

# firepower 위협 방어 라우팅 문제 해결

## 목차

---

### [소개](#)

### [사전 요구 사항](#)

#### [요구 사항](#)

#### [사용되는 구성 요소](#)

#### [배경 정보](#)

##### [FTD 패킷 전달 메커니즘](#)

##### [요점](#)

##### [LINA\(데이터 플레인\) 라우팅 동작](#)

##### [핵심 사항](#)

##### [FTD 운영 순서](#)

### [구성](#)

#### [케이스 1 - 연결 조회를 기반으로 전달](#)

##### [부동 시간 초과](#)

##### [Conn-holddown 시간 초과](#)

#### [케이스 2 - NAT 조회 기반 전달](#)

#### [사례 3 - PBR\(Policy Based Routing\) 기반 전달](#)

#### [사례 4 - 글로벌 라우팅 조회를 기반으로 한 전달](#)

#### [Null0 인터페이스](#)

#### [ECMP\(동일 비용 다중 경로\)](#)

#### [FTD 관리 플레인](#)

#### [FTD LINA 진단 인터페이스 라우팅](#)

---

## 소개

이 문서에서는 FTD(Firepower Threat Defense)가 패킷을 전달하고 다양한 라우팅 개념을 구현하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

- 기본 라우팅 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 41xx Threat Defense 버전 7.1.x

- FMC(Firepower Management Center) 버전 7.1.x

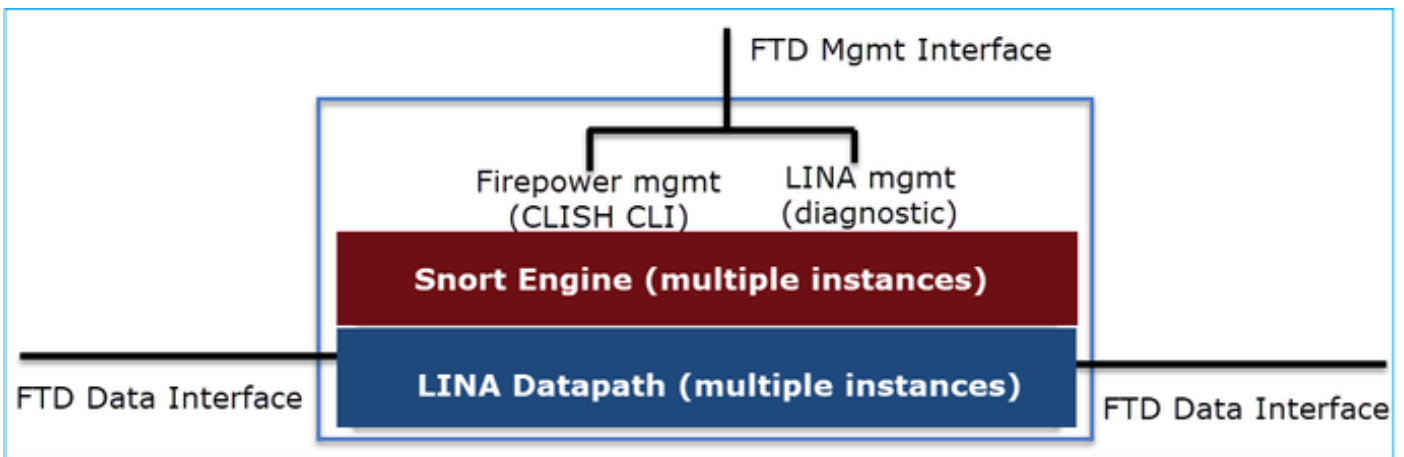
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

### FTD 패킷 전달 메커니즘

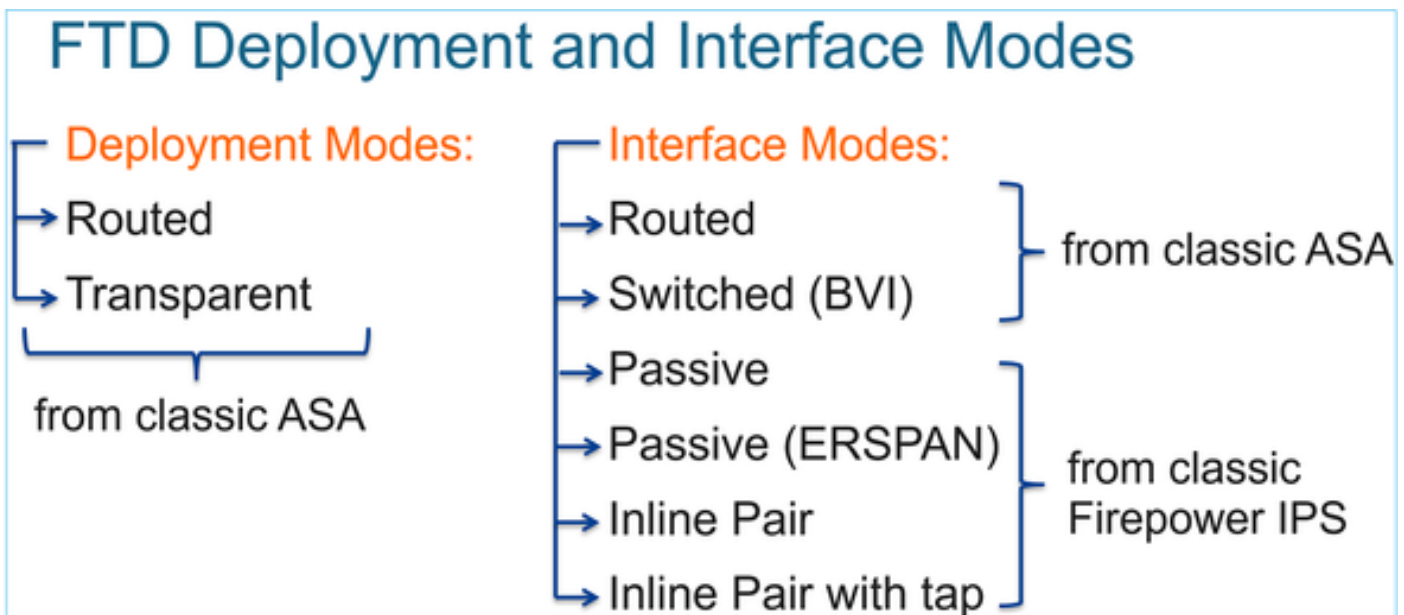
FTD는 2개의 주 엔진으로 구성된 통합 소프트웨어 이미지입니다.

- 데이터 경로 엔진(LINA)
- Snort 엔진



Datapath 및 Snort 엔진은 FTD 데이터 프레임의 주요 부분입니다.

FTD 데이터 프레임 포워딩 메커니즘은 인터페이스 모드에 따라 달라집니다. 다음 그림에는 FTD 구축 모드와 함께 다양한 인터페이스 모드가 요약되어 있습니다.



이 표에서는 FTD가 인터페이스 모드를 기반으로 데이터 평면에서 패킷을 전달하는 방법을 요약합니다. 전달 메커니즘은 환경 설정 순서대로 나열되어 있습니다.

| FTD Deployment mode   | FTD Interface mode   | Forwarding Mechanism  |
|-----------------------|----------------------|---|
| Routed                | Routed               | Packet forwarding based on the following order:<br>1. Connection lookup<br>2. Nat lookup (xlate)<br>3. Policy Based Routing (PBR)<br>4. Global routing table lookup |
| Routed or Transparent | Switched (BVI)       | 1. NAT lookup<br>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  |

\* 투명 모드의 FTD는 경우에 따라 경로 조회를 수행합니다.

### 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.

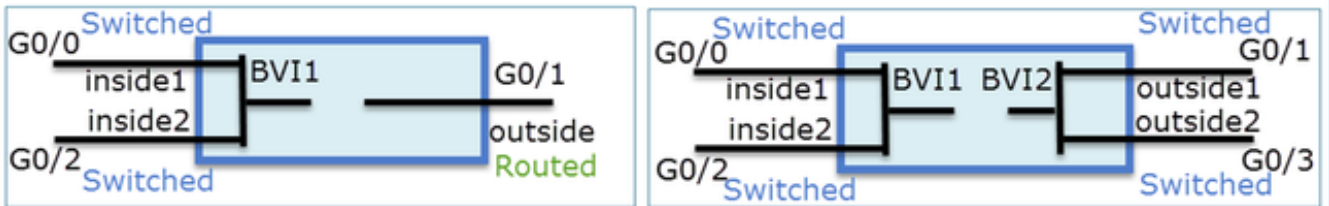


자세한 내용은 [FMC 가이드](#)를 참조하십시오.

6.2.x 버전에서처럼 FTD는 IRB(Integrated Routing and Bridging)를 지원합니다.

## 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 확인 명령:

### 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
```

요점

라우티드 인터페이스 또는 BVI(IRB)의 경우 패킷 전달은 다음 순서를 기반으로 합니다.

- 연결 조회
- NAT 조회(수신 NAT, UN-NAT라고도 함)
- PBR(Policy-Based Routing)
- 전역 라우팅 테이블 조회

소스 NAT는 어떻습니까?

전역 라우팅 조회 후 소스 NAT가 선택됩니다.

이 문서의 나머지 부분에서는 라우티드 인터페이스 모드에 중점을 둡니다.

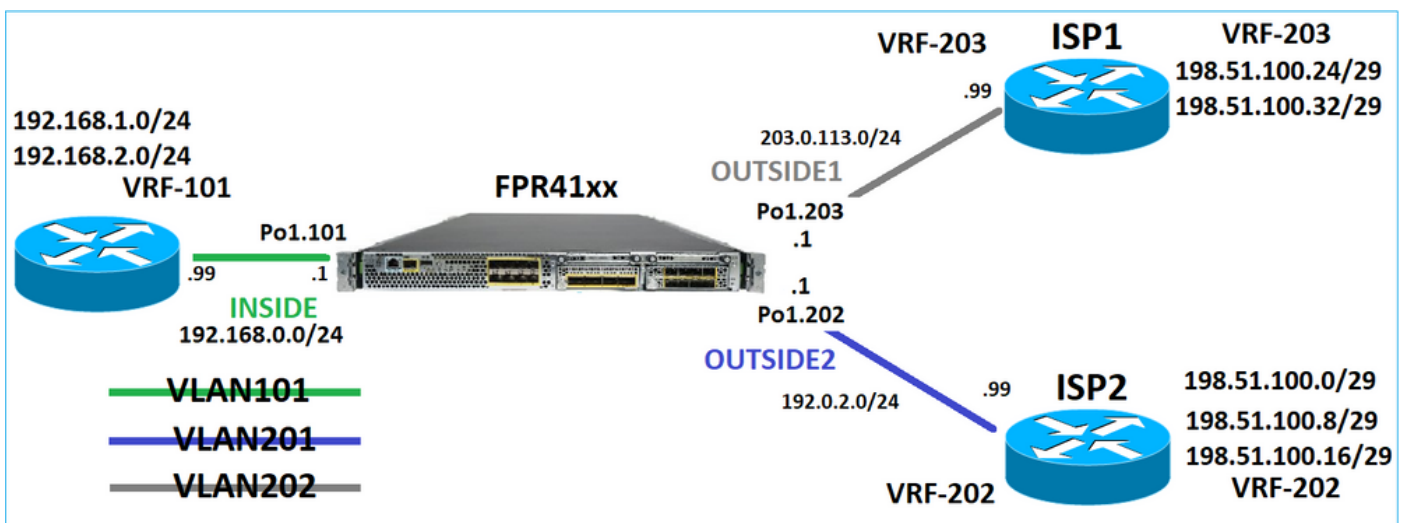
LINA(데이터 플레인) 라우팅 동작

라우티드 인터페이스 모드에서 FTD LINA는 2단계로 패킷을 전달합니다.

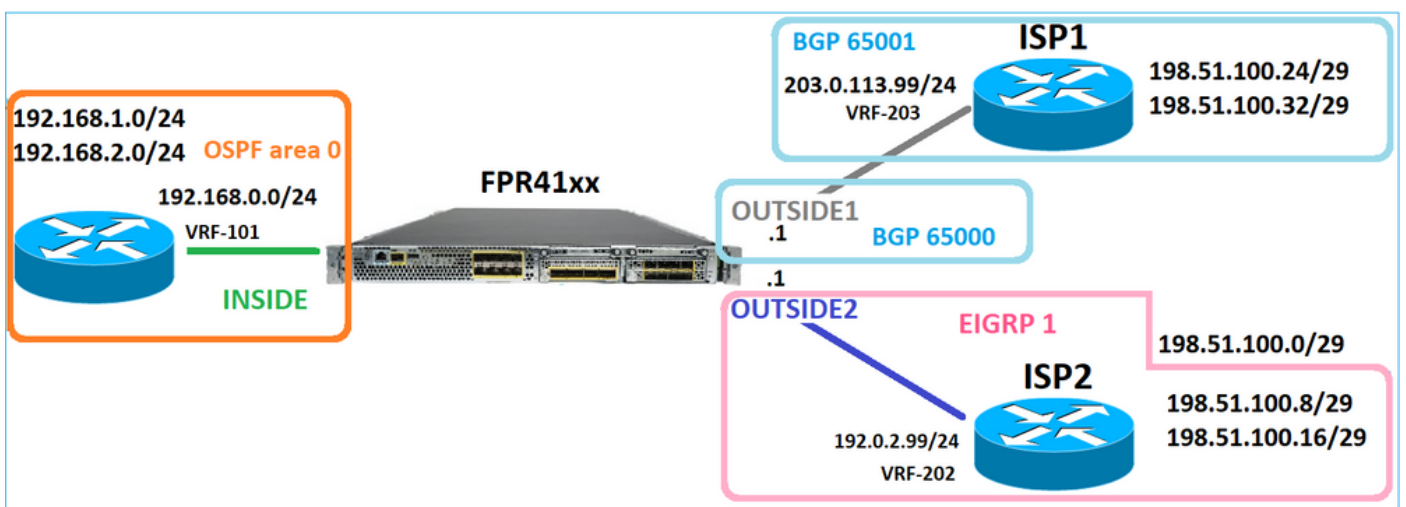
1단계 - 이그레스 인터페이스 결정

2단계 - Next-Hop 선택

다음 토폴로지를 고려하십시오.



그리고 이 라우팅 설계는 다음과 같습니다.



FTD 라우팅 컨피그레이션은 다음과 같습니다.

```
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 RIB(Routing Information Base) - 제어 평면:

```
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
```

## 해당 FTD ASP(Accelerated Security Path) 라우팅 테이블 - 데이터 플레인:

```
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
```

## 핵심 사항

FTD(Adaptive Security Appliance - ASA와 유사한 방식)는 먼저 패킷의 출구(이그레스) 인터페이스를 결정합니다. 즉, ASP 라우팅 테이블의 '수신' 항목을 확인합니다. 그런 다음 확인된 인터페이스에

대해 next-hop을 찾으려고 시도합니다. 즉, ASP 라우팅 테이블의 'out' 항목을 확인합니다. 예를 들면 다음과 같습니다.

```
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
```

마지막으로 확인된 next-hop의 경우 LINA는 ARP 캐시에서 유효한 인접성을 확인합니다.

FTD 패킷 추적기 틀에서 이 프로세스를 확인합니다.

```
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
```

제어 평면에 표시되는 FTD ARP 테이블:

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

ARP 확인을 강제 실행하려면

```
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
```

데이터 평면에 표시되는 FTD ARP 테이블:

```
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

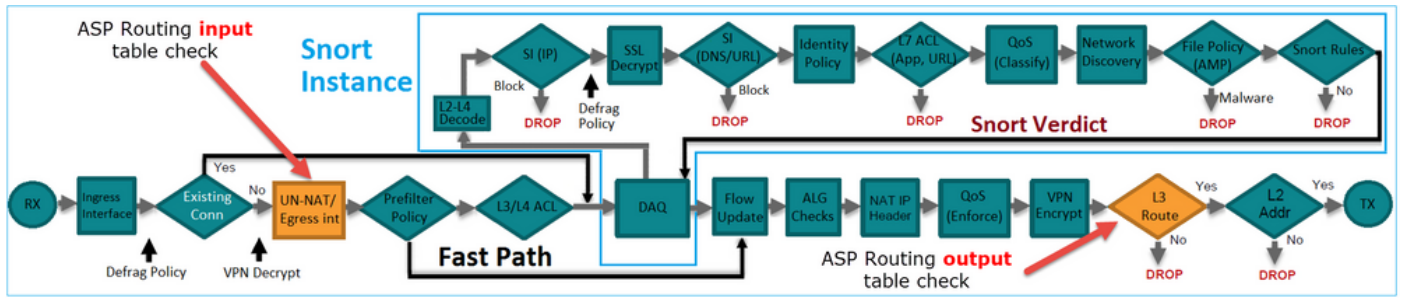
Context: single_vf, Interface: INSIDE
192.168.0.99 Active 4c4e.35fc.fcd8 hits 5 reference 0

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
```

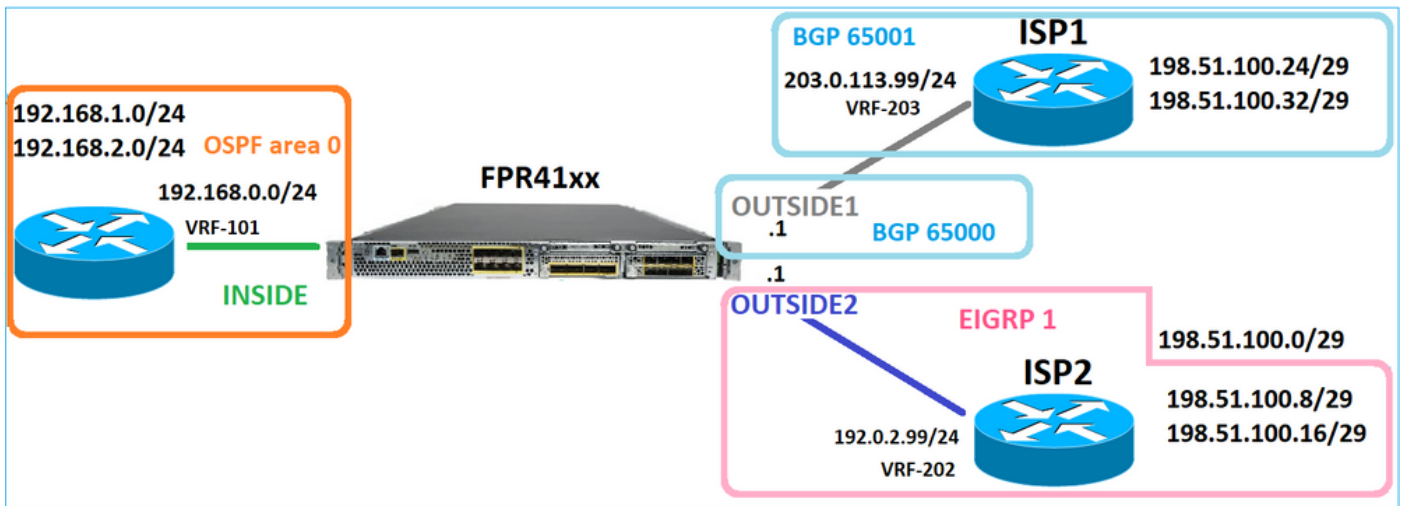
## FTD 운영 순서

이 그림에서는 작업의 순서와 입력 및 출력 ASP 라우팅 검사가 수행되는 위치를 보여 줍니다.



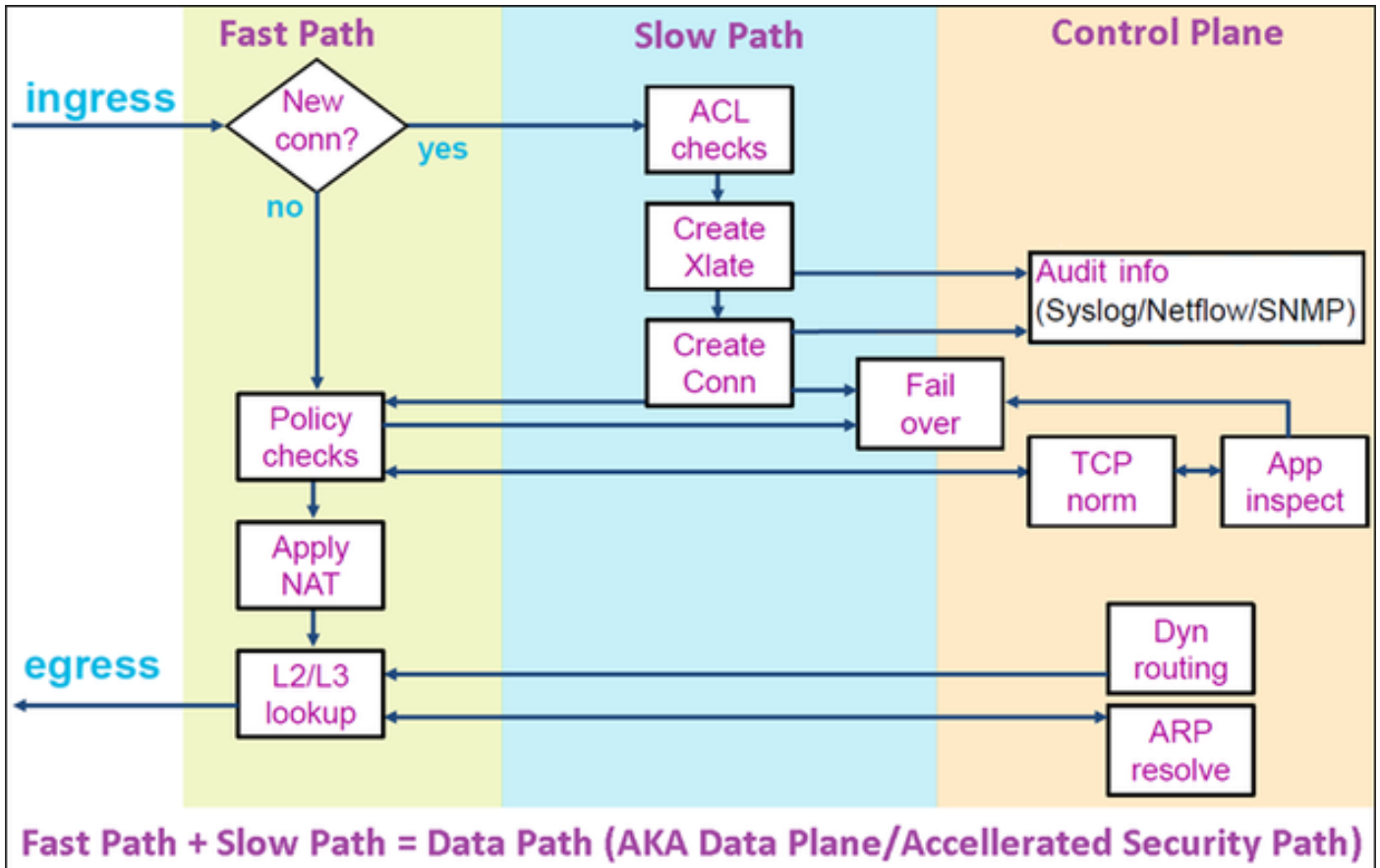
## 구성

### 케이스 1 - 연결 조희를 기반으로 전달



앞서 언급한 대로 FTD LINA Engine의 주요 구성 요소는 데이터 경로 프로세스(디바이스 코어 수를 기반으로 하는 다중 인스턴스)입니다. 또한 Datapath(Accelerated Security Path - ASP라고도 함)는 다음 2개의 경로로 구성됩니다.

1. 느린 경로 = 새로운 연결 설정에 대한 책임(빠른 경로를 채웁니다.)
2. 빠른 경로 = 설정된 연결에 속하는 패킷을 처리합니다.



- show route 및 show arp와 같은 명령은 제어 평면의 내용을 표시합니다.
- 반면 show asp table routing 및 show asp table arp 같은 명령은 실제로 적용되는 ASP(Datapath)의 내용을 표시합니다.

FTD 내부 인터페이스에서 추적을 사용하여 캡처를 활성화합니다.

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

FTD를 통해 텔넷 세션을 엽니다.

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

FTD 캡처는 연결 시작부터 패킷을 표시합니다(TCP 3-way 핸드셰이크 캡처).

```
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)
...
```

첫 번째 패킷(TCP SYN)을 추적합니다. 이 패킷은 FTD LINA Slow Path를 통과하며, 이 경우 글로벌 라우팅 조회가 수행됩니다.

```
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#
```

동일한 흐름에서 다른 인그레스 패킷을 추적합니다. 활성 연결과 일치하는 패킷:

```
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 ...  
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

Module information for reverse flow ...  
snf\_fp\_inspect\_ip\_options  
snf\_fp\_tcp\_normalizer  
snf\_fp\_translate  
snf\_fp\_snort  
snf\_fp\_tcp\_normalizer  
snf\_fp\_adjacency  
snf\_fp\_fragment  
snf\_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#

부동 시간 초과

문제

일시적인 경로 불안정성으로 인해 FTD를 통한 장기(엘리펀트) UDP 연결이 원하는 것과 다른 FTD 인터페이스를 통해 설정될 수 있습니다.

### 솔루션

이 문제를 해결하려면 timeout floating-conn을 비활성화된 기본값과 다른 값으로 설정합니다.

The screenshot shows the Firewall Management Center interface for device FTD4100-1. The left sidebar contains a list of configuration categories, with 'Timeouts' highlighted. The main area displays a table of timeout settings. The 'Floating Connection' setting is highlighted with an orange box. The table includes the following settings:

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

명령 참조에서 다음을 수행합니다.

|                      |  |
|----------------------|--|
| <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. |
|----------------------|--|

자세한 내용은 사례 연구: CiscoLive BRKSEC-3020 세션에서 다시 로드한 후 UDP 연결 실패:

# 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 시간 초과

### 문제

경로가 중단되지만(제거됨) 트래픽은 설정된 연결과 일치합니다.

### 솔루션

Timeout conn-holddown 기능이 ASA 9.6.2에 추가되었습니다. 이 기능은 기본적으로 활성화되어 있지만 현재(7.1.x)는 FMC UI 또는 FlexConfig에서 지원되지 않습니다. 관련 개선 사항: [ENH: FMC에서 컨피그레이션에 timeout conn-holddown을 사용할 수 없습니다.](#)

## ASA CLI 가이드에서

|                      |  |
|----------------------|--|
| <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
```

## 케이스 2 - NAT 조회 기반 전달

### 요건

이 NAT 규칙을 구성합니다.

- 유형: 정적
- 소스 인터페이스: INSIDE
- 대상 인터페이스: OUTSIDE1
- 원본: 192.168.1.1
- Original Destination(원래 대상): 198.51.100.1
- 번역 출처: 192.168.1.1
- Translated Destination(변환된 대상): 198.51.100.1

### 솔루션

|   |           | 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 CLI에 구축된 NAT 규칙:

```
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
```

3개의 캡처를 구성합니다.

```
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
```

192.168.1.1에서 198.51.100.1로의 텔넷 세션을 시작합니다.

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

패킷은 FTD에 도착하지만 OUTSIDE1 또는 OUTSIDE2 인터페이스를 남기는 것은 없습니다.

```
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 패킷을 추적합니다. 3단계(UN-NAT)에서는 NAT(UN-NAT, 특히 UN-NAT)가 다음 홉 조회를 위해 패킷을 OUTSIDE1 인터페이스로 전환했음을 보여줍니다.

```
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_198.51.100.1/23 to 198.51.100.1/23
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




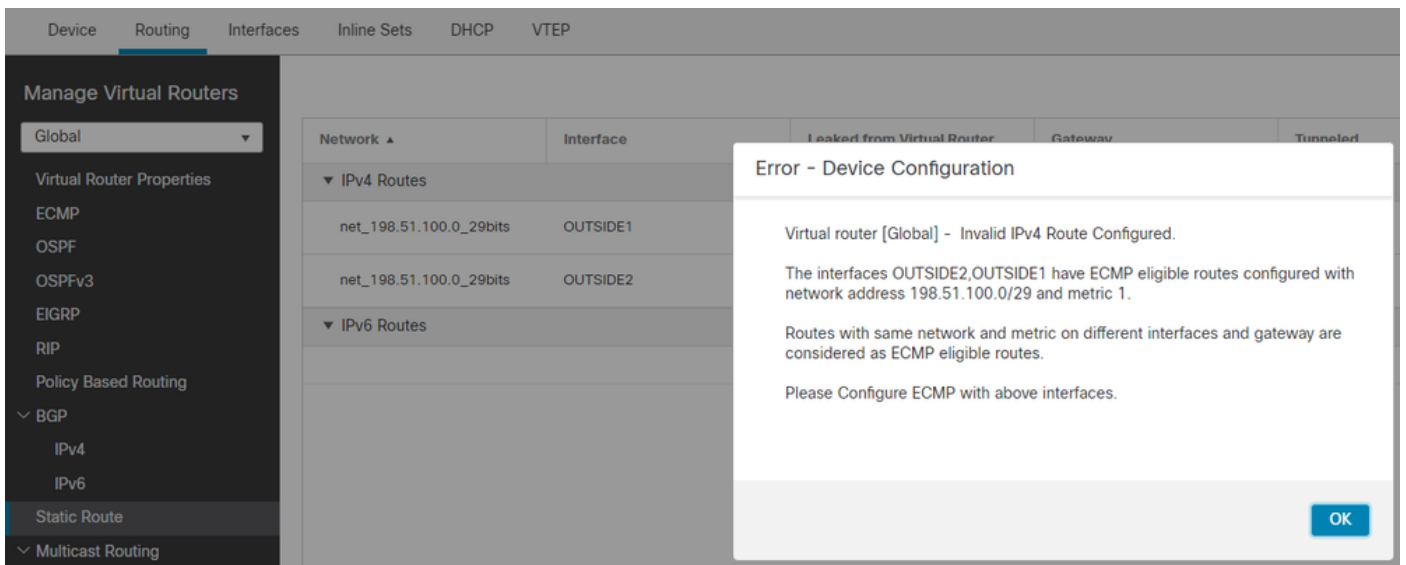
이 경우 SUBOPTIMAL-LOOKUP은 NAT 프로세스(OUTSIDE1)에 의해 결정된 이그레스 인터페이스가 ASP 입력 테이블에 지정된 이그레스 인터페이스와 다를 수 있습니다.

```
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
```

가능한 해결 방법은 OUTSIDE1 인터페이스에 유동 고정 경로를 추가하는 것입니다.

```
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
```

 참고: 이미 존재하는 것과 동일한 메트릭을 가진 고정 경로를 추가하려고 하면 다음 오류가 나타납니다.



 참고: 거리 메트릭이 255인 유동 경로는 라우팅 테이블에 설치되지 않습니다.

텔넷을 통해 FTD를 통해 전송된 패킷이 있는지 확인합니다.

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

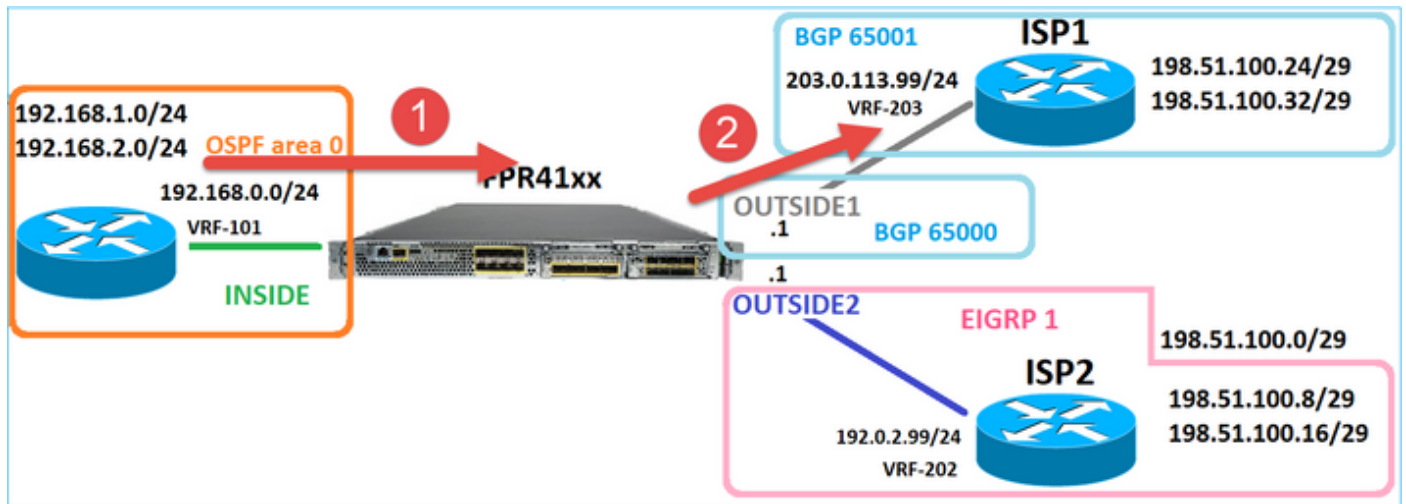
```
firepower# show capture
```

```

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

```

패킷 추적은 NAT 조회로 인해 패킷이 ISP2 대신 ISP1(OUTSIDE1) 인터페이스로 전달됨을 보여줍니다.



```
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 ...
```

```
snp_fp_inspect_ip_options
```

snp\_fp\_tcp\_normalizer  
snp\_fp\_snort  
snp\_fp\_translate  
snp\_fp\_tcp\_normalizer  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_ifc\_stat

Phase: 15

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Subtype: Resolve Preferred Egress interface

Result: ALLOW

Elapsed time: 5798 ns

Config:

Additional Information:

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

Phase: 16

Type: SUBOPTIMAL-LOOKUP

Subtype: suboptimal next-hop

Result: ALLOW

Elapsed time: 446 ns

Config:

Additional Information:

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

Phase: 17

Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Subtype: Lookup Nexthop on interface

Result: ALLOW

Elapsed time: 1784 ns

Config:

Additional Information:

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

Phase: 18

Type: ADJACENCY-LOOKUP

Subtype: Resolve Nexthop IP address to MAC

Result: ALLOW

Elapsed time: 1338 ns

Config:

Additional Information:

Found adjacency entry for Next-hop 203.0.113.99 on interface OUTSIDE1

Adjacency :Active

MAC address 4c4e.35fc.fcd8 hits 106 reference 2

...

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE1(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 723409 ns

1 packet shown

firepower#

흥미롭게도 이 경우 INSIDE 및 두 이그레스 인터페이스에 패킷이 표시됩니다.

```
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 CAPO1
```

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 CAPO2
```

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
```

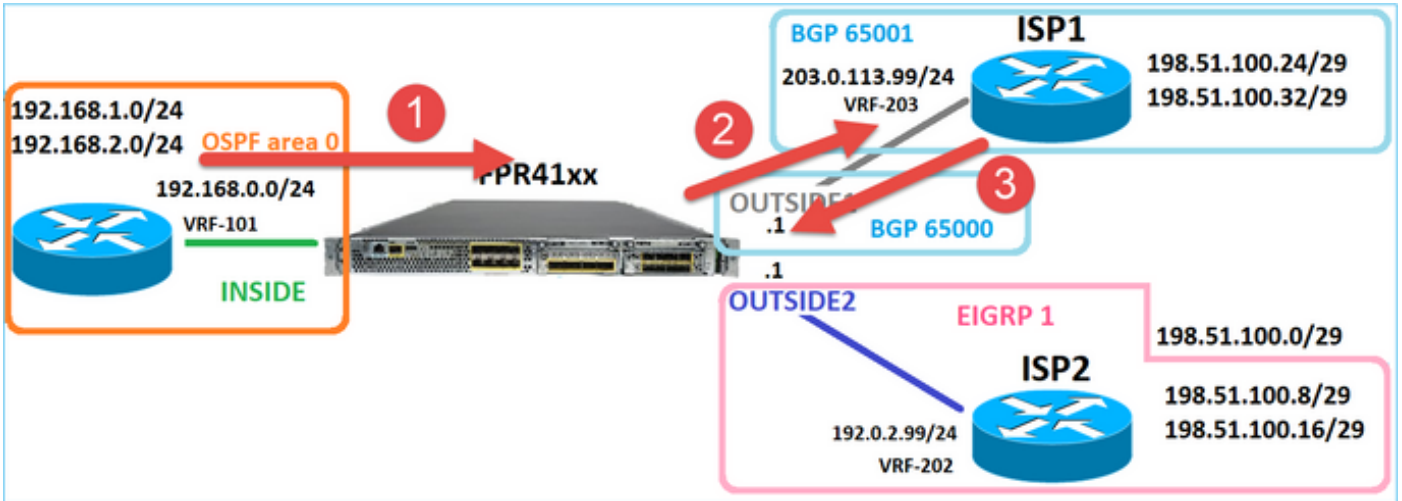
패킷 세부사항에는 MAC 주소 정보가 포함되며, OUTSIDE1 및 OUTSIDE2 인터페이스의 패킷 추적에서는 패킷의 경로를 확인합니다.

```
firepower# show capture CAPO1 detail
```

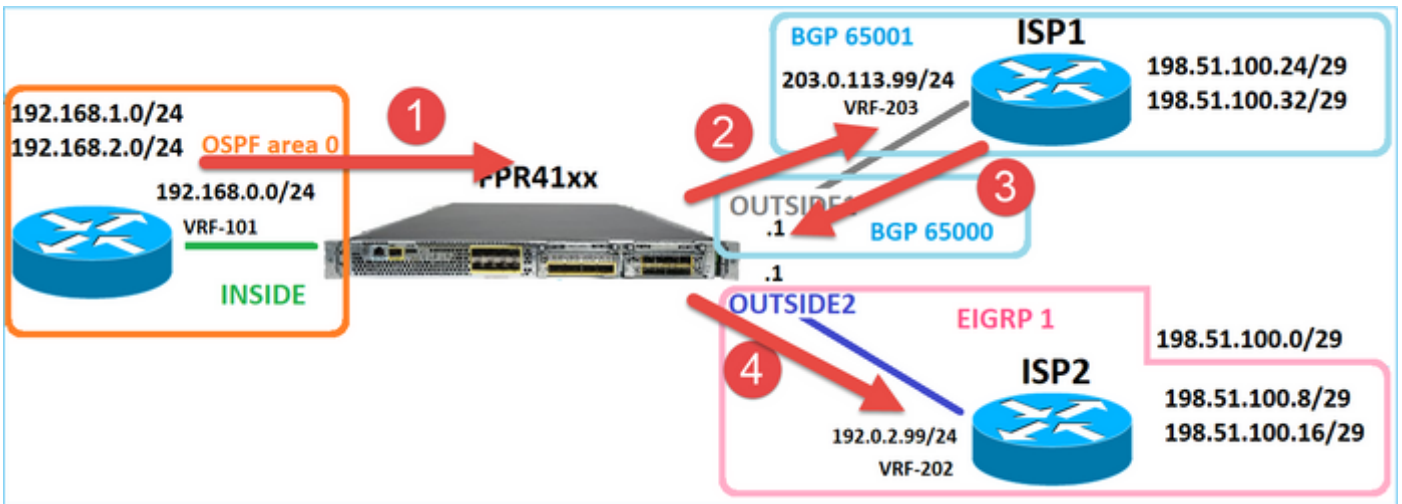
4 packets captured

```
1: 09:03:02.774358 00be.75f6.1dae 4c4e.35fc.fcd8 0x8100 Length: 62
802.1Q vlan#203 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



반환되는 패킷의 추적은 전역 라우팅 테이블 조회로 인한 OUTSIDE2 인터페이스로의 리디렉션을 보여줍니다.



```
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)

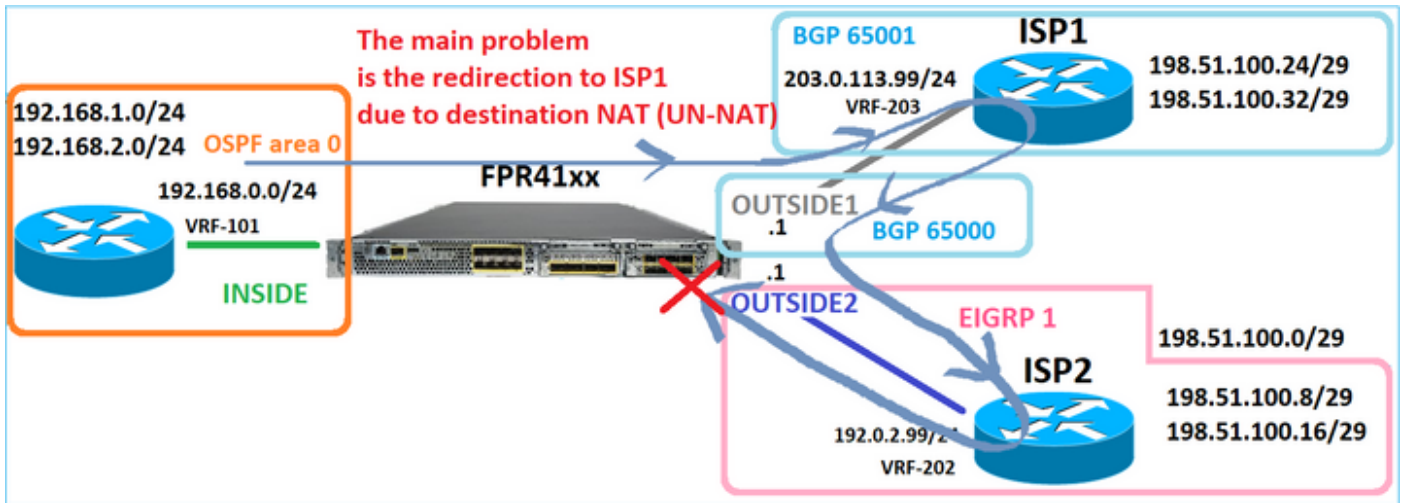
Phase: 14  
Type: ADJACENCY-LOOKUP  
Subtype: Resolve Nexthop IP address to MAC  
Result: ALLOW  
Elapsed time: 1338 ns  
Config:  
Additional Information:  
Found adjacency entry for Next-hop 192.0.2.99 on interface OUTSIDE2  
Adjacency :Active  
MAC address 4c4e.35fc.fcd8 hits 0 reference 1

...

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 라우터가 응답(SYN/ACK)을 전송하지만 이 패킷은 설정된 연결과 일치하므로 ISP1로 리디렉션됩니다. ASP 출력 테이블에 L2 인접성이 없으므로 FTD에서 패킷을 삭제합니다.



```
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
```

## 사례 3 - PBR(Policy Based Routing) 기반 전달

연결 플로우 조회 및 목적지 NAT 조회 후 PBR은 이그레스 인터페이스 결정에 영향을 줄 수 있는 다음 항목입니다. PBR에 대한 설명은 Policy [Based Routing에 나와 있습니다.](#)

FMC의 PBR 컨피그레이션에서는 다음 지침을 숙지해야 합니다.

FlexConfig를 사용하여 7.1 이전 버전의 FTD에 대해 FMC에서 PBR을 구성했습니다. FlexConfig를 계속 사용하여 모든 버전에서 PBR을 구성할 수 있습니다. 그러나 인그레스 인터페이스의 경우 FlexConfig 및 FMC의 Policy Based Routing 페이지를 모두 사용하여 PBR을 구성할 수는 없습니다.

이 사례 연구에서 FTD는 ISP2를 가리키는 198.51.100.0/24에 대한 경로를 가지고 있습니다.

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

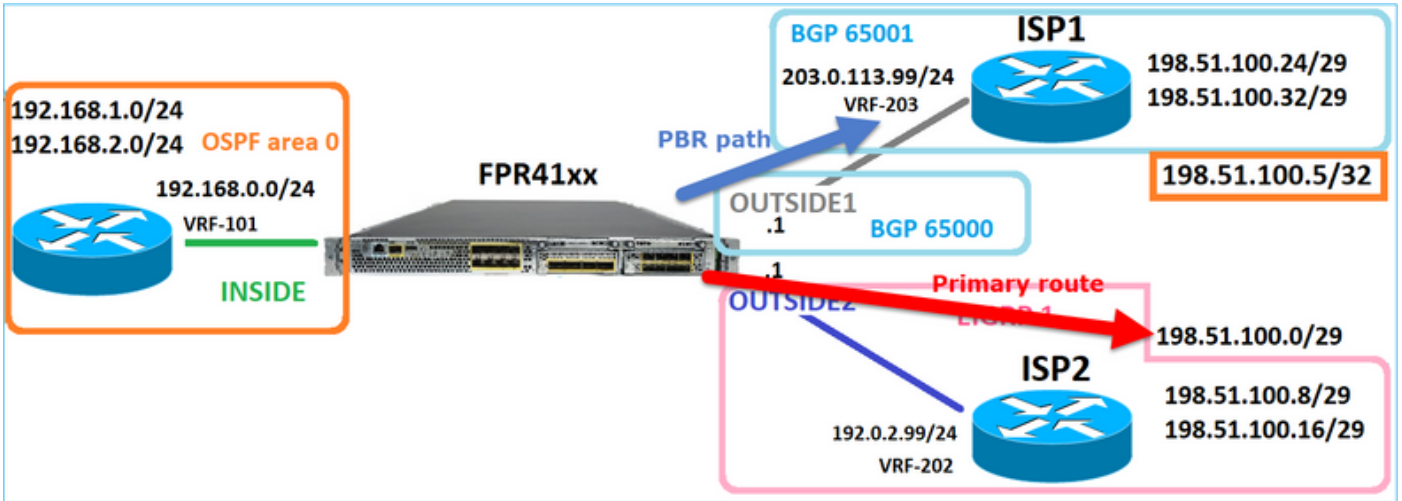
```
C 192.0.2.0 255.255.255.0 is directly connected, OUTSIDE2
L 192.0.2.1 255.255.255.255 is directly connected, OUTSIDE2
C 192.168.0.0 255.255.255.0 is directly connected, INSIDE
L 192.168.0.1 255.255.255.255 is directly connected, INSIDE
O 192.168.1.1 255.255.255.255 [110/11] via 192.168.0.99, 5d01h, 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
```

### 요건

다음 특성을 사용하여 PBR 정책을 구성합니다.

- 198.51.100.5로 향하는 IP 192.168.2.0/24의 트래픽은 ISP1(next-hop 203.0.113.99)로 전송해야 하며 다른 소스는 OUTSIDE2 인터페이스를 사용해야 합니다.





## 솔루션

### 7.1 이전 릴리스에서 PBR을 구성하려면

1. 관심 트래픽과 일치하는 확장 ACL을 생성합니다(예: PBR\_ACL).
2. 1단계에서 생성한 ACL과 일치하는 경로 맵을 만들고 원하는 다음 홉을 설정합니다.
3. 2단계에서 생성한 경로 맵을 사용하여 인그레스 인터페이스에서 PBR을 활성화하는 FlexConfig 개체를 만듭니다.

7.1 이후 릴리스에서는 7.1 이전 방식을 사용하여 PBR을 구성하거나, Device(디바이스) > Routing(라우팅) 섹션 아래에서 새로운 Policy Based Routing(정책 기반 라우팅) 옵션을 사용할 수 있습니다.

1. 관심 트래픽과 일치하는 확장 ACL을 생성합니다(예: PBR\_ACL).
2. PBR 정책을 추가하고 다음을 지정합니다.
  - a. 일치하는 트래픽
  - b. 인그레스 인터페이스
  - c. 다음 홉

### PBR 구성(새로운 방식)

1단계 - 일치하는 트래픽에 대한 액세스 목록을 정의합니다.

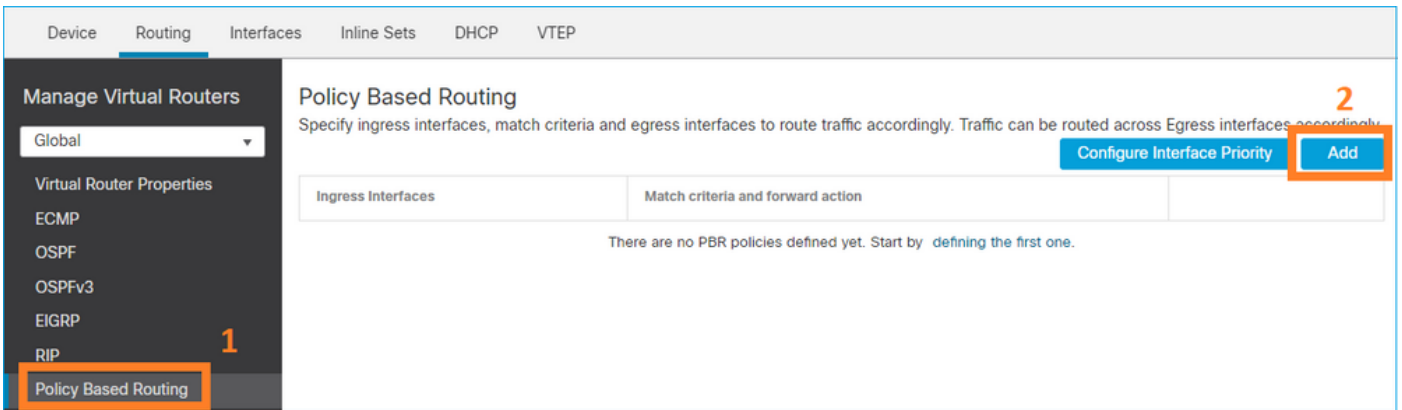
The screenshot shows the Firewall Management Center interface. The 'Objects' tab is selected. The 'Extended' section is expanded, and the 'Edit Extended Access List Object' dialog is open. The Name is 'ACL\_PBR'. The Entries table is as follows:

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

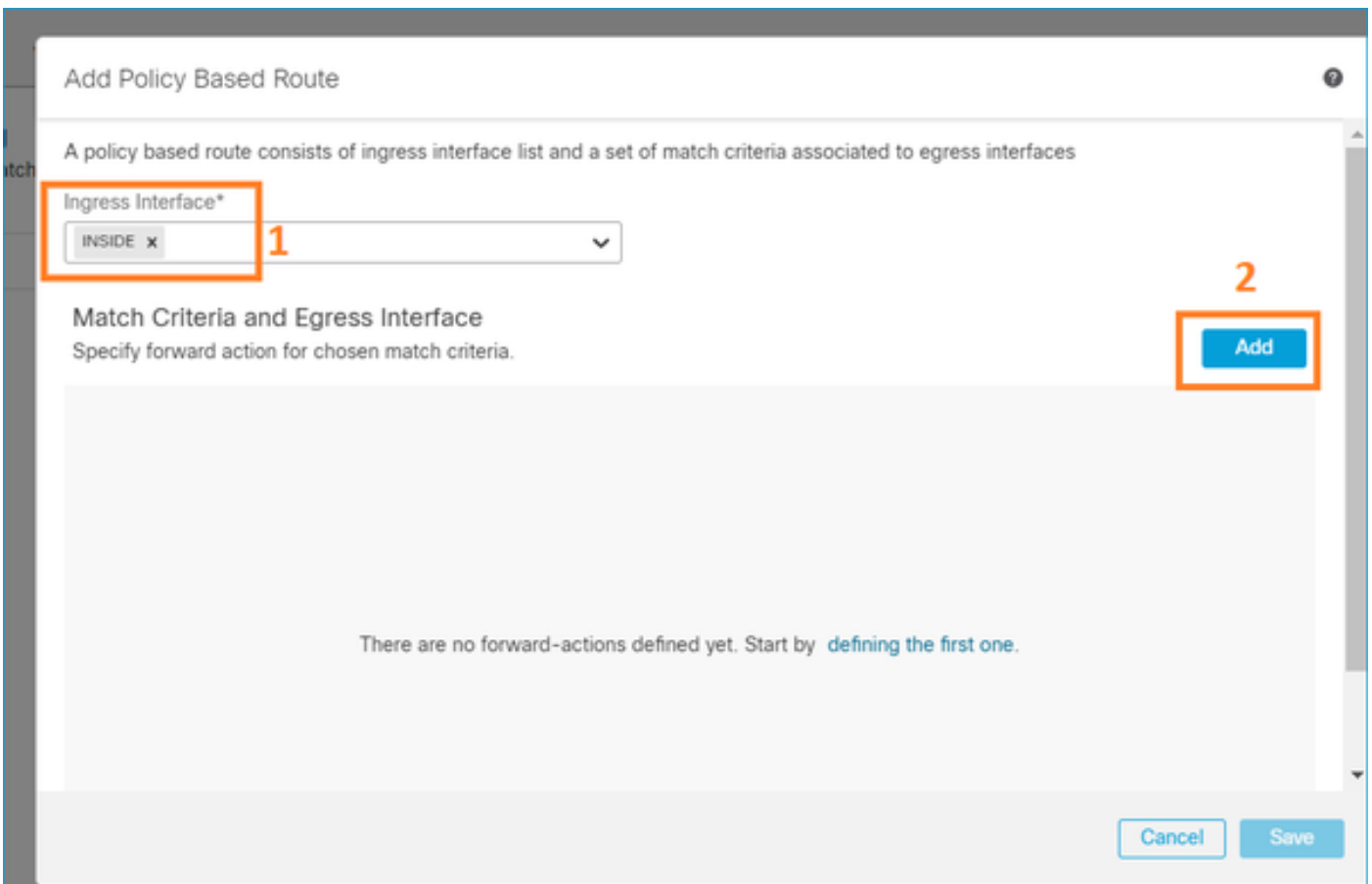
### 2단계 - PBR 정책 추가

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 FTD 디바이스를 수정합니다

. Routing(라우팅) > Policy Based Routing(정책 기반 라우팅)을 선택하고 Policy Based Routing(정책 기반 라우팅) 페이지에서 Add(추가)를 선택합니다.



인그레스 인터페이스를 지정합니다.



전달 작업을 지정합니다.

### Add Forwarding Actions


Match ACL:\*  1

Send To:\*  2

IPv4 Addresses  3

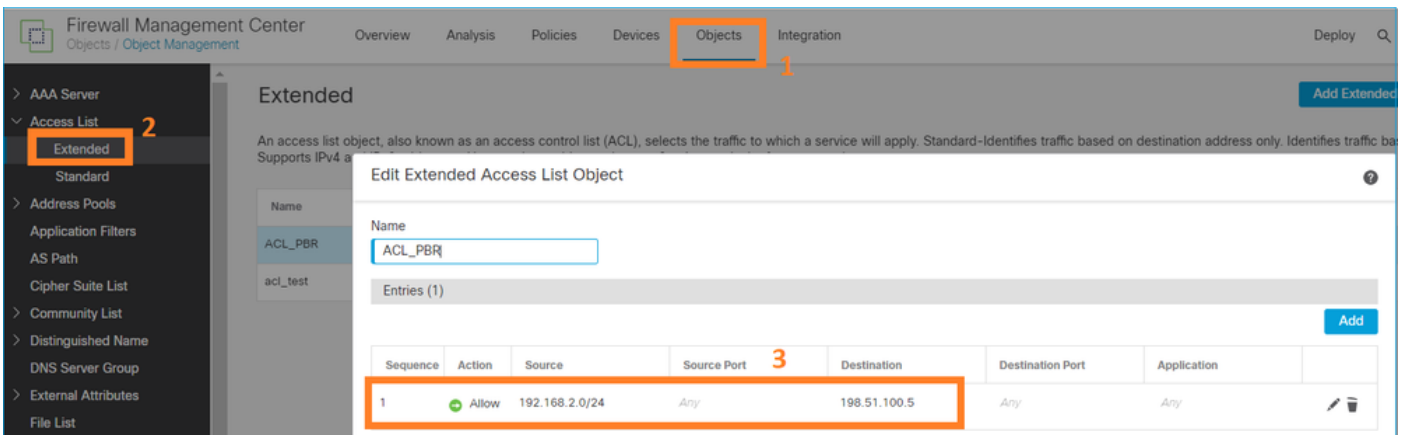
IPv6 Addresses

## 저장 및 배포

 참고: 여러 이그레스 인터페이스를 구성하려면 'Send To' 필드에 'Egress Interfaces' 옵션을 설정해야 합니다(버전 7.0+에서 사용 가능). 자세한 내용은 정책 [기반 라우팅의 컨피그레이션 예](#)를 확인하십시오.

## PBR 구성(기존 방식)

1단계 - 일치하는 트래픽에 대한 액세스 목록을 정의합니다.



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

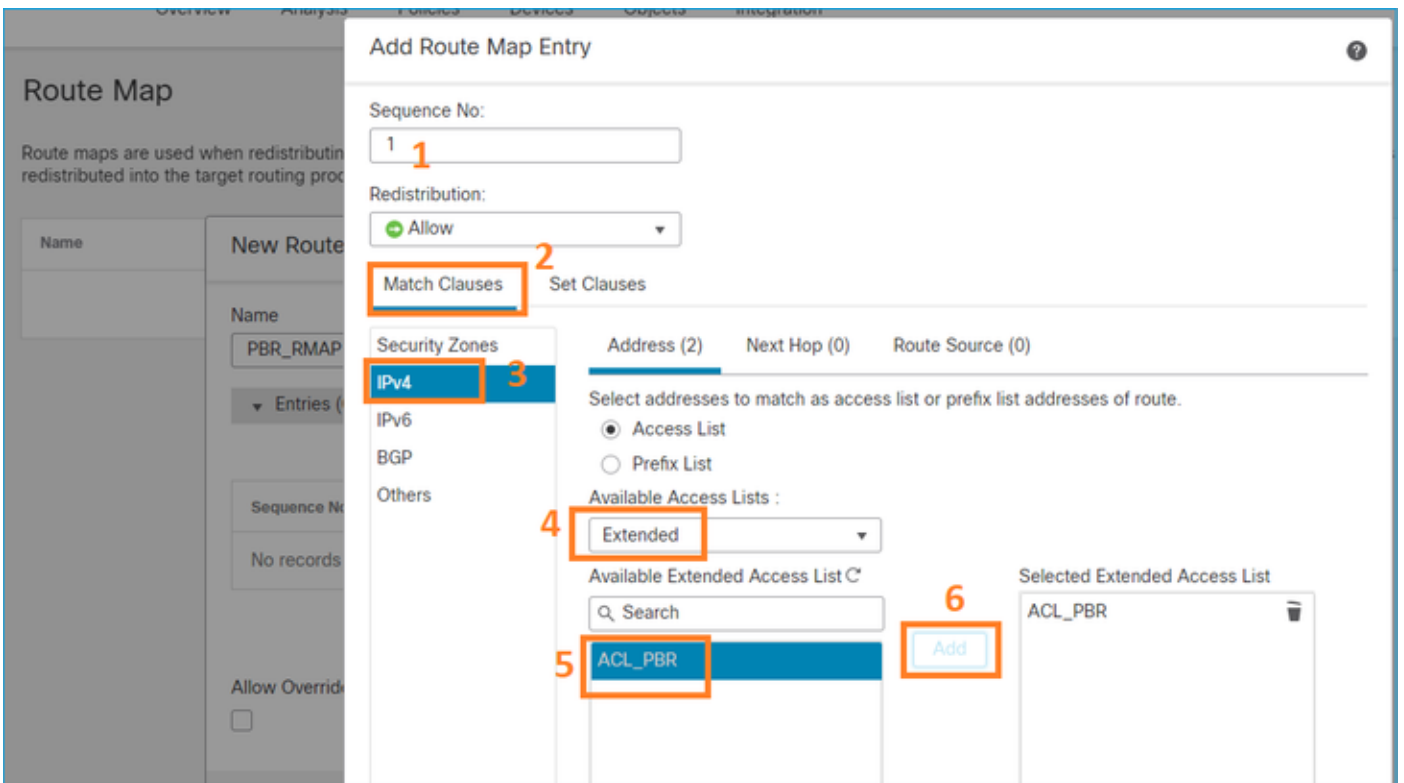
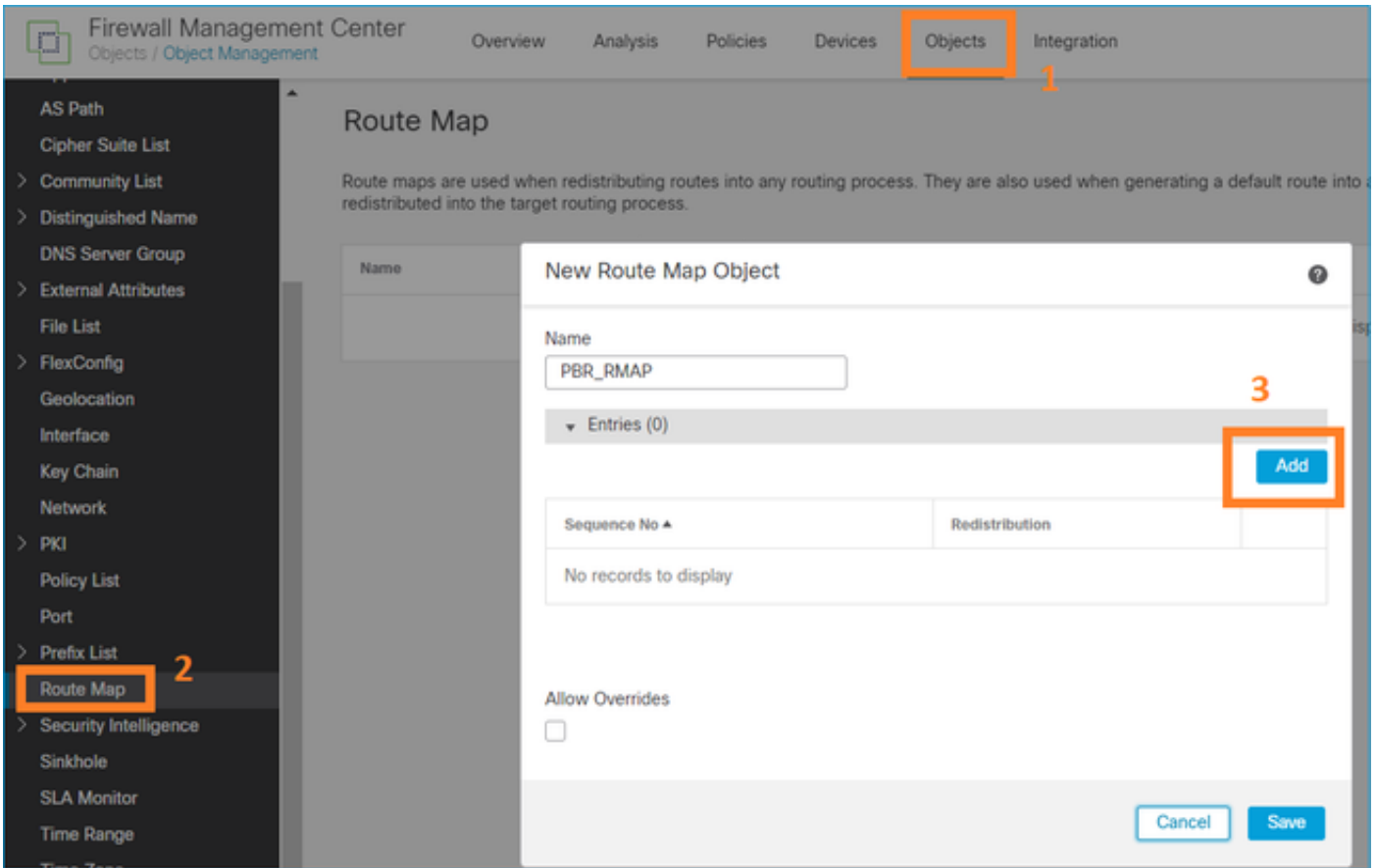
ACL\_PBR

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         |

2단계 - ACL과 일치하고 Next Hop을 설정하는 경로 맵을 정의합니다.

먼저 Match Clause를 정의합니다.



Set 절을 정의합니다.

### 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:

추가 및 저장

3단계 - FlexConfig PBR 객체를 구성합니다.

먼저 기존 PBR 객체를 복사(복제)합니다.

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

Object 이름을 지정하고 미리 정의된 route-map 객체를 제거합니다.

The screenshot shows the 'Add FlexConfig Object' form. The 'Name' field contains 'FTD4100\_PBR' and is annotated with a red box and the number '1' with the text 'Specify a new name'. The 'Description' field contains a template description. Below the description is a warning message: 'Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.' The 'Deployment' dropdown is set to 'Once' and the 'Type' dropdown is set to 'Append'. The CLI configuration is shown as follows:

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

The CLI configuration is annotated with red boxes and numbers: 'Port-channel1.101' is annotated with '2 Specify the correct ingress interface', and 'Sr-map-object' is annotated with '3 Remove this route-map'.

새 경로 맵을 지정합니다.

The screenshot shows the 'Add FlexConfig Object' form. The 'Name' field contains 'FTD4100\_PBR' and the 'Description' field contains a template description. Below the description is a warning message: 'Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.' The 'Deployment' dropdown is set to 'Once' and the 'Type' dropdown is set to 'Append'. The 'Insert' dropdown menu is open, showing the following options:

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

The 'Route Map' option is highlighted with a red box and the number '2'.

### Insert Route Map Variable

Variable Name:  1

Description:

Available Objects ↻

Q Search  2

PBR\_RMAP

3

Selected Object

PBR\_RMAP 🗑

최종 결과는 다음과 같습니다.

### 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
```

4단계 - FTD FlexConfig 정책에 PBR 객체를 추가합니다.

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

1 **FTD4100\_PBR** 2

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... |

Preview Config(컨피그레이션 미리 보기)를 저장하고 선택합니다.

### 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
```

마지막으로, 정책을 구축합니다.

 참고: PBR은 동일한 인그레스 인터페이스에 대해 FlexConfig 및 FMC UI를 사용하여 구성할 수 없습니다.



PBR SLA 컨피그레이션의 경우 다음 문서를 확인하십시오. Configure PBR [with IP SLAs for DUAL ISP on FTD Managed by FMC](#)

## PBR 확인

인그레스 인터페이스 확인:

```
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
```

경로 맵 확인:

```
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)
```

정책 경로 확인:

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

변경 전후의 패킷 추적기:

| PBR 제외   | PBR 포함  |
|--|---|
| <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> |

## 실제 트래픽으로 테스트

추적을 사용하여 패킷 캡처를 구성합니다.

```
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
```

캡처에 표시되는 내용은 다음과 같습니다.

```
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 패킷의 추적:

```
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 테이블에는 정책 적용 횟수가 표시됩니다.

```
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


---

 참고: packet-tracer는 히트 카운터도 늘립니다.

---

## PBR 디버그

---

 경고: 프로덕션 환경에서는 디버그가 많은 메시지를 생성할 수 있습니다.

---

이 디버그를 활성화합니다.

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

실제 트래픽 전송:

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

디버그에는 다음이 표시됩니다.

```
firepower#
```

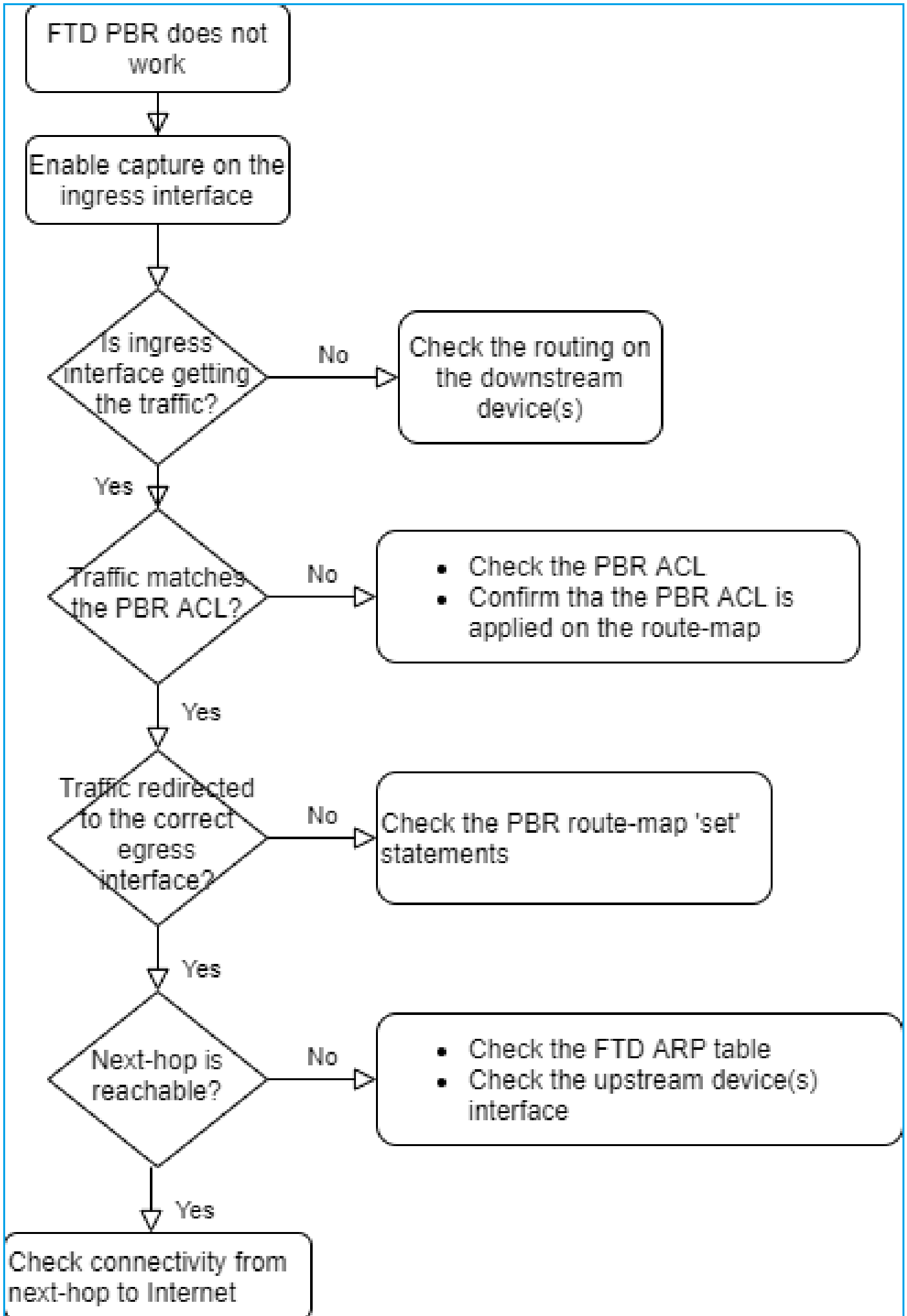
```
pbr: policy based route lookup called for 192.168.2.1/37256 to 198.51.100.5/23 proto 6 sub_proto 0 rece
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1649228271478, sequence 5, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = OUTSIDE1 : next_hop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

---

 참고: Packet-tracer는 디버그 출력도 생성합니다.

---

이 순서도는 PBR 문제를 해결하는 데 사용할 수 있습니다.



show asp drop

### 사례 4 - 글로벌 라우팅 조회를 기반으로 한 전달

연결 조회, NAT 조회 및 PBR 이후에 이그레스(egress) 인터페이스를 확인하기 위해 점검되는 마지막 항목은 전역 라우팅 테이블입니다.

라우팅 테이블 확인

FTD 라우팅 테이블 출력을 살펴보겠습니다.

```

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
       ST - 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

```

라우팅 프로세스의 주요 목표는 다음 흐름을 찾는 것입니다. 경로 선택 순서는 다음과 같습니다.

1. 일치 항목 최장 수
2. 최하위 AD(서로 다른 라우팅 프로토콜 소스 간)
3. Lowest Metric(동일한 소스에서 경로를 학습하는 경우 - 라우팅 프로토콜)

라우팅 테이블이 채워지는 방법:

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

- 로컬 IP(L)

- VPN(V)

- 재배포

- 기본값

라우팅 테이블 요약을 보려면 다음 명령을 사용합니다.

```
<#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>    |

다음 명령을 사용하여 라우팅 테이블 업데이트를 추적할 수 있습니다.

```
<#root>
```

```
firepower#
```

```
debug ip routing
```

```
IP routing debugging is on
```

예를 들어, OSPF 경로 192.168.1.0/24이 전역 라우팅 테이블에서 제거되면 디버그에 표시되는 내용은 다음과 같습니다.

```
<#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
```

다시 추가될 때:

```
<#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
```

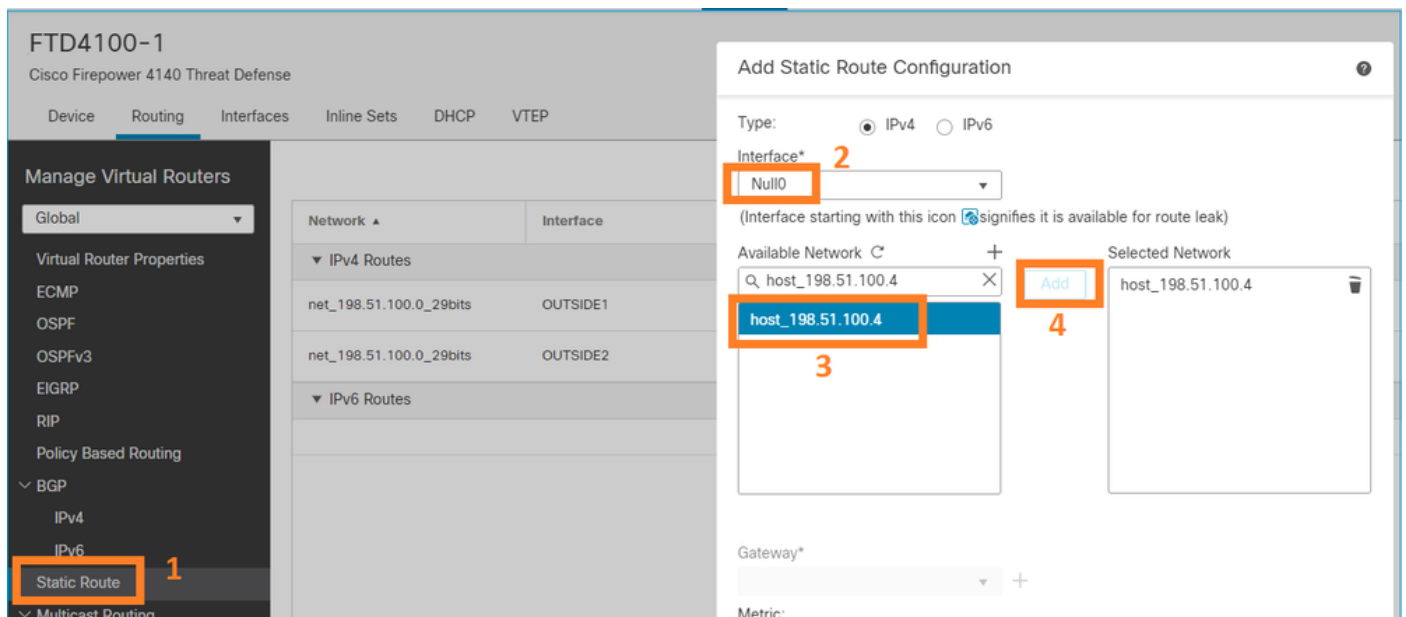
## Null0 인터페이스

Null0 인터페이스를 사용하여 원치 않는 트래픽을 삭제할 수 있습니다. 이 삭제는 ACL(Access Control Policy) 규칙으로 트래픽을 삭제하는 것보다 성능에 미치는 영향이 적습니다.

요건

198.51.100.4/32 호스트에 대해 Null0 경로를 구성합니다.

솔루션



저장 및 구축.

확인:

<#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
```

원격 호스트에 액세스를 시도합니다.

<#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 로그에는 다음이 표시됩니다.

<#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 드롭은 다음을 표시합니다.

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

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

## ECMP(동일 비용 다중 경로)

### 트래픽 영역

- ECMP Traffic Zone(ECMP 트래픽 영역)에서는 사용자가 인터페이스를 함께 그룹화할 수 있습니다(ECMP 영역이라고 함).
- 이를 통해 ECMP 라우팅은 물론 여러 인터페이스 간 트래픽의 로드 밸런싱이 가능합니다.
- 인터페이스가 ECMP Traffic Zone과 연결된 경우 사용자는 인터페이스 전반에 걸쳐 Equal-Cost 고정 경로를 생성할 수 있습니다. Equal-Cost 고정 경로는 메트릭 값이 동일한 대상 네트워크에 대한 경로입니다.

버전 7.1 이전에는 Firepower Threat Defense에서 FlexConfig 정책을 통해 ECMP 라우팅을 지원했습니다. 7.1 릴리스에서처럼 인터페이스를 트래픽 영역으로 그룹화하고 Firepower Management Center에서 ECMP 라우팅을 구성할 수 있습니다.

EMCP에 대한 설명은 [ECMP입니다](#)

이 예에서는 비대칭 라우팅이 있으며 반환 트래픽이 삭제됩니다.

```
<#root>
```

```
firepower#
```

```
show log
```

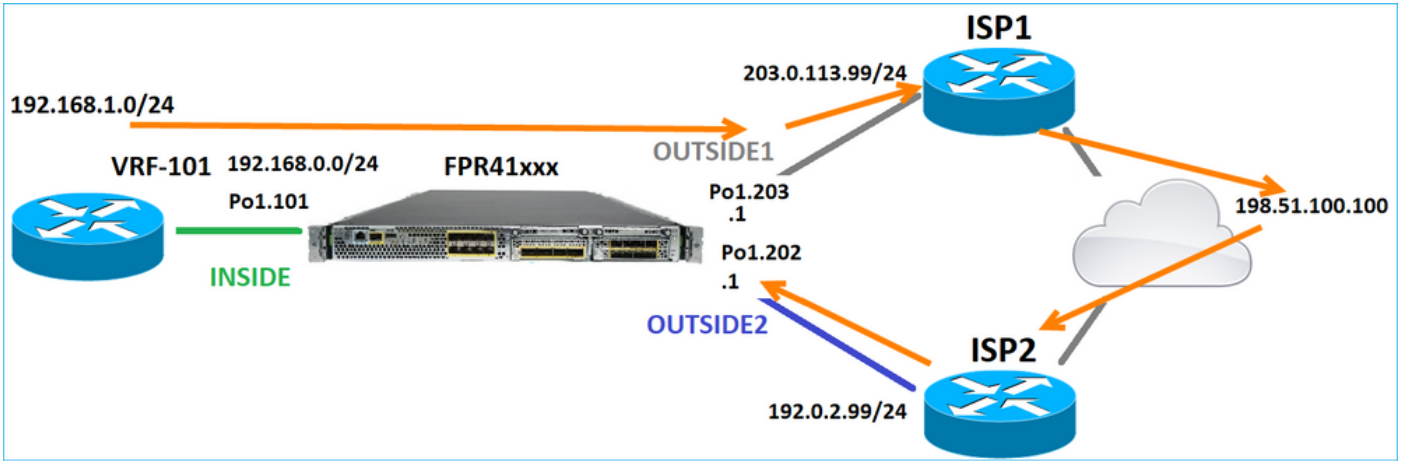
```
Apr 13 2022 07:20:48: %FTD-6-302013:
```

```
B
```

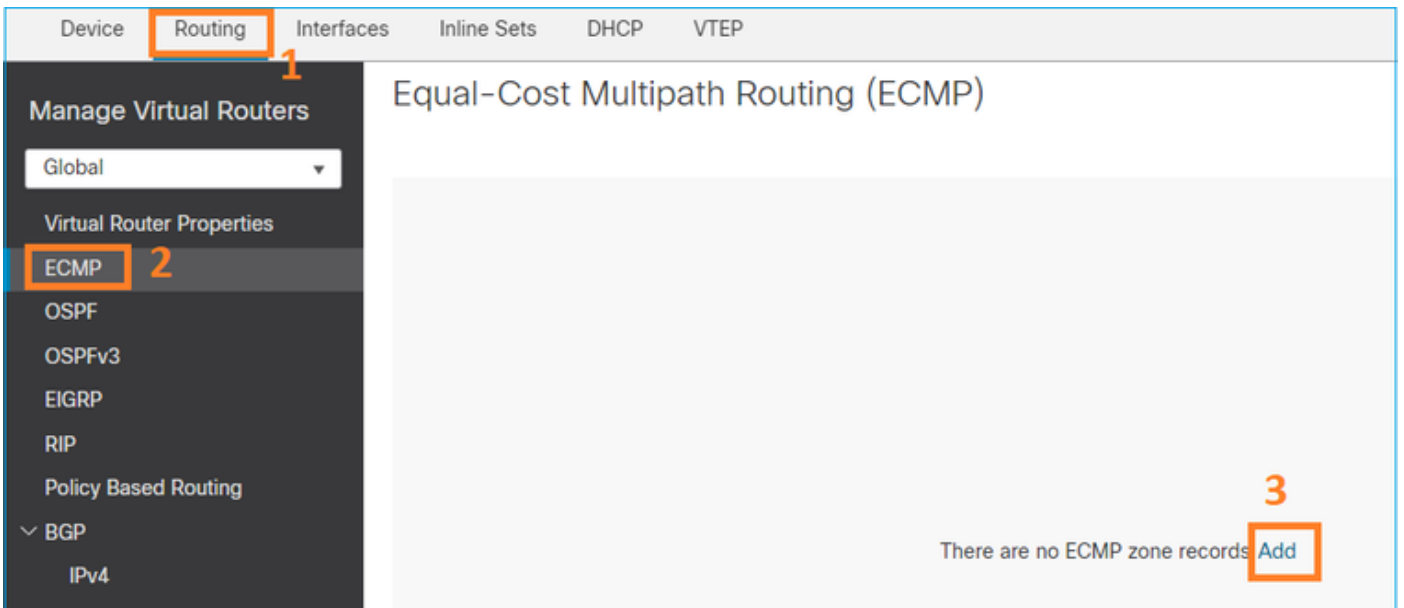
```
uilt inbound TCP connection 4046 for INSIDE:192.168.1.1/23943 (192.168.1.1/23943) to OUTSIDE1:198.51.100.100/23
```

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

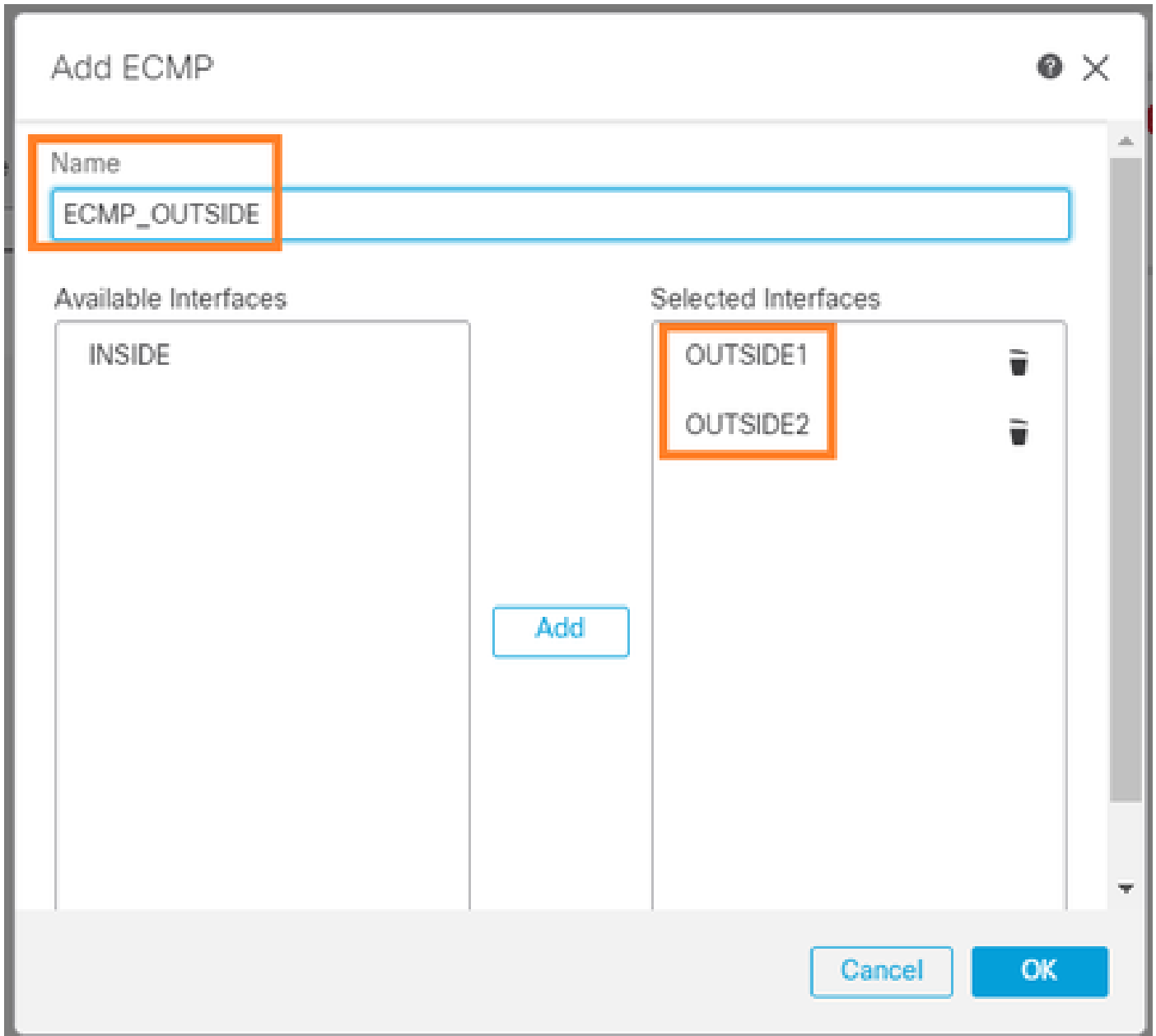
```
Deny TCP (no connection) from 198.51.100.100/23 to 192.168.1.1/23943 flags SYN ACK on interface OUTSIDE2
```



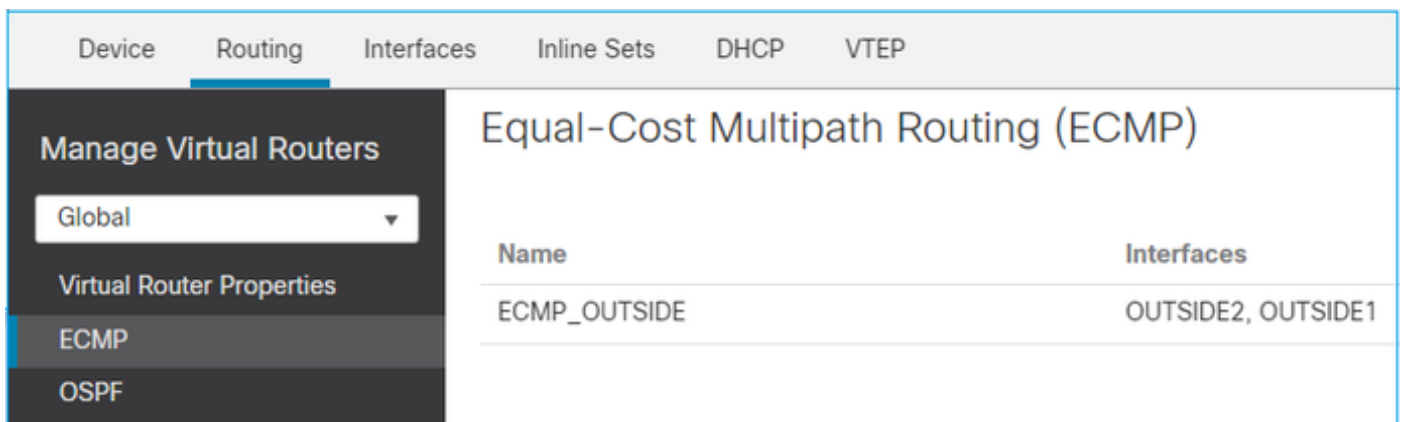
FMC UI에서 ECMP를 구성합니다.



ECMP 그룹에 2개의 인터페이스를 추가합니다.



결과:



저장 및 구축.

ECMP 영역 확인:

<#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
```

인터페이스 확인:

<#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
```

이제 반환 트래픽이 허용되며 연결이 UP입니다.

```
<#root>
```

```
Router1#
```

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

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

ISP1 인터페이스의 캡처는 이그레스 트래픽을 보여줍니다.

```
<#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 인터페이스의 캡처는 반환 트래픽을 보여줍니다.

```
<#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 관리 플레인

FTD에는 2개의 관리 플레인이 있습니다.

- Management0 인터페이스 - Firepower 하위 시스템에 대한 액세스를 제공합니다.
- LINA 진단 인터페이스 - FTD LINA 하위 시스템에 대한 액세스 제공

Management0 인터페이스를 구성하고 확인하려면 `configure network` 및 `show network` 명령을 각각 사용합니다.

반면, LINA 인터페이스는 LINA 자체에 대한 액세스를 제공합니다. FTD RIB의 FTD 인터페이스 항목은 로컬 경로로 표시될 수 있습니다.

```
<#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
```

마찬가지로 ASP 라우팅 테이블의 ID 항목으로 볼 수 있습니다.

```
<#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
```

### 요점

패킷이 FTD에 도착하고 목적지 IP가 ID IP 중 하나와 일치하면 FTD는 패킷을 사용해야 함을 인식합니다.

### FTD LINA 진단 인터페이스 라우팅

FTD(예: post-9.5 코드를 실행하는 ASA)는 관리 전용으로 구성된 모든 인터페이스에 대해 VRF와 유사한 라우팅 테이블을 유지합니다. 이러한 인터페이스의 예로는 진단 인터페이스가 있습니다.

FMC에서는 ECMP가 없는 경우 동일한 메트릭을 사용하여 서로 다른 2개의 인터페이스에서 2개의 기본 경로를 구성할 수 없지만, FTD 데이터 인터페이스에서 1개의 기본 경로를 구성하고 진단 인터페이스에서 다른 기본 경로를 구성할 수 있습니다.

| 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      |

데이터 평면 트래픽은 전역 테이블 기본 게이트웨이를 사용하는 반면, 관리 평면 트래픽은 진단 기본 GW를 사용합니다.

```
<#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
```

전역 라우팅 테이블 게이트웨이:

```
<#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
```

FTD에서 트래픽을 보낼 때(from-the-box traffic) 이그레스 인터페이스는 다음을 기반으로 선택됩니다.

1. 전역 라우팅 테이블
2. 관리 전용 라우팅 테이블

이그레스 인터페이스를 수동으로 지정하는 경우 이그레스 인터페이스 선택을 덮어쓸 수 있습니다.

진단 인터페이스 게이트웨이를 ping해 보십시오. 소스 인터페이스를 지정하지 않으면 FTD가 먼저 전역 라우팅 테이블을 사용하기 때문에 ping이 실패하며, 이 경우 기본 경로가 포함됩니다. 전역 테이블에 경로가 없는 경우 FTD는 관리 전용 라우팅 테이블에서 경로 조회를 수행합니다.

```
<#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 명령을 사용하여 LINA CLI에서 파일을 복사하려는 경우에도 마찬가지입니다.

## BFD(Bidirectional Forwarding Detection)

기존 ASA 버전 9.6에서 BFD 지원이 추가되었으며 BGP 프로토콜(Bidirectional Forwarding [Detection Routing](#))에 대해서만 [지원됩니다](#)

FTD의 경우:

- BGP IPv4 및 BGP IPv6 프로토콜이 지원됩니다(소프트웨어 6.4).
- OSPFv2, OSPFv3 및 EIGRP 프로토콜은 지원되지 않습니다.
- 고정 경로에 대한 BFD는 지원되지 않습니다.

## 가상 라우터(VRF)

VRF 지원은 6.6 릴리스에 추가되었습니다. 자세한 내용은 이 문서 [를 참조하십시오](#).

## 관련 정보

- [FTD 고정 경로 및 기본 경로](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.