

# firepower脅威対策ルーティングのトラブルシューティング

## 内容

---

### [概要](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

#### [FTDパケット転送メカニズム](#)

#### [キーポイント](#)

#### [データプレーン\(LINA\)ルーティングの動作](#)

#### [要点](#)

#### [FTDの処理順序](#)

### [設定](#)

#### [ケース1: 接続ルックアップに基づく転送](#)

##### [フローティングタイムアウト](#)

##### [Conn-holddownタイムアウト](#)

#### [ケース2:NATルックアップに基づく転送](#)

#### [ケース3: ポリシーベースルーティング\(PBR\)に基づく転送](#)

#### [ケース4: グローバルルーティングルックアップに基づく転送](#)

#### [Null0インターフェイス](#)

#### [等コストマルチパス\(ECMP\)](#)

#### [FTD管理プレーン](#)

#### [FTD LINA診断インターフェイスルーティング](#)

---

## 概要

このドキュメントでは、Firepower脅威対策(FTD)がパケットを転送し、さまざまなルーティングの概念を実装する方法について説明します。

## 前提条件

### 要件

- ルーティングの基礎知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CiscoFirepower41xx Threat Defenseバージョン7.1.x
- Firepower Management Center(FMC)バージョン7.1.x

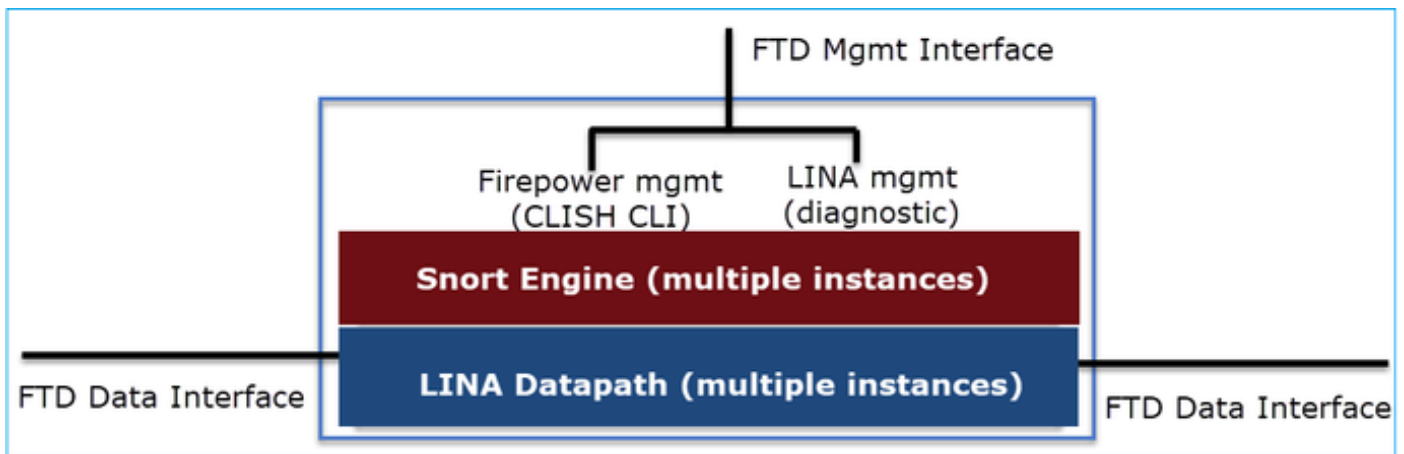
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### FTDパケット転送メカニズム

FTD は、2 つの主要なエンジンで構成される統合ソフトウェアイメージです。

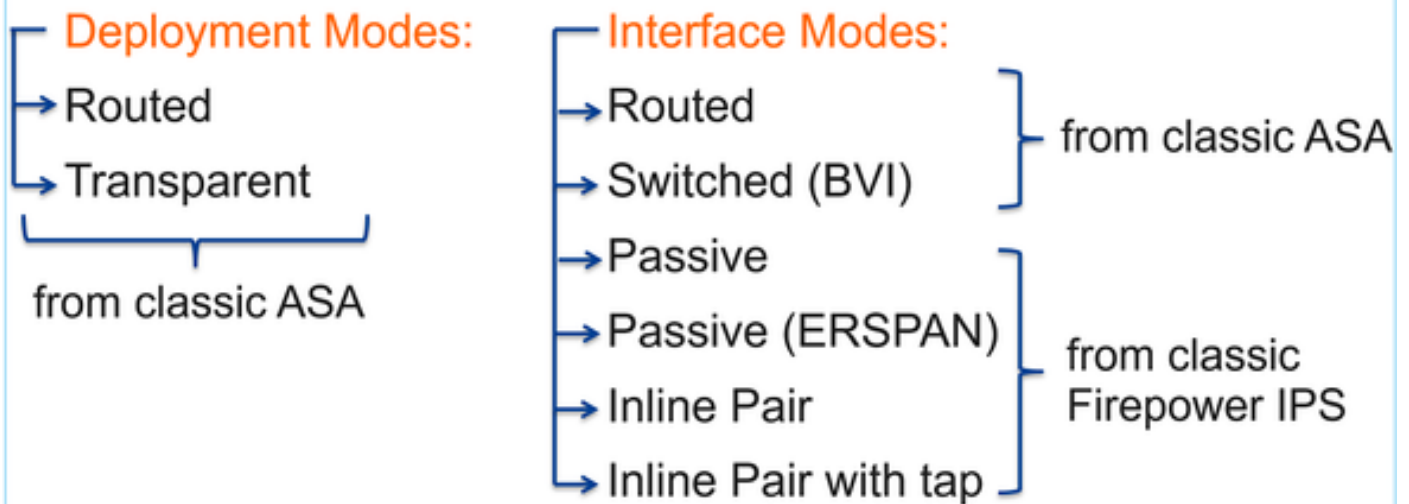
- データパスエンジン(LINA)
- Snortエンジン



データパスとSnortエンジンは、FTDのデータプレーンの主要部分です。

FTDデータプレーン転送メカニズムは、インターフェイスモードによって異なります。次の図は、さまざまなインターフェイスモードとFTD導入モードをまとめたものです。

# FTD Deployment and Interface Modes



次の表は、FTDがインターフェイスモードに基づいてパケットをデータプレーンで転送する方法をまとめたものです。転送メカニズムは、優先順位に従ってリストされます。

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

\*トランスパレントモードのFTDは、次のような状況でルートルックアップを実行します。

## 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.

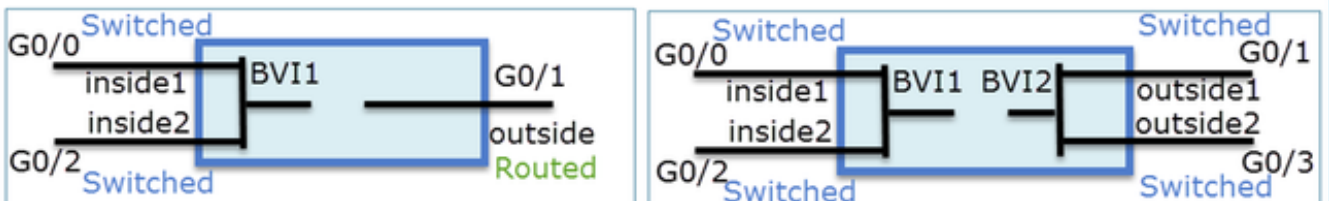


詳細については、『[FMCガイド](#)』を参照してください。

6.2.xバージョンから、FTDはIntegrated Routing and Bridging(IRB)をサポートしています。

## FTD Integrated Routing and Bridging (IRB)

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



BVI検証コマンド：

## 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
```

## キーポイント

ルーテッドインターフェイスまたはBVI(IRB)の場合、パケット転送は次の順序に基づきます。

- 接続ルックアップ
- NATルックアップ (宛先NAT、UN-NATとも呼ばれる)
- ポリシーベース ルーティング (PBR)
- グローバル ルーティング テーブルのルックアップ

送信元NATについてはどうですか。

グローバルルーティングルックアップの後、送信元NATがチェックされます。

このドキュメントの残りの部分では、ルーテッドインターフェイスモードについて説明します。

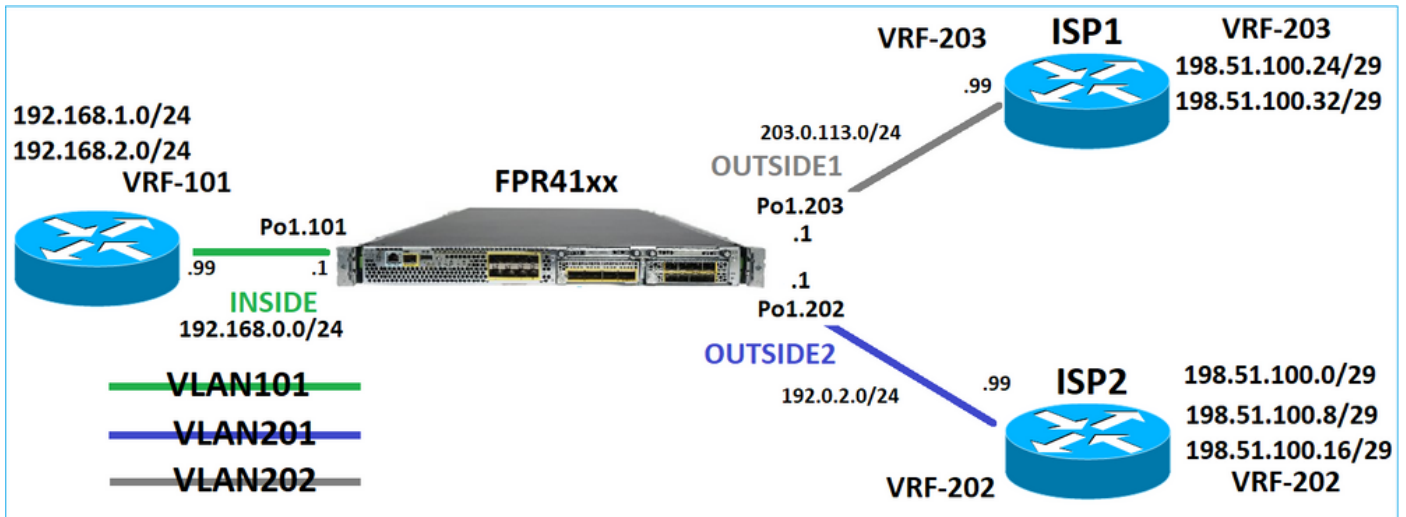
## データプレーン(LINA)ルーティングの動作

ルーテッドインターフェイスモードでは、FTD LINAがパケットを2フェーズで転送します。

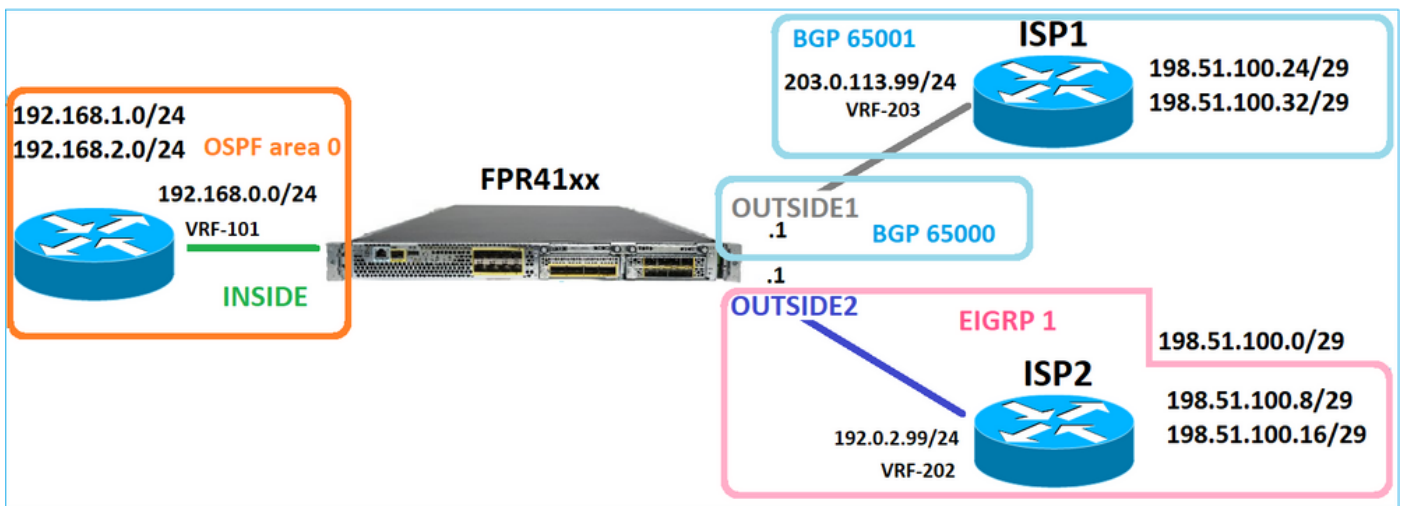
フェーズ1 – 出カインターフェイスの決定

フェーズ2 : ネクストホップの選択

このトポロジを参照してください。



このルーティング設計は次のとおりです。



FTDのルーティング設定 :

```
firepower# show run router
router ospf 1
network 192.168.0.0 255.255.255.0 area 0
log-adj-changes
!
router bgp 65000
bgp log-neighbor-changes
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 203.0.113.99 remote-as 65001
neighbor 203.0.113.99 ebgp-multihop 255
neighbor 203.0.113.99 transport path-mtu-discovery disable
neighbor 203.0.113.99 activate
no auto-summary
no synchronization
exit-address-family
!
router eigrp 1
no default-information in
no default-information out
no eigrp log-neighbor-warnings
```

```
no eigrp log-neighbor-changes
network 192.0.2.0 255.255.255.0
!
firepower# show run route
route OUTSIDE2 198.51.100.0 255.255.255.248 192.0.2.99 1
```

## FTDルーティング情報ベース(RIB) : コントロールプレーン :

```
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
```

## 対応するFTD Accelerated Security Path(ASP)ルーティングテーブル : データプレーン :

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

```

in fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out 255.255.255.255 255.255.255.255 OUTSIDE1
out 203.0.113.1 255.255.255.255 OUTSIDE1
out 203.0.113.0 255.255.255.0 OUTSIDE1
out 224.0.0.0 240.0.0.0 OUTSIDE1
out 255.255.255.255 255.255.255.255 OUTSIDE2
out 192.0.2.1 255.255.255.255 OUTSIDE2
out 198.51.100.0 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.8 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 198.51.100.16 255.255.255.248 via 192.0.2.99, OUTSIDE2
out 192.0.2.0 255.255.255.0 OUTSIDE2
out 224.0.0.0 240.0.0.0 OUTSIDE2
out 255.255.255.255 255.255.255.255 INSIDE
out 192.168.0.1 255.255.255.255 INSIDE
out 192.168.1.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.2.1 255.255.255.255 via 192.168.0.99, INSIDE
out 192.168.0.0 255.255.255.0 INSIDE
out 224.0.0.0 240.0.0.0 INSIDE
out 255.255.255.255 255.255.255.255 cmi_mgmt_int_tap
out 224.0.0.0 240.0.0.0 cmi_mgmt_int_tap
out 255.255.255.255 255.255.255.255 ha_ctl_nlp_int_tap
out 224.0.0.0 240.0.0.0 ha_ctl_nlp_int_tap
out 255.255.255.255 255.255.255.255 ccl_ha_nlp_int_tap
out 224.0.0.0 240.0.0.0 ccl_ha_nlp_int_tap
out 255.255.255.255 255.255.255.255 nlp_int_tap
out 169.254.1.1 255.255.255.255 nlp_int_tap
out 169.254.1.0 255.255.255.248 nlp_int_tap
out 224.0.0.0 240.0.0.0 nlp_int_tap
out fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap
out fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out fe80:: ffc0:: nlp_int_tap
out ff00:: ff00:: nlp_int_tap
out 0.0.0.0 0.0.0.0 via 0.0.0.0, identity
out :: :: via 0.0.0.0, identity

```

## 要点

FTD(適応型セキュリティアプライアンス(ASA)と同様の方法では、最初にパケットの出口 ( 出力 ) インターフェイスを決定します ( ASPルーティングテーブルの「in」エントリを参照します )。次に、決定されたインターフェイスに対して、ネクストホップの検索を試みます ( ネクストホップについては、ASPルーティングテーブルの「out」エントリを参照します )。例 :

```

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

```



最後に、解決されたネクストホップについて、LINAはARPキャッシュで有効な隣接関係を確認します。

FTDパケットトレーサツールによってこのプロセスを確認します。

```
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

コントロールプレーンに表示されるFTD ARPテーブル :

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

ARP解決を強制するには、次のコマンドを実行します。

```

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

```

データプレーンに表示されるFTD ARPテーブル :

```

firepower# show asp table arp

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

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

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

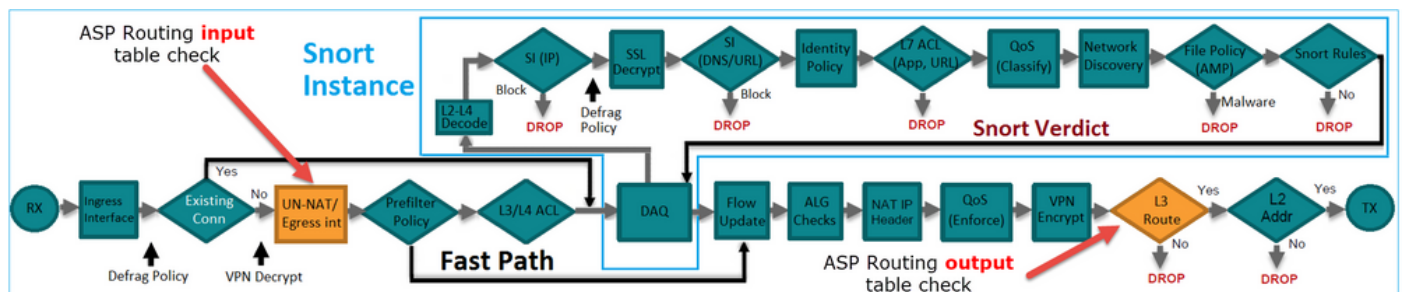
Context: single_vf, Interface: identity
:: Active 0000.0000.0000 hits 0 reference 0
0.0.0.0 Active 0000.0000.0000 hits 848 reference 0

Last clearing of hits counters: Never

```

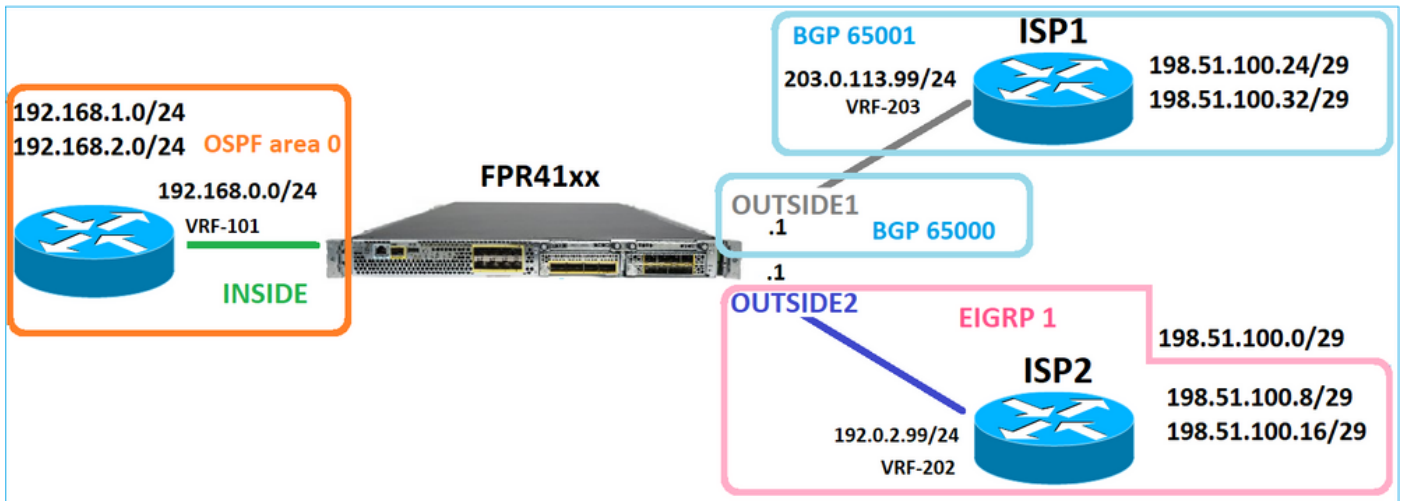
## FTDの処理順序

次の図は、動作の順序と、入出力ASPルーティングチェックが実行される場所を示しています。



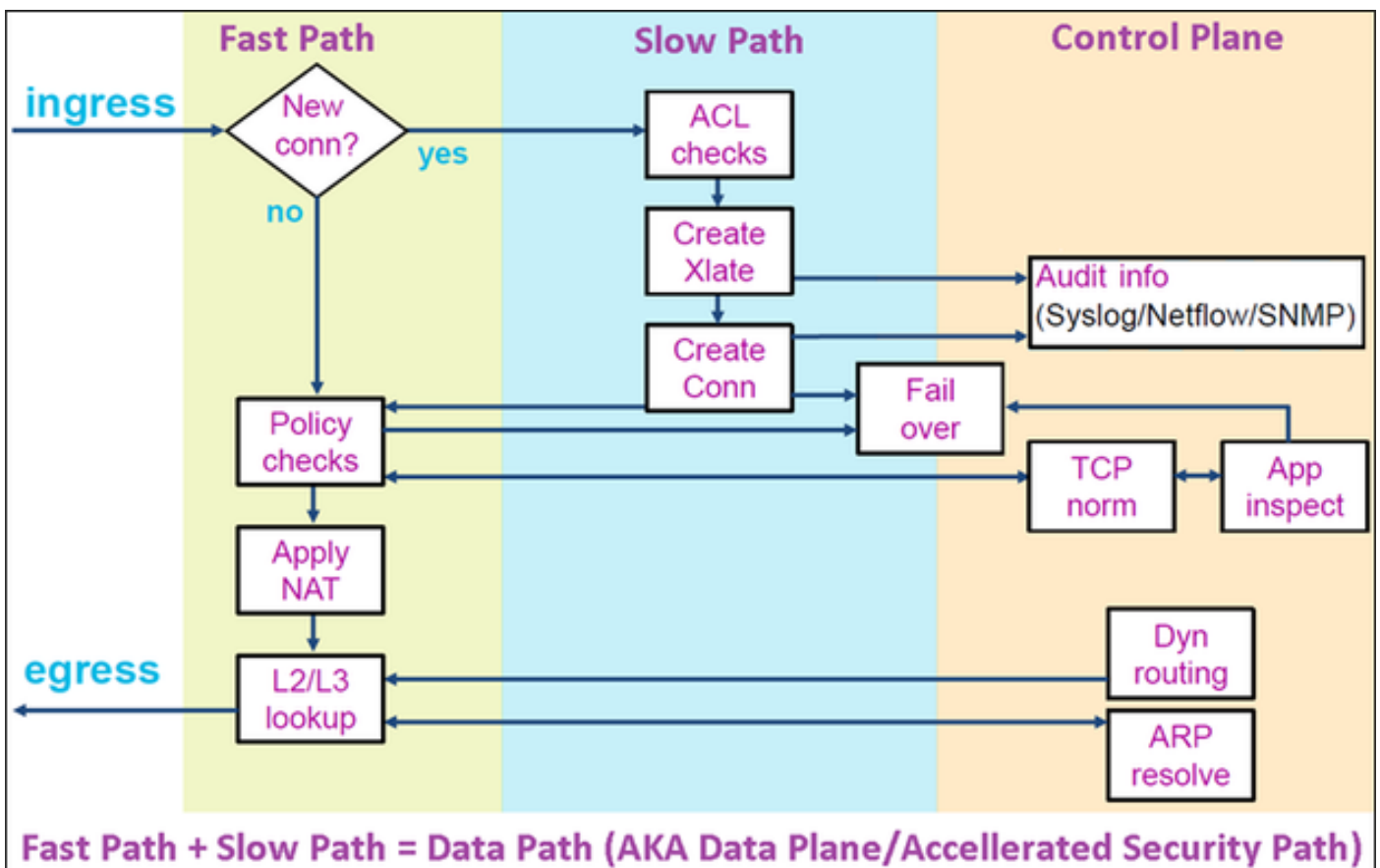
## 設定

ケース1：接続ルックアップに基づく転送



すでに述べたように、FTD LINAエンジンの主なコンポーネントはデータパスプロセスです（デバイスコアの数に基づいて複数のインスタンス）。さらに、Datapath（Accelerated Security Path - ASPとも呼ばれる）は、次の2つのパスで構成されます。

1. 低速パス=新しい接続の確立を担当（高速パスに入力）。
2. ファストパス=確立された接続に属するパケットを処理します。



- show routeやshow arpなどのコマンドは、コントロールプレーンの内容を表示します。
- 一方、show asp table routingやshow asp table arpなどのコマンドは、実際に適用されているASP(Datapath)の内容を表示します。

FTD INSIDEインターフェイスでトレースによるキャプチャを有効にします。

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

FTDを介してTelnetセッションを開きます。

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

FTDキャプチャは、接続の最初からのパケットを示します (TCP 3ウェイハンドシェイクがキャプチャされます)。

```
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)
...
```

最初のパケット(TCP SYN)をトレースします。このパケットはFTD LINA低速パスを通過し、この場合はグローバルルーティングルックアップが実行されます。

```
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#
```

同じフローから別の入力パケットをトレースします。アクティブな接続と一致するパケット :

```
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#

## フローティングタイムアウト

### 問題

一時的なルートの不安定性が原因で、FTDを介した長時間の（エレファントモードの）UDP接続が、意図とは異なるFTDインターフェイスを介して確立される可能性があります。

### 解決策

これを修正するには、timeout floating-connをデフォルト以外の無効な値に設定します。

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)	<span>?</span>
Translation Slot(xlate)	<input type="text" value="Default"/>	3:00:00	(3:0:0 or 0:1:0 - 1193:0:0)
Connection(Conn)	<input type="text" value="Default"/>	1:00:00	(0:0:0 or 0:5:0 - 1193:0:0)
Half-Closed	<input type="text" value="Default"/>	0:10:00	(0:0:0 or 0:0:30 - 1193:0:0)
UDP	<input type="text" value="Default"/>	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
ICMP	<input type="text" value="Default"/>	0:00:02	(0:0:2 or 0:0:2 - 1193:0:0)
RPC/Sun RPC	<input type="text" value="Default"/>	0:10:00	(0:0:0 or 0:1:0 - 1193:0:0)
H.225	<input type="text" value="Default"/>	1:00:00	(0:0:0 or 0:0:0 - 1193:0:0)
H.323	<input type="text" value="Default"/>	0:05:00	(0:0:0 or 0:0:0 - 1193:0:0)
SIP	<input type="text" value="Default"/>	0:30:00	(0:0:0 or 0:5:0 - 1193:0:0)
SIP Media	<input type="text" value="Default"/>	0:02:00	(0:0:0 or 0:1:0 - 1193:0:0)
SIP Disconnect:	<input type="text" value="Default"/>	0:02:00	(0:02:0 or 0:0:1 - 0:10:0)
SIP Invite	<input type="text" value="Default"/>	0:03:00	(0:1:0 or 0:1:0 - 0:30:0)
SIP Provisional Media	<input type="text" value="Default"/>	0:02:00	(0:2:0 or 0:1:0 - 0:30:0)
<b>Floating Connection</b>	<input type="text" value="Default"/>	0:00:00	(0:0:0 or 0:0:30 - 1193:0:0)
Xlate-PAT	<input type="text" value="Default"/>	0:00:30	(0:0:30 or 0:0:30 - 0:5:0)

『コマンドリファレンス :

<b>floating-conn</b>	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.
----------------------	--

詳細については、「ケーススタディ : CiscoLive BRKSEC-3020セッションからのリロード後のUDP接続の失敗 :

# Floating Connection Timeout

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

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

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

## Conn-holddownタイムアウト

### 問題

ルートはダウン ( 削除 ) しますが、トラフィックは確立された接続と一致します。

### 解決策

タイムアウトconn-holddown機能がASA 9.6.2で追加されました。この機能はデフォルトで有効になっていますが、現在(7.1.x)はFMC UIまたはFlexConfigでサポートされていません。関連する機能拡張：[ENH:timeout conn-holddownはFMCの設定には使用できません。](#)

ASA CLIガイドから：

<b>conn-holddown</b>	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
```

## ケース2:NATルックアップに基づく転送

### Requirement

次のNATルールを設定します。

- タイプ : スタティック
- 送信元インターフェイス : INSIDE
- 宛先インターフェイス : OUTSIDE1
- 元の送信元 : 192.168.1.1
- 元の宛先 : 198.51.100.1
- 翻訳元 : 192.168.1.1
- 変換後の宛先 : 198.51.100.1

### 解決方法

		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

FTD CLIに展開されたNATルール :

```
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
```

次の3つのキャプチャを設定します。

```
firepower# capture CAPI trace detail interface INSIDE match ip host 192.168.1.1 host 198.51.100.1
firepower# capture CAP01 interface OUTSIDE1 match ip host 192.168.1.1 any
firepower# capture CAP02 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 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
```

192.168.1.1から198.51.100.1へのtelnetセッションを開始します。

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

パケットはFTDに到着しますが、OUTSIDE1またはOUTSIDE2インターフェイスから発信するものは何也没有せん。

```
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
```

TCP SYNパケットをトレースします。フェーズ3(UN-NAT)は、NAT ( 具体的にはUN-NAT ) がネクストホップルックアップのためにパケットをOUTSIDE1インターフェイスに転送したことを示しています。

```
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

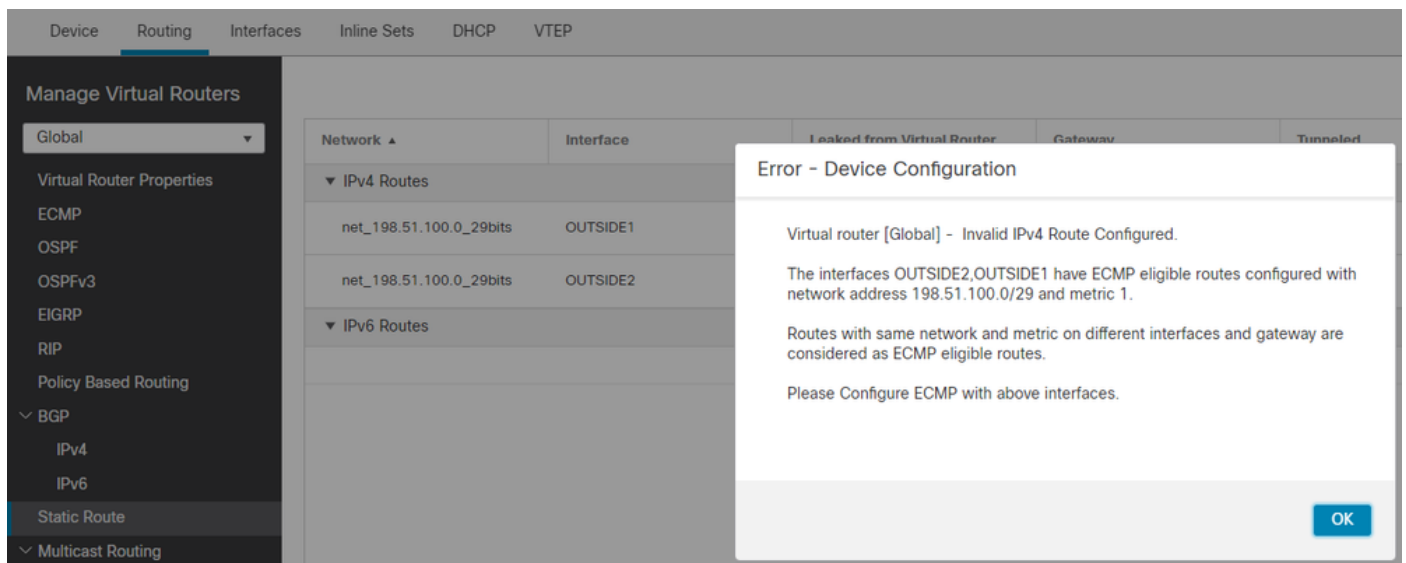
この場合、SUBOPTIMAL-LOOKUPは、NATプロセスによって決定された出カインターフェイス (OUTSIDE1)が、ASP入力テーブルで指定された出カインターフェイスとは異なることを意味します。

```
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
```


可能な回避策は、OUTSIDE1インターフェイスにフローティングスタティックルートを追加することです。

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

 注：既存のメトリックと同じメトリックを持つスタティックルートを追加しようとすると、次のエラーが表示されます。



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

 注：255のディスタンスメトリックを持つフローティングルートは、ルーティングテーブルにインストールされません。

FTDを介して送信されたパケットがあることをTelnetで確認します。

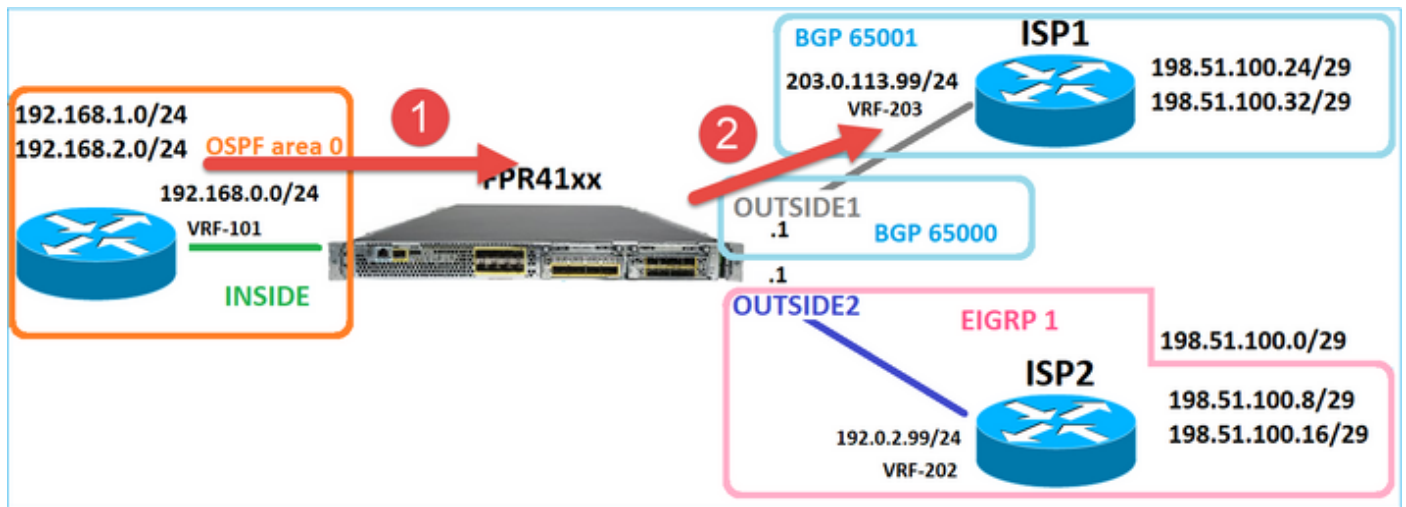
```
Router1# telnet 198.51.100.1 /vrf VRF-101 /source-interface lo1
Trying 198.51.100.1 ...
% Connection timed out; remote host not responding
```

```

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

```

パケットトレースは、NATルックアップにより、パケットがISP2ではなくISP1(OUTSIDE1)インターフェイスに転送されることを示しています。



```

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#
```

興味深いことに、この場合、INSIDEインターフェイスと両方の出カインターフェイスにパケットが表示されます。

```
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
```

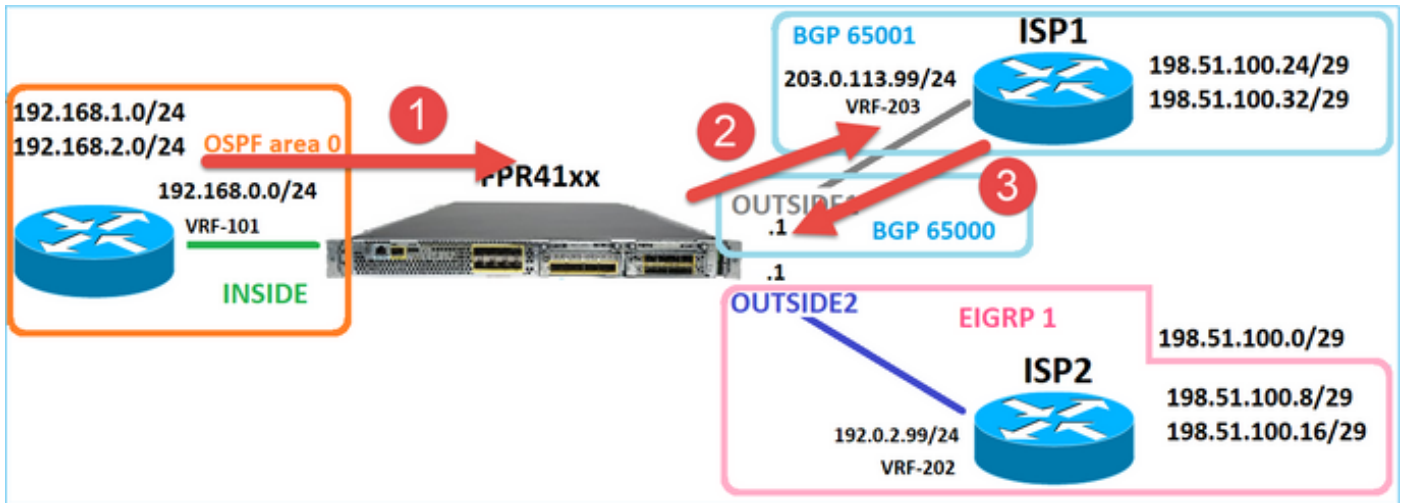
パケットの詳細にはMACアドレス情報が含まれ、OUTSIDE1およびOUTSIDE2インターフェイス上のパケットのトレースによってパケットのパスが明らかになります。

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

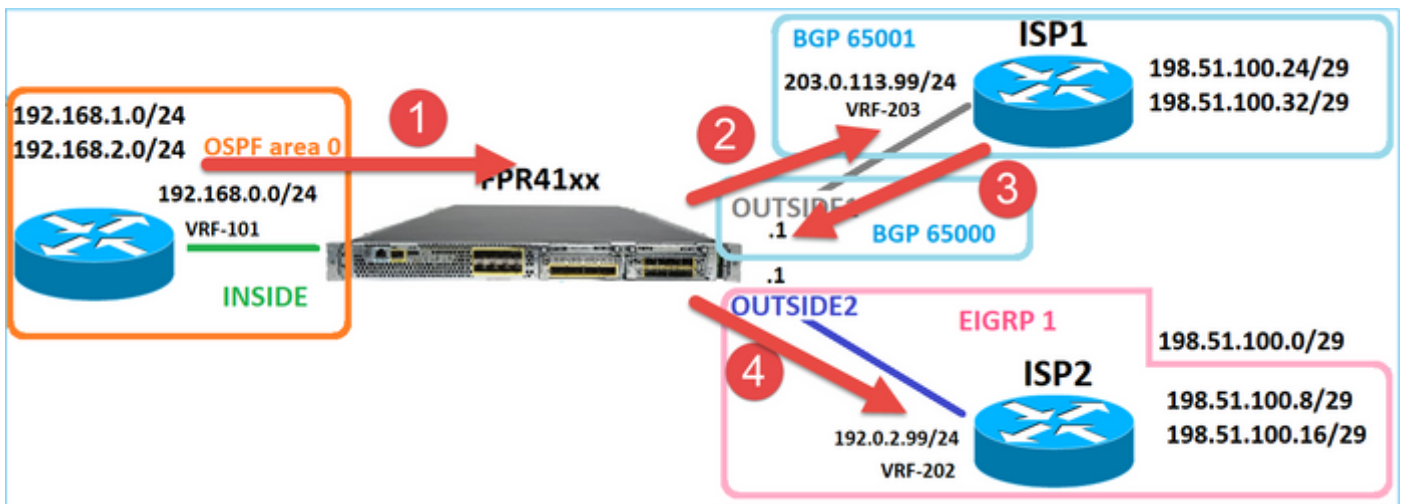
```
4 packets captured
```

```
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
```



戻るパケットのトレースは、グローバルルーティングテーブルの検索によるOUTSIDE2インターフェイスへのリダイレクションを示しています。



```
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)
```

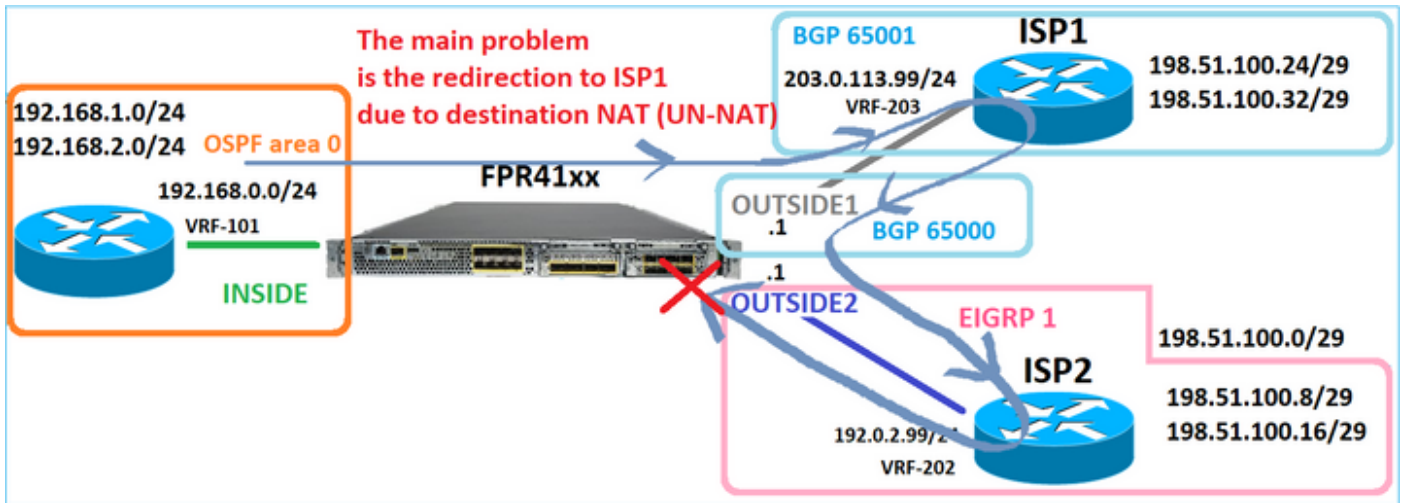
```
Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1338 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2
Adjacency :Active
MAC address 4c4e.35fc.fcd8 hits 0 reference 1
```

...

```
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#
```

ISP2ルータは応答(SYN/ACK)を送信しますが、このパケットは確立された接続と一致するため、ISP1にリダイレクトされます。ASP出力テーブルにL2隣接関係がないため、パケットはFTDによってドロップされます。



```
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
```



### ケース3：ポリシーベースルーティング(PBR)に基づく転送

接続フローのルックアップと宛先NATのルックアップの後、出インターフェイスの決定に影響を与える可能性がある次の項目はPBRです。PBRについては、『[ポリシーベースルーティング\(PBR\)](#)』

FMCでのPBR設定では、次のガイドラインに注意することが重要です。

FlexConfigは、7.1よりも前のバージョンのFTDに対してFMCでPBRを設定するために使用されました。FlexConfigを使用して、すべてのバージョンでPBRを設定できます。ただし、入インターフェイスでは、FlexConfigとFMCのポリシーベースルーティングページの両方を使用してPBRを設定することはできません。

このケーススタディでは、FTDにはISP2をポイントする198.51.100.0/24へのルートがあります。

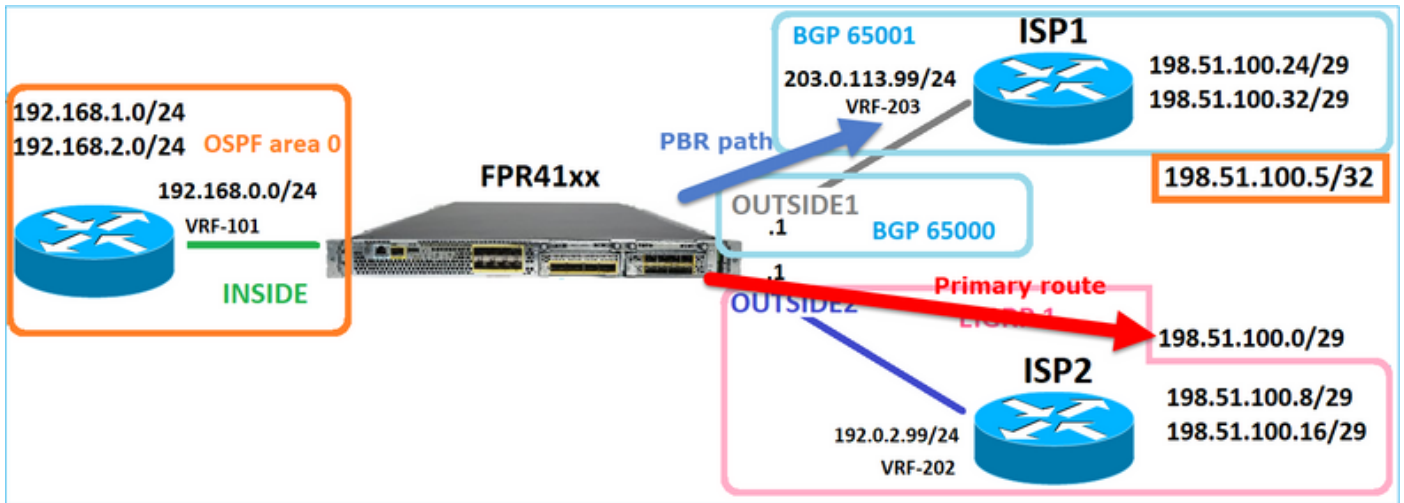
```
firepower# show route | begin Gate
Gateway of last resort is not set
```

```
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
```

#### Requirement

次の特性を持つPBRポリシーを設定します。

- IP 192.168.2.0/24から198.51.100.5宛てのトラフィックはISP1 (ネクストホップ 203.0.113.99) に送信される必要があり、他の送信元はOUTSIDE2インターフェイスを使用する必要があります。



## 解決方法

7.1よりも前のリリースでPBRを設定するには、次の手順を実行します。

- 1.対象トラフィック (たとえば、PBR\_ACL) に一致する拡張ACLを作成します。
- 2.ステップ1で作成したACLと一致するルートマップを作成し、目的のネクストホップを設定します。
- 3.ステップ2で作成したルートマップを使用して、入インターフェイスでPBRを有効にする FlexConfigオブジェクトを作成します。

7.1よりも前のリリースでは、7.1よりも前の方法を使用してPBRを設定できます。また、Device > Routingセクションで新しいPolicy Based Routingオプションを使用することもできます。

- 1.対象トラフィック (たとえば、PBR\_ACL) に一致する拡張ACLを作成します。
2. PBRポリシーを追加し、次を指定します。
  - a.一致するトラフィック
  - b.入インターフェイス
  - c.ネクストホップ

## PBRの設定 (新しい方法)

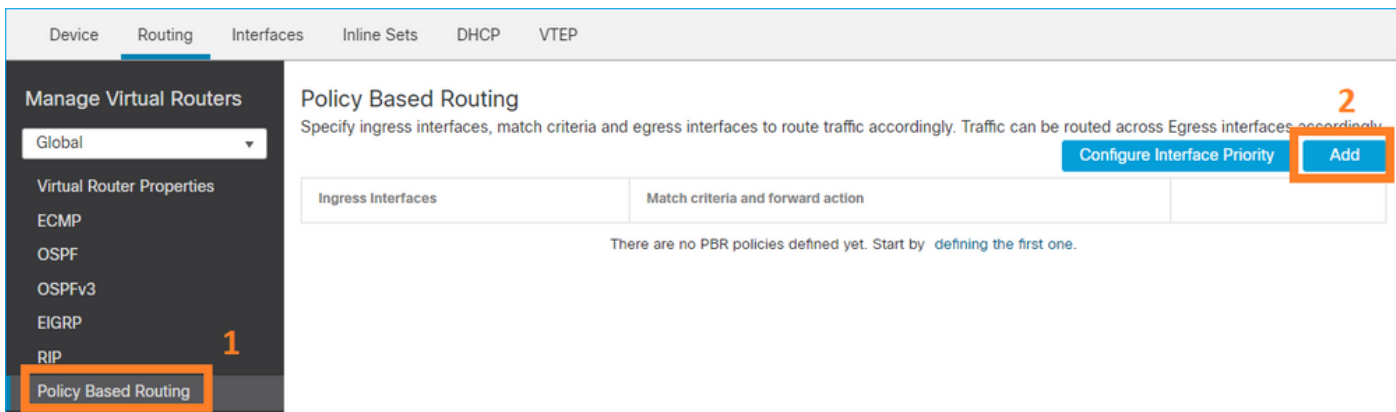
手順1：一致するトラフィックのアクセスリストを定義します。

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

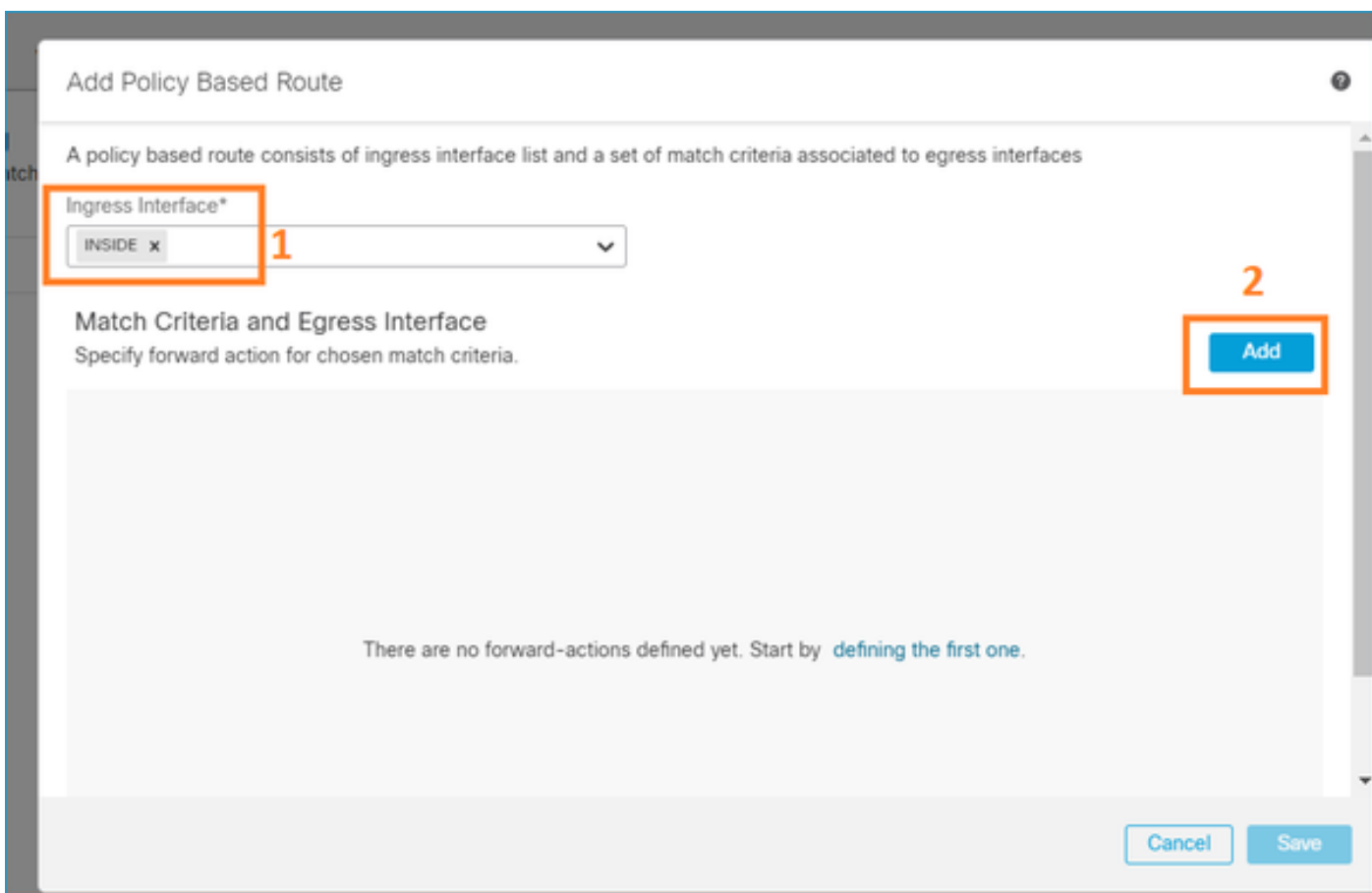
## 手順2:PBRポリシーの追加

Devices > Device Managementの順に移動し、FTDデバイスを編集します。Routing > Policy

Based Routingの順に選択し、Policy Based RoutingページでAddを選択します。



入インターフェイスを指定します。



転送アクションを指定します。

### Add Forwarding Actions


Match ACL:\*  1

Send To:\*  2

IPv4 Addresses  3

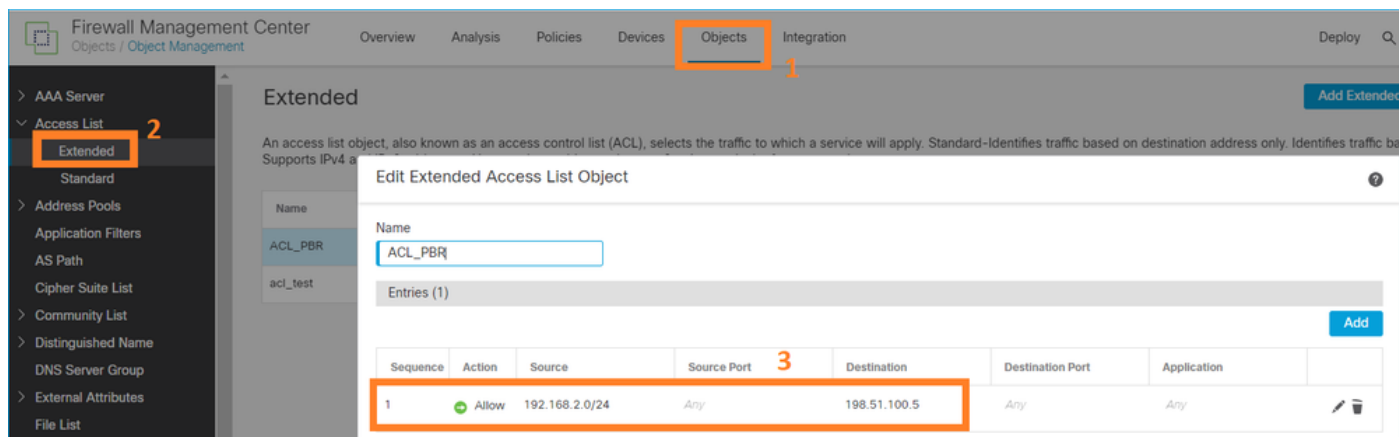
IPv6 Addresses

保存して展開します。

 注：複数の出カインターフェイスを設定する場合は、「Send To」フィールドで「Egress Interfaces」オプション（バージョン7.0+以降で使用可能）を設定する必要があります。詳細については、「[ポリシーベースルーティングの設定例](#)」を参照してください。

## PBRの設定（従来の方法）

手順1：一致するトラフィックのアクセスリストを定義します。



Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

AAA Server

Access List

**Extended** 2

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 and destination addresses. Supports IPv4 and IPv6.

Edit Extended Access List Object

Name

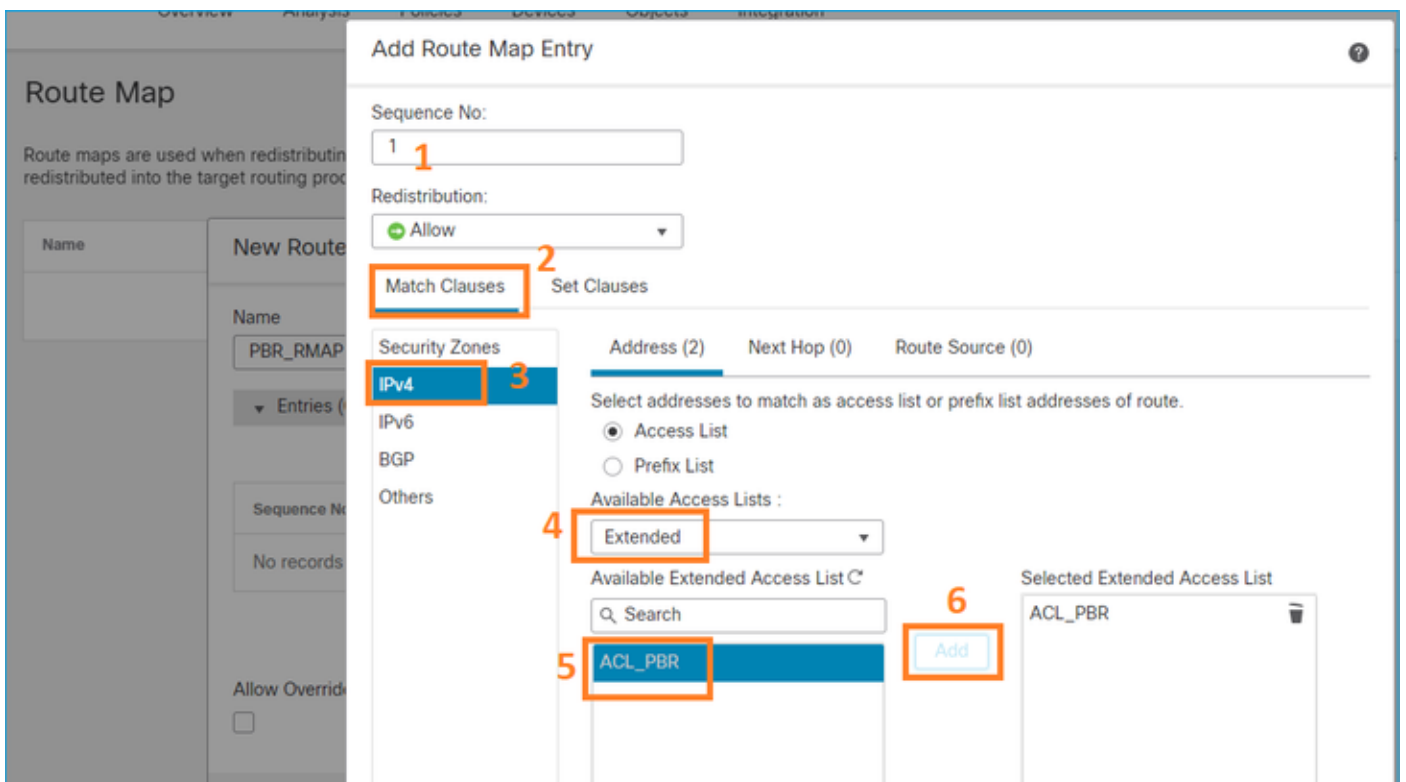
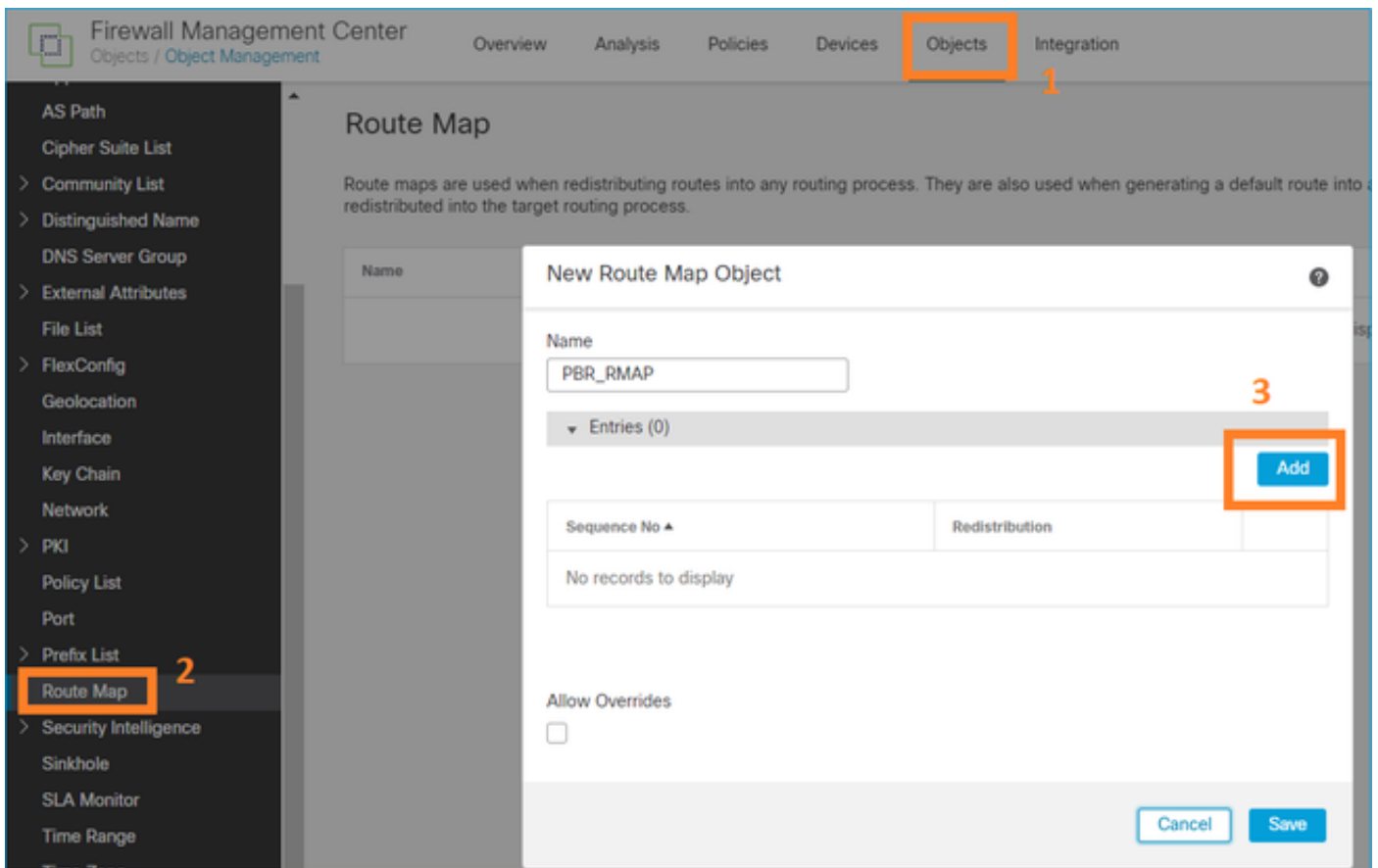
ACL\_PBR

Entries (1)

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

手順2:ACLに一致するルートマップを定義し、ネクストホップを設定します。

最初に、Match句を定義します。



Set句を定義します。

### 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:

追加して保存します。

手順3:FlexConfig PBRオブジェクトを設定します。

まず、既存のPBRオブジェクトをコピー（複製）します。

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 policies.

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

FlexConfig 1

**FlexConfig Object**

Text Object

Geolocation

オブジェクト名を指定し、定義済みのルートマップオブジェクトを削除します。

Add FlexConfig Object

Name: **1** FTD4100\_PBR **Specify a new name**

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

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

Insert | Deployment: Once | Type: Append

**2** interface Port-channel1.101 **Specify the correct ingress interface**

policy-route route-map Sr-map-object **3** route-map Sr-map-object **Remove this route-map**

新しいルートマップを指定します。

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.

**1** Insert | Deployment: Once | Type: Append

- Insert Policy Object
- Insert System Variable
- Insert Secret Key

- Text Object
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object
- 2** Route Map

### Insert Route Map Variable

Variable Name:  
 1

Description:

Available Objects

Search  2

PBR\_RMAP

3

Selected Object  
 PBR\_RMAP

最終的な結果は次のようになります。

### 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
```

手順4:FTD FlexConfigポリシーにPBRオブジェクトを追加します。



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
 

- FTD4100\_PBR** 1
- 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...

保存してPreview Configを選択します。

### 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

```

最後に、ポリシーを展開します。

 注：FlexConfigとFMC UIを同じ入カインターフェイスに使用してPBRを設定することはできません。

PBR SLA設定については、次のドキュメントを確認してください。 [FMCによって管理されるFTDのデュアルISPに対するIP SLAを使用したPBRの設定](#)

## PBRの検証

入インターフェイスの検証：

```
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
```

ルートマップの検証：

```
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)
```

ポリシールート of 検証：

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

変更前後のPacket-Tracer:

PBRなし	PBRを使用
<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>

実際のトラフィックを使用したテスト

トレースを使用してパケットキャプチャを設定します。

```
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
```

キャプチャは次のように表示されます。

```
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
```

TCP SYNパケットのトレース：

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

44 packets captured

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

Phase: 3

Type: SUBOPTIMAL-LOOKUP

Subtype: suboptimal next-hop

Result: ALLOW

Elapsed time: 13826 ns

Config:

Additional Information:

Input route lookup returned ifc OUTSIDE2 is not same as existing ifc OUTSIDE1

Phase: 4

Type: ECMP load balancing

Subtype:

Result: ALLOW

Elapsed time: 1784 ns

Config:

Additional Information:

ECMP load balancing

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

Phase: 5

Type: PBR-LOOKUP

Subtype: policy-route

Result: ALLOW

Elapsed time: 446 ns

Config:

route-map FMC\_GENERATED\_PBR\_1649228271478 permit 5

match ip address ACL\_PBR

set adaptive-interface cost OUTSIDE1

Additional Information:

Matched route-map FMC\_GENERATED\_PBR\_1649228271478, sequence 5, permit

Found next-hop 203.0.113.99 using egress ifc OUTSIDE1

...

Phase: 15

Type: ADJACENCY-LOOKUP

Subtype: Resolve Nexthop IP address to MAC

Result: ALLOW

Elapsed time: 4906 ns

Config:

Additional Information:

Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1

Adjacency :Active

MAC address 4c4e.35fc.fcd8 hits 348 reference 2

...

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE1(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 222106 ns

ASP PBRテーブルにポリシーヒットカウントが表示されません。

```
firepower# show asp table classify domain pbr
```

Input Table

in id=0x1505f26d3420, priority=2147483642, domain=pbr, deny=false

hits=7, user\_data=0x1505f26e7590, cs\_id=0x0, use\_real\_addr, flags=0x0, protocol=0

src ip/id=192.168.2.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=198.51.100.5, mask=255.255.255.255, port=0, tag=any, dscp=0x0, nsg\_id=none

input\_ifc=INSIDE(vrfid:0), output\_ifc=any


Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never


---

 注：パケットトレーサはヒットカウンタも増加させます。

---

## PBRデバッグ

---

 警告：実稼働環境では、デバッグによって多くのメッセージが生成される可能性があります。

---

次のデバッグを有効にします。

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

実際のトラフィックの送信：


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

デバッグには次のように表示されます。

```
firepower#
```

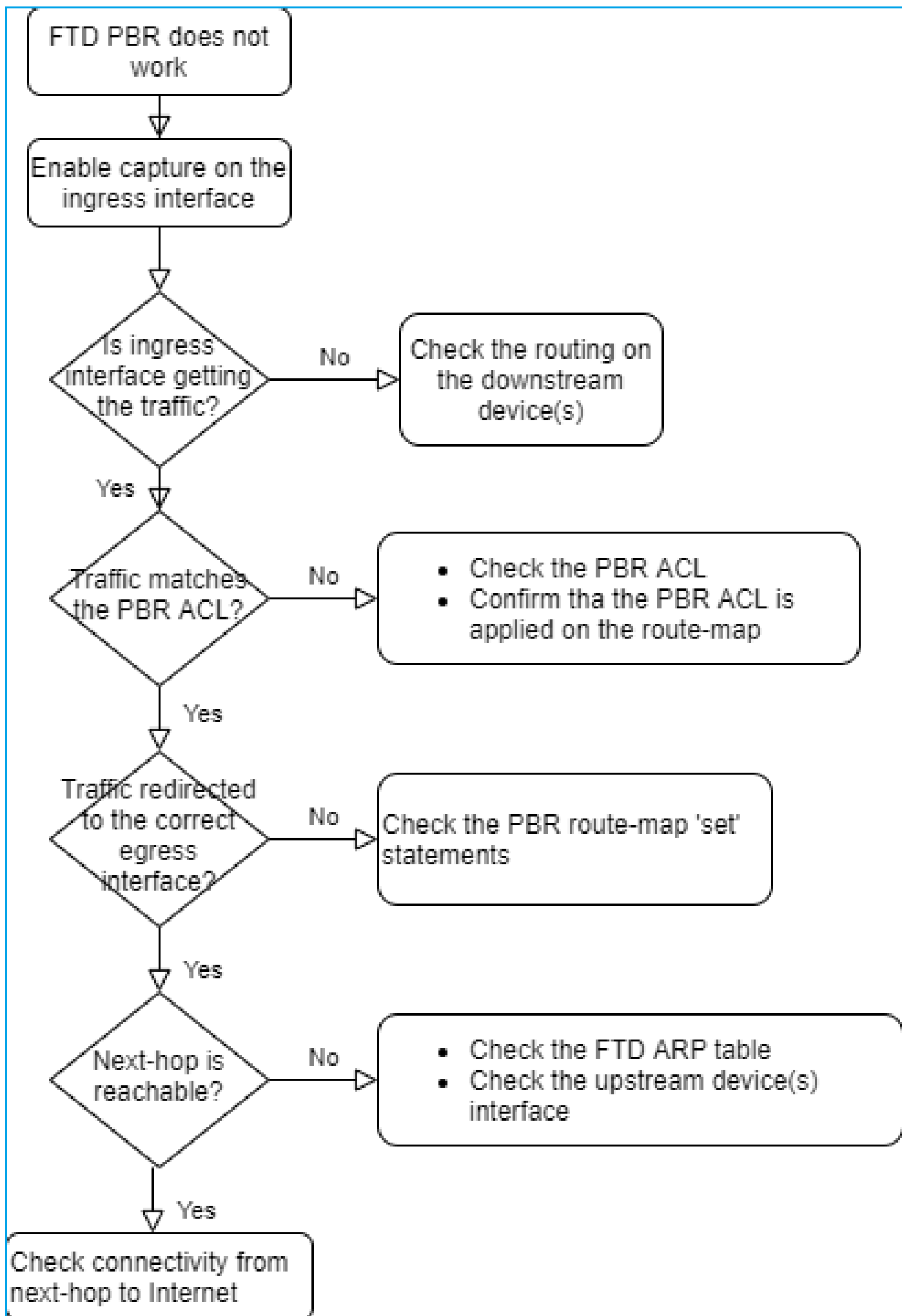
```
pbr: policy based route lookup called for 192.168.2.1/37256 to 198.51.100.5/23 proto 6 sub_proto 0 rece
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1649228271478, sequence 5, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = OUTSIDE1 : next_hop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

---

 注：Packet-Tracerでもデバッグ出力が生成されます。

---

このフローチャートは、PBRのトラブルシューティングに使用できます。



show asp drop

## ケース4：グローバルルーティングルックアップに基づく転送

接続ルックアップ、NATルックアップ、およびPBRの後、出カインターフェイスを決定するために最後にチェックされる項目は、グローバルルーティングテーブルです。

ルーティングテーブルの確認

FTDルーティングテーブルの出力を調べます。

```
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
```

ルーティングプロセスの主な目的は、ネクストホップを見つけることです。ルートを選択は次の順序になります。

1. 最長一致による勝利
2. 最も低いAD (異なるルーティングプロトコルソース間)
3. 最小メトリック (ルートが同じ送信元から学習された場合 - ルーティングプロトコル)

ルーティングテーブルへのデータの入力方法：

- IGP(R, D, EX, O, IA, N1, N2, E1, E2, i, su, L1, L2, ia, o)
- BGP(B)
- BGP InterVRF(BI)
- スタティック(S)
- スタティックInterVRF(SI)
- 接続済み(C)



- ローカルIP(L)

- VPN(V)

-再配布

-デフォルト

ルーティングテーブルの要約を表示するには、次のコマンドを使用します。

```
<#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
<b>Total</b>	<b>7</b>	<b>15</b>	<b>0</b>	<b>1360</b>	<b>7560</b>

次のコマンドを使用して、ルーティングテーブルの更新を追跡できます。

```
<#root>
```

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

たとえば、OSPFルート192.168.1.0/24がグローバルルーティングテーブルから削除された場合のデバッグの表示を次に示します。

```
<#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
```

再び追加されると、次のようになります。

```
<#root>
```

```
firepower#
```

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

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

## Null0インターフェイス

Null0インターフェイスは、不要なトラフィックをドロップするために使用できます。この廃棄は、アクセスコントロールポリシー(ACL)ルールによるトラフィックの廃棄よりもパフォーマンスへの影響が少ない。

### Requirement

198.51.100.4/32ホストのNull0ルートを設定します。

### 解決方法

The screenshot shows the Cisco Firepower 4140 Threat Defense configuration interface. The main window displays the 'Add Static Route Configuration' dialog. The dialog is open to the 'Static Route' configuration page. The 'Interface' dropdown is set to 'Null0'. The 'Available Network' list contains 'host\_198.51.100.4', which is selected. The 'Selected Network' list also contains 'host\_198.51.100.4'. The 'Add' button is highlighted. The 'Gateway' field is empty. The 'Metric' field is empty. The background shows the 'Manage Virtual Routers' sidebar with 'Static Route' selected under 'IPv6'.

保存して展開します。

検証：

```
<#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
```

リモートホストへのアクセスを試みます。

```
<#root>
```

```
Router1#
```

```
ping vrf VRF-101 198.51.100.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 198.51.100.4, timeout is 2 seconds:
```

```
.....
```

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

FTD のログは次のとおりです。

```
<#root>
```

```
firepower#
```

```
show log | include 198.51.100.4
```

```
Apr 12 2022 12:35:28:
```

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

ASPドロップの表示：

```
<#root>
firepower#
show asp drop
```

Frame drop:

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

## 等コストマルチパス(ECMP)

### トラフィックゾーン

- ECMPトラフィックゾーンを使用すると、ユーザはインターフェイスをグループ化できます ( ECMPゾーンと呼ばれます )。
- これにより、ECMPルーティングと、複数のインターフェイス間でのトラフィックのロードバランシングが可能になります。
- インターフェイスがECMPトラフィックゾーンに関連付けられている場合、ユーザはインターフェイス全体で等コストスタティックルートを作成できます。等コストスタティックルートは、同じ宛先ネットワークへの同じメトリック値を持つルートです。

バージョン7.1より前のFirepower Threat Defenseでは、FlexConfigポリシーを使用したECMPルーティングがサポートされていました。7.1リリースから、インターフェイスをトラフィックゾーンにグループ化し、Firepower Management CenterでECMPルーティングを設定できるようになりました。

EMCPは、[ECMP](#)で文書化されています。

この例では、非対称ルーティングがあり、リターントラフィックはドロップされます。

```
<#root>
firepower#
show log
```

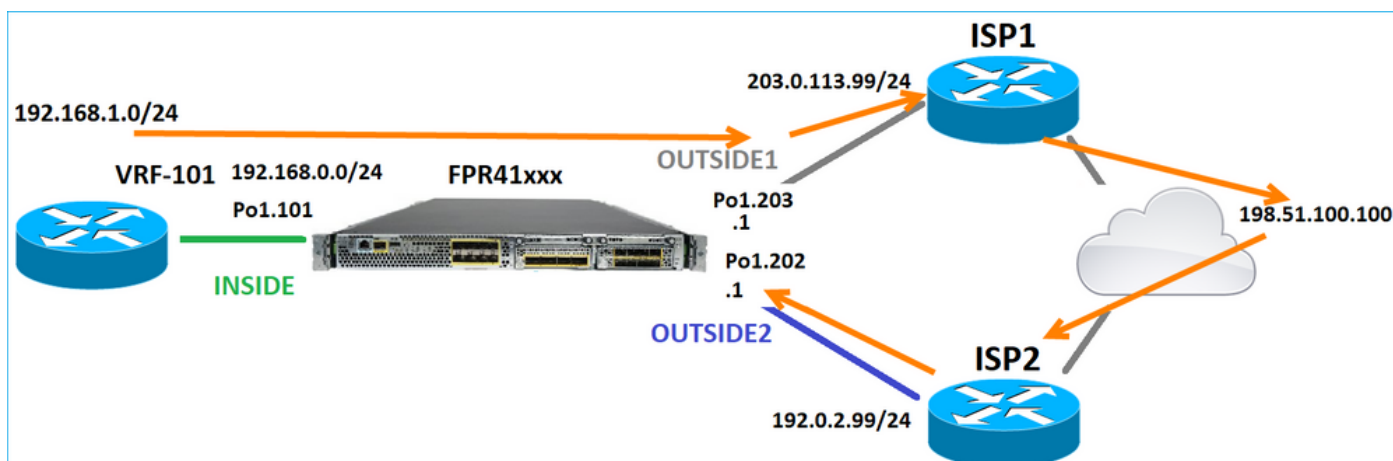
```
Apr 13 2022 07:20:48: %FTD-6-302013:
```

```
B
```

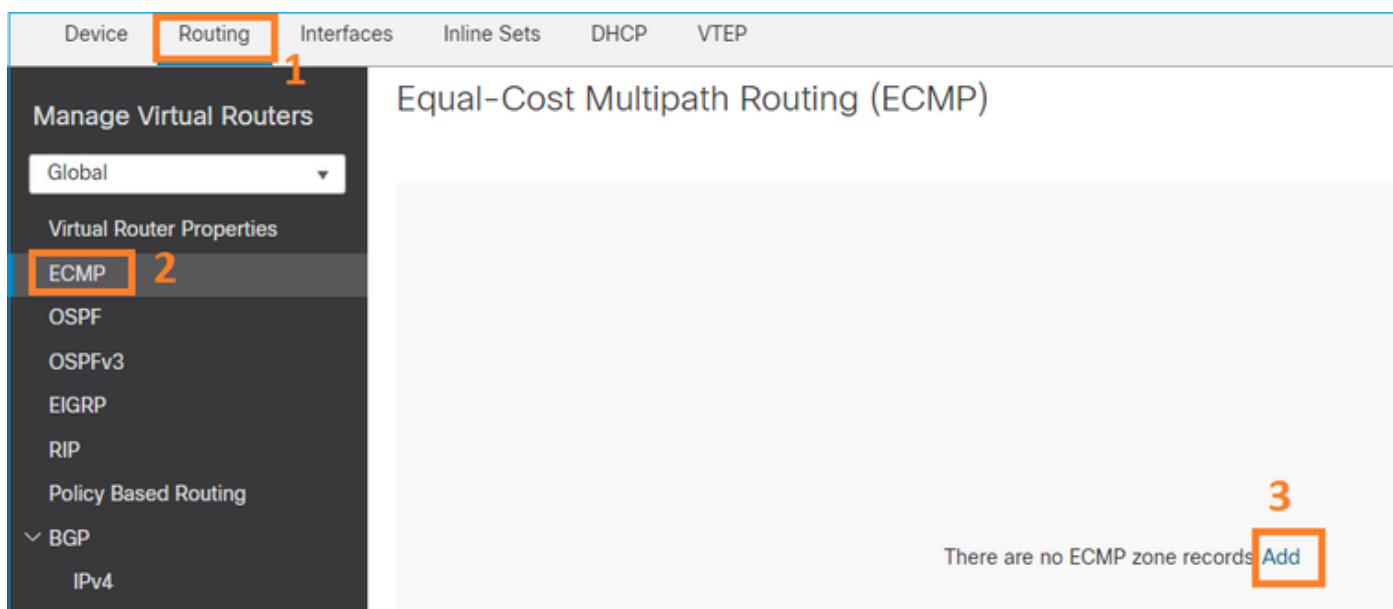
```
uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE1:198.51.100.100
```

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

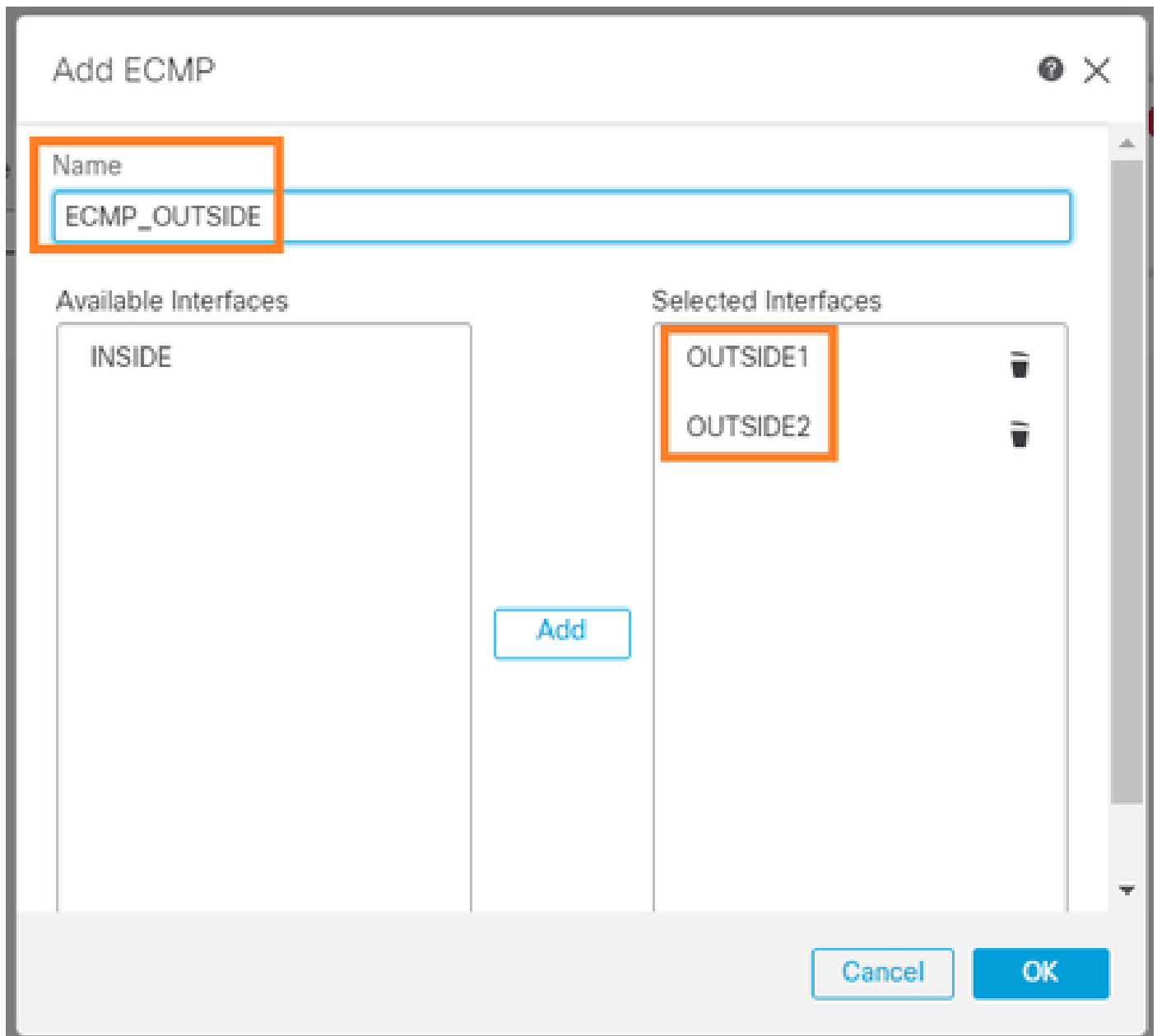
Deny TCP (no connection) from 198.51.100.100/23 to 192.168.1.1/23943 flags SYN ACK on interface OUTSIDE2



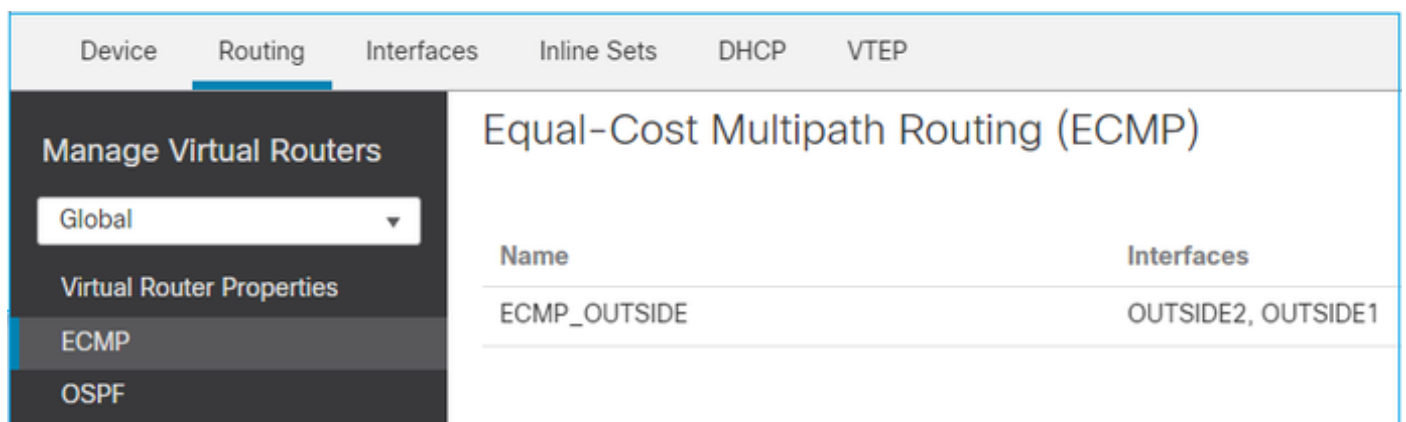
FMC UIからECMPを設定します。



ECMPグループに2つのインターフェイスを追加します。



結果は、次のとおりです。



保存して展開します。

ECMPゾーンの検証：

<#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
```

インターフェイスの検証:

<#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
```

これで、リターントラフィックが許可され、接続がUPになりました。

```
<#root>
```

```
Router1#
```

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

```
Trying 198.51.100.100 ... Open
```

ISP1インターフェイスのキャプチャは、出カトラフィックを示しています。

```
<#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
```

ISP2インターフェイスのキャプチャは、リターントラフィックを示しています。

```
<#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

## FTD管理プレーン

FTDには2つの管理プレーンがあります。

- Management0インターフェイス : Firepowerサブシステムへのアクセスを提供します。
- LINA診断インターフェイス : FTD LINAサブシステムへのアクセスを提供します。

Management0インターフェイスを設定および確認するには、それぞれconfigure networkコマンドとshow networkコマンドを使用します。

一方、LINAインターフェイスはLINA自体へのアクセスを提供します。FTD RIBのFTDインターフェイスエントリは、ローカルルートとして表示できます。

```
<#root>
```

```
firepower#
```

```
show route | include L
```

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

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
```

```
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
```

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

同様に、これらはASPルーティングテーブルでIDエントリとして表示される場合があります。

```
<#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
```

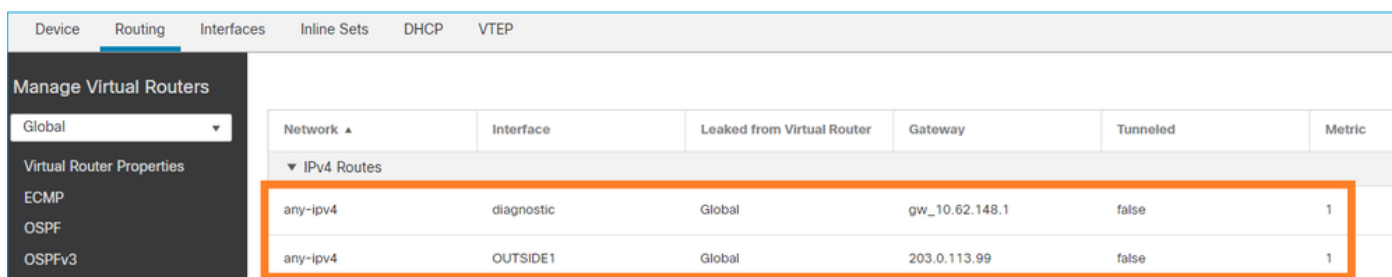
## 主要ポイント

パケットがFTDに到着し、宛先IPがアイデンティティIPの1つと一致すると、FTDはパケットを消費する必要があることを認識します。

## FTD LINA診断インターフェイスルーティング

FTD ( 9.5以降のコードを実行するASAなど ) は、管理専用として設定されているインターフェイスに対して、VRFに似たルーティングテーブルを維持します。このようなインターフェイスの例として、診断インターフェイスがあります。

FMCでは ( ECMPを使用せずに ) 同じメトリックを持つ2つの異なるインターフェイスに2つのデフォルトルートを設定できませんが、FTDデータインターフェイスに1つのデフォルトルートを設定し、診断インターフェイスに別のデフォルトルートを設定できます。



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

データプレーントラフィックはグローバルテーブルデフォルトゲートウェイを使用し、管理プレーントラフィックは診断デフォルトゲートウェイを使用します。

```
<#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
```

グローバルルーティングテーブルゲートウェイ :

```
<#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
```

FTDからトラフィックを送信する ( ボックスからトラフィックを送信する ) 場合、出カインターフェイスは次に基づいて選択されます。

1. グローバルルーティングテーブル
2. 管理専用ルーティングテーブル

出カインターフェイスを手動で指定すると、出カインターフェイスの選択を上書きできます。

診断インターフェイスゲートウェイへのpingを試行します。送信元インターフェイスを指定しない場合、FTDは最初にグローバルルーティングテーブルを使用するため、pingは失敗します。この場合、FTDにはデフォルトルートが含まれています。グローバルテーブルにルートがない場合、FTDは管理専用ルーティングテーブルでルートルックアップを実行します。

```
<#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
```

copyコマンドを使用してLINA CLIからファイルをコピーする場合も同じです。

## 双方向フォワーディング検出(BFD)

BFDのサポートは従来のASAバージョン9.6で追加され、BGPプロトコルに対してのみ追加されました：[双方向フォワーディング検出ルーティング](#)

FTD：

- BGP IPv4およびBGP IPv6プロトコルがサポートされています (ソフトウェア6.4)。
- OSPFv2、OSPFv3、およびEIGRPプロトコルはサポートされていません。
- スタティックルートのBFDはサポートされていません。

## 仮想ルータ(VRF)

VRFサポートは6.6リリースで追加されました。詳細については、このドキュメントの「[仮想ルータの設定例](#)」を参照してください。

## 関連情報

- [FTDのスタティックルートとデフォルトルート](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。