

Dépannage du routage Firepower Threat Defense

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Mécanismes de transfert de paquets FTD](#)

[Point clé](#)

[Comportement de routage du plan de données \(LINA\)](#)

[Points clés](#)

[Ordre des opérations FTD](#)

[Configurer](#)

[Cas 1 - Transfert basé sur la recherche de connexion](#)

[Temporisation flottante](#)

[Délai de retenue des appels](#)

[Cas 2 - Transfert basé sur la recherche NAT](#)

[Cas 3 - Transfert basé sur le routage basé sur les politiques \(PBR\)](#)

[Cas 4 - Transfert basé sur la recherche de routage globale](#)

[Interface Null0](#)

[Protocole ECMP \(Equal Cost Multi-Path\)](#)

[Plan de gestion FTD](#)

[Routage d'interface de diagnostic LINA FTD](#)

Introduction

Ce document décrit comment Firepower Threat Defense (FTD) transfère les paquets et met en oeuvre divers concepts de routage.

Conditions préalables

Exigences

- Connaissances de base du routage

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco Firepower 41xx Threat Defense Version 7.1.x
- Firepower Management Center (FMC) version 7.1.x

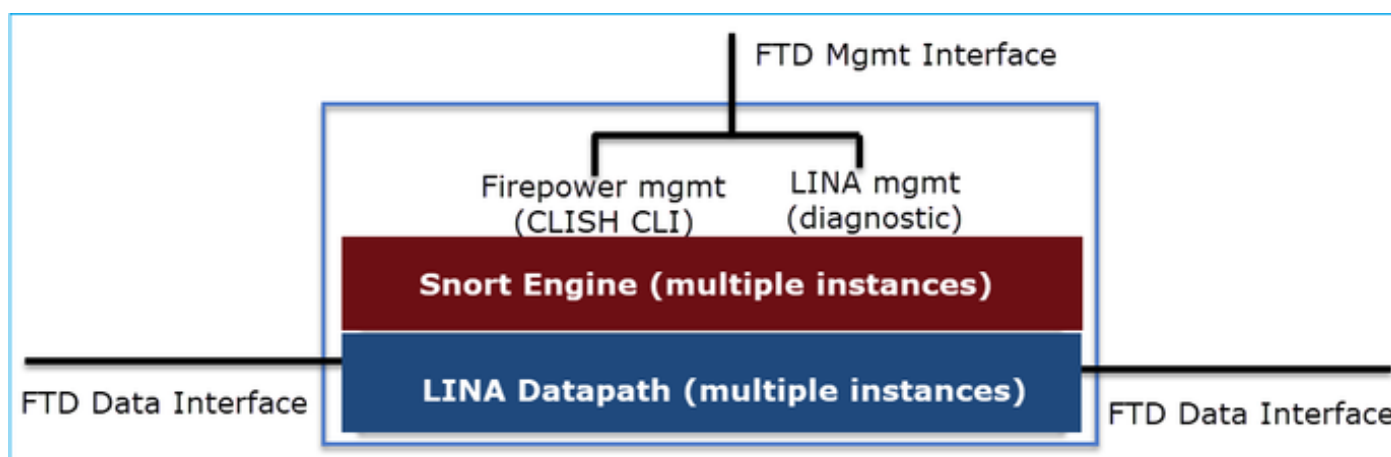
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Mécanismes de transfert de paquets FTD

Cisco Firepower Threat Defense (FTD) est une image logicielle unifiée qui comprend deux moteurs principaux :

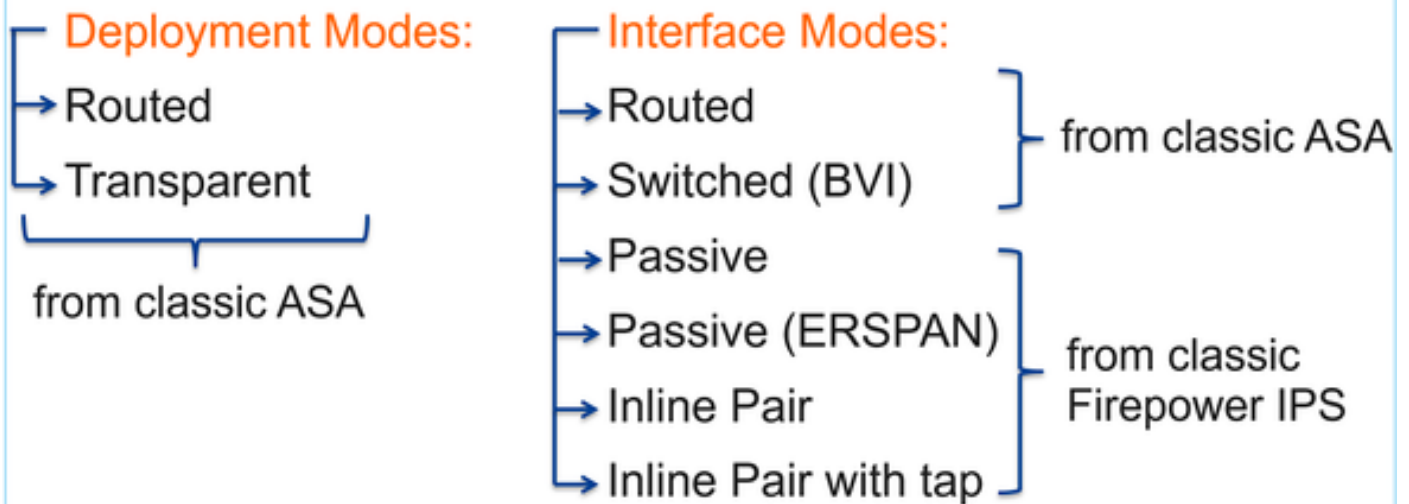
- Moteur de chemin de données (LINA)
- Moteur du renifleur



Le chemin de données et le moteur Snort sont les principales parties du plan de données du FTD.

Le mécanisme de transfert du plan de données FTD dépend du mode d'interface. L'image suivante résume les différents modes d'interface ainsi que les modes de déploiement FTD :

FTD Deployment and Interface Modes



Le tableau résume la façon dont le FTD transmet les paquets dans le plan de données en fonction du mode d'interface. Les mécanismes de transfert sont répertoriés par ordre de préférence :

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 mode transparent effectue une recherche de route dans certaines situations :

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.

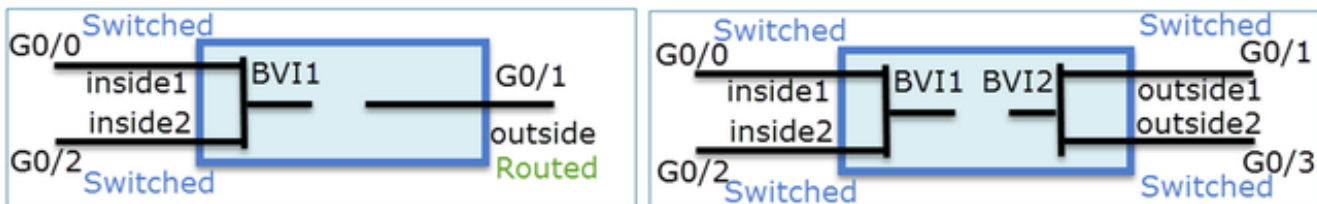


Consultez le [guide FMC](#) pour plus de détails.

À partir de la version 6.2.x, le FTD prend en charge le routage et le pontage intégrés (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



Commandes de vérification 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 configuration

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

Point clé

Pour les interfaces routées ou les interfaces BVI (IRB), le transfert de paquets est basé sur cet ordre :

- Recherche de connexion
- Recherche NAT (destination NAT, également appelée UN-NAT)
- Routage basé sur des politiques (PBR)
- Recherche de table de routage globale

Et la NAT source ?

La NAT source est vérifiée après la recherche de routage globale.

Le reste de ce document se concentre sur le mode d'interface Routed.

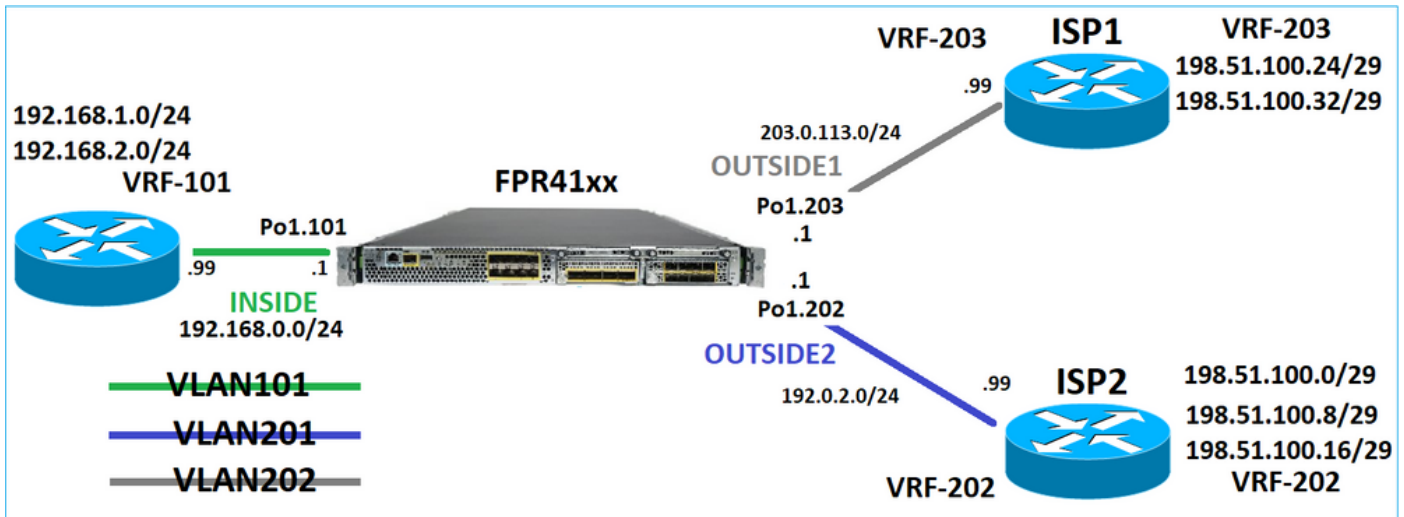
Comportement de routage du plan de données (LINA)

En mode d'interface routée, FTD LINA transfère les paquets en 2 phases :

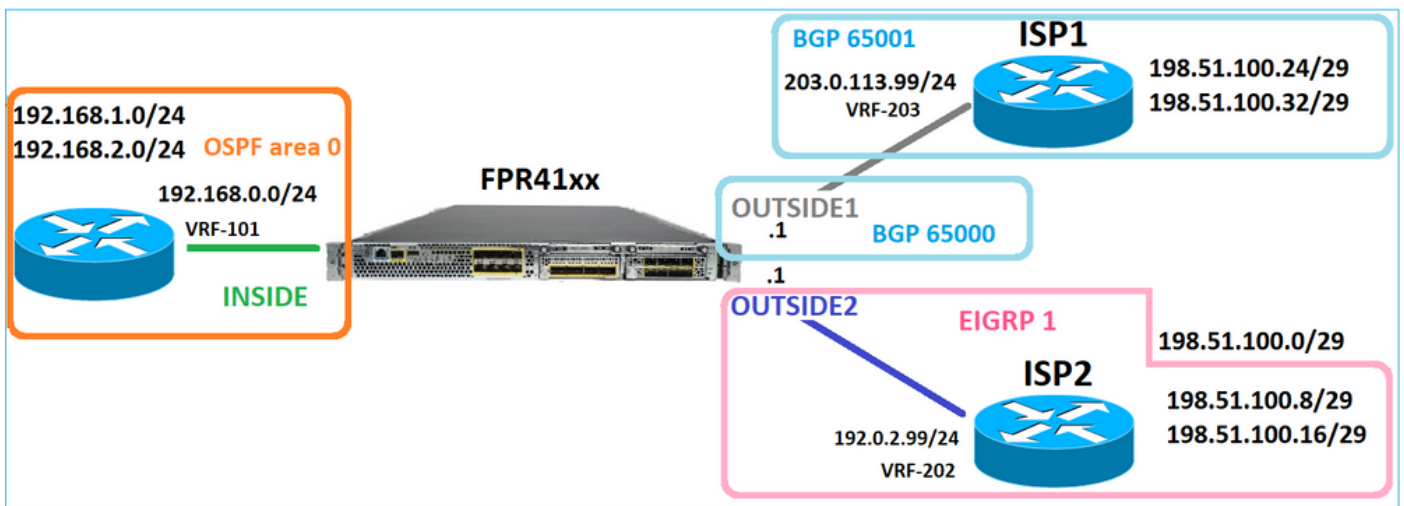
Phase 1 - Détermination de l'interface de sortie

Phase 2 - Sélection du tronçon suivant

Considérez cette topologie :



Et cette conception de routage :



La configuration de routage 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
```

La base d'informations de routage FTD (RIB) - Plan de contrôle :

```
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
```

Table de routage FTD du chemin de sécurité accéléré (ASP) correspondant - Plan de données :

```
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

```

Points clés

Le FTD (d'une manière similaire à un dispositif de sécurité adaptatif - ASA), détermine d'abord l'interface de sortie (de sortie) d'un paquet (pour cela, il examine les entrées « in » de la table de routage ASP). Ensuite, pour l'interface déterminée, il essaie de trouver le tronçon suivant (pour cela, il regarde les entrées 'out' de la table de routage ASP). Exemple :

```

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

```


Enfin, pour le saut suivant résolu, le protocole LINA recherche une contiguïté valide dans le cache ARP.

L'outil FTD packet-tracer confirme ce processus :

```
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 table FTD ARP telle qu'elle apparaît dans le plan de contrôle :

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

Pour forcer la résolution 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 table FTD ARP telle qu'elle apparaît dans le plan de données :

```

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

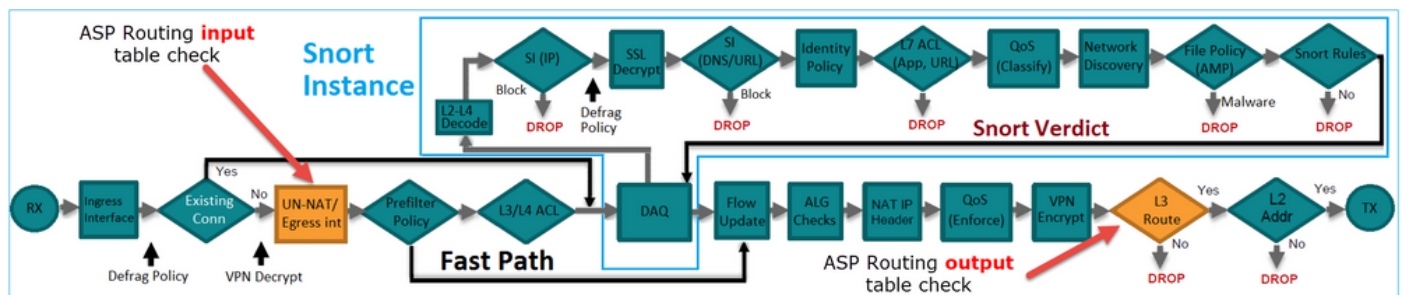
Context: single_vf, Interface: identity
:: Active 0000.0000.0000 hits 0 reference 0
0.0.0.0 Active 0000.0000.0000 hits 848 reference 0

Last clearing of hits counters: Never

```

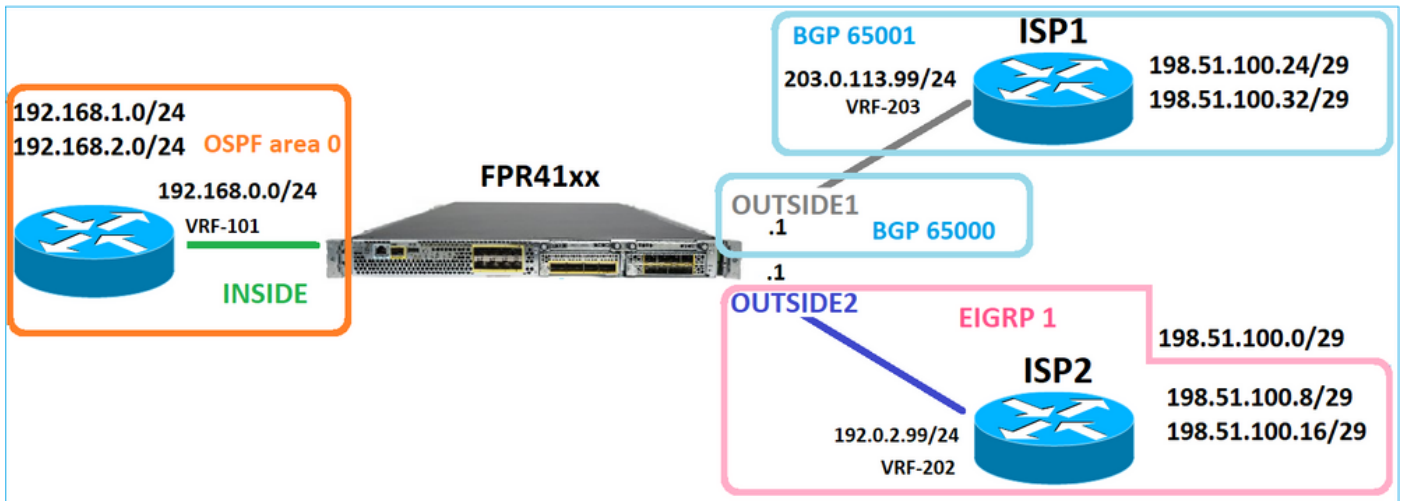
Ordre des opérations FTD

L'image montre l'ordre des opérations et l'endroit où les contrôles de routage ASP d'entrée et de sortie sont effectués :



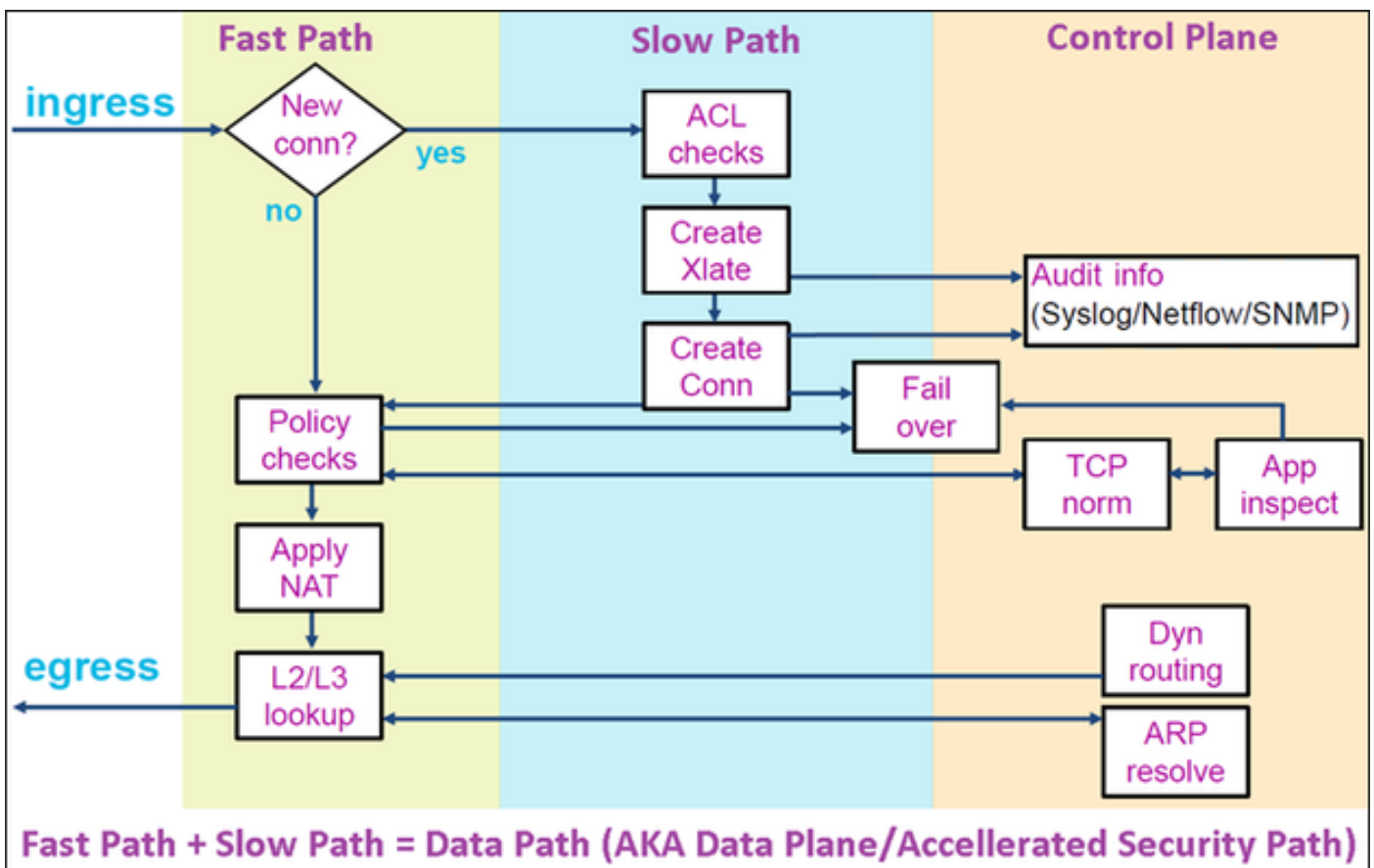
Configurer

Cas 1 - Transfert basé sur la recherche de connexion



Comme mentionné précédemment, le principal composant du moteur FTD LINA est le processus Datapath (plusieurs instances basées sur le nombre de coeurs de périphériques). En outre, le chemin de données (également appelé chemin de sécurité accéléré - ASP) se compose de 2 chemins :

1. Chemin lent = Responsable de l'établissement de la nouvelle connexion (il renseigne le chemin rapide).
2. Fast Path = gère les paquets qui appartiennent aux connexions établies.



- Les commandes telles que show route et show arp affichent le contenu du plan de contrôle.
- D'autre part, les commandes comme show asp table routing et show asp table arp affichent le contenu d'ASP (Datapath) qui est réellement appliqué.

Activez la capture avec trace sur l'interface FTD INSIDE :

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

Ouvrez une session Telnet via le FTD :

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

Les captures FTD montrent les paquets depuis le début de la connexion (la connexion TCP en trois étapes est capturée) :

```
firepower# show capture CAPI
```

26 packets captured

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

Suivez le premier paquet (TCP SYN). Ce paquet passe par le chemin lent LINA FTD, et une recherche de routage global est effectuée dans ce cas :

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

26 packets captured

```
1: 10:50:38.407190 802.1Q vlan#101 PO 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#
```

Suivre un autre paquet entrant du même flux. Le paquet qui correspond à une connexion active :

```
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#

Temporisation flottante

Le problème

Une instabilité de route temporaire peut entraîner l'établissement de connexions UDP (éléphantes) à longue durée de vie via le FTD par le biais d'interfaces FTD différentes de celles souhaitées.

La solution

Pour remédier à cela, définissez le délai d'attente « Floating-conn » sur une valeur différente de la valeur par défaut qui est désactivée :

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

FTD4100-1
Enter Description

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP Access
- ICMP Access
- SSH Access
- SMTP Server
- SNMP
- SSL
- Syslog
- Timeouts**
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Console Timeout*	<input type="text" value="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)

Dans le Guide de référence des commandes :

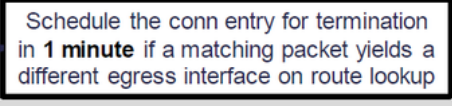
floating-conn	When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The 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.
----------------------	--

Pour plus d'informations, consultez l'étude de cas : Échec des connexions UDP après rechargement à partir de la session CiscoLive BRKSEC-3020 :

Floating Connection Timeout

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

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



Délai de retenue des appels

Le problème

Une route tombe en panne (elle est supprimée), mais le trafic correspond à une connexion établie.

La solution

La fonctionnalité de retenue de connexion a été ajoutée sur ASA 9.6.2. La fonctionnalité est activée par défaut, mais actuellement (7.1.x) n'est pas prise en charge par l'interface utilisateur FMC ou FlexConfig. Améliorations associées : [ENH : timeout conn-holddown not available for configuration in FMC](#)

Dans le guide ASA CLI :

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
```

Cas 2 - Transfert basé sur la recherche NAT

Exigence

Configurez cette règle NAT :

- Type : Statique
- Interface source : INSIDE
- Interface de destination : OUTSIDE1
- Source originale : 192.168.1.1
- Destination initiale : 198.51.100.1
- Source traduite : 192.168.1.1
- Destination traduite : 198.51.100.1

Solution

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

La règle NAT déployée sur l'interface de ligne de commande FTD :

```
firepower# show run nat
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
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_198.51.100.1
translate_hits = 0, untranslate_hits = 0
```

Configurez 3 captures :

```
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 CAP02 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
```

Lancez une session Telnet de 192.168.1.1 à 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
```

Les paquets arrivent sur FTD, mais rien ne sort des interfaces OUTSIDE1 ou 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 CAP01 type raw-data interface OUTSIDE1 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
capture CAP02 type raw-data interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.1.1 any
```

Suivez le paquet TCP SYN. La phase 3 (UN-NAT) montre que NAT (UN-NAT en particulier) a renvoyé le paquet vers l'interface OUTSIDE1 pour la recherche de tronçon suivant :

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

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

2 packets captured

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

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
```


Elapsed time: 6244 ns
Config:
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
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

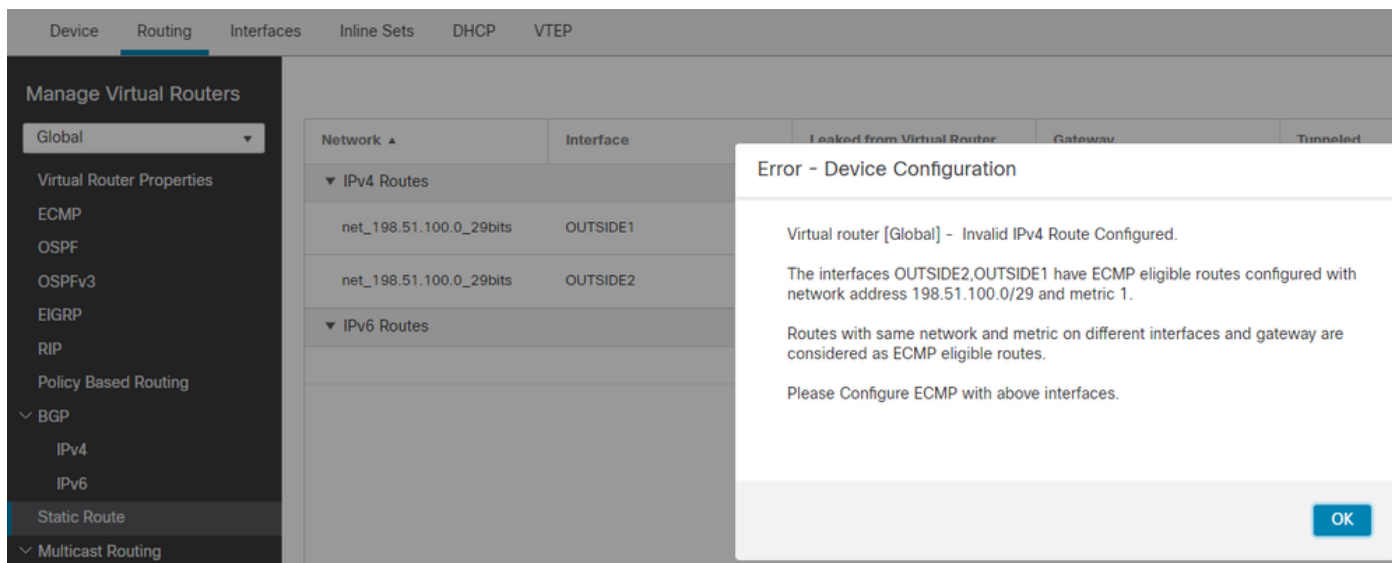
Dans ce cas, la fonction SUBOPTIMAL-LOOKUP signifie que l'interface de sortie déterminée par le processus NAT (OUTSIDE1) est différente de l'interface de sortie spécifiée dans la table d'entrée ASP :

```
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
```


Une solution de contournement possible consiste à ajouter une route statique flottante sur l'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
```

 Remarque : si vous tentez d'ajouter une route statique avec la même métrique que celle qui existe déjà, cette erreur apparaît :



The screenshot shows the Cisco Firepower Management Center interface. The 'Routing' tab is selected, and the 'Static Route' configuration page is visible. An error dialog box is displayed, titled 'Error - Device Configuration'. The error message reads: 'Virtual router [Global] - Invalid IPv4 Route Configured. The interfaces OUTSIDE2, OUTSIDE1 have ECMP eligible routes configured with network address 198.51.100.0/29 and metric 1. Routes with same network and metric on different interfaces and gateway are considered as ECMP eligible routes. Please Configure ECMP with above interfaces.' The background shows a table with columns for Network, Interface, Leaked from Virtual Router, Gateway, and Tunneled. The table lists two IPv4 routes for the network 198.51.100.0/29: one with interface OUTSIDE1 and another with interface OUTSIDE2.

 Remarque : une route flottante avec une métrique de distance de 255 n'est pas installée dans la table de routage.

Essayez d'établir une connexion Telnet avec les paquets envoyés via le FTD :

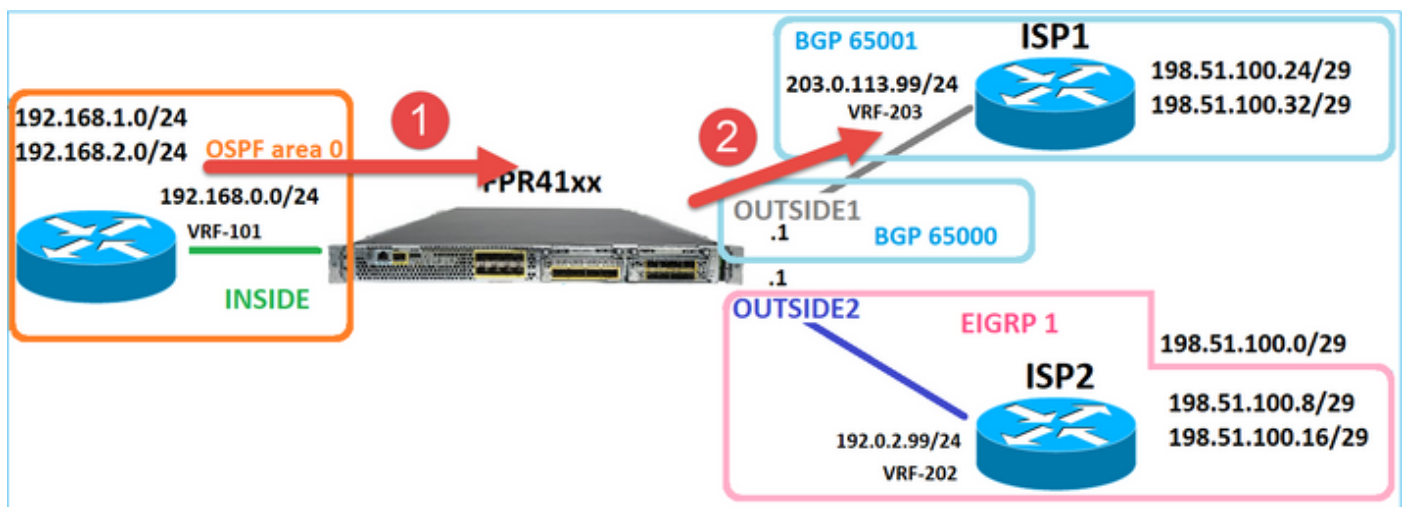
```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

```

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 CAP01 type raw-data interface OUTSIDE1 [Capturing - 312 bytes]
match ip host 192.168.1.1 any
capture CAP02 type raw-data interface OUTSIDE2 [Capturing - 386 bytes]
match ip host 192.168.1.1 any

```

Packet trace indique que les paquets sont transférés vers l'interface ISP1 (OUTSIDE1) au lieu d'ISP2 en raison de la recherche 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) w
...

```

```

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 4460 ns
Config:
nat (INSIDE,OUTSIDE1) source static host_192.168.1.1 host_192.168.1.1 destination static host_198.51.100.1
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 ...
snf_fp_inspect_ip_options
snf_fp_tcp_normalizer
snf_fp_snort
snf_fp_translate
snf_fp_tcp_normalizer
snf_fp_adjacency
snf_fp_fragment
snf_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#
```

Il est intéressant de noter que dans ce cas, il y a des paquets affichés à l'INTÉRIEUR et les deux interfaces de sortie :

```
firepower# show capture CAPI
```

```
2 packets captured
```

```
1: 09:03:02.773962 802.1Q vlan#101 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) w
2: 09:03:05.176565 802.1Q vlan#101 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3031010184:3031010184(0) w
```

```
2 packets shown
```

```
firepower# show capture CAP01
```

```
4 packets captured
```

```
1: 09:03:02.774358 802.1Q vlan#203 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
2: 09:03:02.774557 802.1Q vlan#203 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
3: 09:03:05.176702 802.1Q vlan#203 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
4: 09:03:05.176870 802.1Q vlan#203 PO 192.168.1.1.32134 > 198.51.100.1.23: S 3249840142:3249840142(0) w
```

```
4 packets shown
```

```
firepower# show capture CAP02
```

```
5 packets captured
```

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

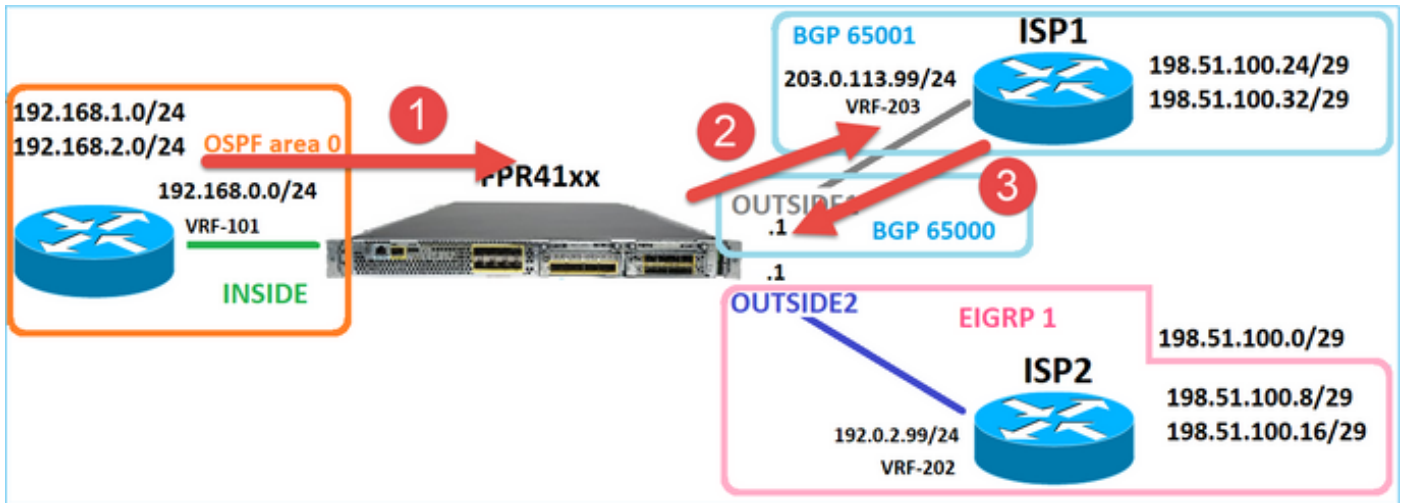
Les détails du paquet incluent les informations d'adresse MAC, et une trace des paquets sur les interfaces OUTSIDE1 et OUTSIDE2 révèle le chemin des paquets :

```
firepower# show capture CAP01 detail
```

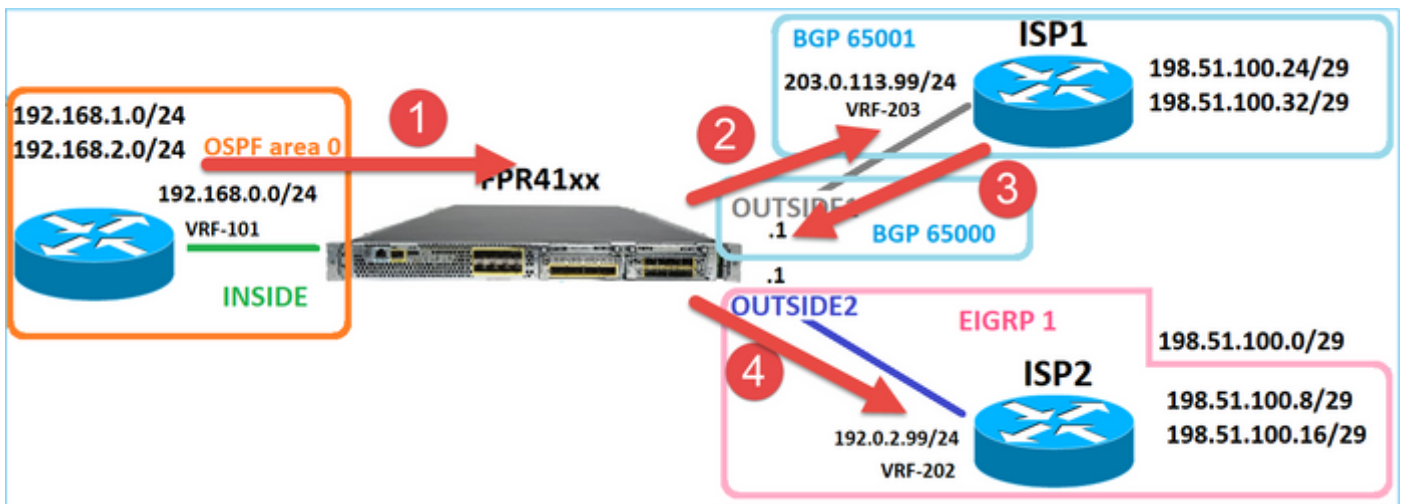
```
4 packets captured
```

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

```
4 packets shown
```



La trace du paquet qui retourne montre la redirection vers l'interface OUTSIDE2 en raison de la recherche dans la table de routage globale :



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

```
4 packets captured
```

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

```
Phase: 3
```

```
Type: INPUT-ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Elapsed time: 7136 ns
```

```
Config:
```

```
Additional Information:
```

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

```
...
```

```
Phase: 10
```

```
Type: FLOW-CREATION
```

```
Subtype:
```

```
Result: ALLOW
```

Elapsed time: 12488 ns
Config:
Additional Information:
New flow created with id 13156, packet dispatched to next module

...

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

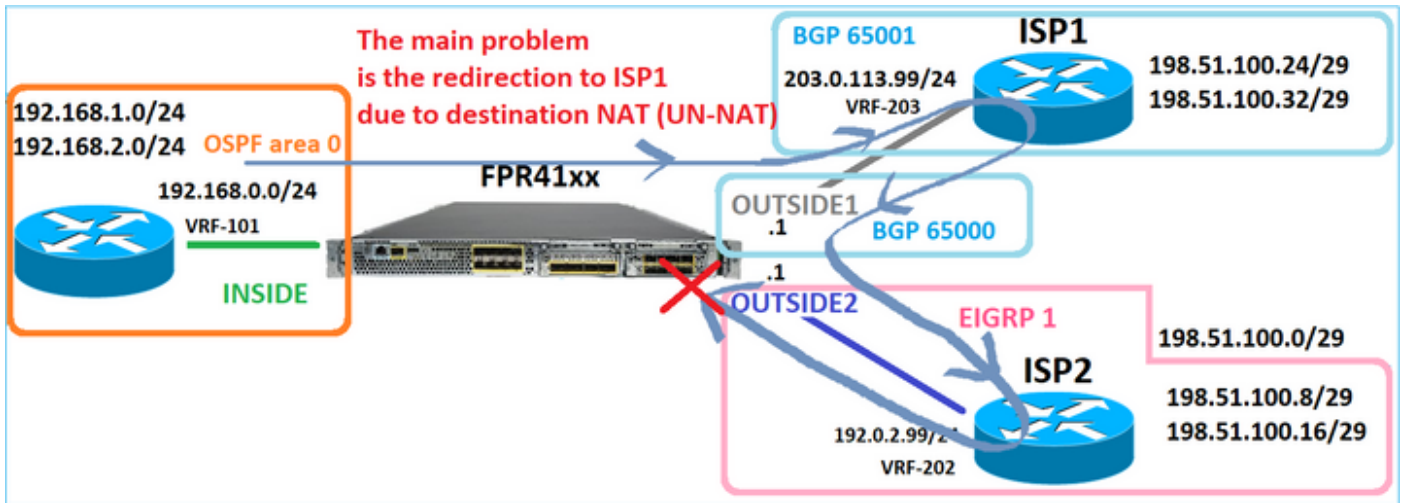
Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1

...

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

1 packet shown
firepower#

Le routeur ISP2 envoie la réponse (SYN/ACK), mais ce paquet est redirigé vers ISP1 car il correspond à la connexion établie. Le paquet est abandonné par le FTD en raison de l'absence de contiguïté de couche 2 dans la table ASP out :



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

```
5 packets captured
```

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

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

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

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


Cas 3 - Transfert basé sur le routage basé sur les politiques (PBR)

Après la recherche du flux de connexion et la recherche NAT de destination, PBR est l'élément suivant qui peut influencer la détermination de l'interface de sortie. PBR est documenté dans :

[Routage basé sur des politiques](#)

Pour la configuration PBR sur FMC, il est important de connaître cette directive :

FlexConfig a été utilisé pour configurer PBR dans FMC pour les versions FTD antérieures à 7.1.

Vous pouvez toujours utiliser FlexConfig pour configurer PBR dans toutes les versions.

Cependant, pour une interface d'entrée, vous ne pouvez pas configurer PBR à l'aide de FlexConfig et de la page Policy Based Routing de FMC.

Dans cette étude de cas, le FTD dispose d'une route vers 198.51.100.0/24 qui pointe vers 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
```

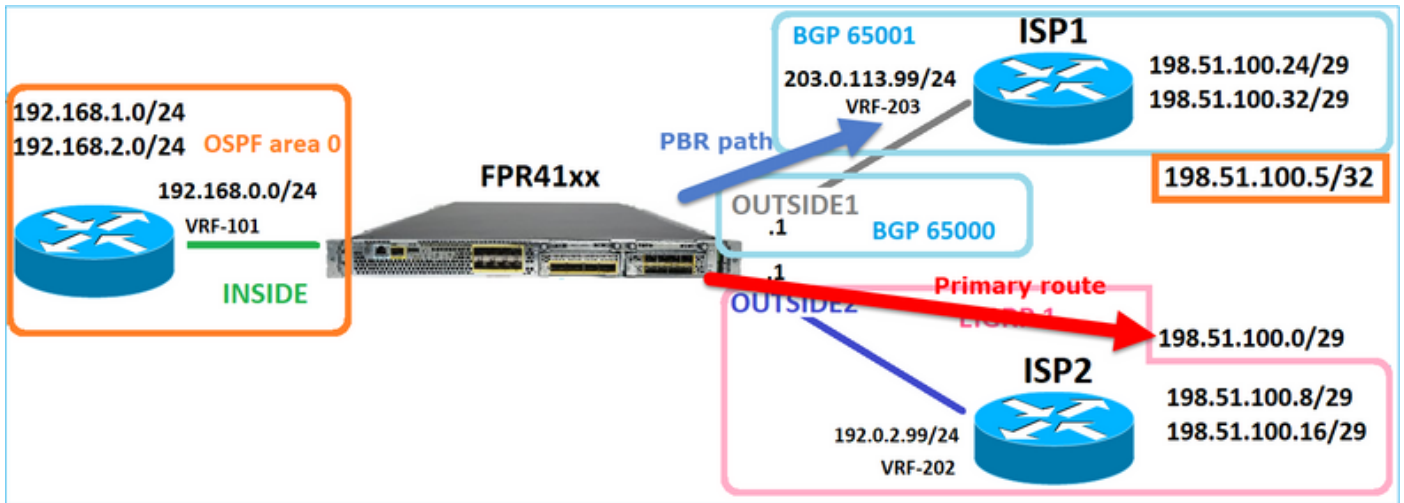
```
C 203.0.113.0 255.255.255.0 is directly connected, OUTSIDE1
```

```
L 203.0.113.1 255.255.255.255 is directly connected, OUTSIDE1
```

Exigence

Configurez une stratégie PBR avec les caractéristiques suivantes :

- Le trafic provenant de l'adresse IP 192.168.2.0/24 et destiné à l'adresse 198.51.100.5 doit être envoyé à ISP1 (tronçon suivant 203.0.113.99), tandis que les autres sources doivent utiliser l'interface OUTSIDE2.



Solution

Dans les versions antérieures à la version 7.1, pour configurer PBR :

1. Créez une liste de contrôle d'accès étendue correspondant au trafic intéressant (par exemple, PBR_ACL).
2. Créez une route-map correspondant à la liste de contrôle d'accès créée à l'étape 1, puis définissez le tronçon suivant souhaité.
3. Créez un objet FlexConfig qui active PBR sur l'interface d'entrée à l'aide de la carte de routage créée à l'étape 2.

Dans les versions postérieures à la version 7.1, vous pouvez configurer PBR de la manière antérieure à la version 7.1, ou vous pouvez utiliser la nouvelle option Policy Based Routing sous Device > Routing :

1. Créez une liste de contrôle d'accès étendue correspondant au trafic intéressant (par exemple, PBR_ACL).
2. Ajoutez une stratégie PBR et spécifiez :
 - a. Le trafic correspondant
 - b. L'interface d'entrée
 - c. Le tronçon suivant

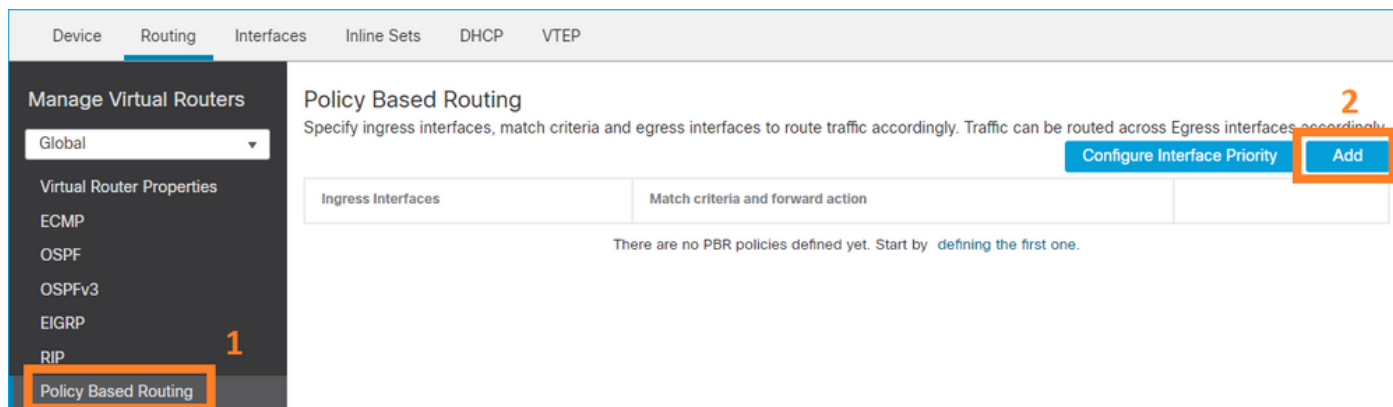
Configurer PBR (nouvelle méthode)

Étape 1 : définition d'une liste d'accès pour le trafic correspondant

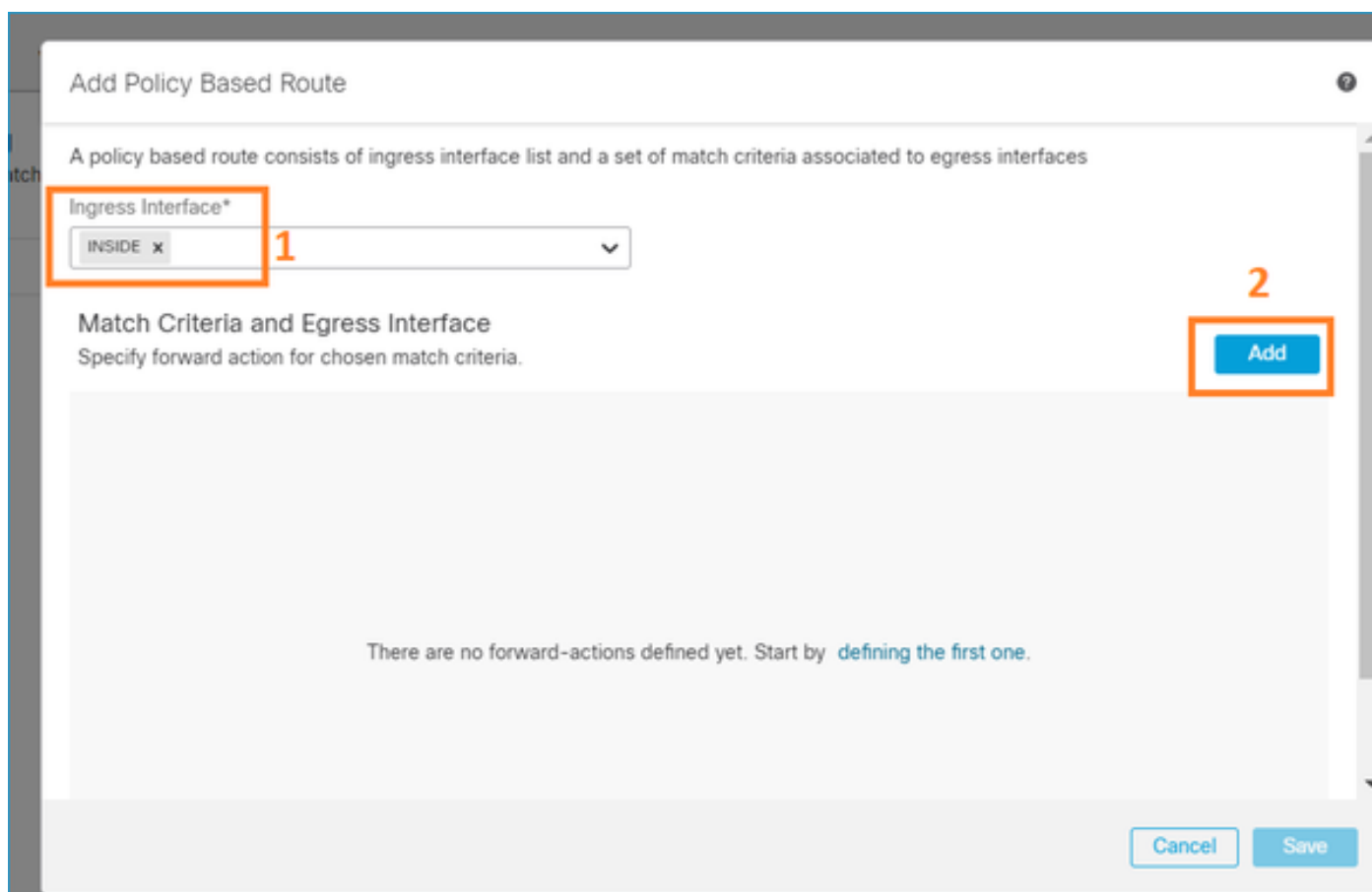
Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Allow	192.168.2.0/24	Any	198.51.100.5	Any	Any

Étape 2 : ajout d'une stratégie PBR

Accédez à Devices > Device Management et modifiez le périphérique FTD. Choisissez Routing > Policy Based Routing, et sur la page Policy Based Routing, sélectionnez Add.



Spécifiez l'interface d'entrée :



Spécifiez les actions de transfert :

Add Forwarding Actions


Match ACL:* 1

Send To:* 2

IPv4 Addresses 3

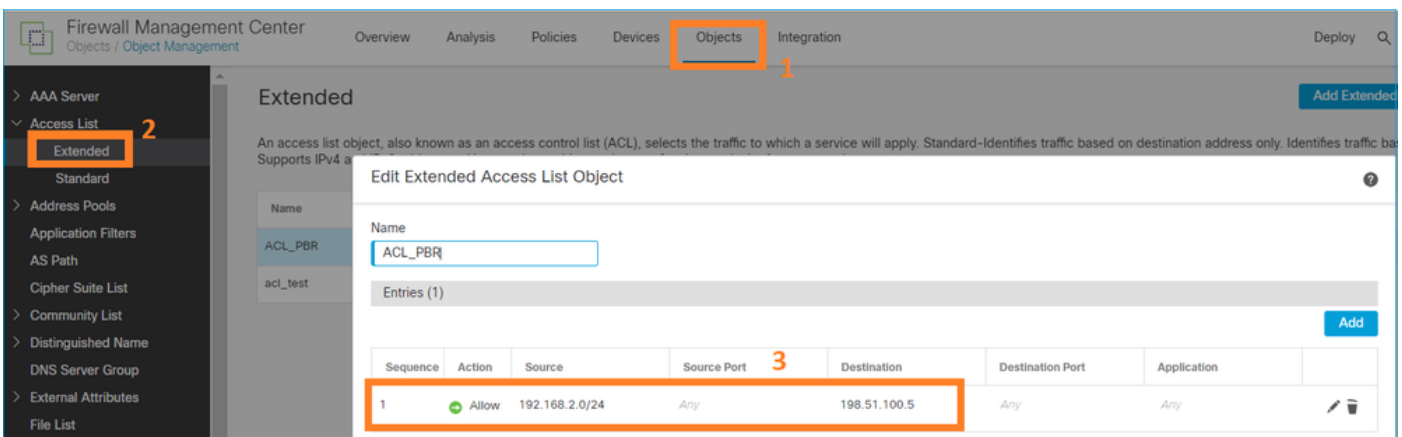
IPv6 Addresses

Enregistrer et déployer

 Remarque : si vous voulez configurer plusieurs interfaces de sortie, vous devez définir dans le champ 'Send To' l'option 'Egress Interfaces' (disponible depuis la version 7.0+). Pour plus de détails, consultez : [Exemple de configuration du routage basé sur des stratégies](#)

Configurer PBR (méthode héritée)

Étape 1 : définition d'une liste d'accès pour le trafic correspondant



Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

AAA Server
Access List
Extended
Standard
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source address only. Supports IPv4 and IPv6.

Edit Extended Access List Object

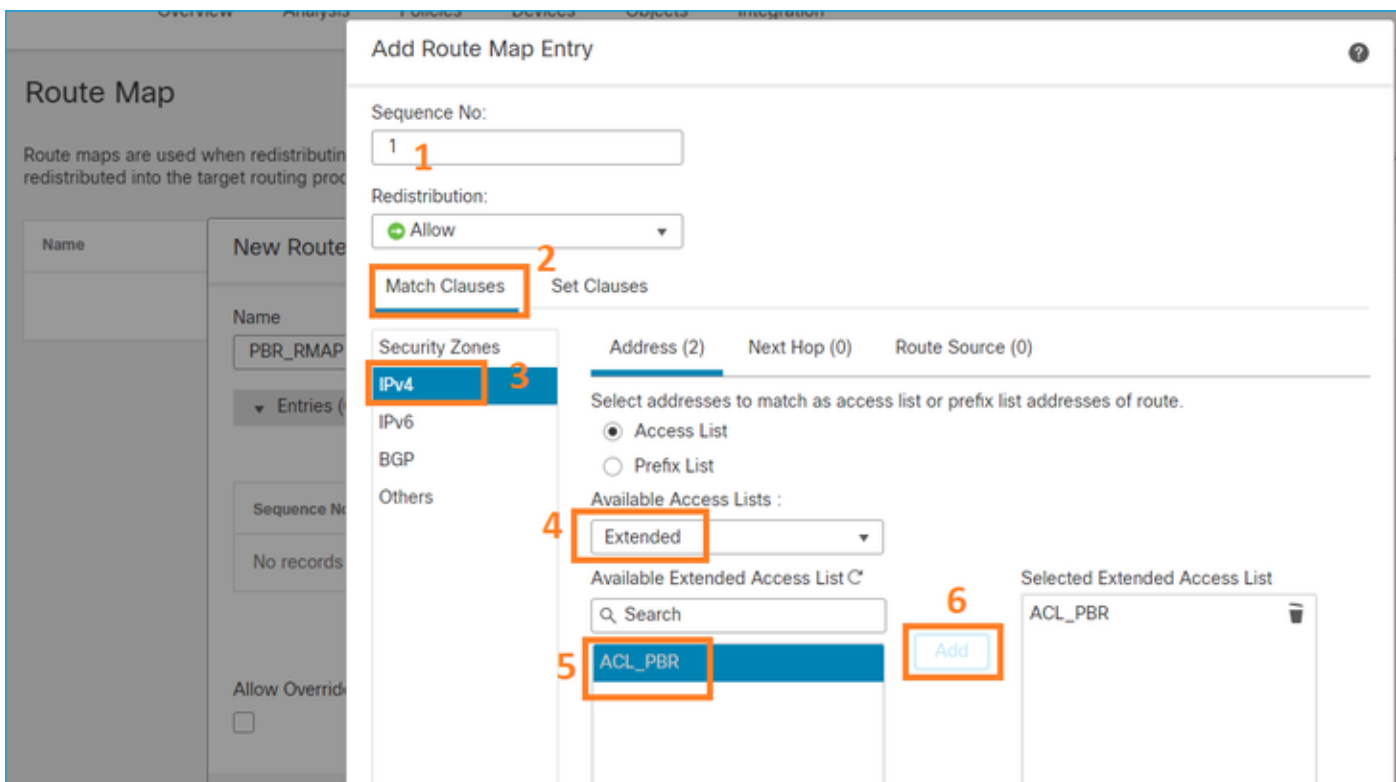
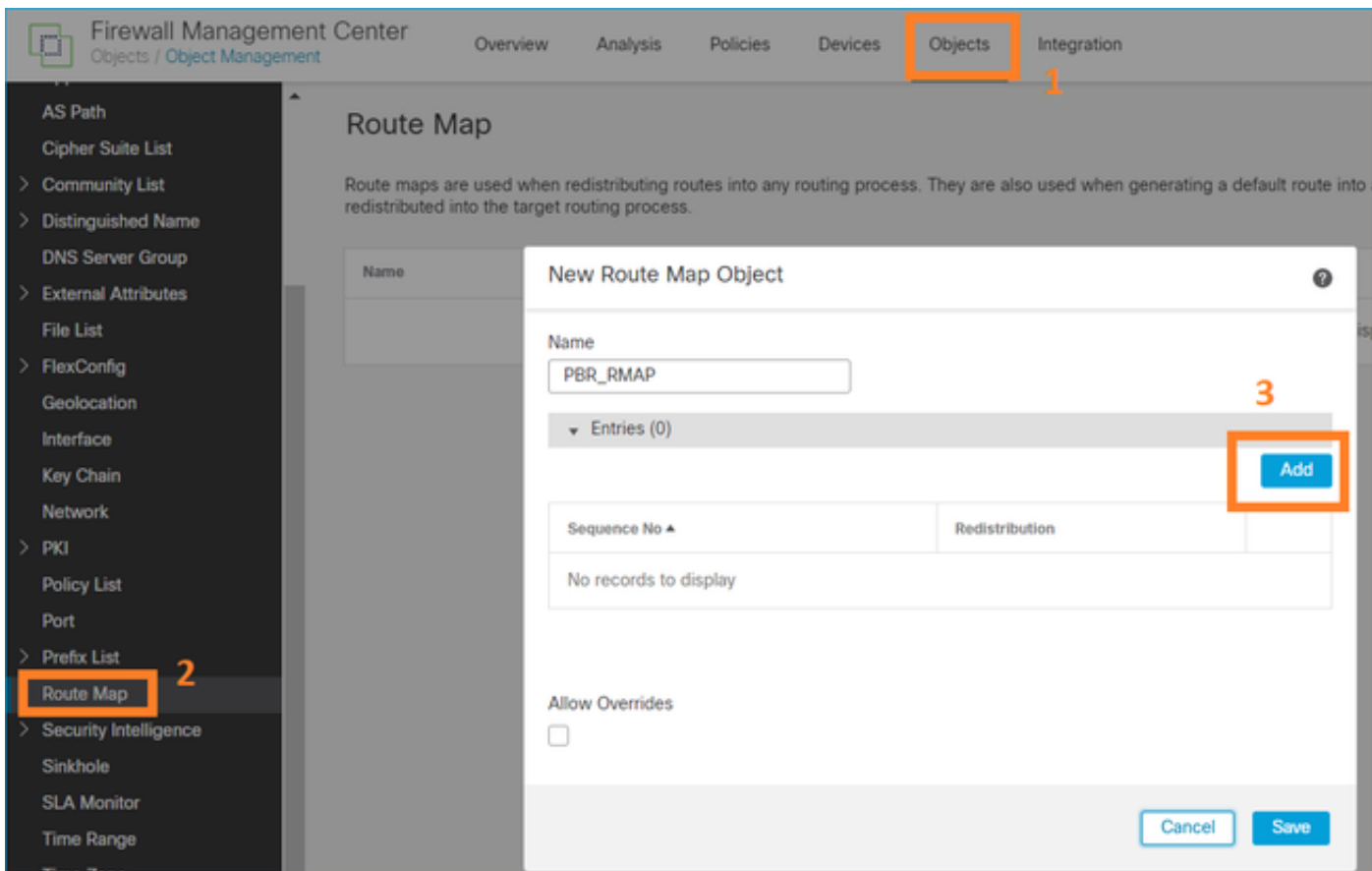
Name:

Entries (1)

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

Étape 2 : définition d'une route-map correspondant à la liste de contrôle d'accès et définition du tronçon suivant

Définissez d'abord la clause Match :



Définissez la clause Set :

Edit Route Map Entry

Sequence No:

Redistribution:

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:

4

Specific IP :
Use comma to separate multiple values

Prefix List:

IPv6 settings:

Ajouter et enregistrer.

Étape 3 : configuration de l'objet PBR FlexConfig

Tout d'abord, copiez (dupliquez) l'objet PBR existant :

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

FlexConfig Object 2

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

Name	Domain	Description
Policy_Based_Routing	Global	The template is an ex... 3
Policy_Based_Routing_Clear	Global	Clear configuration of ...

AS Path
Cipher Suite List
> Community List
> Distinguished Name
DNS Server Group
> External Attributes
File List
> FlexConfig 1
FlexConfig Object
Text Object
Geolocation

Spécifiez le nom de l'objet et supprimez l'objet route-map prédéfini :

Add FlexConfig Object

Name: **1 Specify a new name**

Description:

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

Insert | | Type:

```
interface Port-channel1.101
policy-route route-map Sr-map-object
```

2 Specify the correct ingress interface
3 Remove this route-map

Spécifiez la nouvelle route-map :

Add FlexConfig Object

Name:

Description:

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

1 Insert | | Type:

- Insert Policy Object ▶ Text Object
- Insert System Variable ▶ Network
- Insert Secret Key Security Zones
- Standard ACL Object
- Extended ACL Object
- 2** Route Map

Insert Route Map Variable

Variable Name: 1

Description:

Available Objects 2

PBR_RMAP

3

Selected Object

PBR_RMAP

Voici le résultat final :

Add FlexConfig Object

Name:

Description:

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

Insert Deployment: Type:

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

Étape 4 - Ajoutez l'objet PBR à la stratégie FTD FlexConfig.

Firewall Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects Integration Deploy

FTD4100_FlexConfig Preview Config Save Cancel

Enter Description Policy Assignments (1)

Available FlexConfig FlexConfig Object

User Defined **1**
 FTD4100_PBR **2**
 no_ICMP
 System Defined
 Default_DNS_Configure
 Default_Inspection_Protocol_Disable
 Default_Inspection_Protocol_Enable
 DHCPv6_Prefix_Delegation_Configure
 DHCPv6_Prefix_Delegation_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

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

Enregistrez et sélectionnez Aperçu de la configuration :

Preview FlexConfig

Select Device:

```

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
  
```

Enfin, déployez la stratégie.

 Remarque : PBR ne peut pas être configuré avec FlexConfig et l'interface utilisateur FMC pour la même interface d'entrée.

Pour la configuration du SLA de PBR, consultez ce document : [Configure PBR with IP SLAs for DUAL ISP on FTD Managed by FMC](#)

Vérification PBR

Vérification de l'interface entrante :

```
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
```

Vérification de la carte de routage :

```
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)
```

Vérification du routage de la politique :

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

Packet-Tracer avant et après la modification :

Sans PBR	Avec PBR
<pre> firepower# packet-tracer input INSIDE tcp 192.168.2.100 1111 198.51.100.5 23 Phase: 3 Type: INPUT-ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Elapsed time: 11596 ns Config: Additional Information: Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0) ... Phase: 13 Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP Subtype: Resolve Preferred Egress interface Result: ALLOW Elapsed time: 6244 ns Config: Additional Information: Found next-hop 192.0.2.99 using egress ifc OUTSIDE2(vrfid:0) Phase: 14 Type: ADJACENCY-LOOKUP Subtype: Resolve Nexthop IP address to MAC Result: ALLOW Elapsed time: 2230 ns Config: Additional Information: Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2 Adjacency :Active MAC address 4c4e.35fc.fcd8 hits 0 reference 1 Result: input-interface: INSIDE(vrfid:0) input-status: up input-line-status: up output-interface: OUTSIDE2(vrfid:0) output-status: up output-line-status: up Action: allow Time Taken: 272058 ns </pre>	<pre> firepower# packet-tracer i ... Phase: 3 Type: SUBOPTIMAL-LOOKUP Subtype: suboptimal next-h Result: ALLOW Elapsed time: 39694 ns Config: Additional Information: Input route lookup returne Phase: 4 Type: ECMP load balancing Subtype: Result: ALLOW Elapsed time: 2230 ns Config: Additional Information: ECMP load balancing Found next-hop 203.0.113.9 Phase: 5 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Elapsed time: 446 ns Config: route-map FMC_GENERATED_PE 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 </pre>

Test avec le trafic réel

Configurez la capture de paquets avec un suivi :

```
firepower# capture CAPI trace interface INSIDE match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAP01 trace interface OUTSIDE1 match ip host 192.168.2.1 host 198.51.100.5
firepower# capture CAP02 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 capture montre :

```
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 CAP01 type raw-data trace interface OUTSIDE1 [Capturing - 4389 bytes]
match ip host 192.168.2.1 host 198.51.100.5
capture CAP02 type raw-data trace interface OUTSIDE2 [Capturing - 0 bytes]
match ip host 192.168.2.1 host 198.51.100.5
```

Trace du paquet SYN TCP :

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

44 packets captured

```
1: 13:26:38.485585 802.1Q vlan#101 PO 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

Le tableau ASP PBR indique le nombre de succès de la stratégie :

```
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

 Remarque : le traceur de paquets augmente également le compteur de succès.

Débogage PBR

 Avertissement : dans un environnement de production, le débogage peut produire beaucoup de messages.

Activez ce débogage :

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


Envoyer le trafic réel :

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

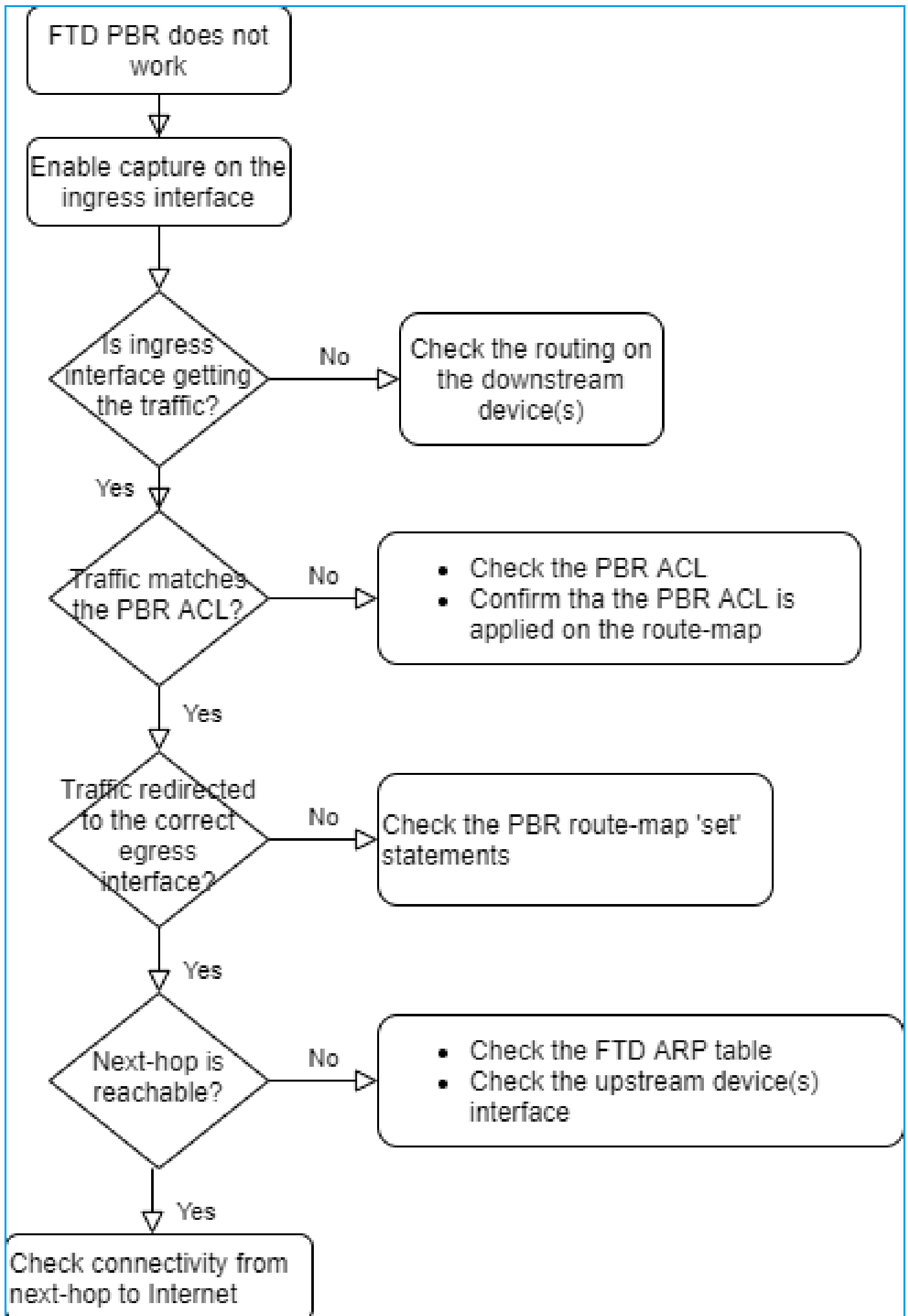
Le débogage indique :

```
firepower#
```

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

 Remarque : Packet-tracer génère également une sortie de débogage.

Cet organigramme peut être utilisé pour dépanner PBR :



show asp drop

Cas 4 - Transfert basé sur la recherche de routage globale

Après la recherche de connexion, la recherche NAT et PBR, le dernier élément qui est vérifié pour déterminer l'interface de sortie est la table de routage globale.

Vérification de la table de routage

Examinons le résultat d'une table de routage 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 level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

Dest. Mask  Dest. Network  Administrative Distance  Metric  Next Hop
-----
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
```

L'objectif principal du processus de routage est de trouver le saut suivant. La sélection de la route se fait dans l'ordre suivant :

1. Victoires du match le plus long
2. AD le plus bas (entre différentes sources de protocole de routage)
3. Métrique la plus basse (si les routes sont apprises à partir de la même source - protocole de routage)

Mode de remplissage de la table de routage :

- IGP (R, D, EX, O, IA, N1, N2, E1, E2, i, su, L1, L2, ia, o)
- BGP (B)
- BGP InterVRF (BI)
- Statique (S)
- InterVRF statique (SI)

- Connecté (C)
- IP locales (L)
- VPN (V)
- Redistribution
- Par défaut

Pour afficher le résumé de la table de routage, utilisez cette commande :

```
<#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

Vous pouvez suivre les mises à jour de la table de routage avec cette commande :

```
<#root>
```

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

Par exemple, voici ce que le débogage montre lorsque la route OSPF 192.168.1.0/24 est supprimée de la table de routage globale :

```
<#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:1
```

```
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
```

Lors de son rajout :

```
<#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

L'interface Null0 peut être utilisée pour supprimer le trafic indésirable. Cette suppression a moins d'impact sur les performances que la suppression du trafic avec une règle de politique de contrôle d'accès (ACL).

Exigence

Configurez une route Null0 pour l'hôte 198.51.100.4/32.

Solution

The screenshot shows the configuration interface for a Cisco Firepower 4140 Threat Defense device. The main window displays the 'Routing' tab with a table of routes. A sidebar on the left shows the 'Manage Virtual Routers' menu, with 'Static Route' highlighted (1). A dialog box titled 'Add Static Route Configuration' is open, showing the following configuration:

- Type: IPv4 (selected)
- Interface*: Null0 (2)
- Available Network: host_198.51.100.4 (3)
- Selected Network: host_198.51.100.4 (4)
- Gateway*: (empty)
- Metric: (empty)

Enregistrer et déployer.

Vérification :

```
<#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
```

Essayez d'accéder à l'hôte distant :

```
<#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)
```

Les journaux FTD indiquent :

```
<#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

Les abandons ASP montrent :

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

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

Protocole ECMP (Equal Cost Multi-Path)

Zones de trafic

- La zone de trafic ECMP permet à un utilisateur de regrouper des interfaces (appelée zone ECMP).
- Cela permet le routage ECMP ainsi que l'équilibrage de charge du trafic sur plusieurs interfaces.
- Lorsque des interfaces sont associées à la zone de trafic ECMP, l'utilisateur peut créer des routes statiques à coût égal à travers les interfaces. Les routes statiques à coût égal sont des routes vers le même réseau de destination avec la même valeur métrique.

Avant la version 7.1, Firepower Threat Defense prenait en charge le routage ECMP via des politiques FlexConfig. À partir de la version 7.1, vous pouvez regrouper des interfaces dans des zones de trafic et configurer le routage ECMP dans Firepower Management Center.

EMCP est documenté dans : [ECMP](#)

Dans cet exemple, il y a un routage asymétrique et le trafic de retour est abandonné :

```
<#root>
```

```
firepower#
```

```
show log
```

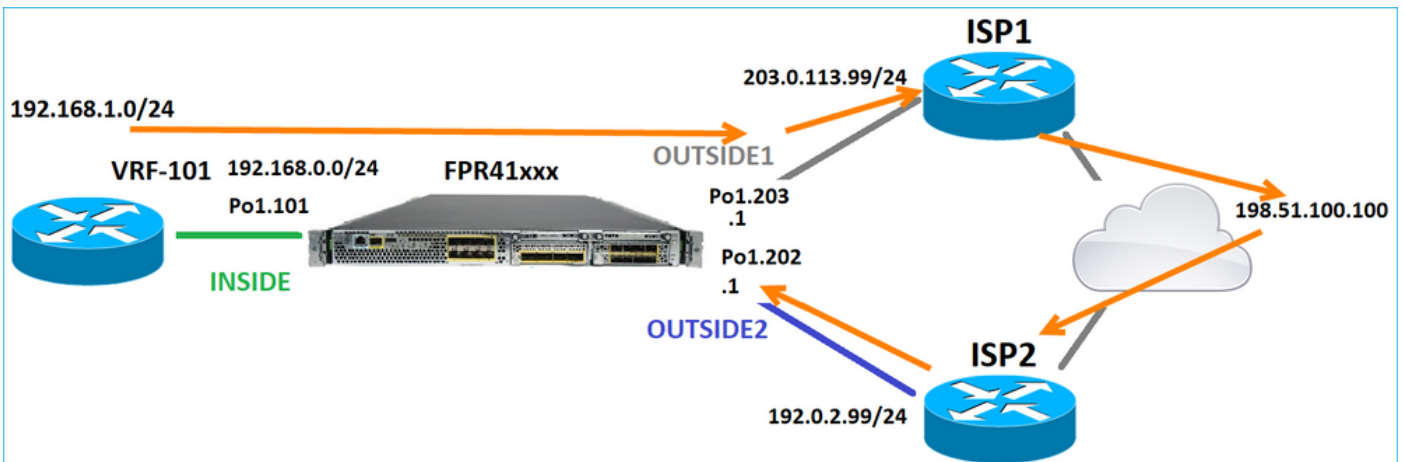
Apr 13 2022 07:20:48: %FTD-6-302013:

```
B
```

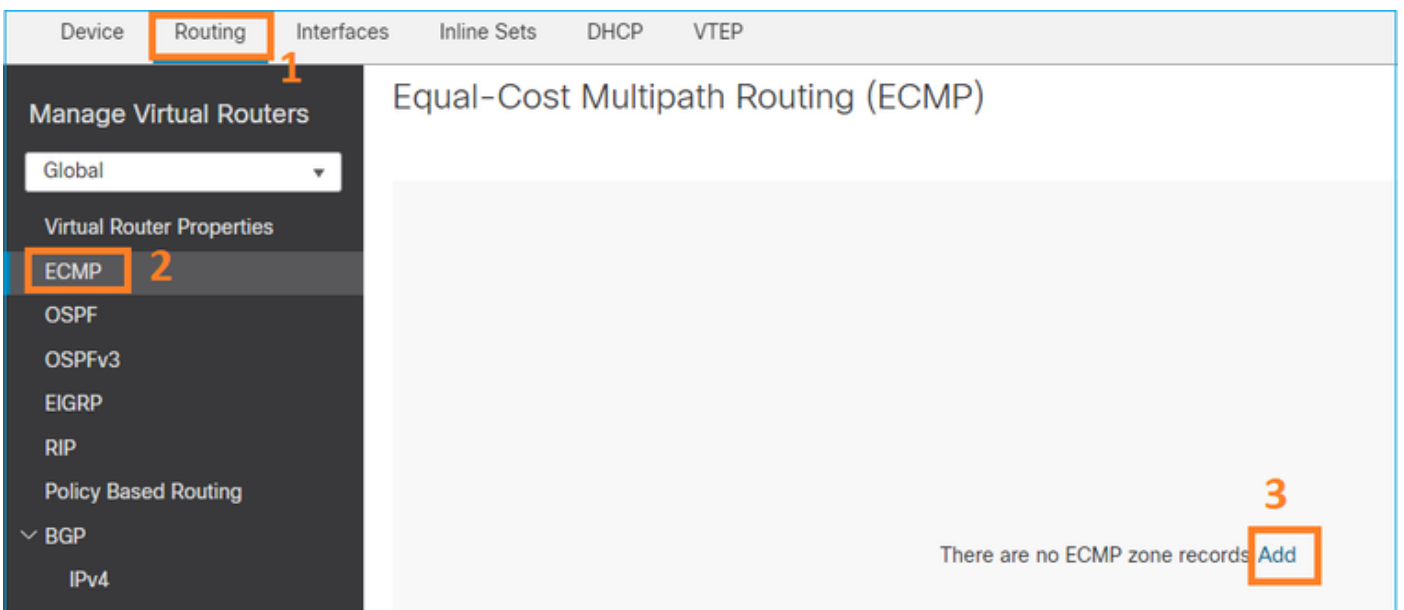
```
uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE1:198.51.100.4/0
```

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

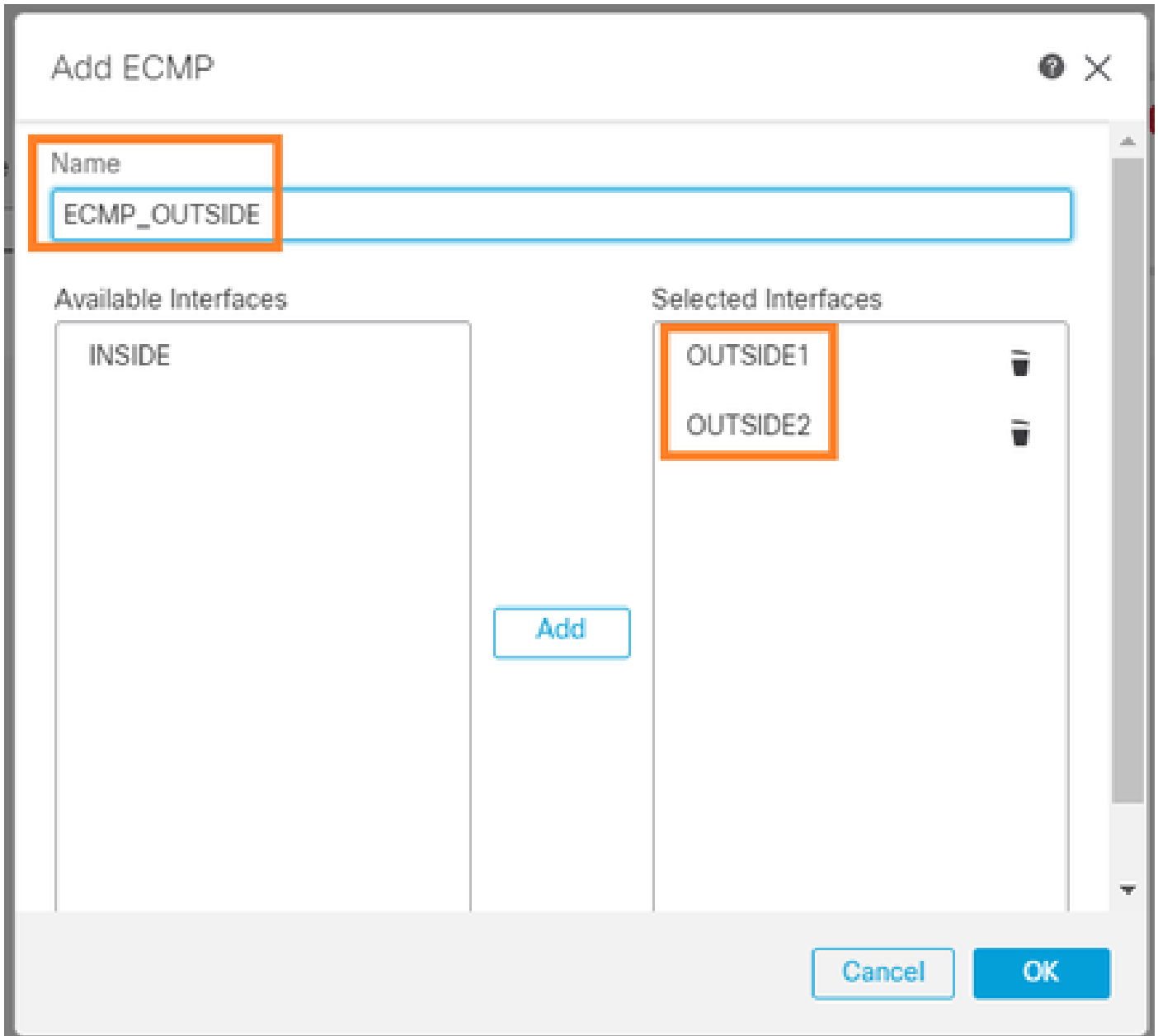
Deny TCP (no connection) from 198.51.100.100/23 to 192.168.1.1/23943 flags SYN ACK on interface OUTSIDE2



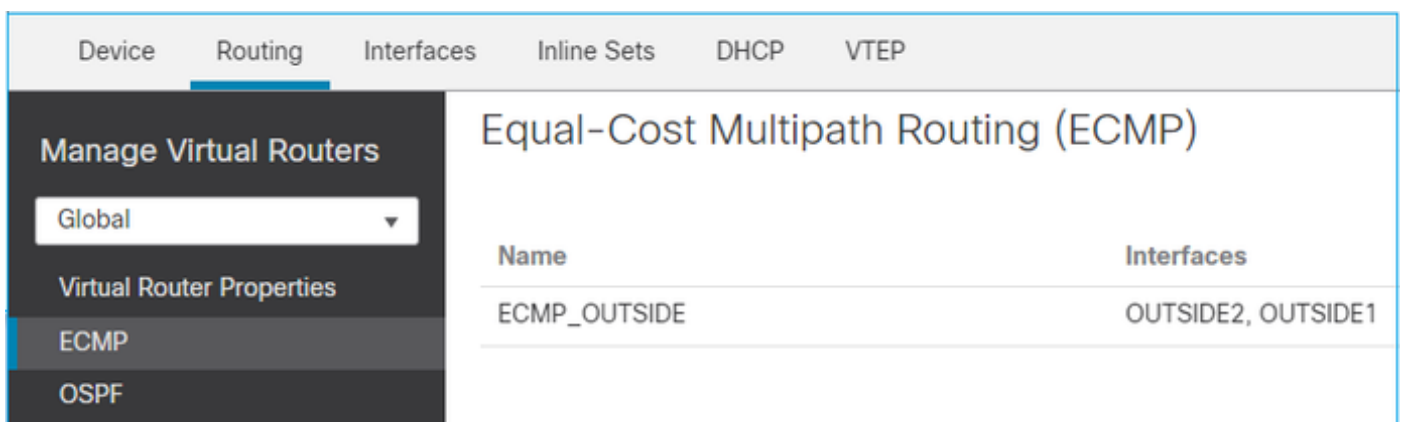
Configurez ECMP à partir de l'interface utilisateur FMC :



Ajoutez les 2 interfaces dans le groupe ECMP :



Le résultat :



Enregistrer et déployer.

Vérification de la zone 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
```

Vérification des interfaces :

<#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
```

Maintenant, le trafic de retour est autorisé et la connexion est UP :

```
<#root>  
Router1#  
telnet 198.51.100.100 /vrf VRF-101 /source-interface lo1  
  
Trying 198.51.100.100 ... Open
```

La capture sur l'interface ISP1 affiche le trafic de sortie :

```
<#root>  
firepower#  
show capture CAP1  
  
5 packets captured  
1: 10:03:52.620115 802.1Q vlan#203 PO 192.168.1.1.56199 > 198.51.100.100.23: S 1782458734:1782458734(0)  
2: 10:03:52.621992 802.1Q vlan#203 PO 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128  
3: 10:03:52.622114 802.1Q vlan#203 PO 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128  
4: 10:03:52.622465 802.1Q vlan#203 PO 192.168.1.1.56199 > 198.51.100.100.23: P 1782458735:1782458753(18  
5: 10:03:52.622556 802.1Q vlan#203 PO 192.168.1.1.56199 > 198.51.100.100.23: . ack 2000807246 win 4128
```

La capture sur l'interface ISP2 affiche le trafic de retour :

```
<#root>  
firepower#  
show capture CAP2
```


6 packets captured

1: 10:03:52.621305 802.1Q vlan#202 PO 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 PO 198.51.100.100.23 > 192.168.1.1.56199: . ack 1782458753 win 64222

Plan de gestion FTD

Le FTD dispose de 2 plans de gestion :

- Interface Management0 - Permet d'accéder au sous-système Firepower
- Interface de diagnostic LINA - Fournit un accès au sous-système LINA FTD

Pour configurer et vérifier l'interface Management0, utilisez respectivement les commandes configure network et show network.

D'autre part, les interfaces LINA fournissent un accès à la LINA elle-même. Les entrées d'interface FTD dans le RIB FTD peuvent être considérées comme des routes 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 même, elles peuvent être vues comme des entrées d'identité dans la table de routage 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
```

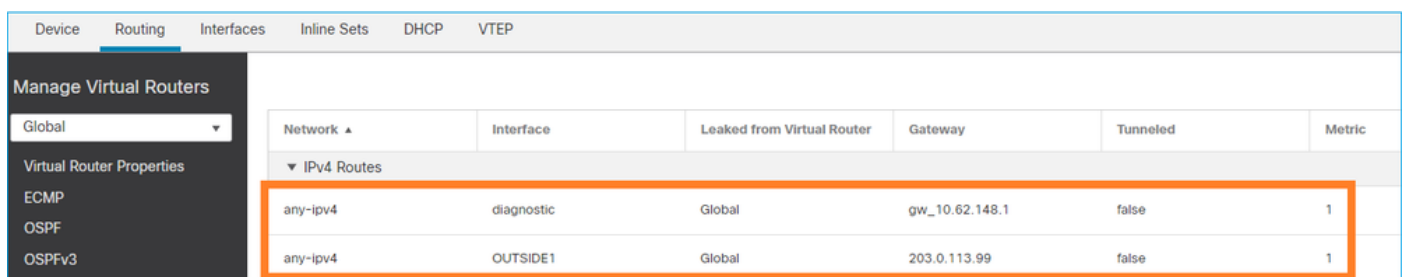
Point principal

Lorsqu'un paquet arrive sur FTD et que l'adresse IP de destination correspond à l'une des adresses IP d'identité, le FTD sait qu'il doit consommer le paquet.

Routage d'interface de diagnostic LINA FTD

FTD (comme un ASA qui exécute le code post-9.5) gère une table de routage de type VRF pour toute interface configurée en tant que gestion seule. L'interface de diagnostic est un exemple d'une telle interface.

Tandis que FMC ne vous permet pas (sans ECMP) de configurer 2 routes par défaut sur 2 interfaces différentes avec la même métrique, vous pouvez configurer 1 route par défaut sur une interface de données FTD et une autre route par défaut sur l'interface de diagnostic :



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

Le trafic du plan de données utilise la passerelle par défaut de la table globale, tandis que le trafic du plan de gestion utilise la passerelle de diagnostic par défaut :

```
<#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
```

La passerelle de la table de routage globale :

```
<#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
```

Lorsque vous envoyez du trafic à partir du FTD (trafic prêt à l'emploi), l'interface de sortie est sélectionnée en fonction des éléments suivants :

1. Table de routage globale
2. Table de routage de gestion uniquement

Vous pouvez remplacer la sélection de l'interface de sortie si vous spécifiez manuellement l'interface de sortie.

Essayez d'envoyer une requête ping à la passerelle d'interface de diagnostic. Si vous ne spécifiez pas l'interface source, la requête ping échoue car FTD utilise d'abord la table de routage globale qui, dans ce cas, contient une route par défaut. S'il n'y a pas de route dans la table globale, le FTD effectue une recherche de route sur la table de routage de gestion uniquement :

```
<#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
```

Il en va de même si vous tentez de copier un fichier à partir de l'interface de ligne de commande LINA à l'aide de la commande copy.

Détection de transfert bidirectionnel (BFD)

La prise en charge BFD a été ajoutée sur la version 9.6 classique d'ASA et seulement pour le protocole BGP : [Routage de détection de transfert bidirectionnel](#)

Sur FTD :

- Les protocoles IPv4 et IPv6 BGP sont pris en charge (logiciel 6.4).
- Les protocoles OSPFv2, OSPFv3 et EIGRP ne sont pas pris en charge.
- BFD pour les routes statiques n'est pas pris en charge.

Routeurs virtuels (VRF)

La prise en charge VRF a été ajoutée à la version 6.6. Pour plus de détails, consultez ce

document : [Exemples de configuration pour les routeurs virtuels](#)

Informations connexes

- [Routes statiques et par défaut FTD](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.