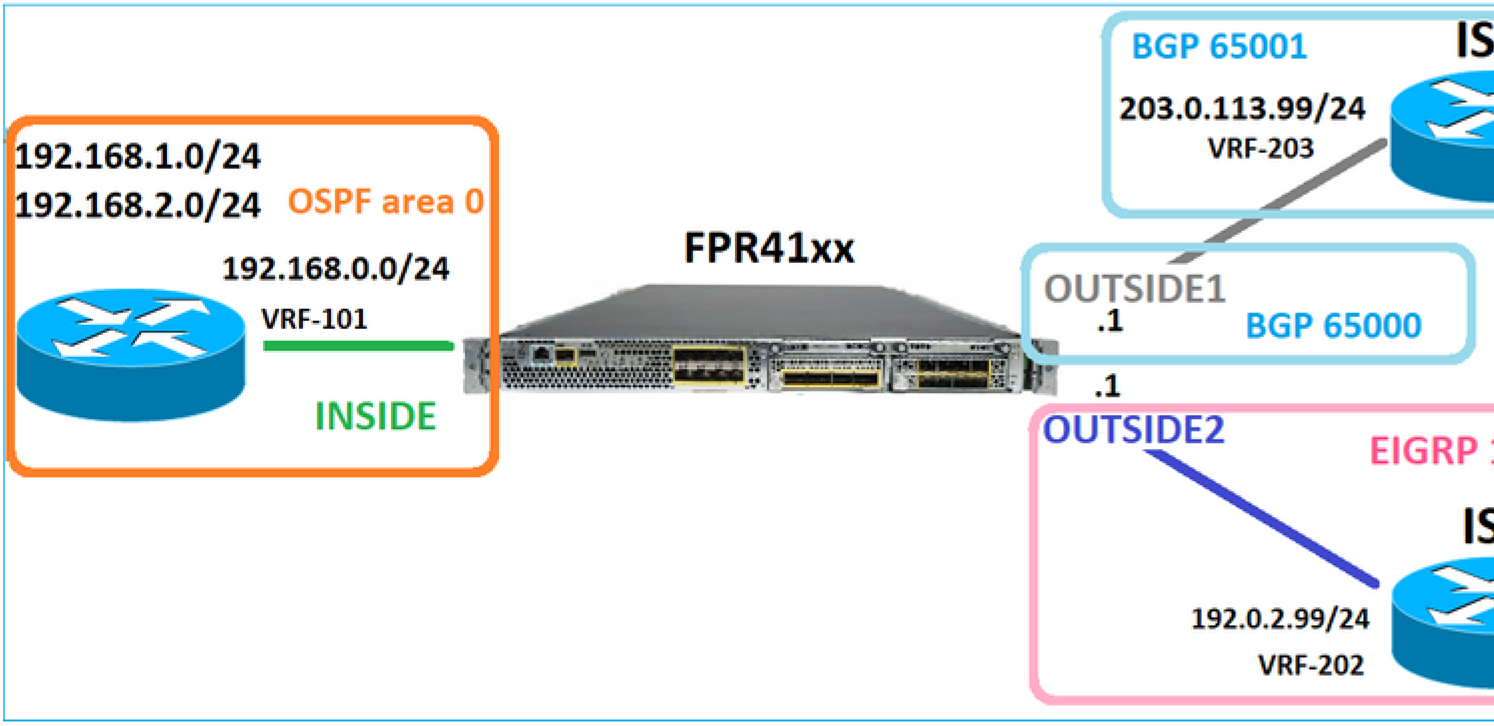
Fase 1 - Determinação da interface de saída

Fase 2 - Seleção do próximo salto

Considere esta topologia:



E este projeto de roteamento:



A configuração de roteamento 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
```

A Base de Informações de Roteamento (RIB - Routing Information Base) do FTD - Plano de Controle:

```
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
```

A tabela de roteamento do Caminho de Segurança Acelerado (ASP) do FTD correspondente - Plano de Dados:

```
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
```

Pontos principais

O FTD (de forma semelhante a um Adaptive Security Appliance - ASA) determina primeiro a interface de saída (saída) de um pacote (para isso, ele examina as entradas de entrada da tabela de roteamento do ASP). Em seguida, para a interface determinada, ele tenta encontrar o próximo salto (para isso, ele examina as entradas 'out' da tabela de roteamento ASP). Por exemplo:

```
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 o próximo salto resolvido, o LINA verifica o cache ARP em busca de uma adjacência válida.

A ferramenta packet-tracer do FTD confirma este processo:

```
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
```

A tabela ARP do FTD como é vista no plano de controle:

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

Para forçar a resolução ARP:

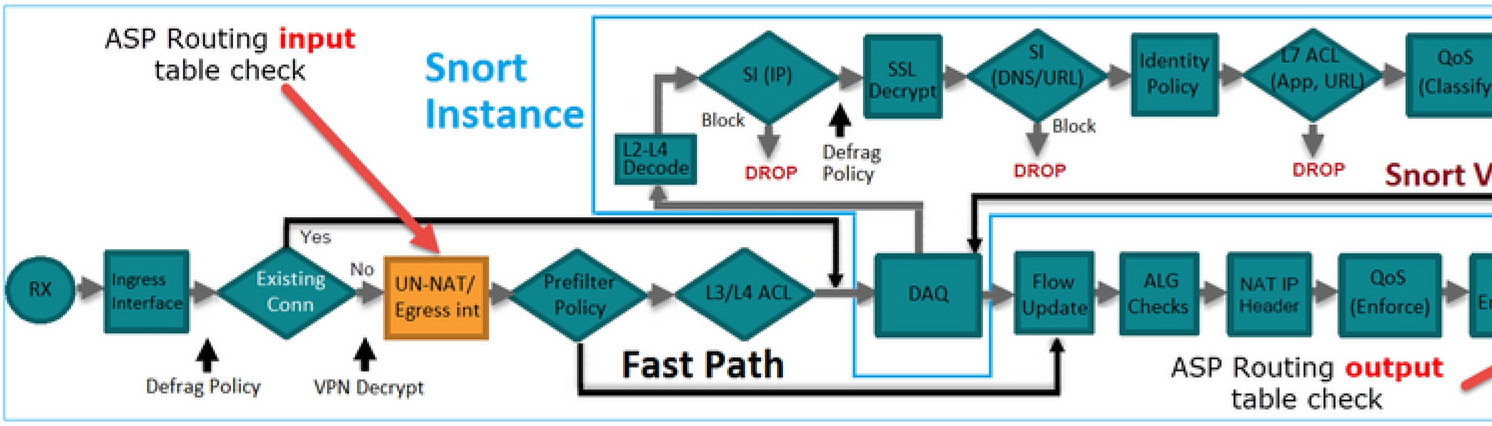
```
firepower# ping 192.168.0.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
firepower# show arp
INSIDE 192.168.0.99 4c4e.35fc.fcd8 45
OUTSIDE1 203.0.113.99 4c4e.35fc.fcd8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

A tabela ARP de FTD como é vista no plano de dados:

```
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
```

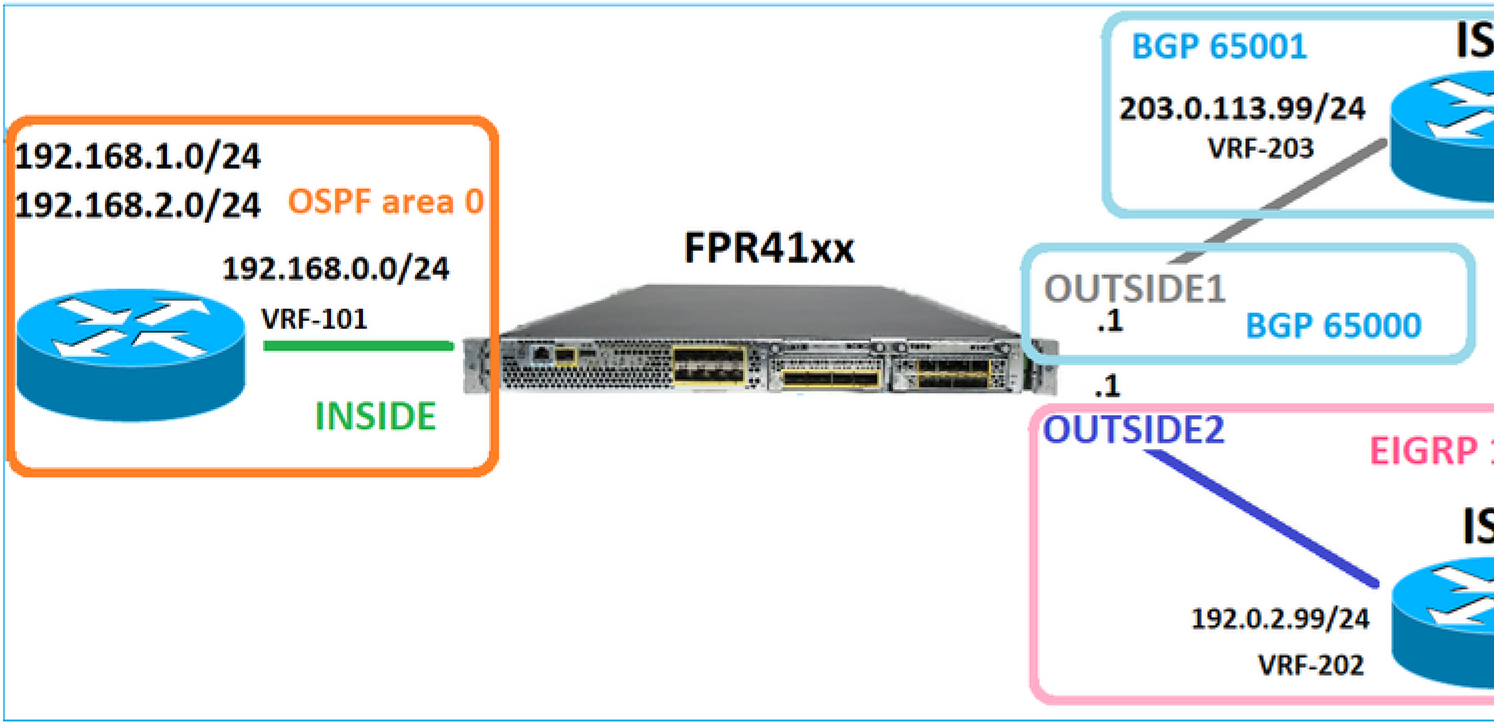
Ordem de Operações do FTD

A imagem mostra a ordem das operações e onde as verificações de roteamento ASP de entrada e saída são feitas:



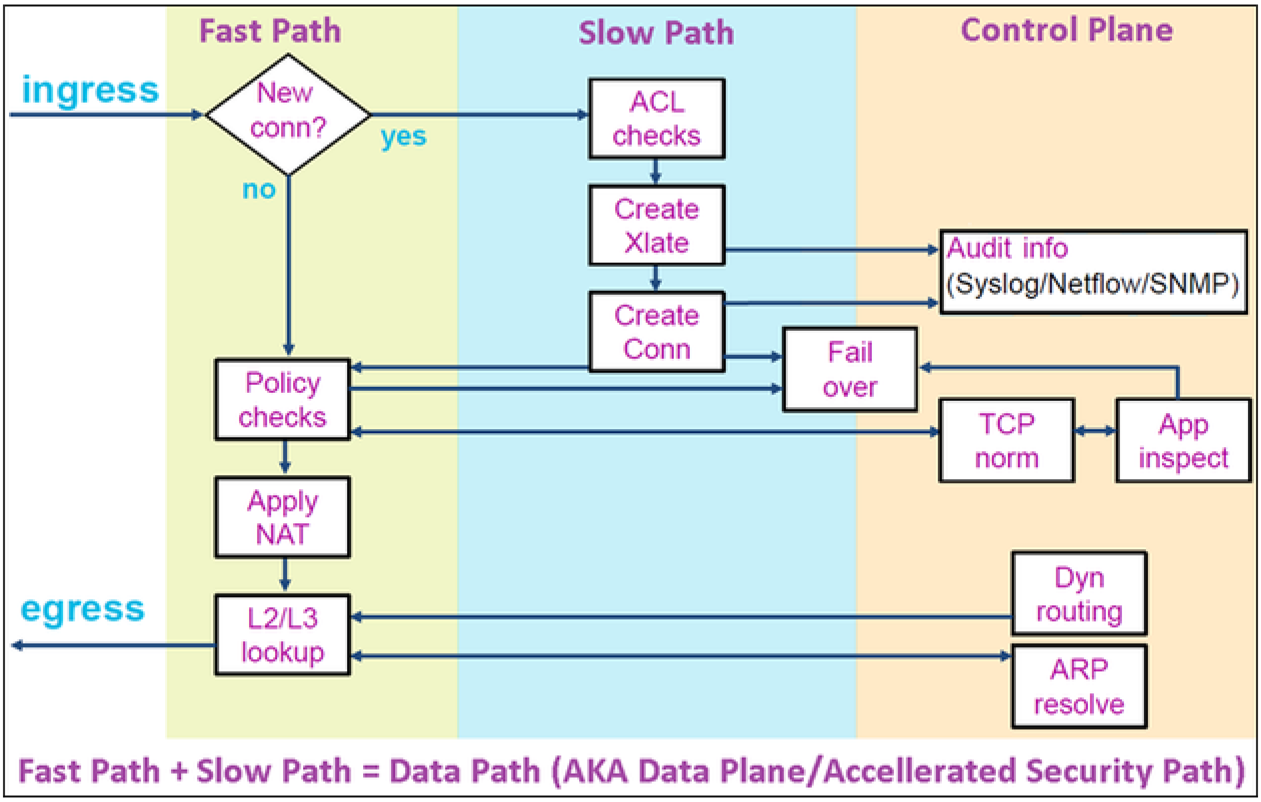
Configurar

Caso 1 - Encaminhamento com base na pesquisa de conexão



Como já foi mencionado, o principal componente do FTD LINA Engine é o processo Datapath (várias instâncias com base no número de núcleos de dispositivos). Além disso, o caminho de dados (também conhecido como caminho de segurança acelerado - ASP) consiste em dois caminhos:

1. Caminho Lento = Responsável pelo estabelecimento de uma nova conexão (ele preenche o Caminho Rápido).
2. Caminho Rápido = Trata pacotes que pertencem a conexões estabelecidas.



- Comandos como show route e show arp mostram o conteúdo do Plano de controle.
- Por outro lado, comandos como show asp table routing e show asp table arp mostram o conteúdo do ASP (Datapath) que é realmente aplicado.

Habilitar captura com rastreamento na interface FTD INSIDE:

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

Abra uma sessão Telnet por meio do FTD:

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

As capturas de FTD mostram os pacotes desde o início da conexão (o handshake triplo do TCP é capturado):

```
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)
...
```

Rastreie o primeiro pacote (TCP SYN). Este pacote passa pelo Caminho Lento LINA do FTD e uma consulta de Roteamento Global é feita neste 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#
```

Rastreie outro pacote de entrada do mesmo fluxo. O pacote que corresponde a uma conexão ativa:

```
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#
```

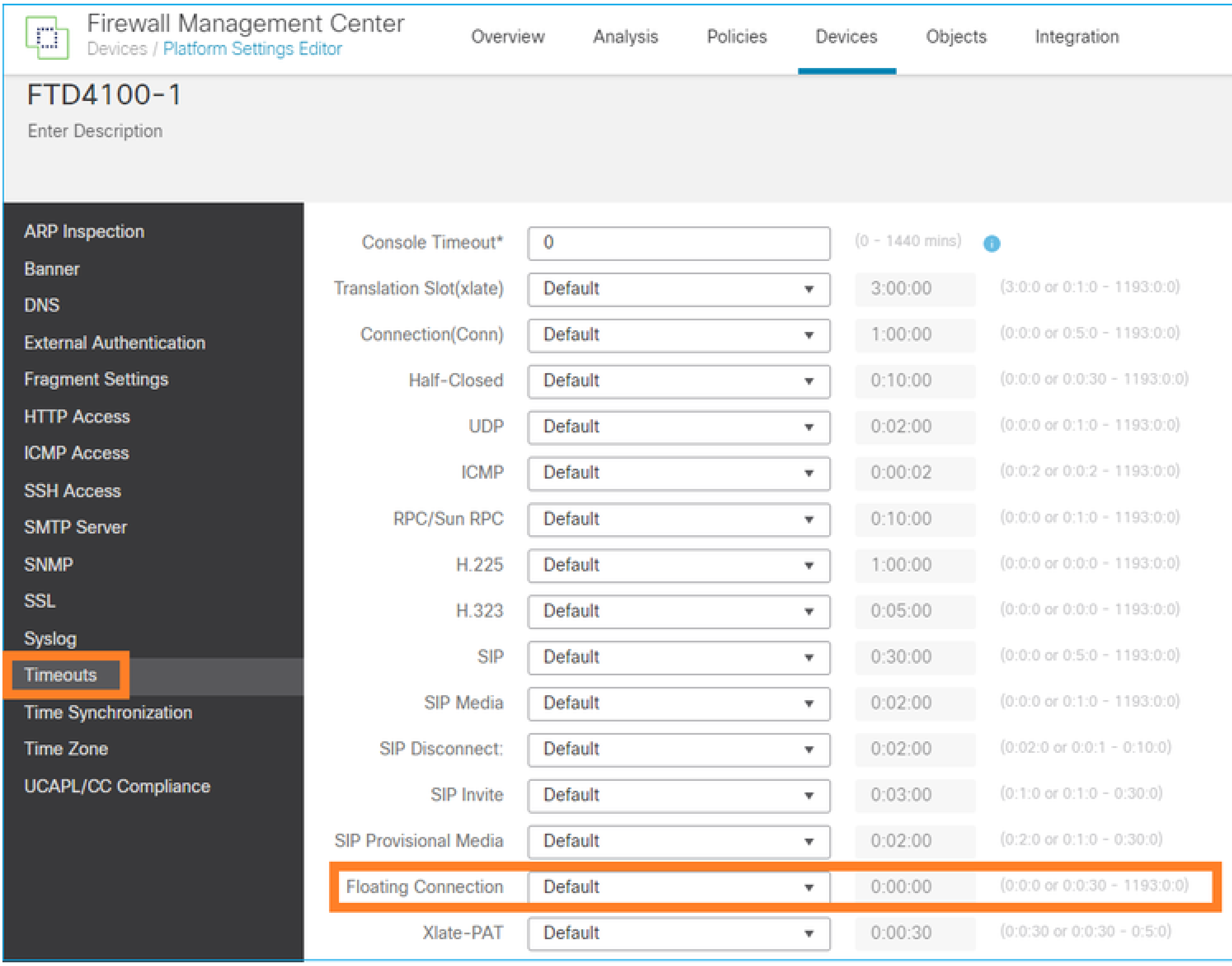
Tempo limite flutuante

O problema

A instabilidade de rota temporária pode fazer com que conexões UDP de longa duração (elefante) através do FTD sejam estabelecidas através de interfaces FTD diferentes das desejadas.

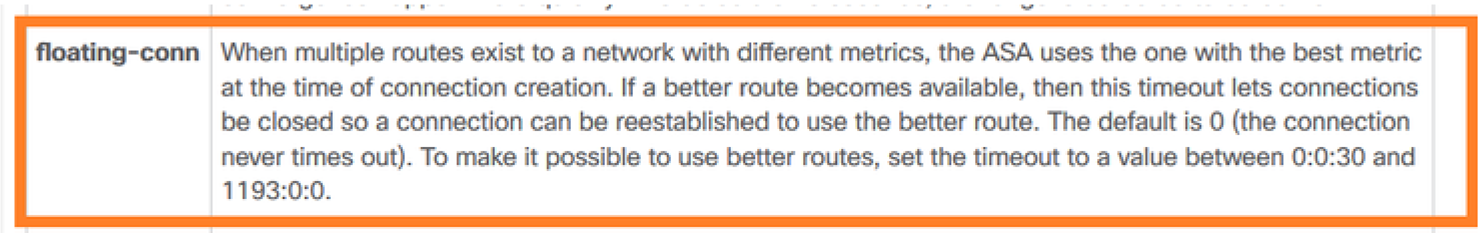
A solução

Para corrigir isso, defina timeout floating-conn com um valor diferente do padrão que está desabilitado:



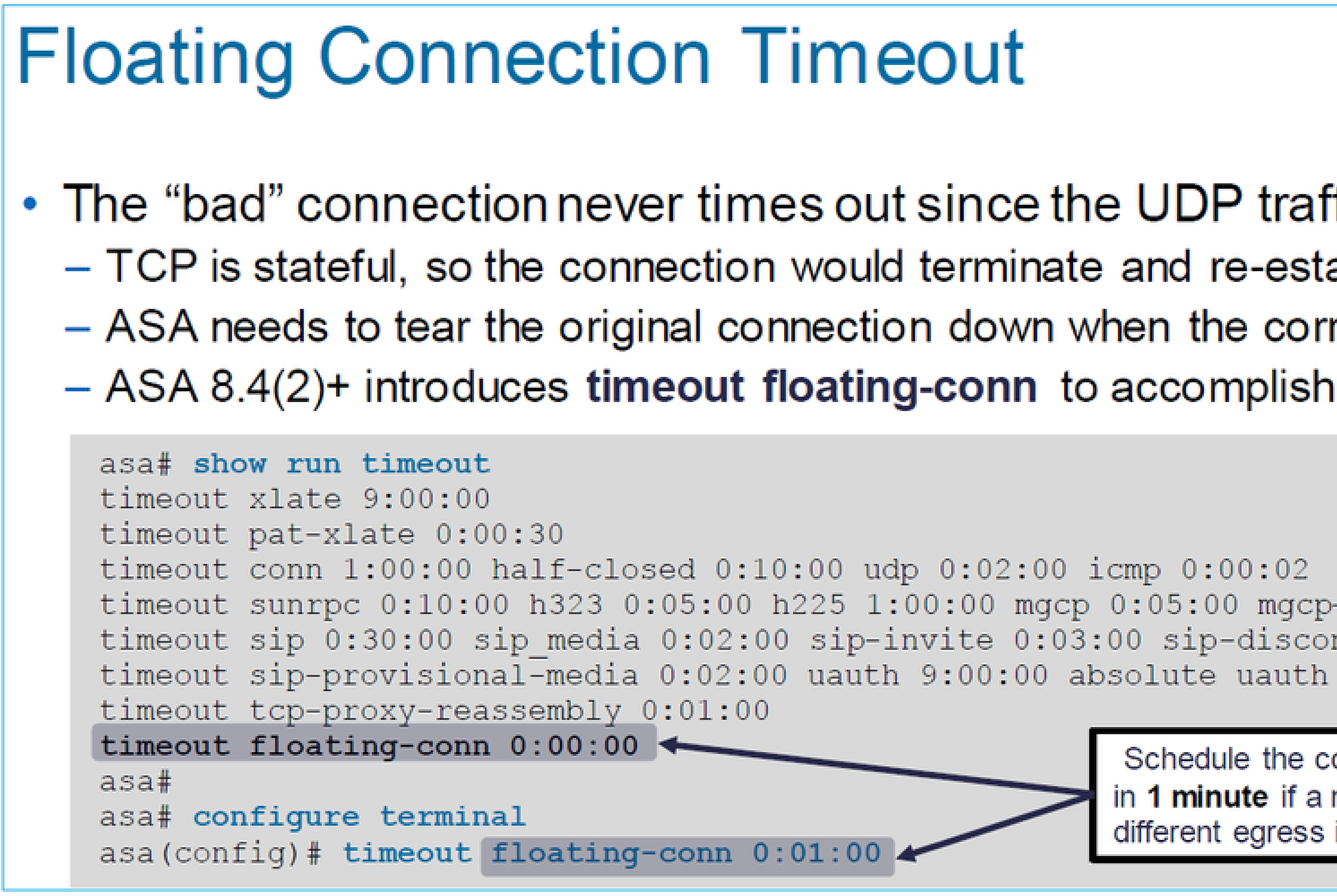
Console Timeout*	0	(0 - 1440 mins)	
Translation Slot(xlate)	Default	3:00:00	(3:0:0 or 0:1:0 - 1193:0:0)
Connection(Conn)	Default	1:00:00	(0:0:0 or 0:5:0 - 1193:0:0)
Half-Closed	Default	0:10:00	(0:0:0 or 0:0:30 - 1193:0:0)
UDP	Default	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
ICMP	Default	0:00:02	(0:0:2 or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

Na Referência 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 obter mais detalhes, consulte Estudo de caso: Conexões UDP falham após recarregamento na sessão 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

Tempo limite de retenção de conn

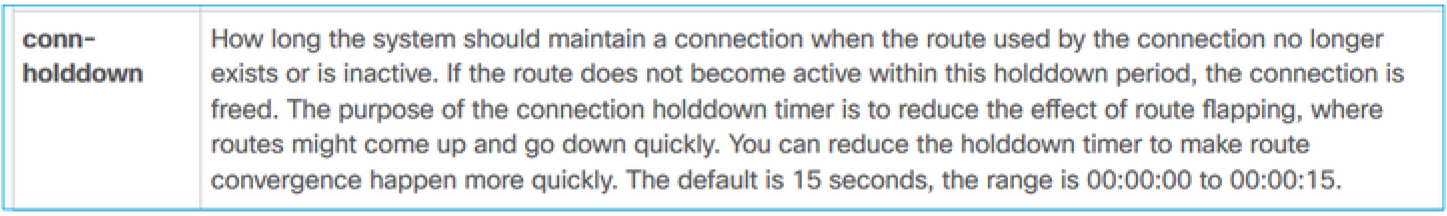
O problema

Uma rota fica inativa (é removida), mas o tráfego corresponde a uma conexão estabelecida.

A solução

O recurso de tempo limite de retenção foi adicionado ao ASA 9.6.2. O recurso está habilitado por padrão, mas atualmente (7.1.x) não é suportado pela interface do FMC ou FlexConfig. Aprimoramento relacionado: [ENH: timeout conn-holddown not available for configuration in FMC]()

No guia da CLI do 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
```

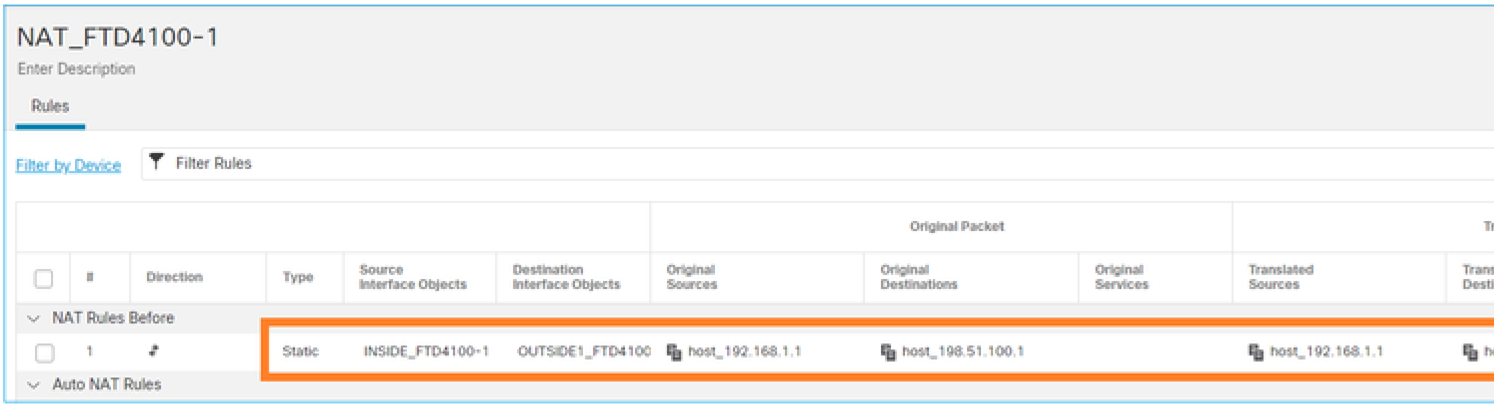
Caso 2 - Encaminhamento com base na pesquisa de NAT

Requisitos

Configure esta regra de NAT:

- Tipo: estático
- Interface de origem: INSIDE
- Interface de destino: OUTSIDE1
- Fonte original: 192.168.1.1
- Destino original: 198.51.100.1
- Fonte traduzida: 192.168.1.1
- Destino traduzido: 198.51.100.1

Solução



NAT_FTD4100-1

Enter Description

						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										

A regra NAT implantada na CLI do 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
```

Configure 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 uma sessão telnet de 192.168.1.1 a 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
```

Os pacotes chegam no FTD, mas nada deixa as interfaces OUTSIDE1 nem 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
```

Rastreie o pacote TCP SYN. A Fase 3 (UN-NAT) mostra que o NAT (UN-NAT especificamente) desviou o pacote para a interface OUTSIDE1 para consulta do próximo 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
```

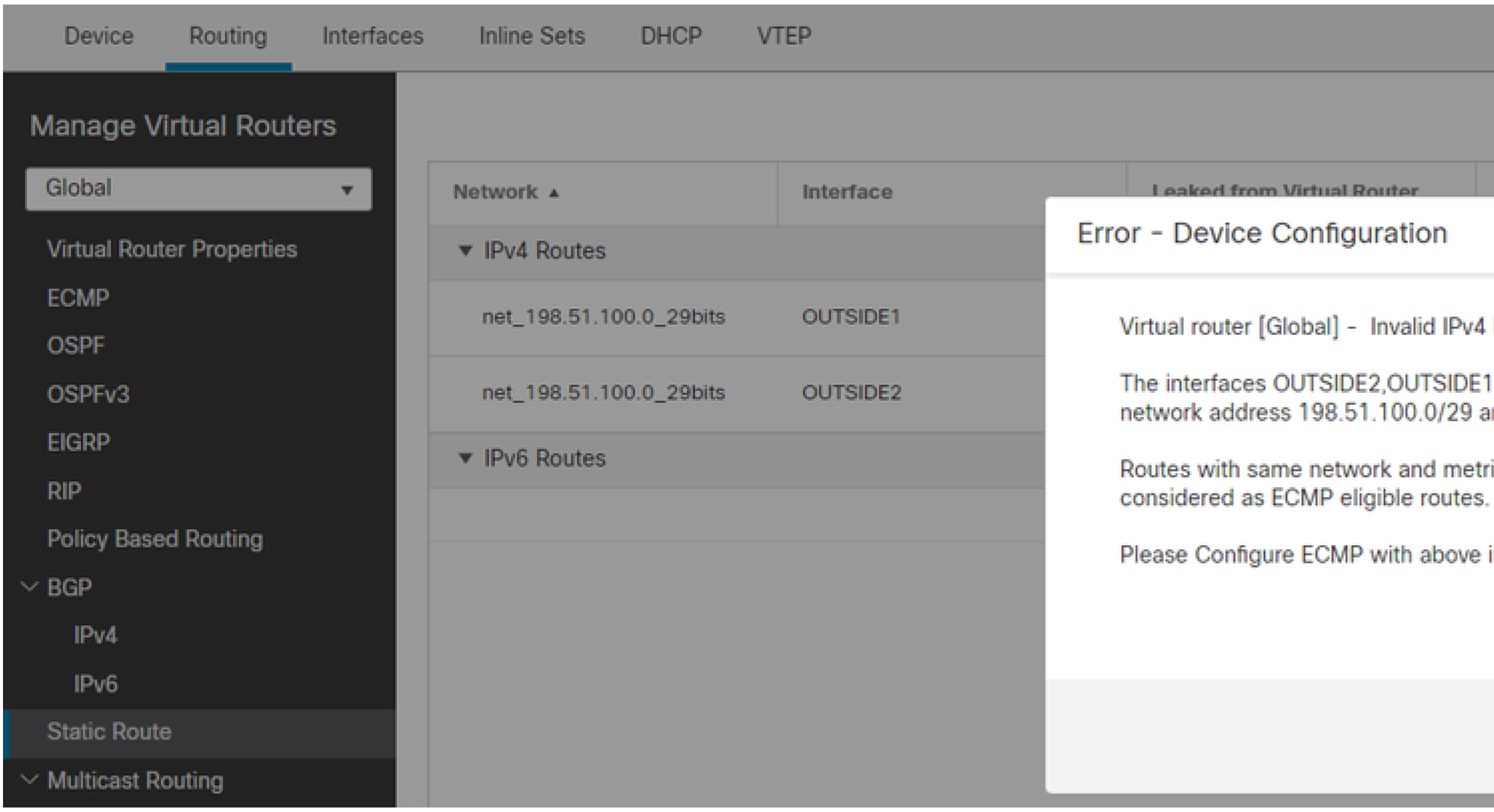
Neste caso, SUBOPTIMAL-LOOKUP significa que a interface de saída determinada pelo processo NAT (OUTSIDE1) é diferente da interface de saída especificada na tabela de entrada do ASP:

```
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
```

Uma solução possível é adicionar uma rota estática flutuante na interface 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
```

> Observação: se você tentar adicionar uma rota estática com a mesma métrica da que já existe, este erro será exibido:



Network ▲	Interface	Leaked from Virtual Router
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

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

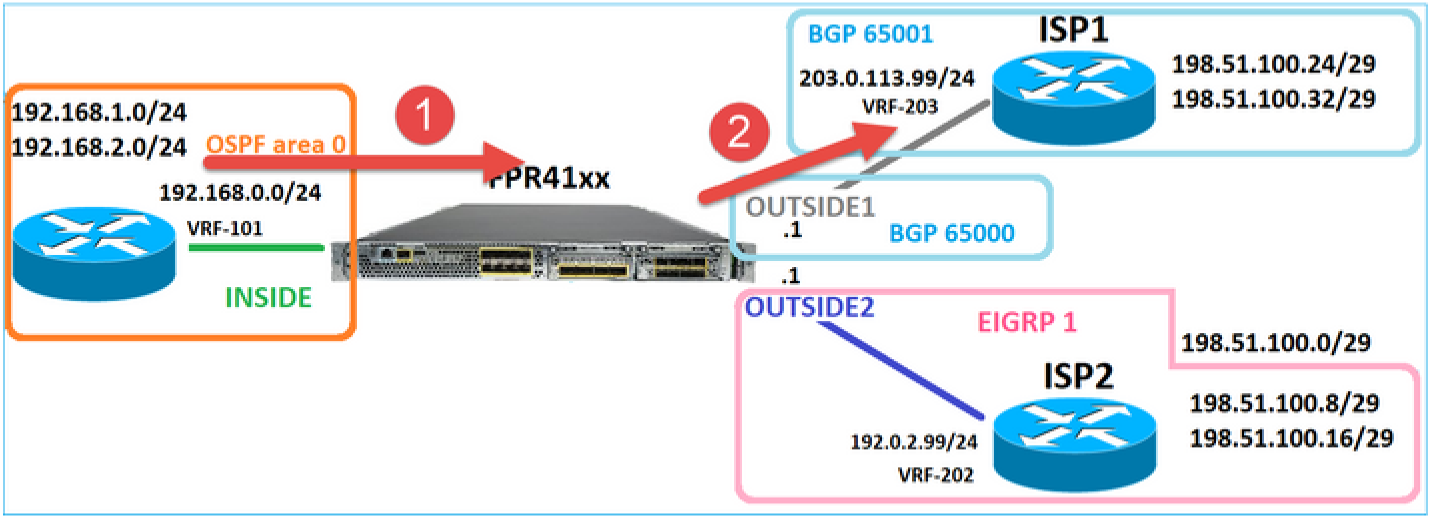
> Observação: a rota flutuante com uma métrica de distância de 255 não está instalada na tabela de roteamento.

Tente executar telnet para confirmar que há pacotes enviados através do 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
```

O rastreamento de pacotes mostra que os pacotes são encaminhados para a interface ISP1 (OUTSIDE1) em vez de ISP2 devido à pesquisa 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#
```

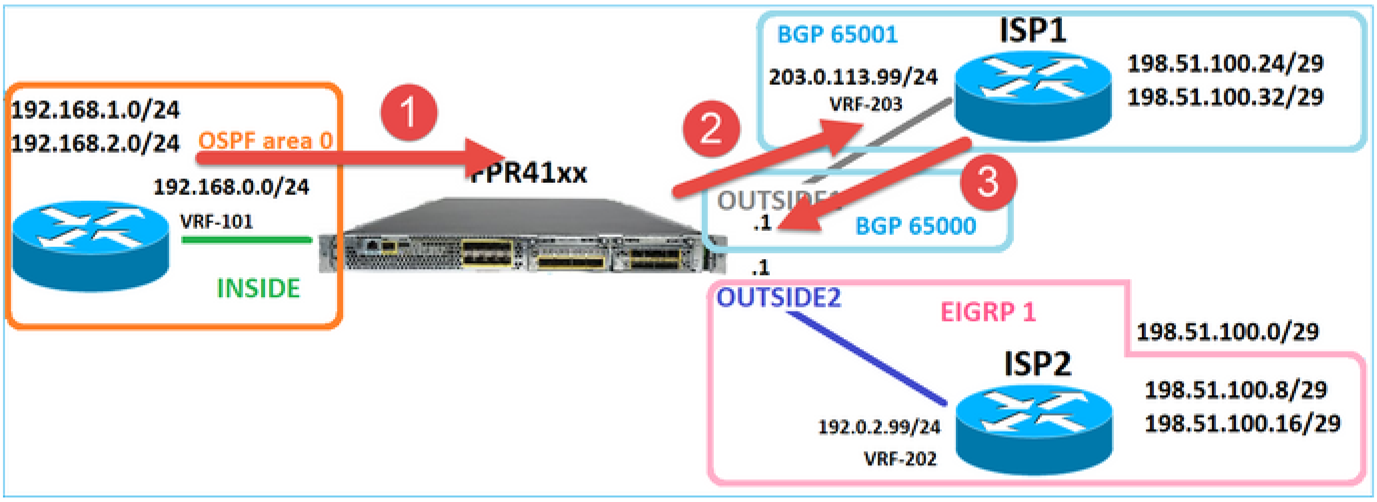
Curiosamente, neste caso, há pacotes mostrados no INSIDE e em ambas as interfaces de saída:

```
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
```

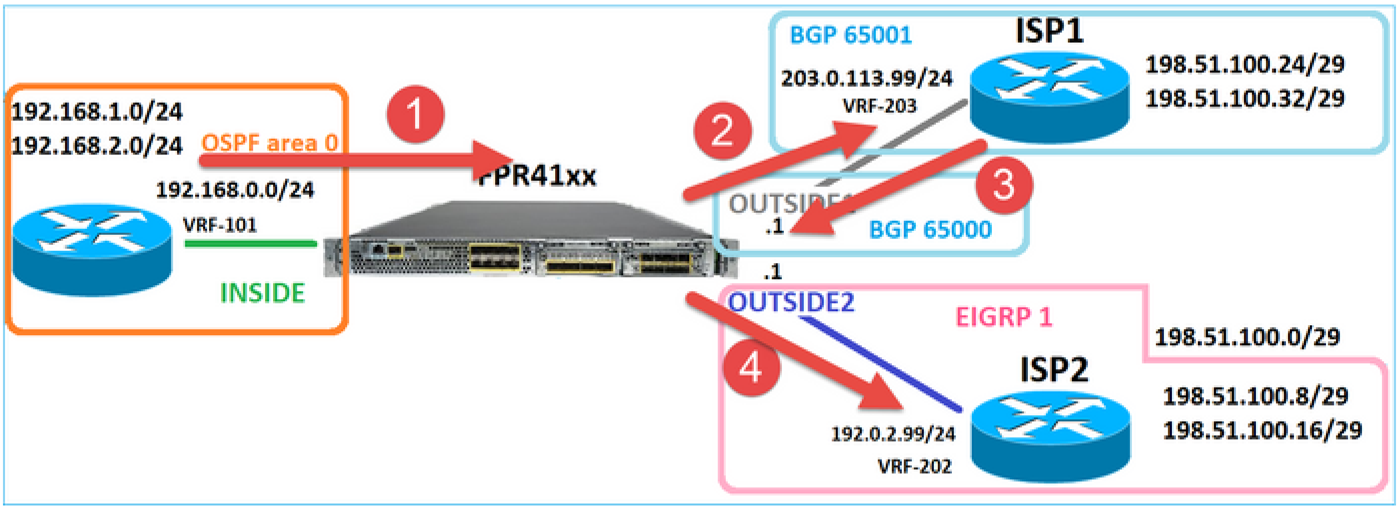
Os detalhes do pacote incluem as informações de endereço MAC e um rastreamento dos pacotes nas interfaces OUTSIDE1 e OUTSIDE2 revela o caminho dos pacotes:

```
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
```



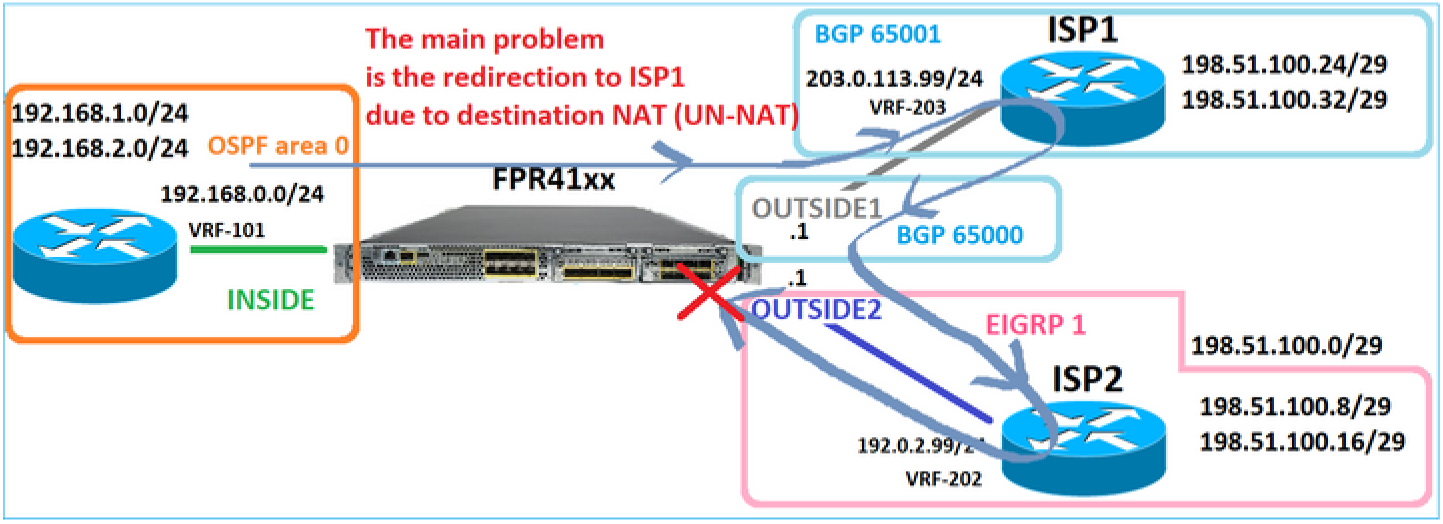
O rastreamento do pacote que retorna mostra o redirecionamento para a interface OUTSIDE2 devido à Pesquisa da tabela de Roteamento Global:



```
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#
```

O roteador ISP2 envia a resposta (SYN/ACK), mas esse pacote é redirecionado para ISP1 porque corresponde à conexão estabelecida. O pacote é descartado pelo FTD devido a nenhuma adjacência L2 na tabela de saída ASP:



```
firepower# show capture CAP02 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 - Encaminhamento baseado em Roteamento Baseado em Política (PBR)

Após a consulta do fluxo de conexão e a consulta do NAT de destino, o PBR é o próximo item que pode influenciar a determinação da interface de saída. O PBR está documentado em: Roteamento baseado em política

Para a configuração do PBR no FMC, é importante estar ciente desta diretriz:
O FlexConfig foi usado para configurar o PBR no FMC para versões do FTD anteriores à 7.1. Você ainda pode usar o FlexConfig para configurar o PBR em todas as versões. No entanto, para uma interface de entrada, não é possível configurar o PBR usando tanto a página FlexConfig quanto o Roteamento baseado em políticas do FMC.

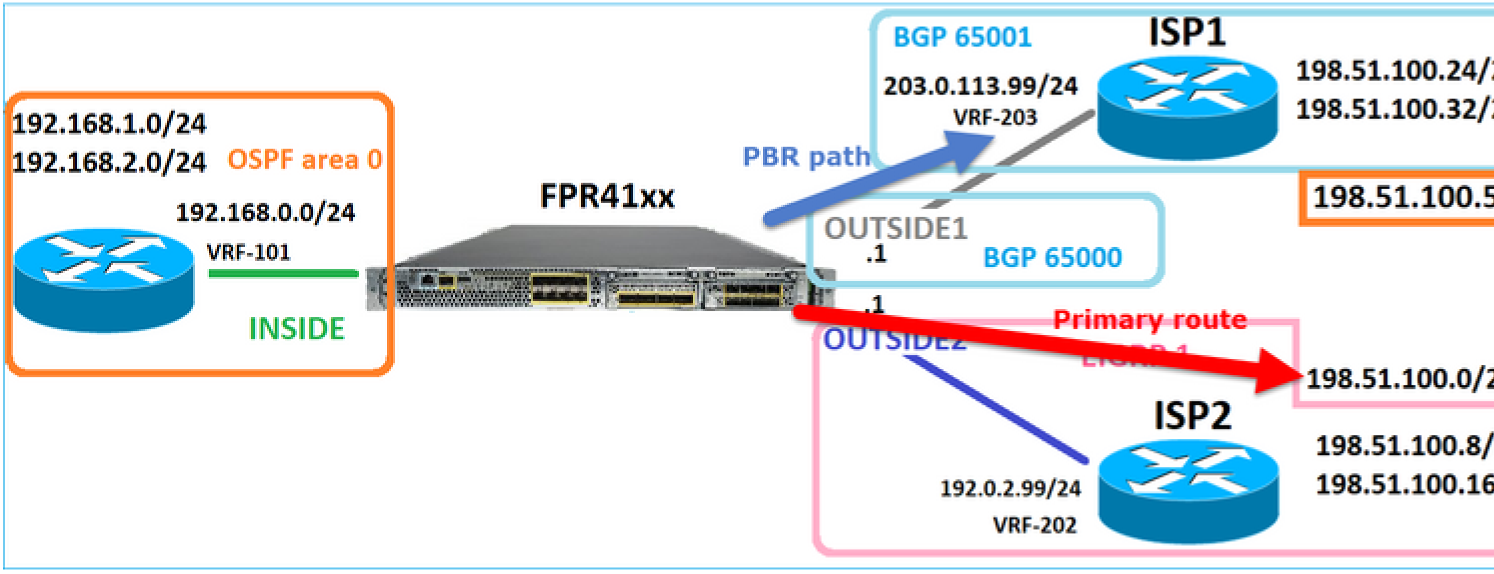
Neste estudo de caso, o FTD tem uma rota para 198.51.100.0/24 que aponta para o ISP2:

```
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
```

Requisitos

Configure uma política de PBR com estas características:

- O tráfego do IP 192.168.2.0/24 destinado a 198.51.100.5 deve ser enviado ao ISP1 (próximo salto 203.0.113.99) enquanto outras origens devem usar a interface EXTERNA2.



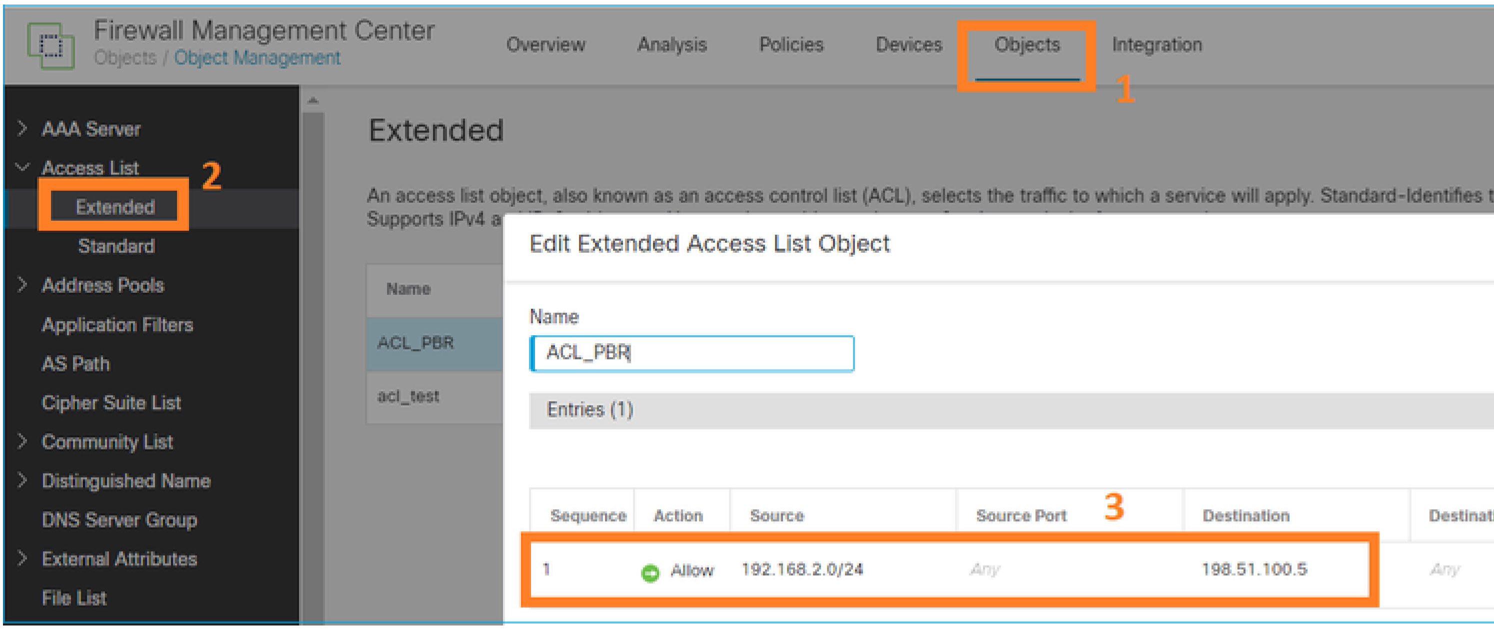
Solução

Em versões anteriores à 7.1, para configurar o PBR:
1. Crie uma ACL estendida que corresponda ao tráfego interessante (por exemplo, PBR_ACL).
2. Crie um mapa de rota que corresponda à ACL criada na Etapa 1 e defina o próximo salto desejado.
3. Crie um Objeto FlexConfig que ative o PBR na interface de entrada usando o mapa de rotas criado na Etapa 2.

Em versões posteriores à 7.1, você pode configurar o PBR usando a forma anterior à 7.1 ou pode usar a nova opção Roteamento baseado em política na seção Dispositivo > Roteamento:
1. Crie uma ACL estendida que corresponda ao tráfego interessante (por exemplo, PBR_ACL).
2. Adicione uma política de PBR e especifique:
a. O tráfego correspondente
b. A interface de entrada
c. O salto seguinte

Configurar o PBR (nova maneira)

Etapa 1 - Definir uma lista de acesso para o tráfego correspondente.



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

Edit Extended Access List Object

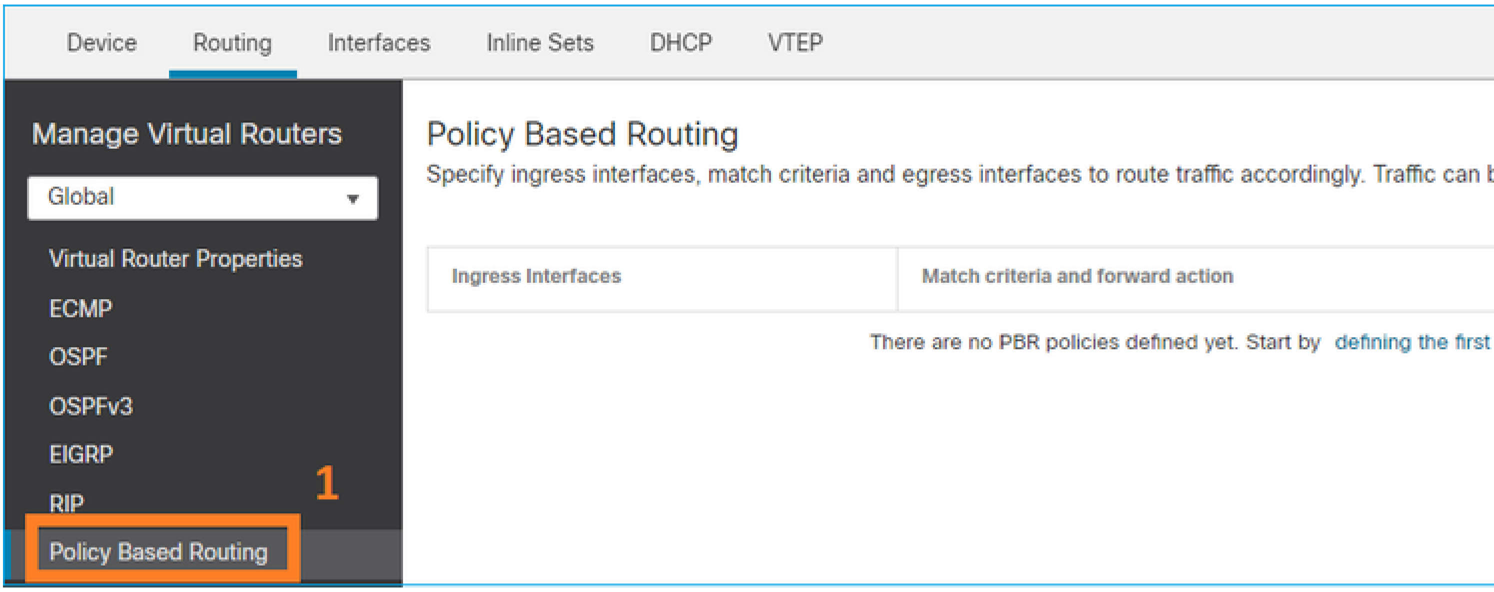
Name
ACL_PBR

Entries (1)

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

Etapa 2 - Adicionar uma política de PBR

Navegue até Devices > Device Management e edite o dispositivo FTD. Escolha Roteamento > Roteamento Baseado em Política e, na página Roteamento Baseado em Política, selecione Adicionar.

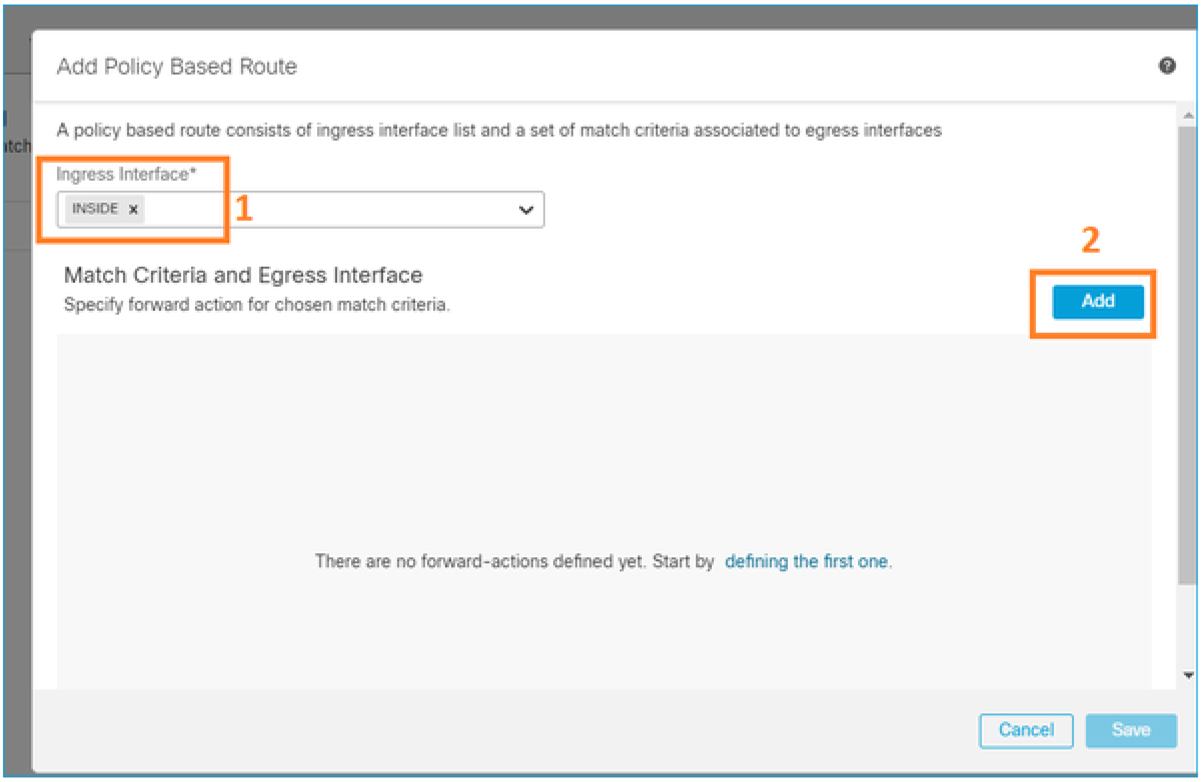


Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can b

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

Especifique a interface de entrada:



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

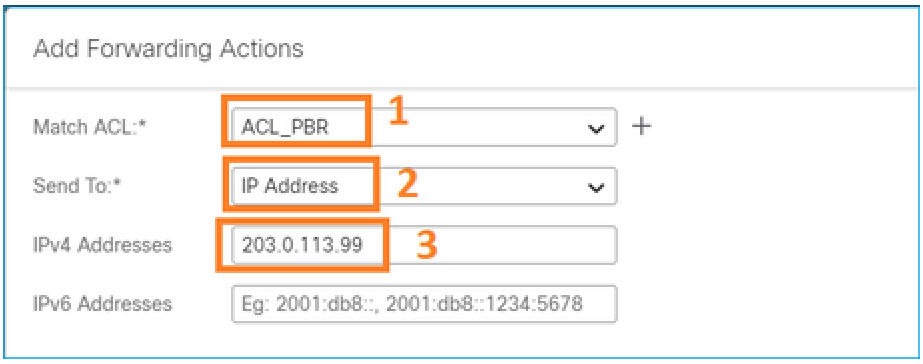
Ingress Interface*: INSIDE

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.

Especifique as ações de encaminhamento:



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

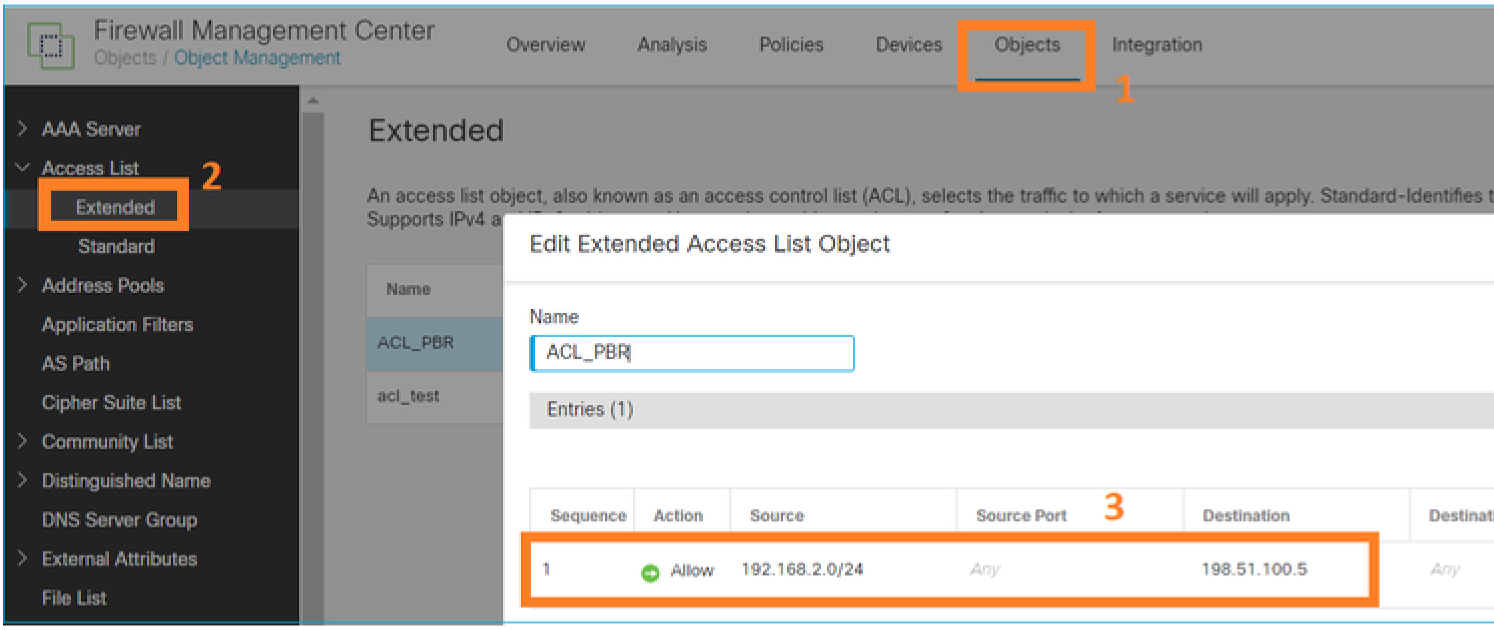
Salvar e implantar

> Observação: para configurar várias interfaces de saída, você deve definir a opção 'Interfaces de saída' no campo 'Enviar para' (disponível a partir da versão 7.0 e posteriores). Para obter mais detalhes, verifique: Exemplo de configuração para roteamento baseado em política

---

Configurar o PBR (modo herdado)

Etapa 1 - Definir uma lista de acesso para o tráfego correspondente.



Firewall Management Center
Objects / Object Management

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

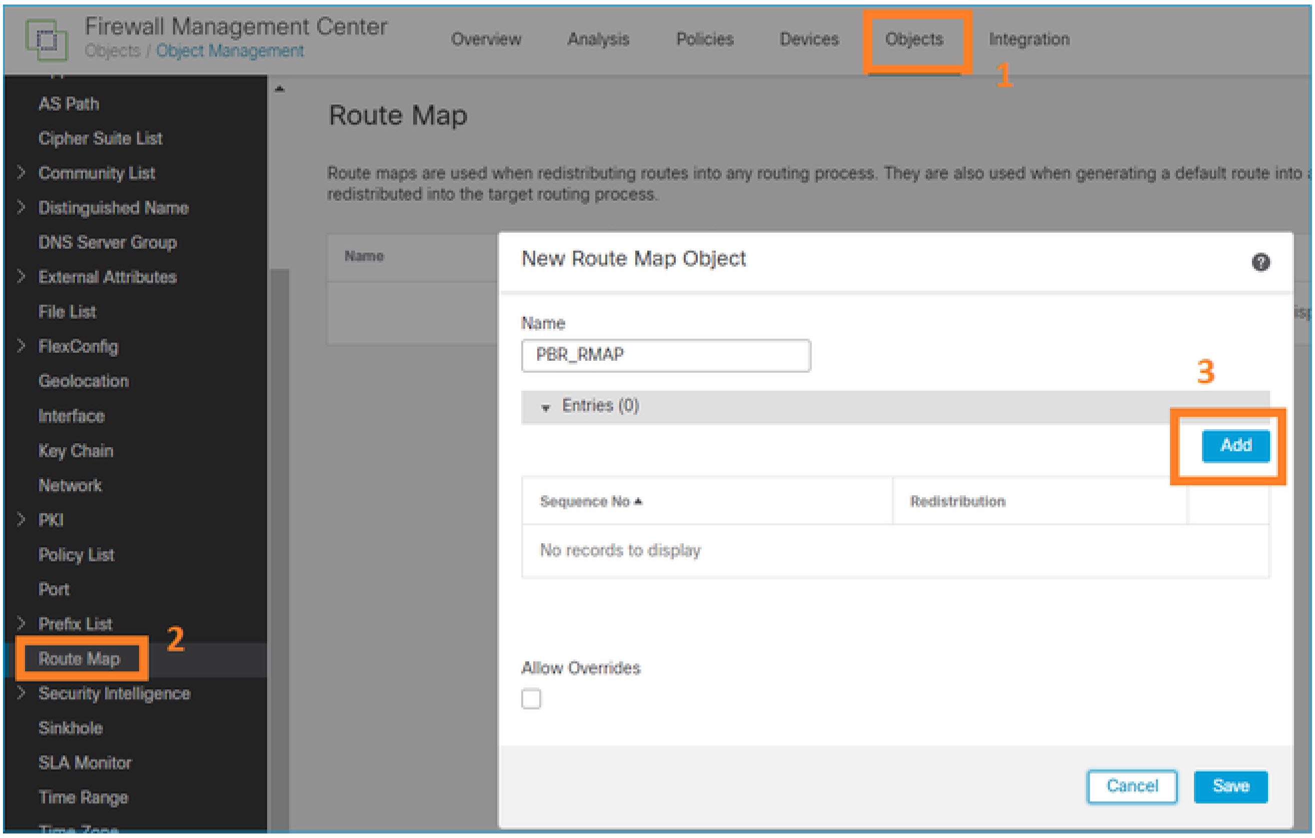
Name ACL_PBR

Entries (1)

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

Etapa 2 - Definir um mapa de rota que corresponda à ACL e defina o próximo salto.

Primeiro, defina a Cláusula Match:



Route Map

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.

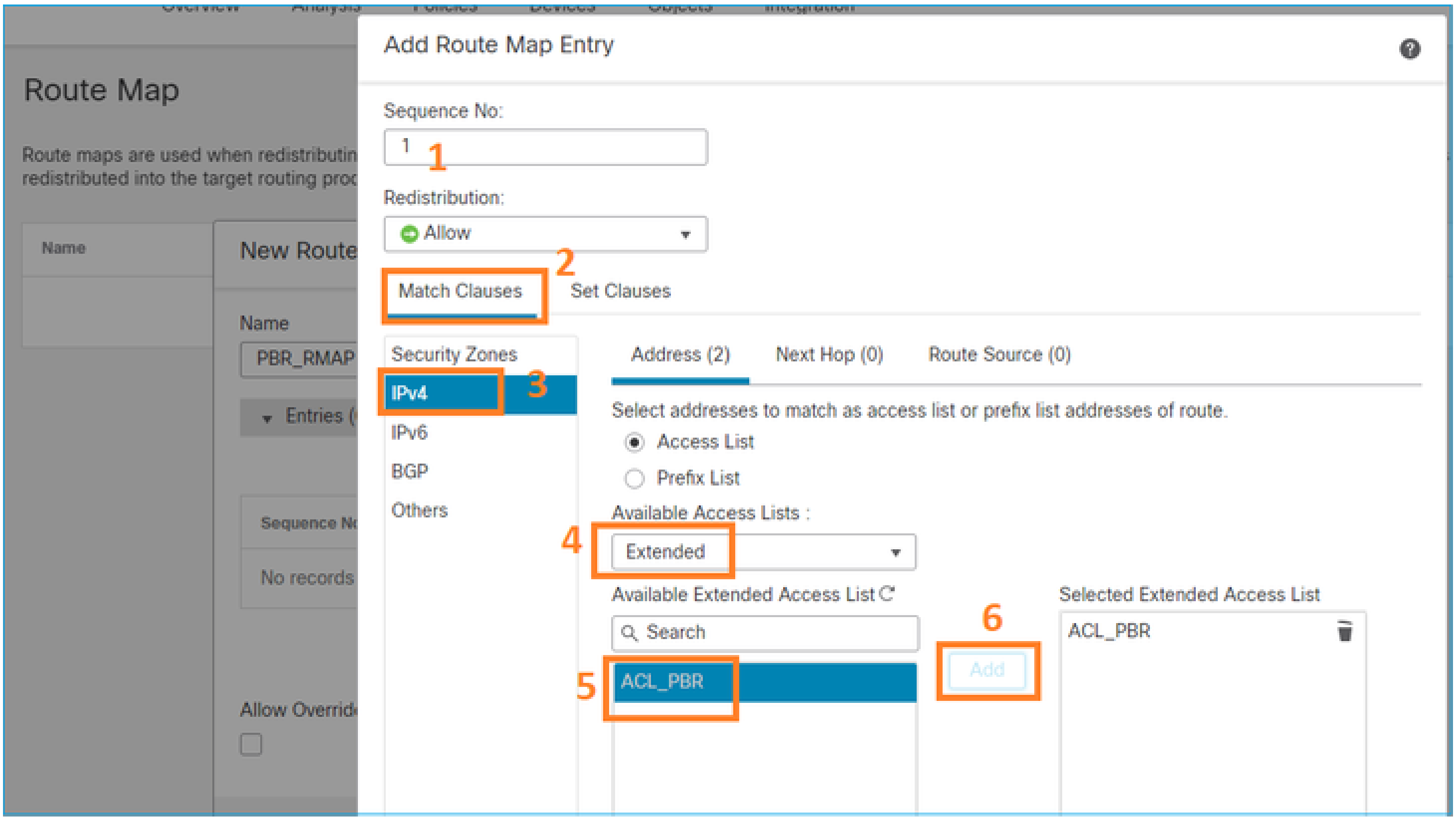
New Route Map Object

Name: PBR_RMAP

Entries (0)

No records to display

Allow Overrides ☐



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

Add Route Map Entry

Sequence No: 1

Redistribution: Allow

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

● Access List

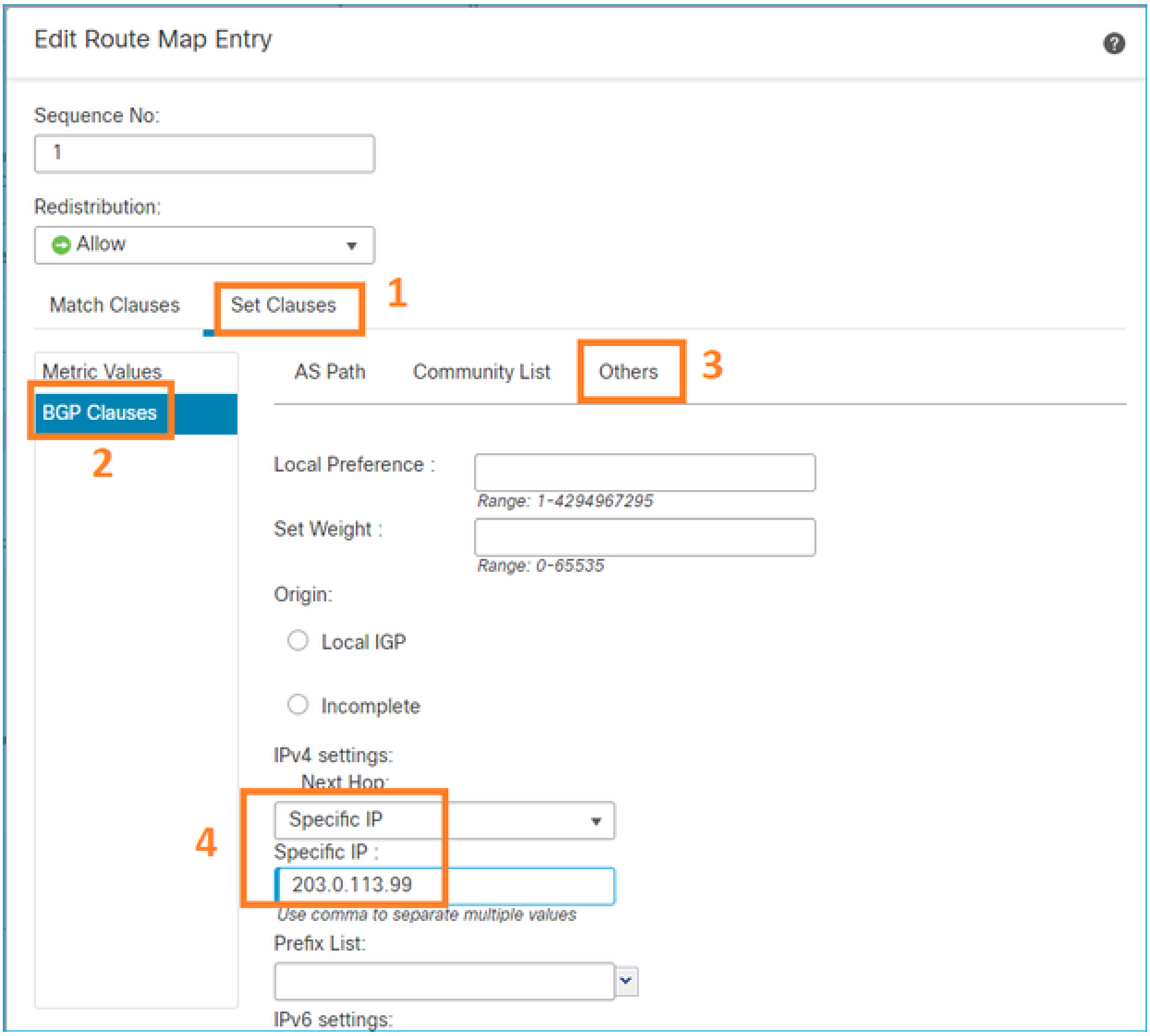
○ Prefix List

Available Access Lists : Extended

Available Extended Access List: ACL_PBR

Selected Extended Access List: ACL_PBR

Defina a Cláusula Set:



Edit Route Map Entry

Sequence No: 1

Redistribution: Allow

Match Clauses | Set Clauses (1)

Metric Values | BGP Clauses (2)

AS Path | Community List | Others (3)

Local Preference :

Range: 1-4294967295

Set Weight :

Range: 0-65535

Origin:

○ Local IGP

○ Incomplete

IPv4 settings:

Next Hop: Specific IP (4)

Specific IP : 203.0.113.99

Use comma to separate multiple values

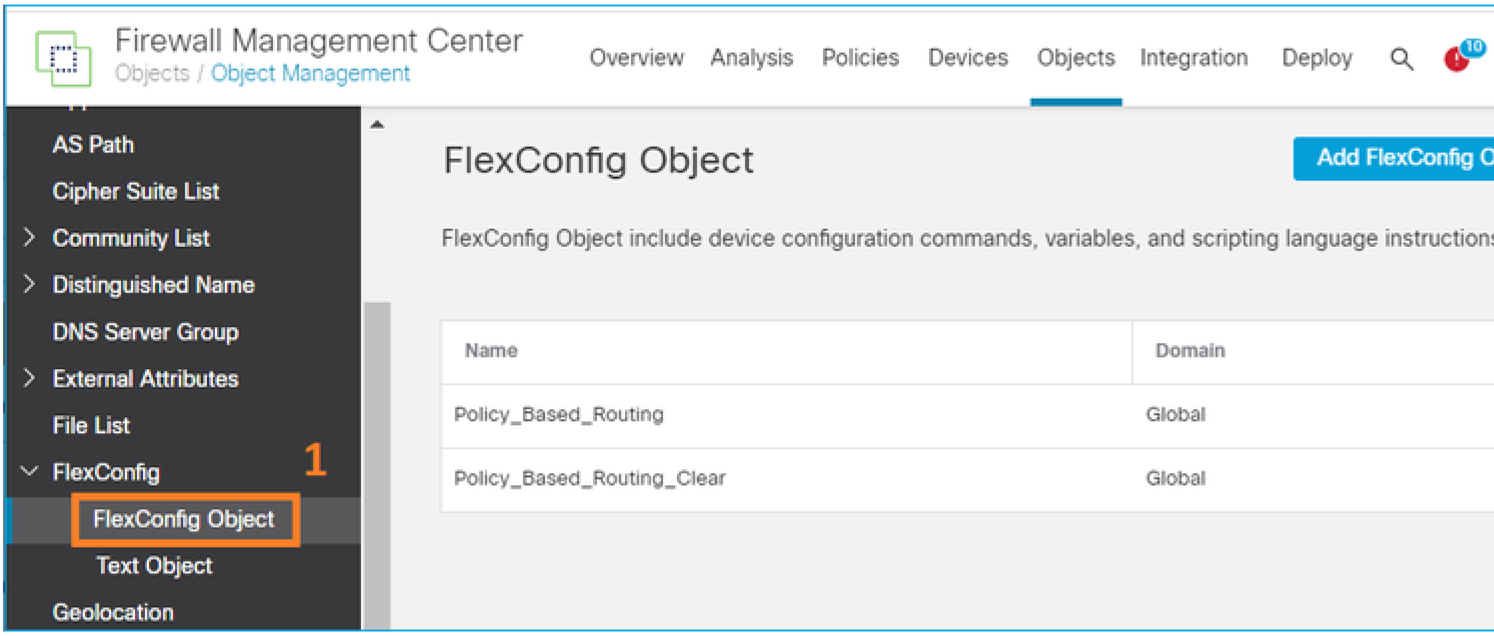
Prefix List:

IPv6 settings:

Adicionar e salvar.

Etapa 3 - Configurar o objeto PBR FlexConfig.

Primeiro, copie (duplique) o objeto PBR existente:



Firewall Management Center

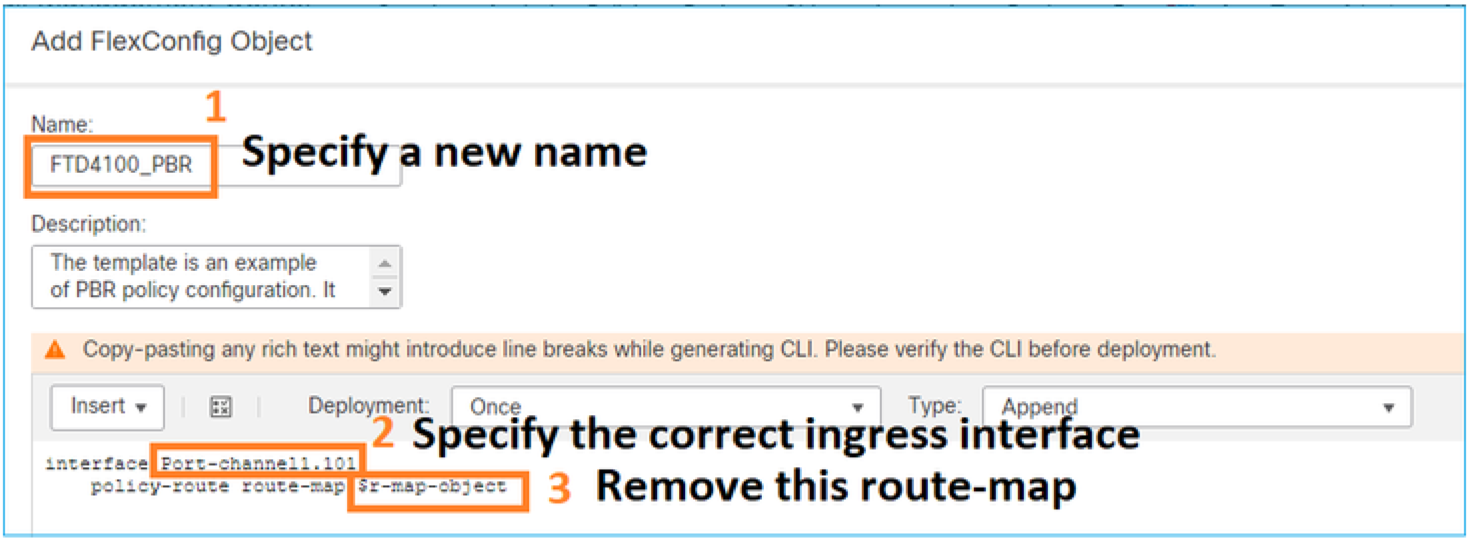
Objects / Object Management

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 o Nome do objeto e remova o objeto de mapa de rota predefinido:



Add FlexConfig Object

1 Specify a new name

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

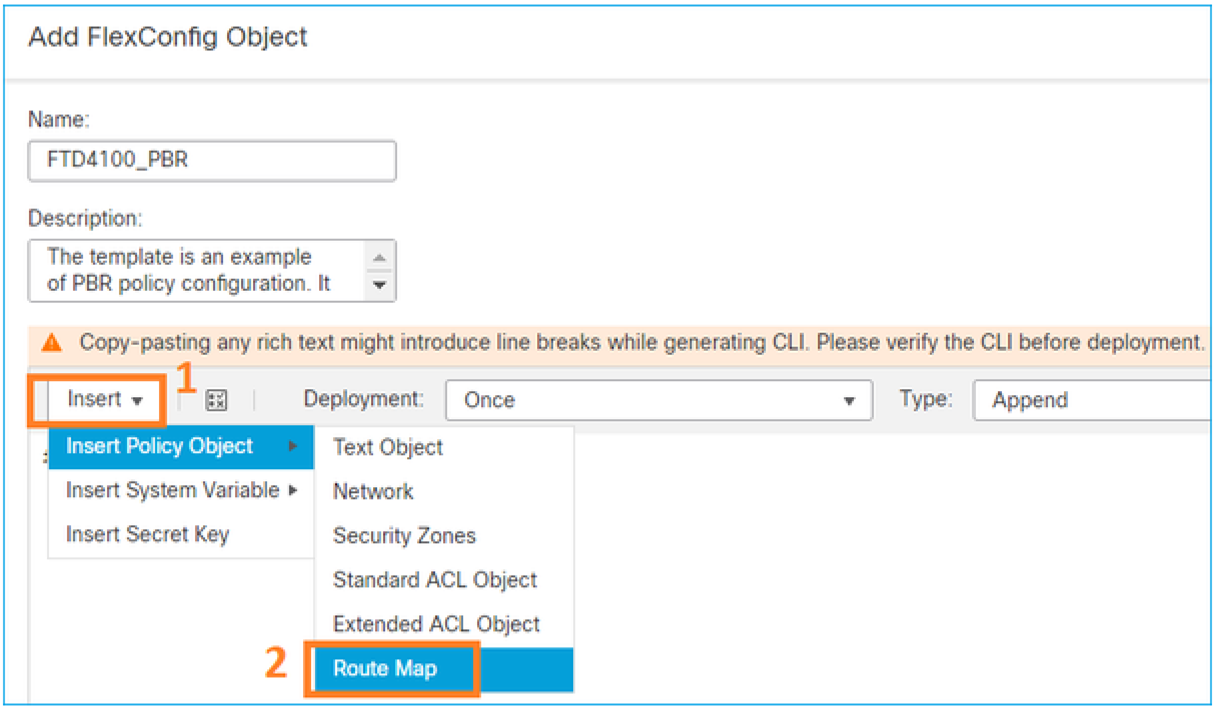
Type: Append

2 Specify the correct ingress interface

3 Remove this route-map

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

Especifique o novo mapa de rota:



Add FlexConfig Object

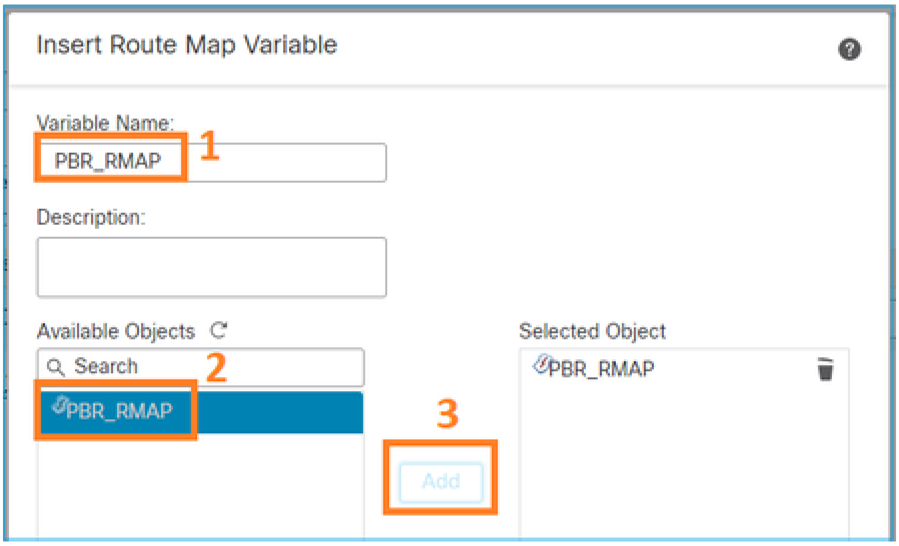
Name: FTD4100_PBR

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

1

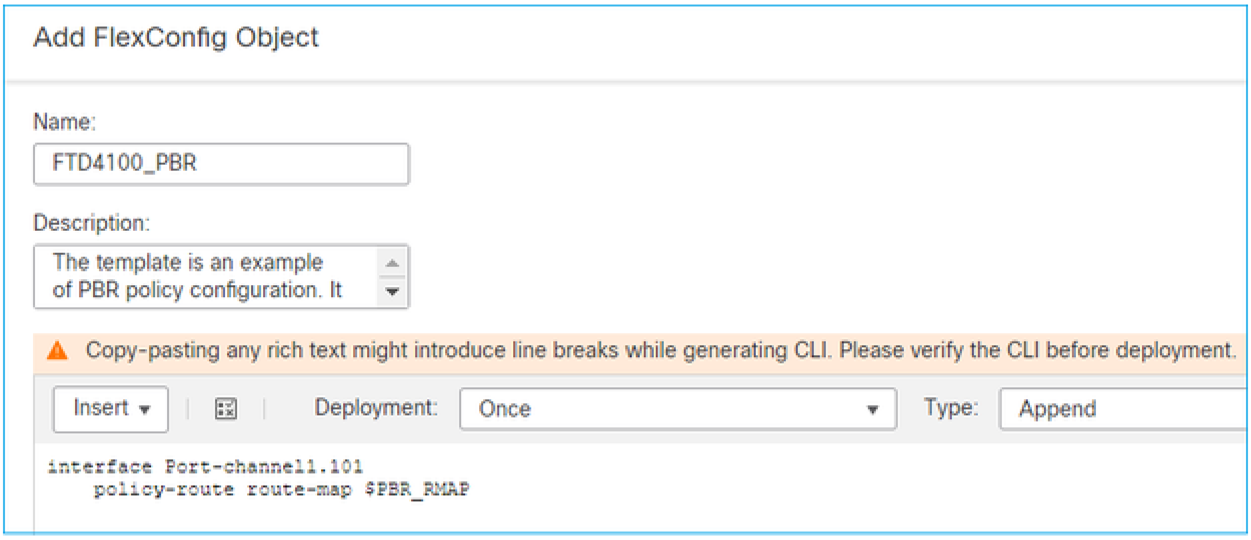
Variable Name: PBR_RMAP

Description:

Available Objects

Selected Object: PBR_RMAP

Este é o resultado final:



Add FlexConfig Object

Name: FTD4100_PBR

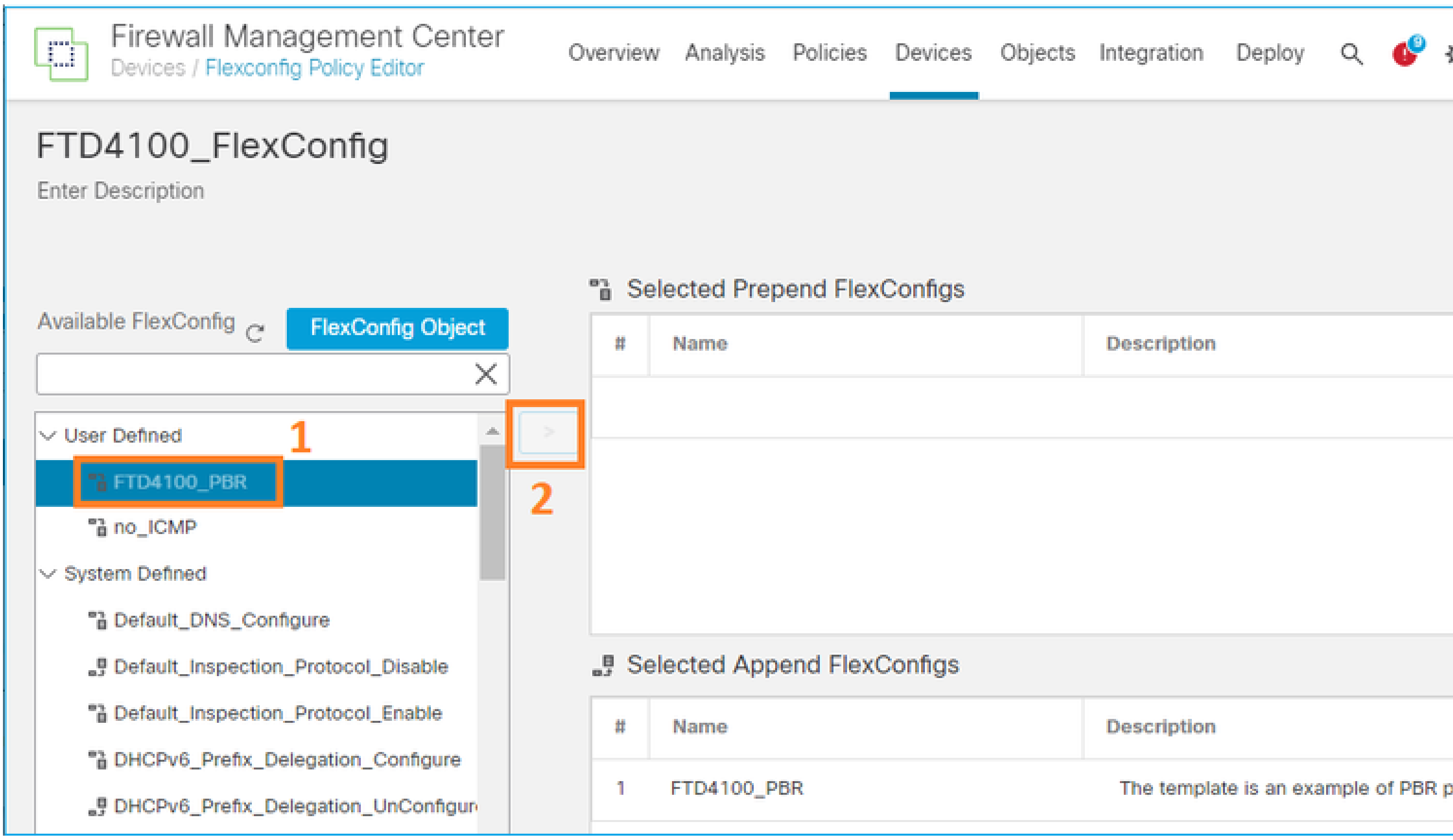
Description: The template is an example of PBR policy configuration. It

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

Insert ▾ | Deployment: Once ▾ | Type: Append

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

Etapa 4 - Adicionar o objeto PBR à política FlexConfig de FTD.



Firewall Management Center
Devices / Flexconfig Policy Editor
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
FTD4100_FlexConfig
Enter Description
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
>

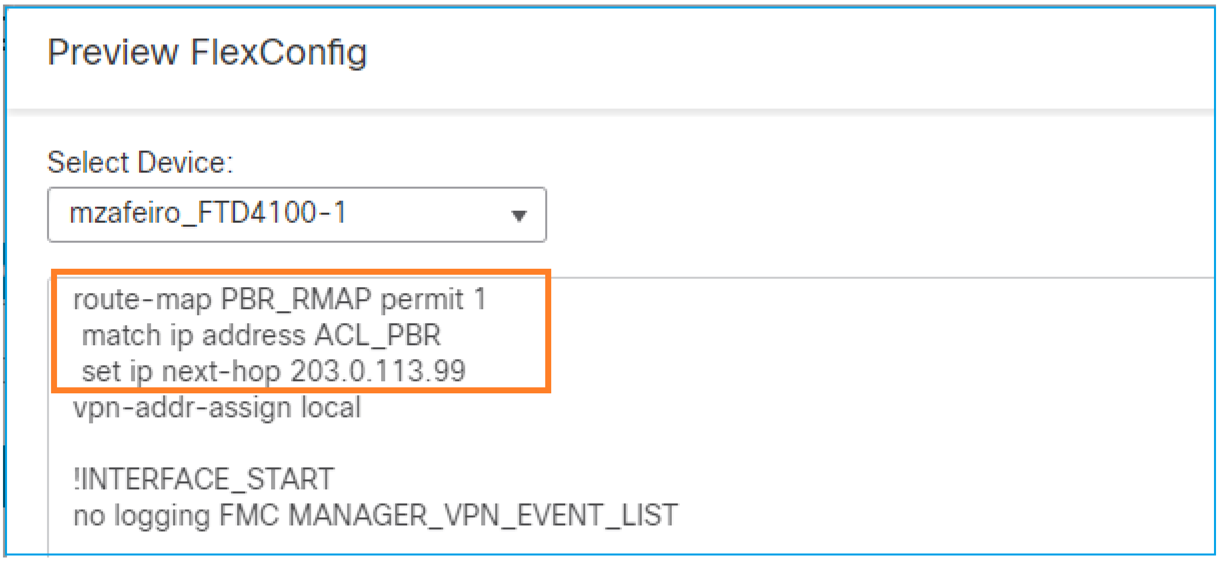
Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

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

Salve e selecione Visualizar configuração:

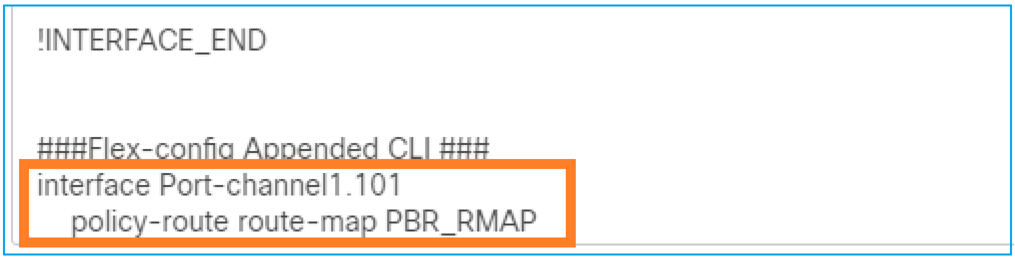


Preview FlexConfig

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
```

Finalmente, Implante a política.

> Observação: o PBR não pode ser configurado usando FlexConfig e FMC UI para a mesma interface de entrada.

Para a configuração do SLA PBR, consulte este documento: Configurar o PBR com SLAs IP para ISP DUAL no FTD Gerenciado pelo FMC

Verificação de PBR

Verificação da interface de entrada:

```
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
```

Verificação do mapa de rotas:

```
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)
```

Verificação de rota de política:

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

Packet Tracer antes e depois da alteração:

Sem PBR	Com 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
```

Teste com tráfego real

Configurar a captura de pacotes com um rastreamento:

```
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
```

A captura mostra:

```
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
```

Rastreamento do pacote 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
```

A tabela ASP PBR mostra as contagens de ocorrências da 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
```

Observação: o packet-tracer também aumenta o contador de acertos.

Depuração PBR

Aviso: em um ambiente de produção, a depuração pode produzir muitas mensagens.

Habilitar esta depuração:

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

Enviar tráfego real:

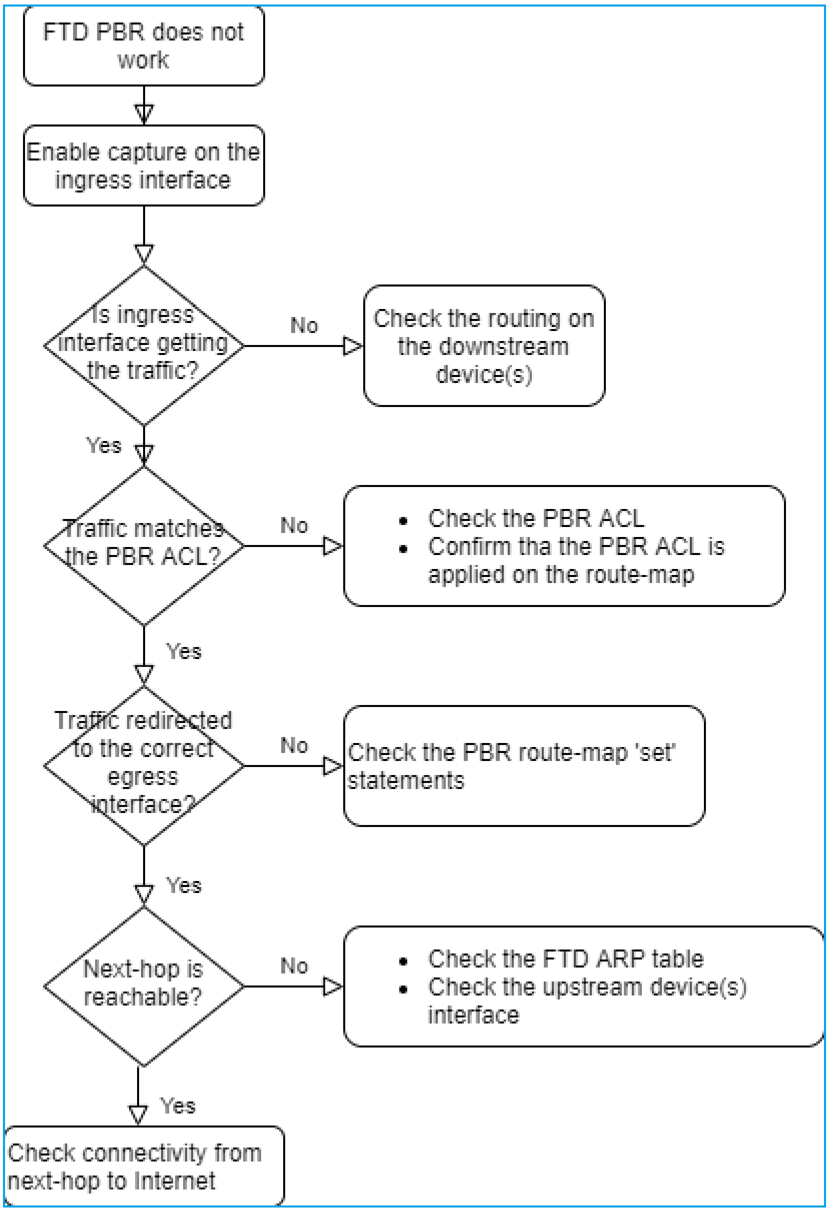
```
Router1# telnet 198.51.100.5 /vrf VRF-101 /source-interface lo2
Trying 198.51.100.5 ... Open
```

A depuração mostra:

```
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
```

> Observação: o Packet Tracer também gera uma saída de depuração.

Este fluxograma pode ser usado para solucionar problemas do 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

Resumo dos comandos PBR

Para verificar a configuração:

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

Caso o Monitor do SLA também seja usado com o PBR:

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

Para verificar a operação:

```
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
```

Caso o Monitor do SLA também seja usado com o PBR:

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

Para depurar o PBR:

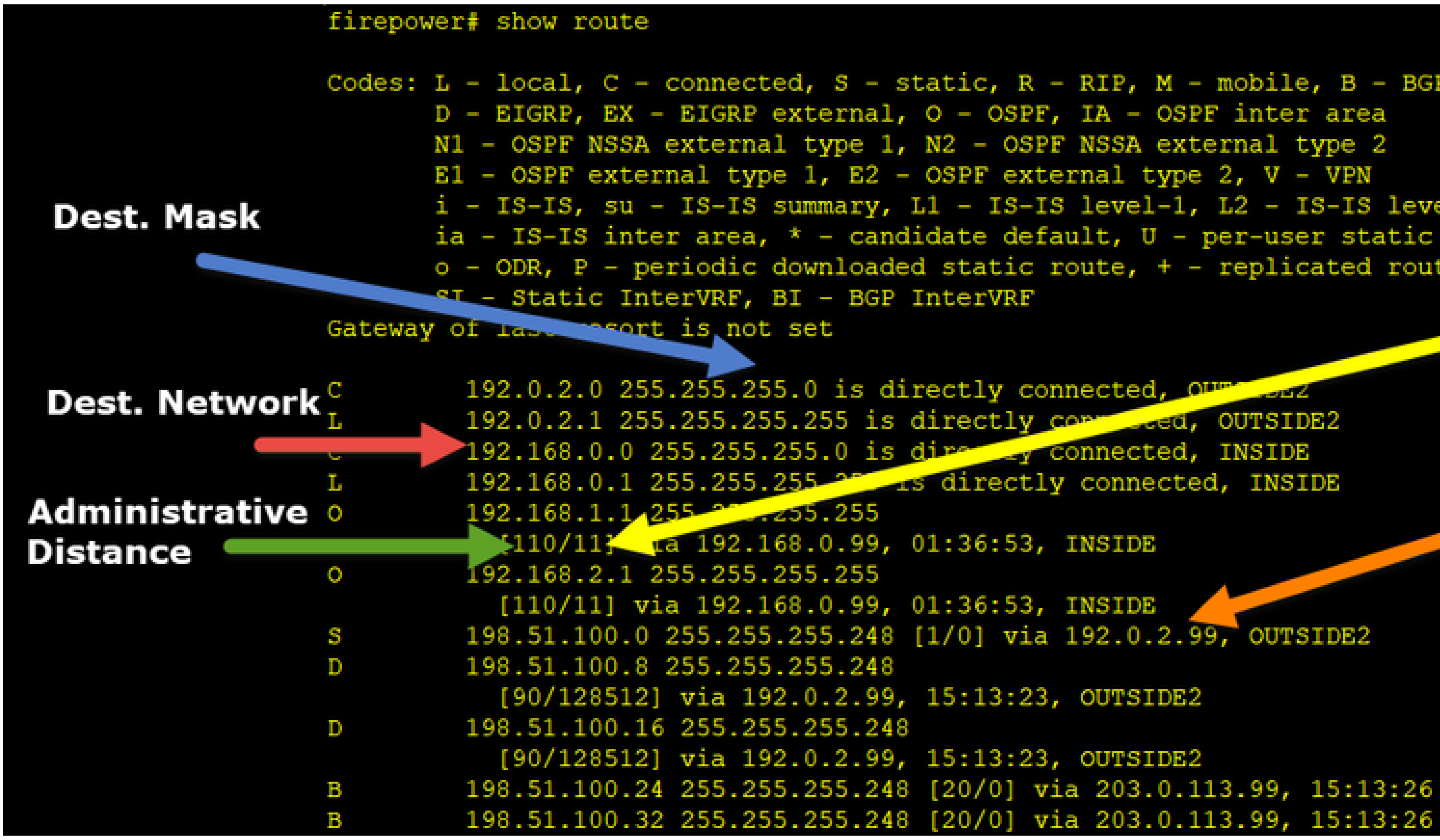
```
debug policy-route
show asp drop
```

Caso 4 - Encaminhamento com base na pesquisa de roteamento global

Após a pesquisa de conexão, a pesquisa de NAT e o PBR, o último item verificado para determinar a interface de saída é a tabela de roteamento global.

Verificação da Tabela de Roteamento

Vamos examinar a saída de uma tabela de roteamento FTD:



```
firepower# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGI
       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
```

O principal objetivo do processo de roteamento é encontrar o próximo salto. A seleção da rota está nesta ordem:

1. Maior número de vitórias
2. AD mais baixa (entre diferentes origens de protocolo de roteamento)
3. Métrica Mais Baixa (caso as rotas sejam aprendidas da mesma origem - protocolo de roteamento)

Como a tabela de roteamento é preenchida:

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

- BGP (B)

- BGP InterVRF (BI)

- Estático (S)

- InterVRF (SI) estático

- Conectado (C)

- IPs locais (L)

- VPN (V)

-Redistribuição

-Padrão

Para exibir o resumo da tabela de roteamento, use 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
```

Você pode rastrear as atualizações da tabela de roteamento com este comando:

<#root>

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

Por exemplo, isso é o que a depuração mostra quando a rota OSPF 192.168.1.0/24 é removida da tabela de roteamento 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
```

Quando é adicionado de volta:

<#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
```

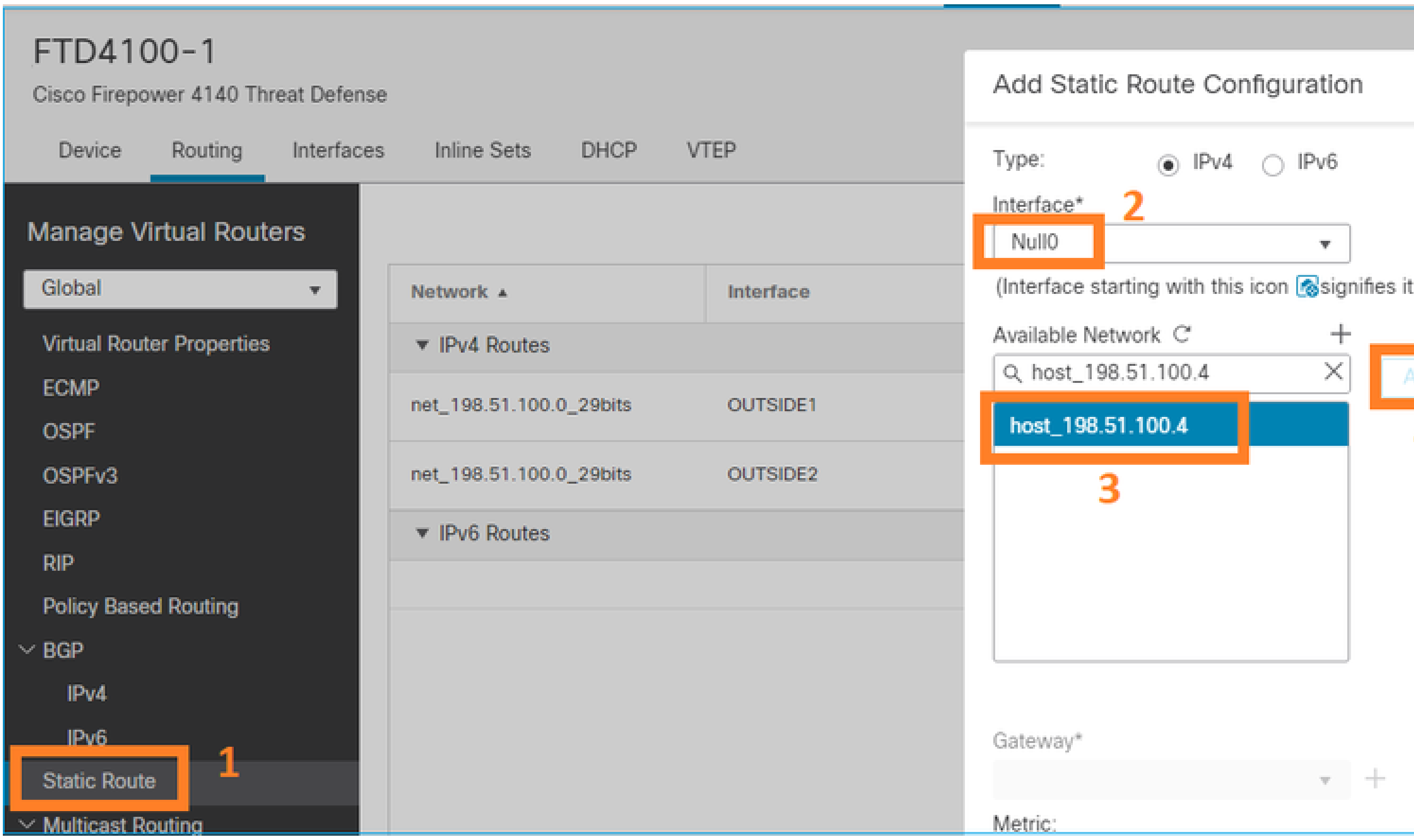
Interface Null0

A interface Null0 pode ser usada para descartar tráfego indesejado. Essa queda tem menos impacto no desempenho do que a queda no tráfego com uma regra de ACL (Access Control Policy, política de controle de acesso).

Requisitos

Configure uma rota Null0 para o host 198.51.100.4/32.

Solução



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

Type: ● IPv4 ○ IPv6

Interface* Null0

(Interface starting with this icon signifies it

Available Network

host_198.51.100.4

host_198.51.100.4

Salvar e implantar.

Verificação:

<#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
```

Tente acessar o 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)
```

Os registros de FTD mostram:

<#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
```

As quedas de ASP mostram:

<#root>

```
firepower#

show asp drop


Frame drop:
```

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

Multicaminho de Custo Igual (ECMP)

Zonas de tráfego

- A zona de tráfego ECMP permite que um usuário agrupe interfaces (chamada de zona ECMP).
- Isso permite o roteamento ECMP, bem como o balanceamento de carga do tráfego em várias interfaces.
- Quando as interfaces são associadas à zona de tráfego ECMP, o usuário pode criar rotas estáticas de custo igual nas interfaces. As rotas estáticas de custo igual são rotas para a mesma rede destino com o mesmo valor de métrica.

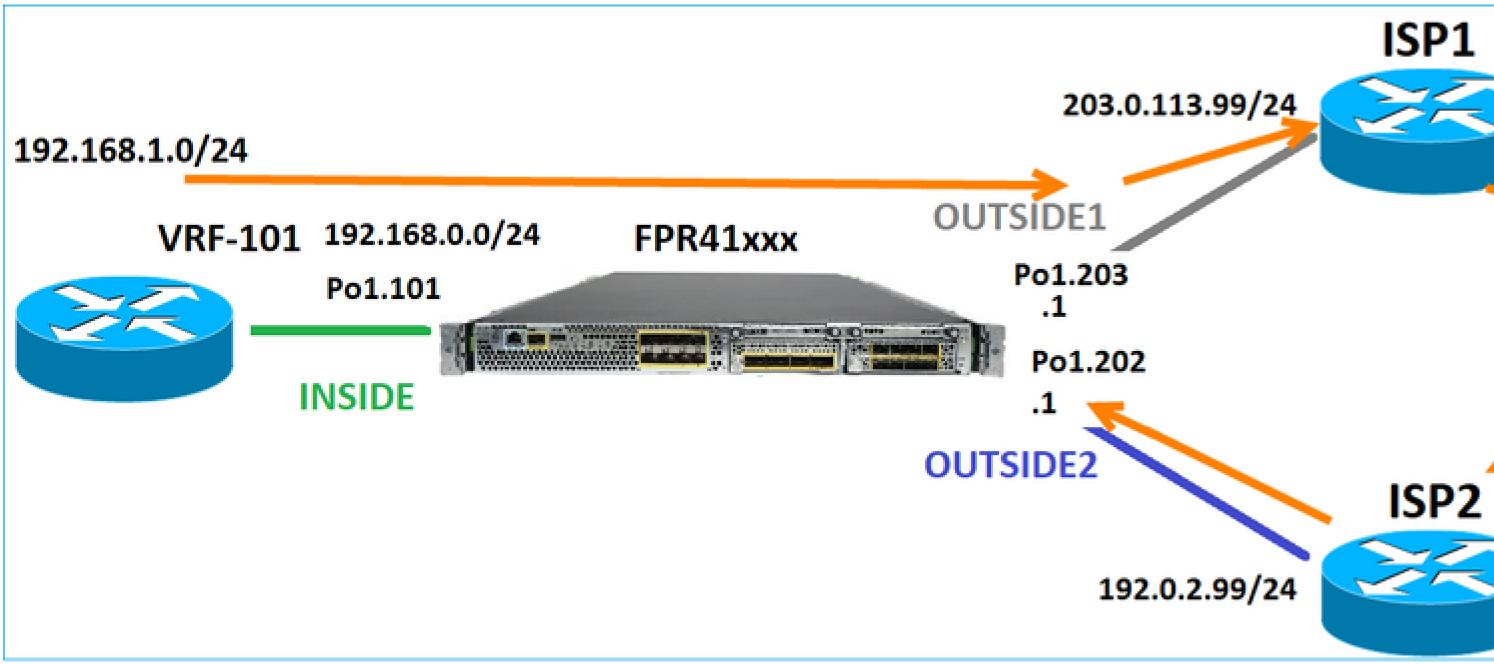
Antes da versão 7.1, o Firepower Threat Defense oferecia suporte ao roteamento ECMP por meio de políticas FlexConfig. A partir da versão 7.1, você pode agrupar interfaces em zonas de tráfego e configurar o roteamento ECMP no Firepower Management Center.

O EMCP está documentado em: ECMP

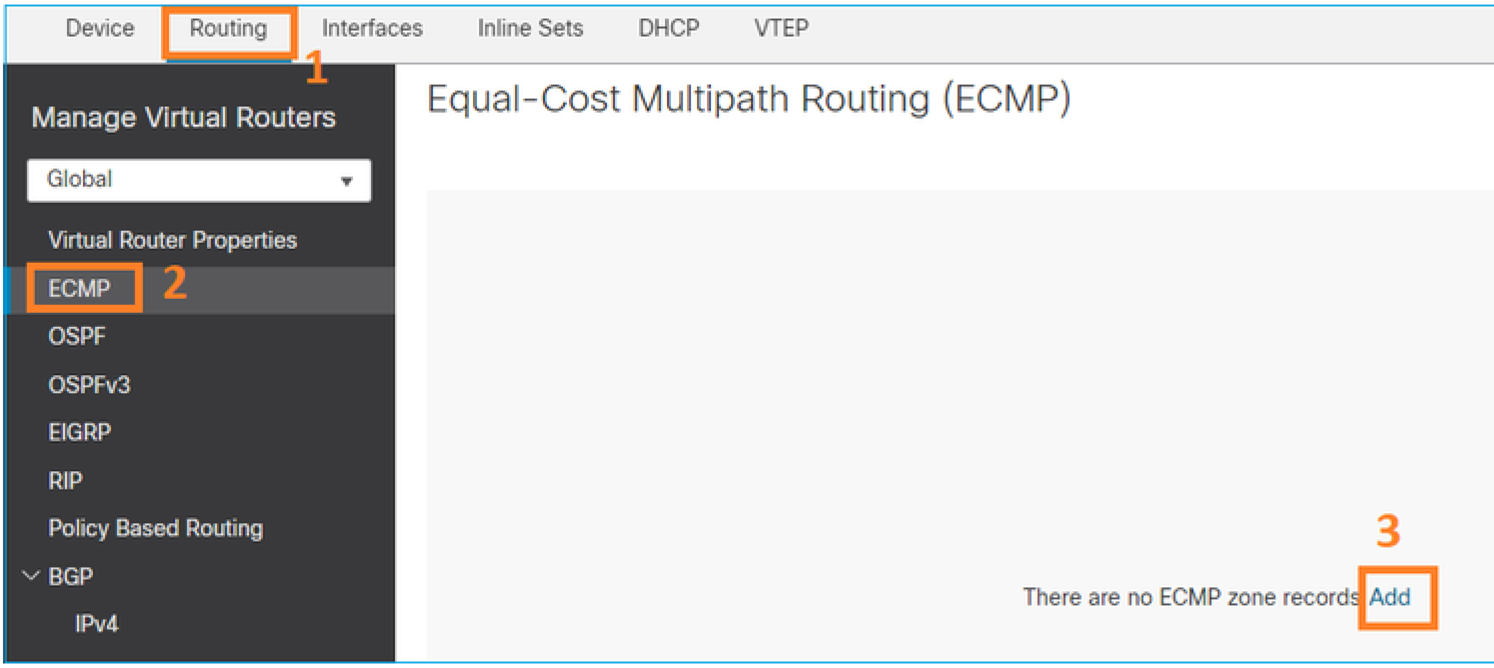
Neste exemplo, há roteamento assimétrico e o tráfego de retorno é descartado:

<#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
```



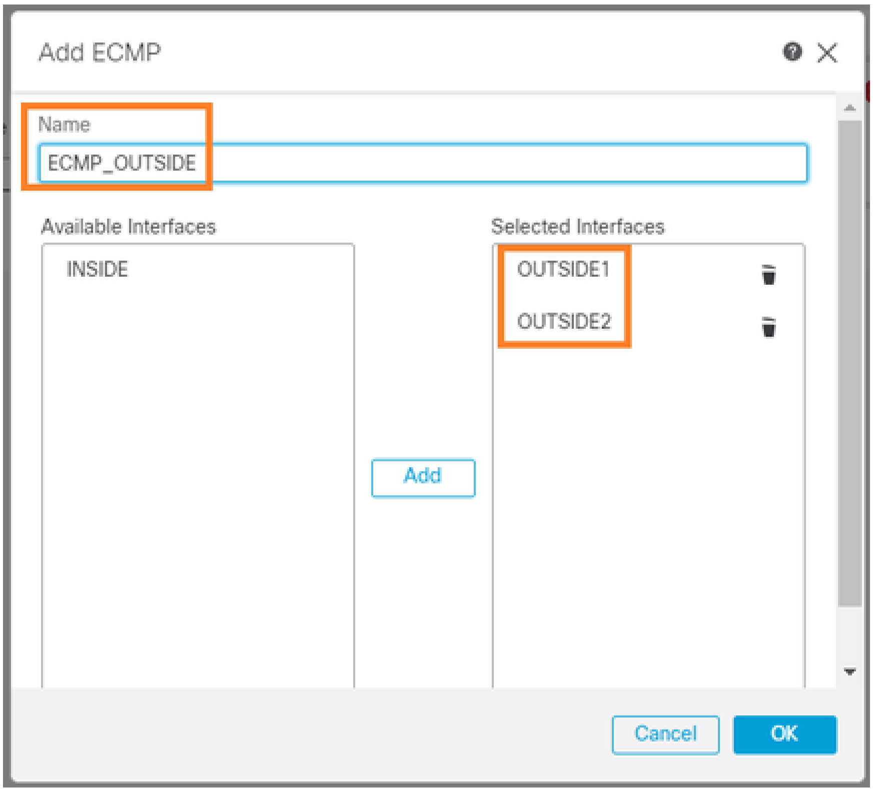
Configure o ECMP na interface do FMC:



Equal-Cost Multipath Routing (ECMP)

There are no ECMP zone records

Adicione as 2 interfaces no grupo ECMP:

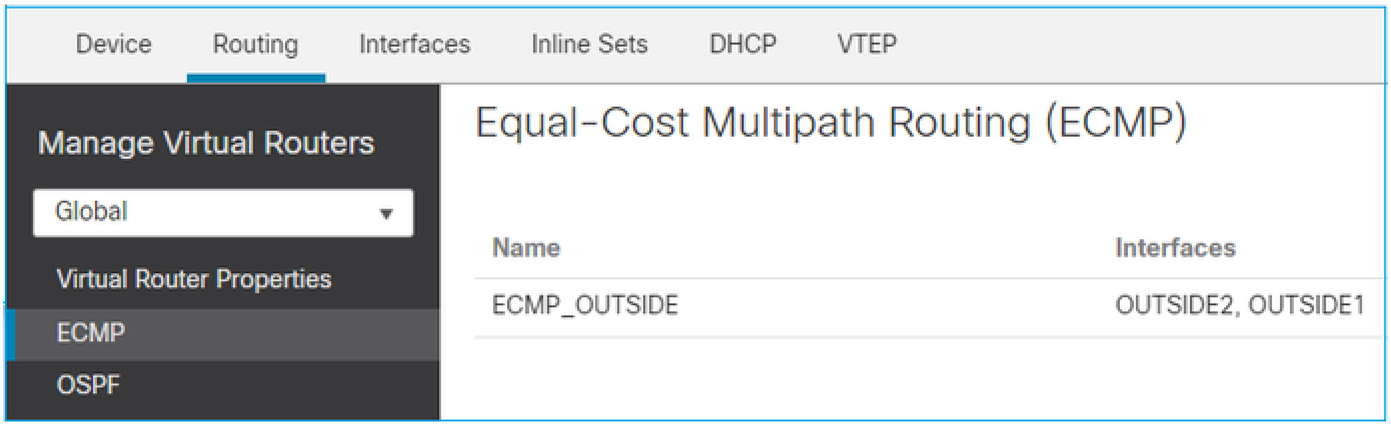


Name: ECMP_OUTSIDE

Available Interfaces: INSIDE

Selected Interfaces: OUTSIDE1, OUTSIDE2

O resultado:



Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP_OUTSIDE	OUTSIDE2, OUTSIDE1

Salvar e implantar.

Verificação 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
```

Verificação de interface:

<#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
```

Agora, o tráfego de retorno é permitido e a conexão é UP:

<#root>

```
Router1#
telnet 198.51.100.100 /vrf VRF-101 /source-interface lo1


Trying 198.51.100.100 ... Open
```

A captura na interface ISP1 mostra o tráfego de saída:

<#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
```

A captura na interface ISP2 mostra o tráfego 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 Gerenciamento do FTD

O DTF tem 2 planos de gestão:

- Interface Management0 - fornece acesso ao subsistema Firepower
- Interface de diagnóstico LINA - Fornece acesso ao subsistema LINA do FTD

Para configurar e verificar a interface Management0, use os comandos configure network e show network, respectivamente.

Por outro lado, as interfaces LINA fornecem acesso ao próprio LINA. As entradas de interface FTD no RIB FTD podem ser vistas como rotas locais:

<#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
```

Da mesma forma, eles podem ser vistos como entradas de identidade na tabela de roteamento 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
```

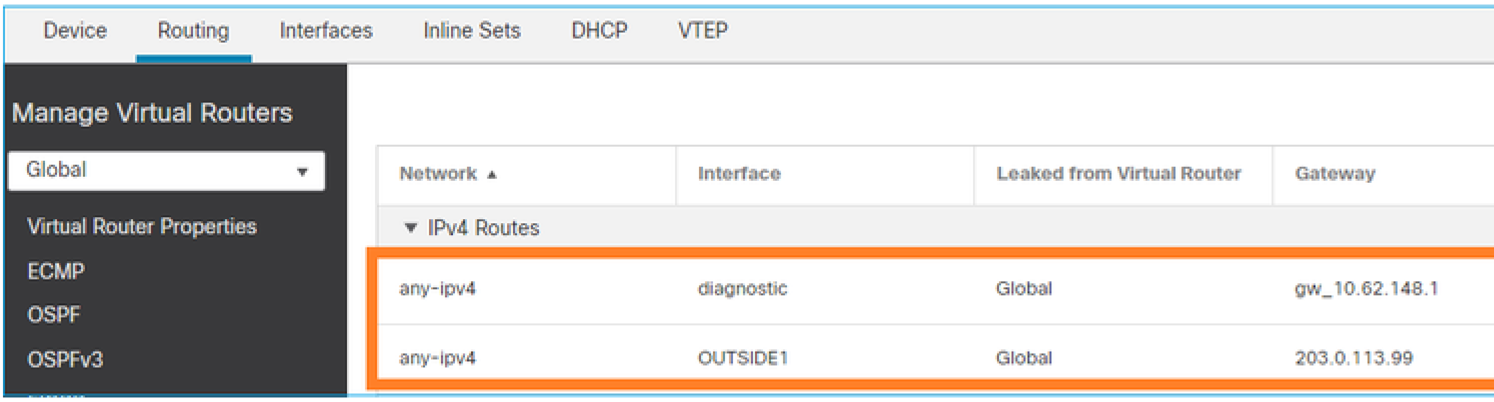
Ponto principal

Quando um pacote chega no FTD e o IP de destino corresponde a um dos IPs de identidade, o FTD sabe que precisa consumir o pacote.

Roteamento de Interface de Diagnóstico LINA FTD

O FTD (como um ASA que executa o código pós-9.5) mantém uma tabela de roteamento semelhante ao VRF para qualquer interface configurada como somente de gerenciamento. Um exemplo dessa interface é a interface de diagnóstico.

Embora o FMC não permita que você (sem ECMP) configure 2 rotas padrão em 2 interfaces diferentes com a mesma métrica, você pode configurar 1 rota padrão em uma interface de dados FTD e outra rota padrão na interface 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

O tráfego do plano de dados usa o gateway padrão da tabela global, enquanto o tráfego do plano de gerenciamento usa o GW padrão 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
```

O gateway da tabela de roteamento 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
```

Quando você envia tráfego do FTD (tráfego pronto para usar), a interface de saída é selecionada com base em:

1. Tabela de roteamento global
2. Tabela de roteamento somente de gerenciamento

Você pode substituir a seleção da interface de saída se especificar manualmente a interface de saída.

Tente fazer ping no gateway da interface de diagnóstico. Se você não especificar a interface de origem, o ping falhará porque o FTD usa primeiro a tabela de roteamento global que, nesse caso, contém uma rota padrão. Se não houver rota na tabela global, o FTD fará uma pesquisa de rota na tabela de roteamento somente de gerenciamento:

<#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
```

O mesmo se aplica se você tentar copiar um arquivo do LINA CLI com o comando copy.

Detecção de encaminhamento bidirecional (BFD)

O suporte a BFD foi adicionado ao ASA clássico versão 9.6 e somente para o protocolo BGP: Roteamento de detecção de encaminhamento bidirecional

No FTD:

- Os protocolos BGP IPv4 e BGP IPv6 são suportados (software 6.4).
- Os protocolos OSPFv2, OSPFv3 e EIGRP não são suportados.
- Não há suporte para BFD para rotas estáticas.

Roteadores virtuais (VRF)

O suporte a VRF foi adicionado na versão 6.6. Para obter mais detalhes, consulte este documento: Exemplos de configuração para roteadores virtuais

Informações Relacionadas

- Rotas FTD estáticas e padrão

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.