Secure Firewall 3100 FDM 7.7.0 하드웨어 바이패스 구성

목차

소개

이 문서에서는 FDM(Firepower Device Manager) 관리 Secure Firewall 7.7.0에서 인라인 집합에 대해 하드웨어 우회를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 인라인 집합
- Secure Firewall 3100 시리즈
- Firepower 장치 관리자 그래픽 사용자 인터페이스(GUI)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall 3100(v7.7.0 실행)
- Cisco Secure Firewall Device Manager v7.7.0.

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

인라인 집합 기능이 7.4.1에서 FDM에 추가되었습니다. 인라인 집합을 사용하면 라우팅할 필요 없이 L2 네트워크에서 검사를 수행할 수 있습니다. 인라인 쌍 모드에서 FTD 인터페이스 구성

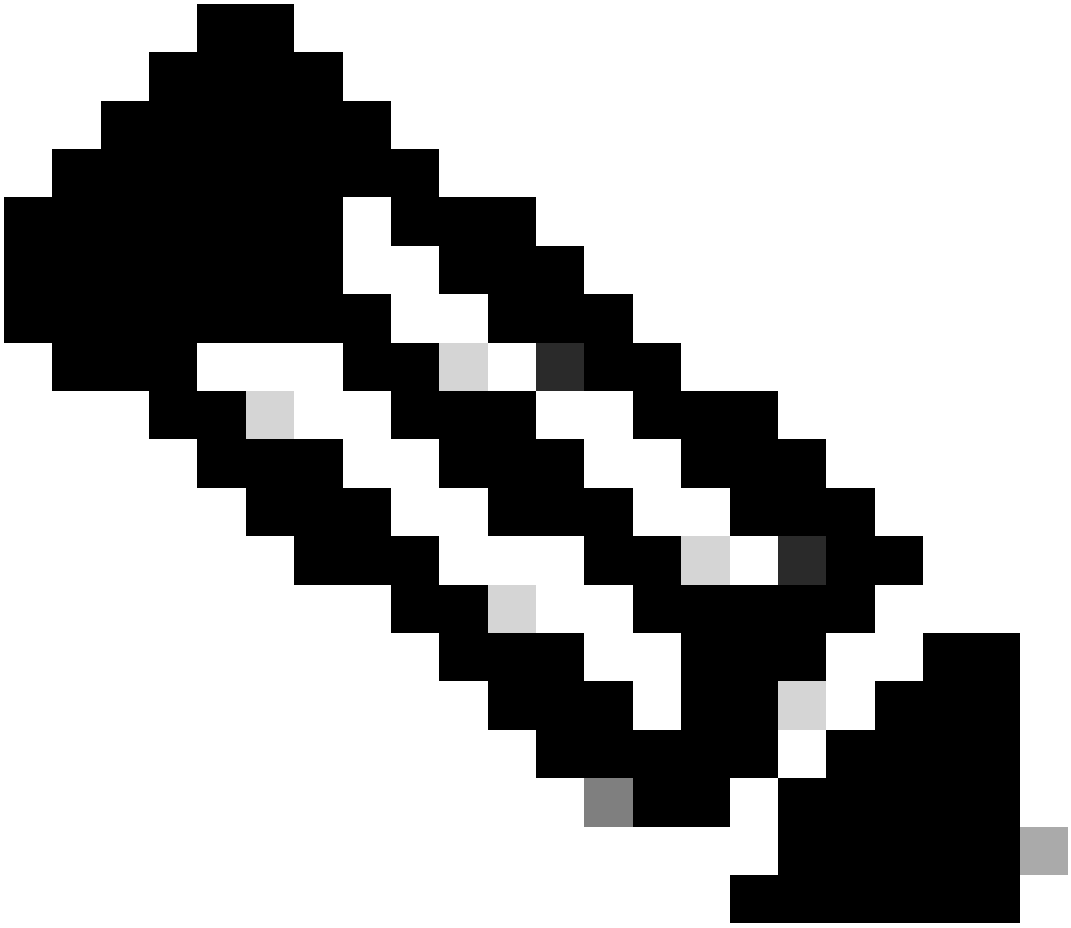
이번 릴리스에 대한 이전 버전 대비

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• Inline Sets is available. • Hardware Bypass is not supported.		• Added support for Hardware Bypass.

Secure Firewall 7.0 바이패스 기능

새로운 기능

- 하드웨어 검사 Bypass는 정전 시 인라인 인터페이스 쌍 간에 트래픽이 계속 흐르도록 보장합니다.
- 이 기능은 소프트웨어 또는 하드웨어 장애 시 네트워크 연결을 유지하는 데 사용됩니다.
- 이제 FDM 3100 Series 플랫폼의 인라인 집합에 대해 하드웨어 우회를 사용할 수 있습니다.



참고: Firepower Management Center 컨피그레이션 가이드

구축 시나리오

- 이 기능은 프로덕션 환경에 어떻게 적합합니까?
  - 인라인 집합은 IPS(또는 IDS) 활용 사례에 사용됩니다.
  - 라우팅 컨피그레이션 없이 트래픽 검사를 활성화합니다. 하드웨어 우회를 통해 유닛에 오류가 발생할 경우 트래픽 흐름을 허용합니다.
- . 실제 예:
  - 레이어 3 없이도 어디서나 빠르고 쉽게 레이어 2 네트워크 검사를 설정할 수 있습니다.
  - 완전히 격리된 네트워크에 매우 중요하며 인터넷 액세스가 없습니다.
  - 독립형 방화벽을 위한 심층 패킷 검사를 위한 투명한 인라인 삽입 - 기존 프로덕션 레이어 2 아키텍처.

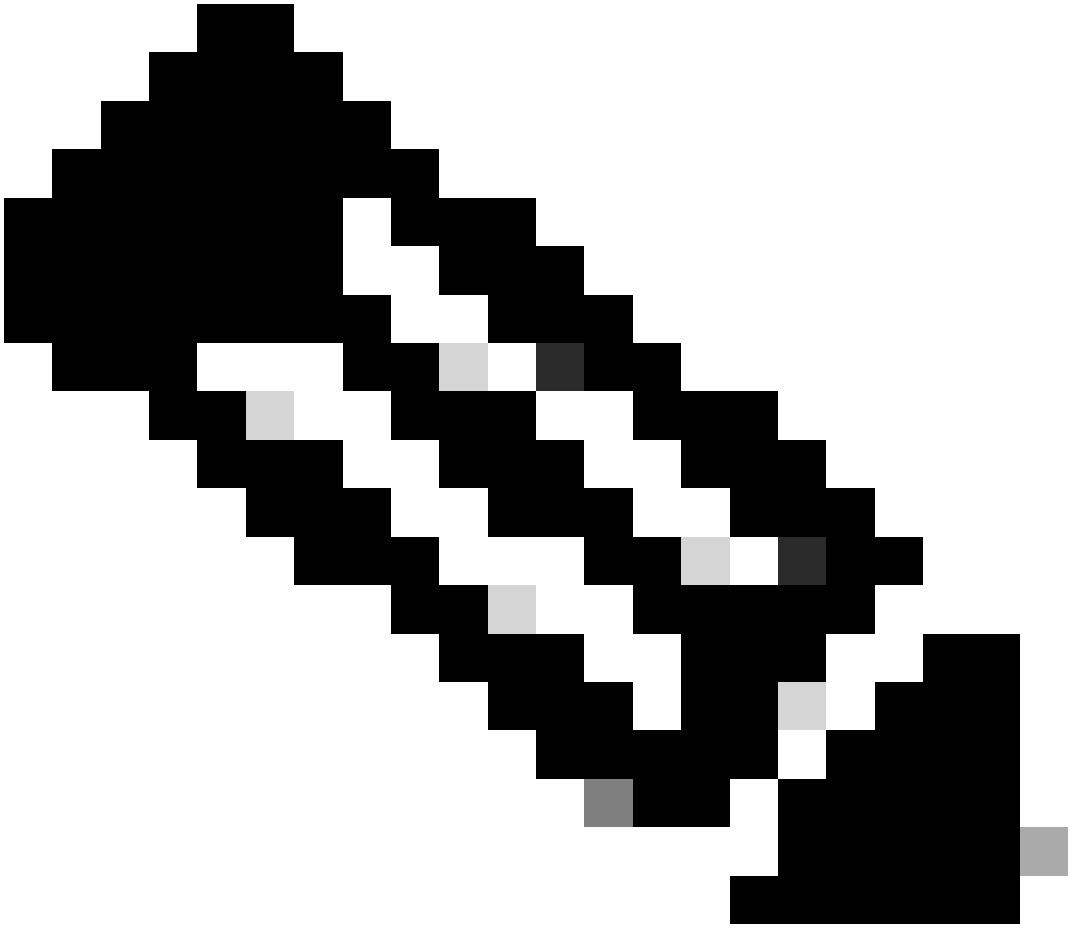
기본: 지원되는 플랫폼, 라이센싱

소프트웨어 및 하드웨어 버전

FDM		
	Inline Sets – before 7.7.0	Inline Sets with Hardware Bypass
FDM	7.4.1	7.7.0
REST API	7.4.1	7.7.0

Platforms	1000, 2100 (up to 7.4 only), and 3100 Series	3100 Series equipped with a network module:
		• 8 Ports:
		  ○ FPR-X-NM-6X1SXF
		• 6 Ports:
		  ○ FPR-X-NM-6X10SRF
		  ○ FPR-X-NM-6X10LRF
		  ○ FPR-X-NM-6X25SRF
		  ○ FPR-X-NM-6X25LRF

소프트웨어 및 하드웨어



참고: 3100 Series 및 하드웨어 바이패스 정보

기타 지원 측면

FDM			
Inline Sets		Inline Sets with Hardware Bypass	
Licenses Required	Essentials	Licenses Required	Essentials
Works in Evaluation Mode	Yes	Works in Evaluation Mode	Yes
IP Addressing	Not required	IP Addressing	Not required
Supported with HA'd devices	Yes	Supported with HA'd devices	No
Other (only routed mode)	Yes	Other (only routed mode)	Yes
Multi-instances supported?	Not Supported on 3100 Series	Multi-instances supported?	Not Supported on 3100 Series
Supported with clustered devices?	Not Supported on 3100 Series	Supported with clustered devices?	Not Supported on 3100 Series

라이센싱 및 호환성

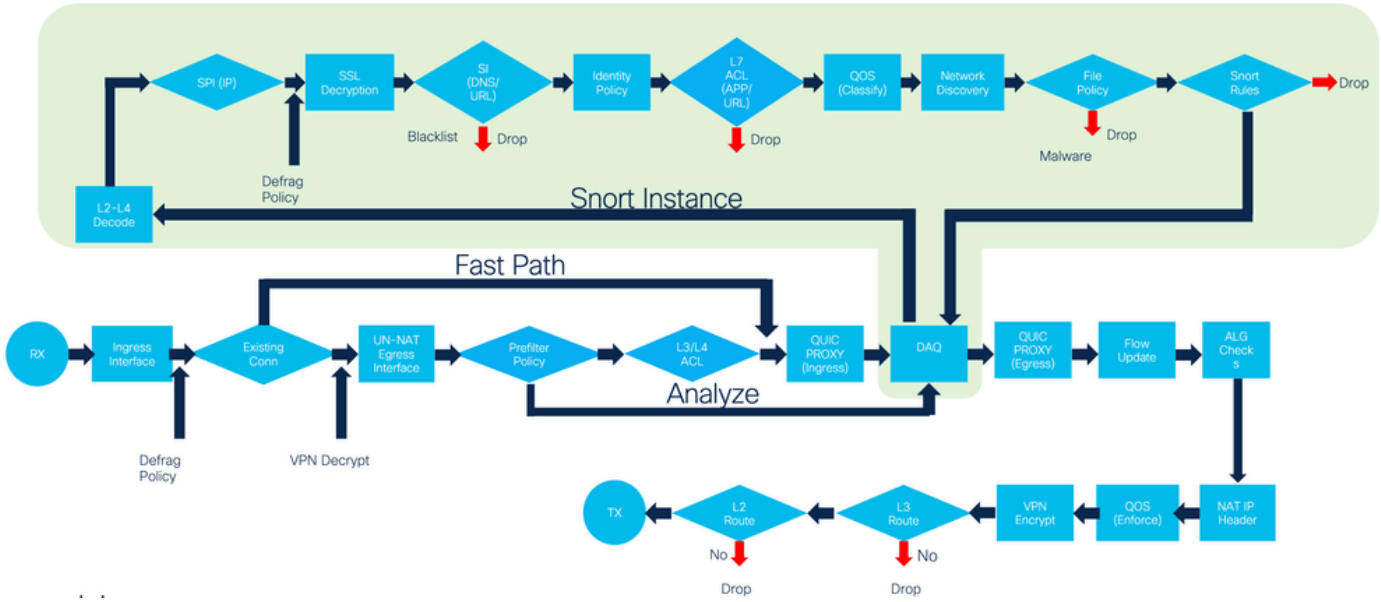
기능 설명 및 연습

기능 기능 설명

- 인라인 집합 네트워크 다이어그램

인라인 집합 네트워크 다이어그램

- 트래픽은 물리적 연결만 사용하여 라우터 1에서 인터페이스 A 및 B를 통해 라우터 2로 이동합니다.
- FDM 인라인 세트 패킷 처리 흐름 다이어그램:



순서도

- 인라인 집합:
  - 인라인 집합은 물리적 인터페이스 및 EtherChannel에서 지원됩니다.

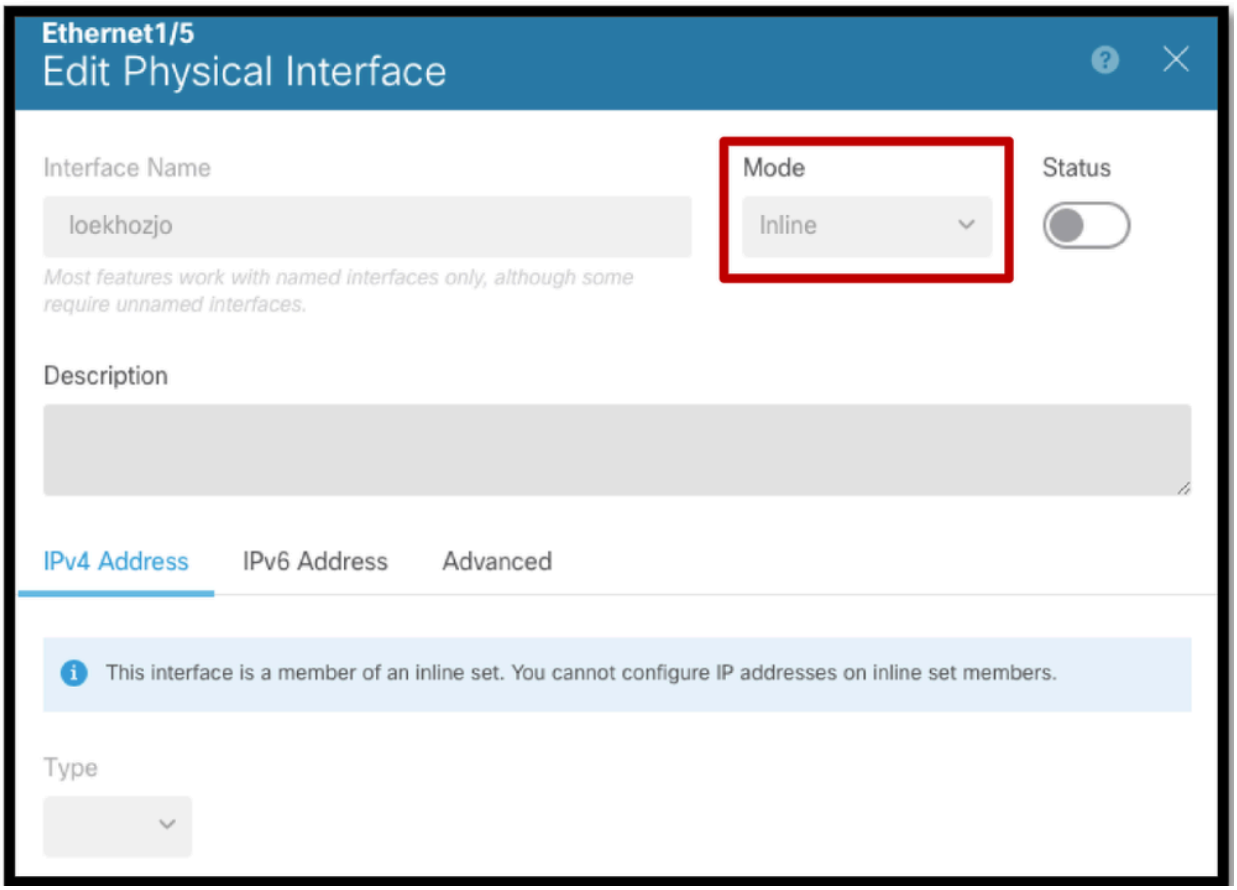
- 하드웨어 바이패스:
  - 하드웨어 바이패스가 있는 인라인 집합은 미리 결정된 물리적 인터페이스 쌍에서 지원됩니다.
    이더넷 1 및 2
    이더넷 2 및 3
    이더넷 4 및 5
    이더넷 5 및 6

- 인터페이스 지원:
  - 인라인 쌍의 일부인 인터페이스:
    이름을 지정해야 합니다.
    어떤 것으로부터도 자유로워지세요P, DHCP 또는 PPPoE 구성
    수동 모드가 아니어야 합니다.
    관리 인터페이스가 아니어야 합니다.
    한 번에 하나의 인라인 쌍에서만 사용해야 합니다.

- 인라인 모드 세부 정보
  - 인라인 모드는 물리적 인터페이스, EtherChannel 및 보안 영역에 사용할 수 있습니다.
  - 인라인 모드에서 인터페이스 및 EtherChannel을 인라인 쌍에서 사용할 경우 인라인 모드가 자동으로 설정됩니다.
  - 인라인 모드에서는 관련 인터페이스 및 EtherChannel을 인라인 쌍에서 제거할 때까지 해당 인터페이스에서 변경할 수 없습니다.
  - 인라인 모드에 있는 인터페이스는 인라인 모드로 설정된 보안 영역과 연결할 수 있습니다.

- 인라인 모드 GUI

- Edit Interface(인터페이스 수정) 대화 상자에는 인터페이스 또는 EtherChannel이 인라인 모드에 있음을 반영합니다.
- 인라인 모드에서는 인터페이스를 변경할 수 없습니다. Edit Physical Interface(물리적 인터페이스 수정)(또는 Edit EtherChannel) 대화 상자는 읽기 전용입니다.

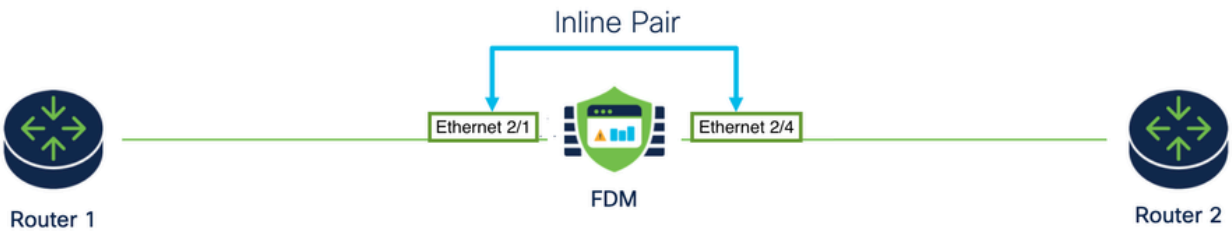


GUI에서 인터페이스 편집

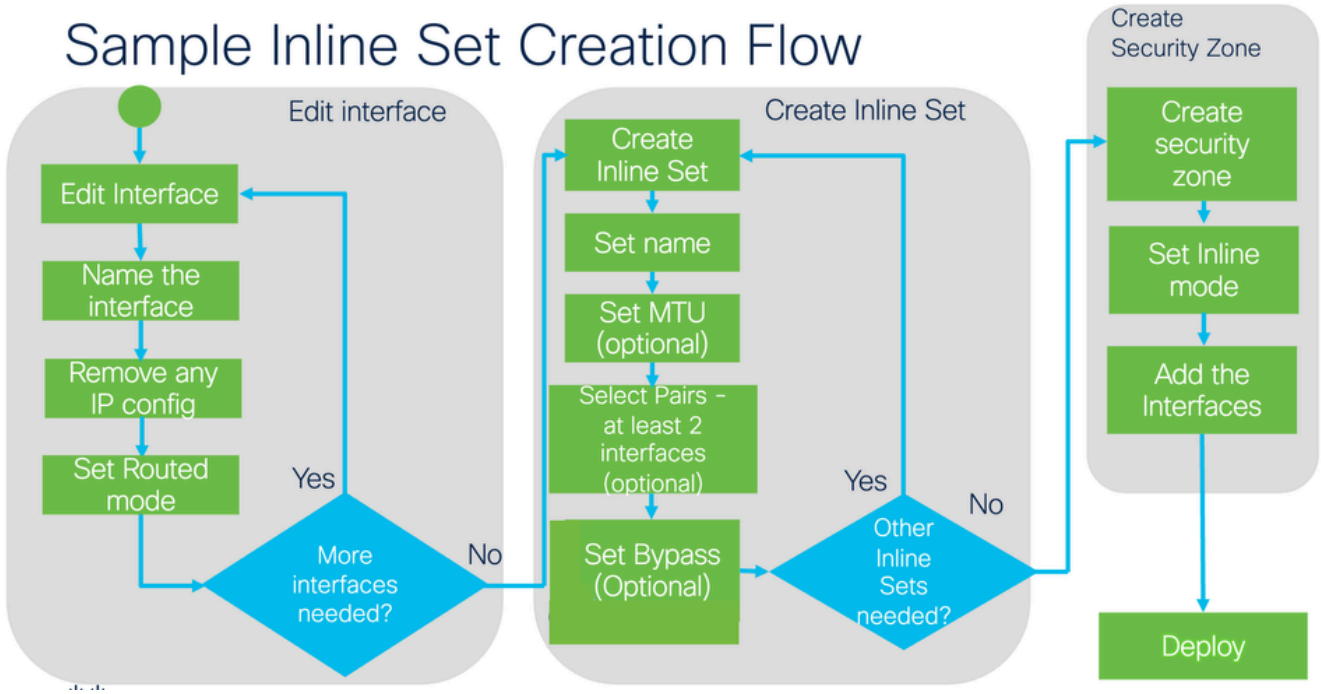
- 업그레이드, 가져오기/내보내기, 백업/복원, 구축
  - 업그레이드에 미치는 영향
    사용자는 제한 없이 FDM을 업그레이드할 수 있습니다.
    이전 버전에서 업그레이드할 때 기존 인라인 집합 개체는 바이패스 필드가 Disabled로 설정된 상태로 구성됩니다.
  - 가져오기/내보내기 관련
    Inline Set 객체는 가져오고 내보냅니다.
  - 백업/복원
    인라인 집합 개체는 백업/복원 중에 처리됩니다.
  - 구축
    객체는 정상적으로 구축됩니다.
    특정 오류가 구현되었습니다.

구성

네트워크 다이어그램



네트워크 다이어그램



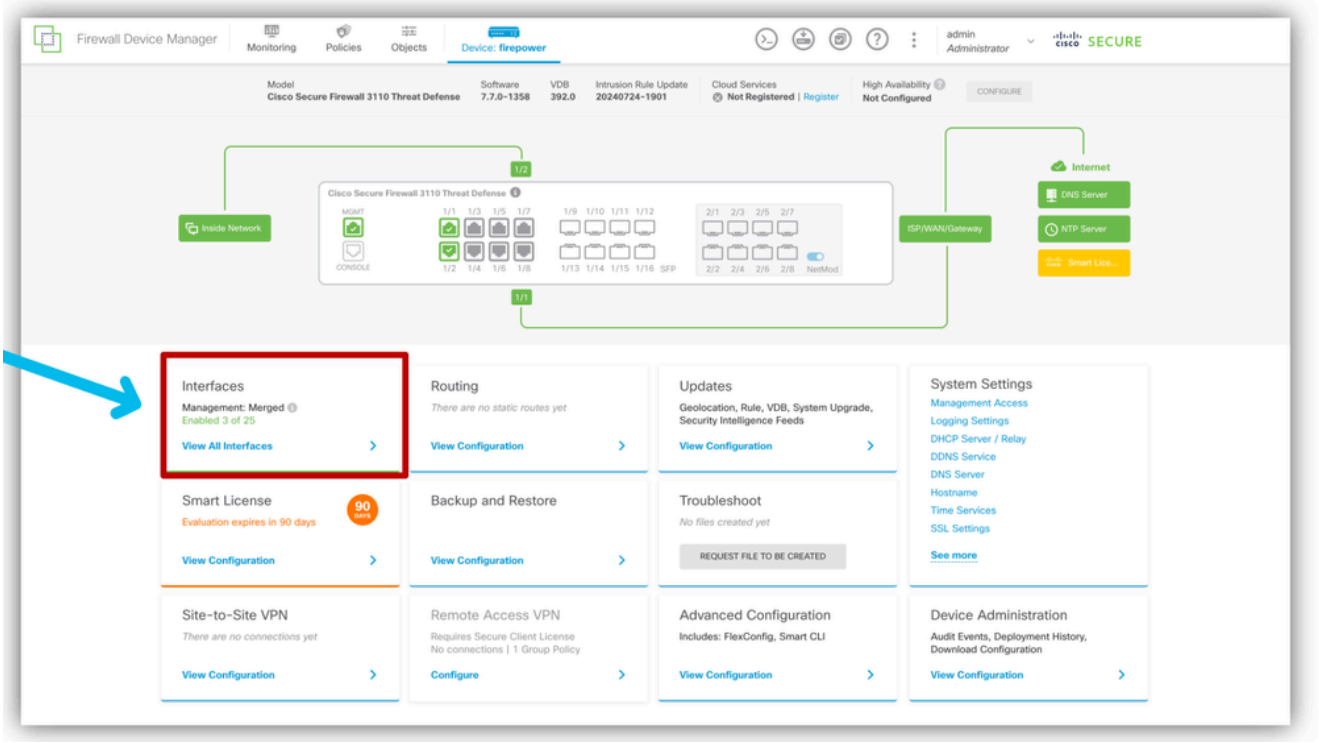
인라인 집합 생성 흐름

설정

이 섹션에서는 FDM에서 하드웨어 우회를 구성하는 단계를 설명합니다

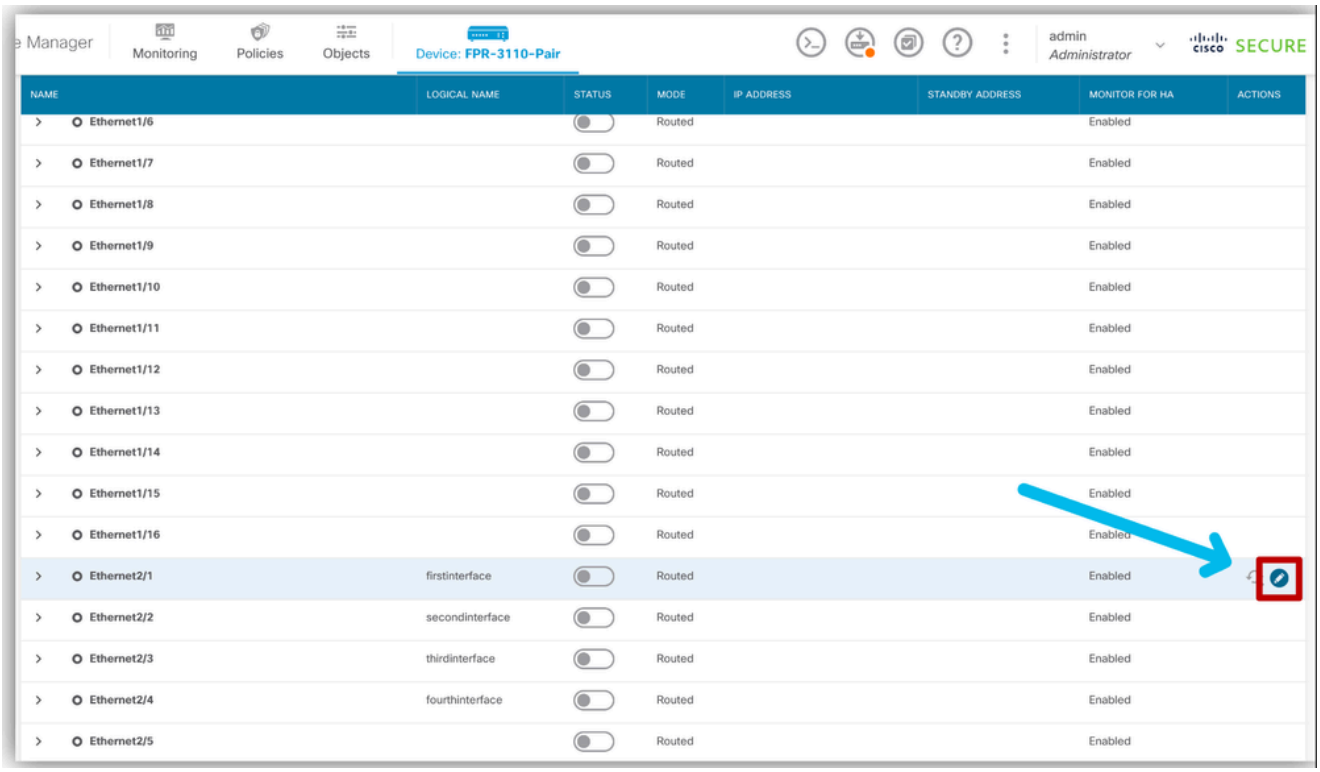
1단계: 인터페이스 수정

- FDM 및 n에 로그인탐색 대상 인터페이스 관리.
- FDM 대시보드에서 Interfaces(인터페이스) 카드를 클릭합니다.



인터페이스 선택

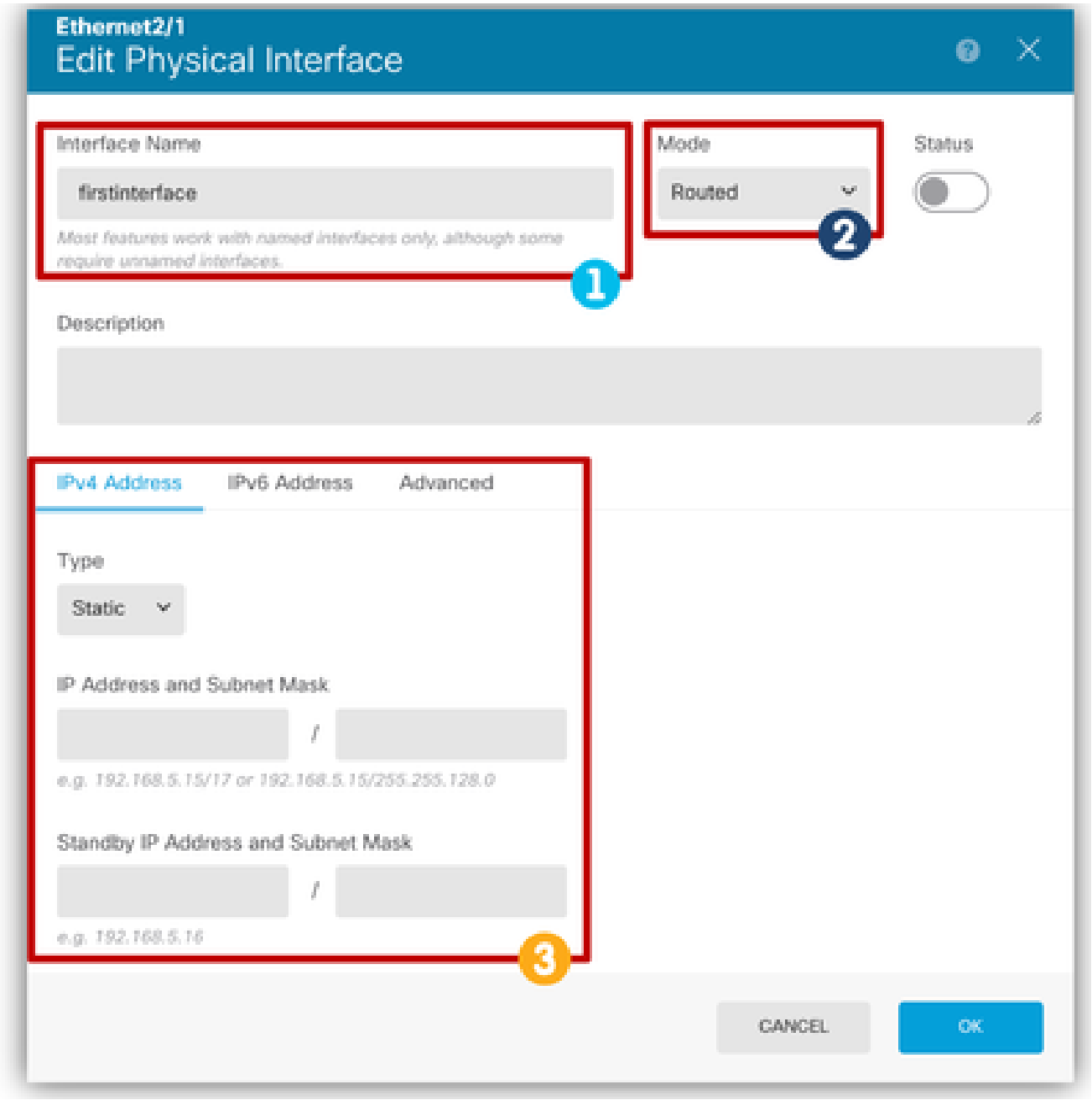
- 인라인 집합에서 사용되는 인터페이스를 편집합니다.
- 인터페이스를 수정하려면 인터페이스의 편집(연필) 아이콘을 클릭합니다.



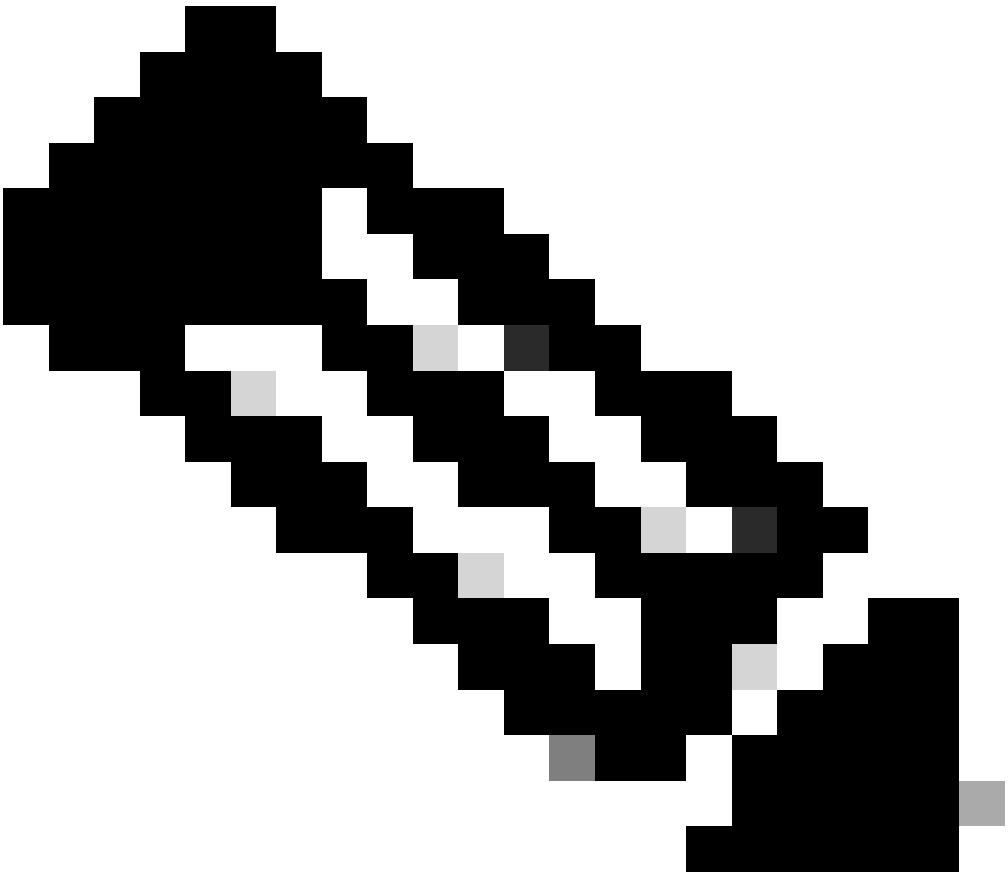
인터페이스 편집

- 물리적 인터페이스 편집:
  1. 인터페이스의 이름입니다.

2. 라우팅 모드를 선택합니다.
3. IP 구성을 제거합니다.



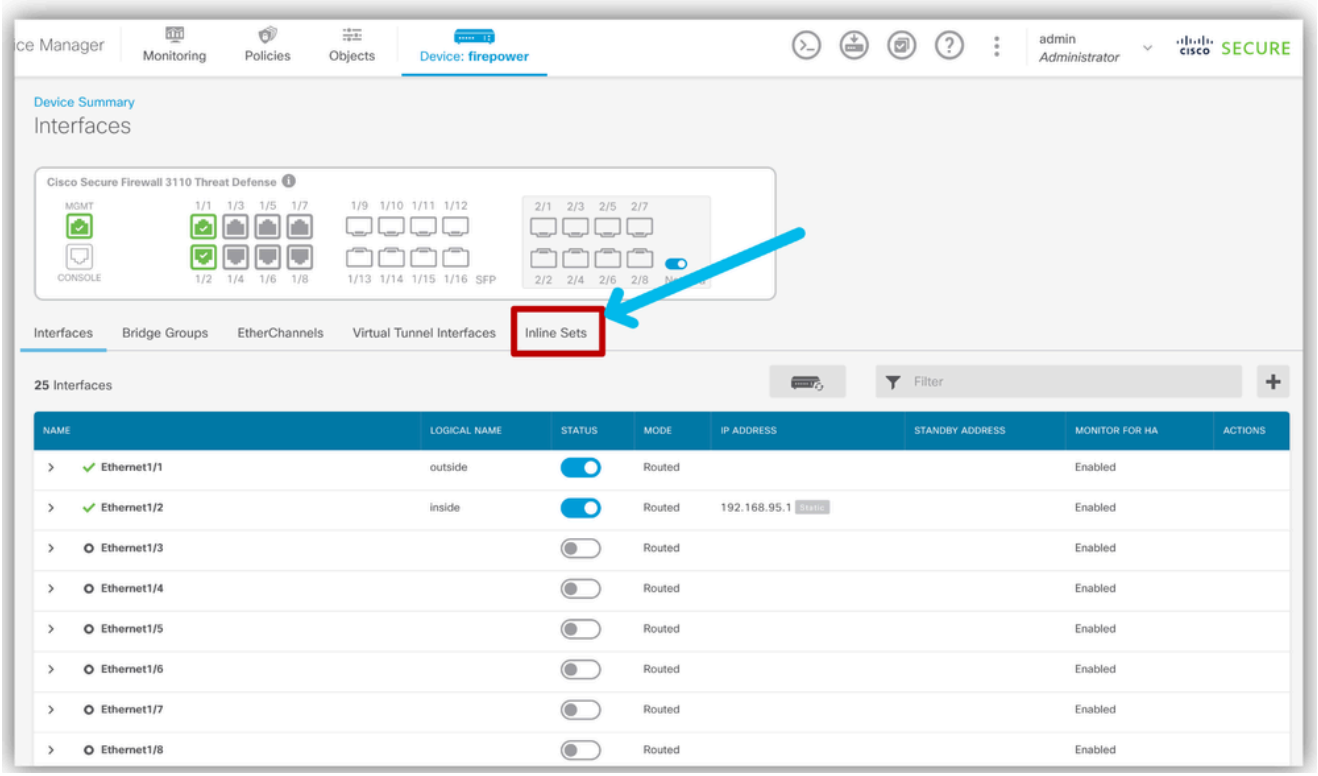
매개변수 구성



참고: 인터페이스가 인라인 쌍에 추가되면 모드가 자동으로 인라인으로 변경됩니다.

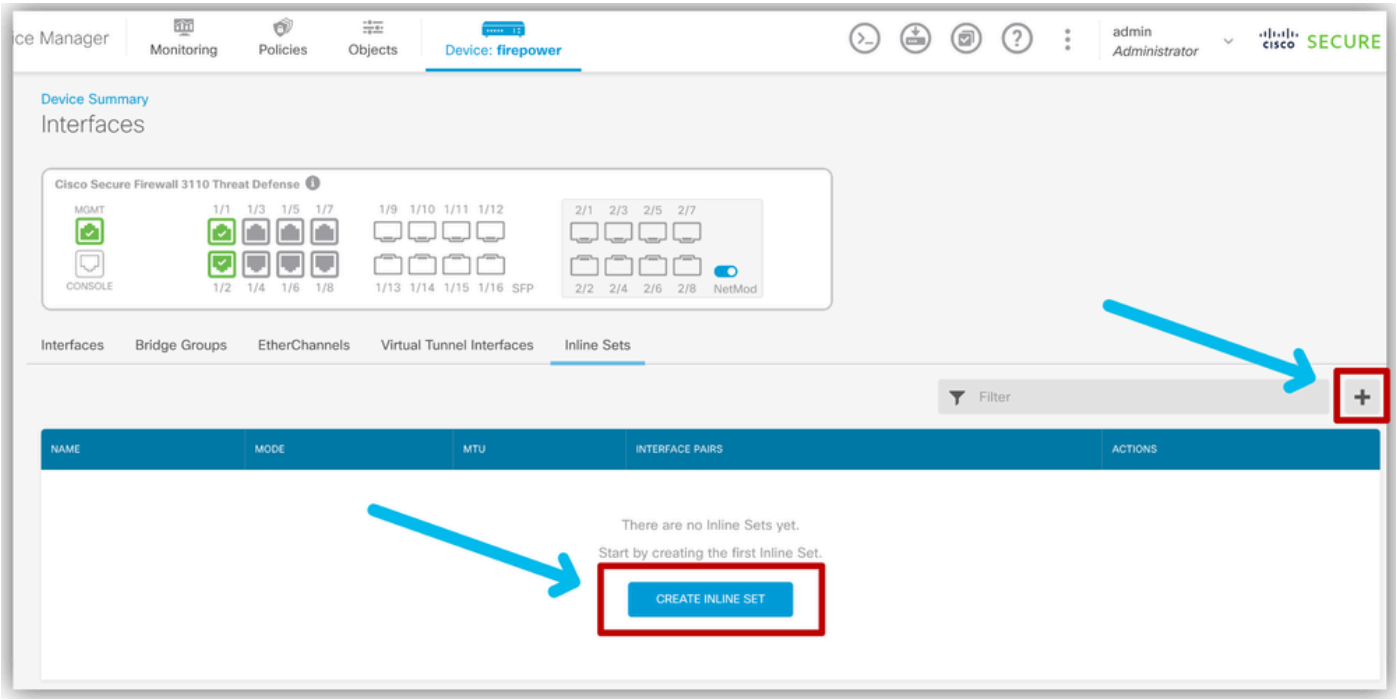
2단계: 인라인 집합을 생성합니다.

- Device(디바이스) > Interfaces(인터페이스) > Inline sets(인라인 집합) 탭으로 이동합니다.



Inline Sets(인라인 집합) 탭으로 이동

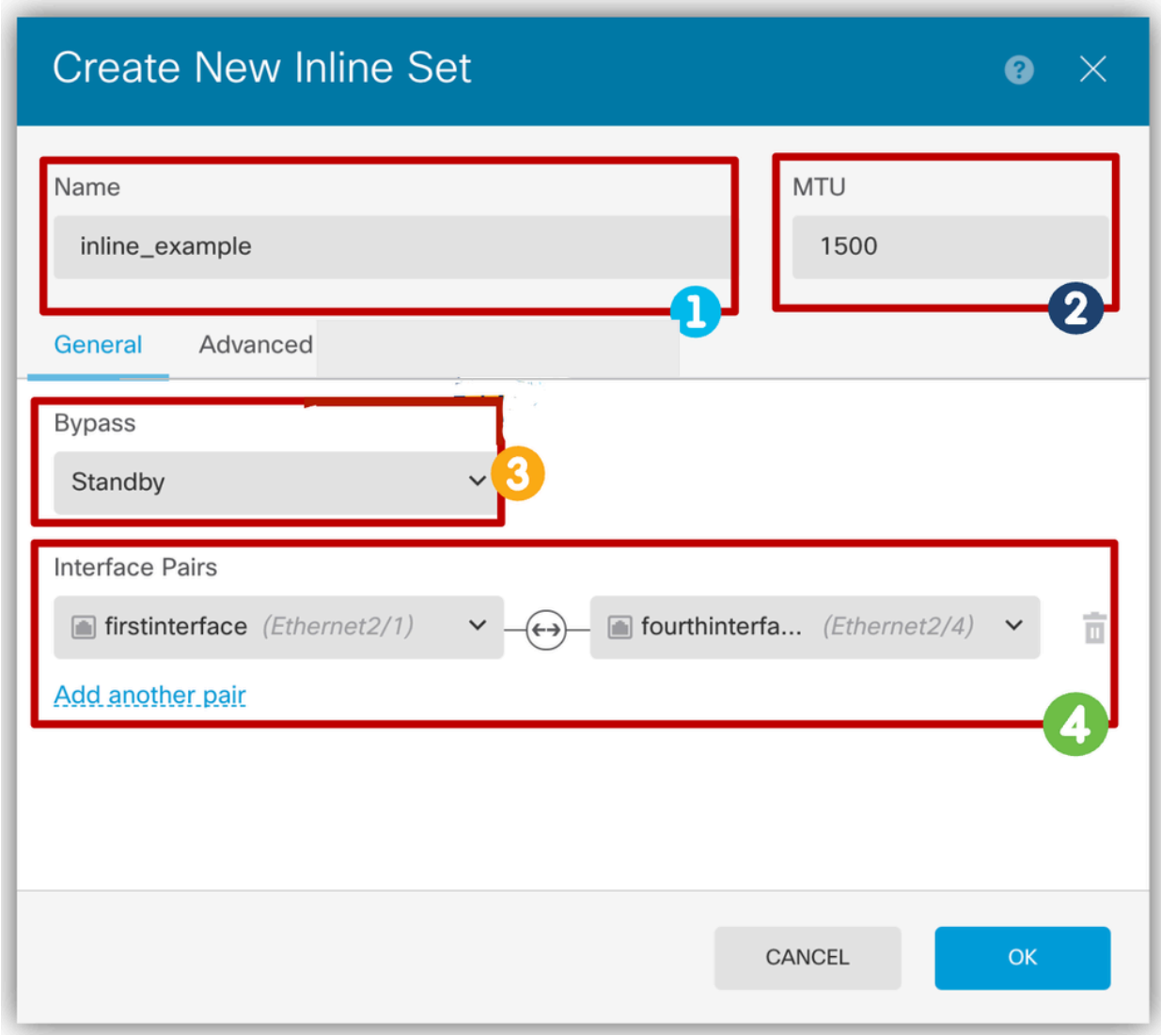
- 새 인라인 집합을 추가합니다.
- + 아이콘 또는 Create Inline Set 버튼을 클릭합니다.



인라인 집합 생성

.

- 기본 설정을 구성합니다.
  1. 이름을 설정합니다.
  2. 원하는 MTU를 설정합니다(선택 사항). 기본값은 1500이며, 이는 지원되는 최소 MTU입니다.
  3. 하드웨어 Bypass(다음 섹션에서 사용 가능한 세부 정보)를 선택합니다. Bypass에 대한 새 드롭다운 메뉴가 추가되었습니다.
  4. Interface Pairs 섹션에서 interfaces를 선택합니다.
  5. 명명된 인터페이스는 선택에 사용할 수 있습니다. 추가 쌍이 필요한 경우 Add another pair(다른 쌍 추가) 링크를 클릭합니다.



설정 구성

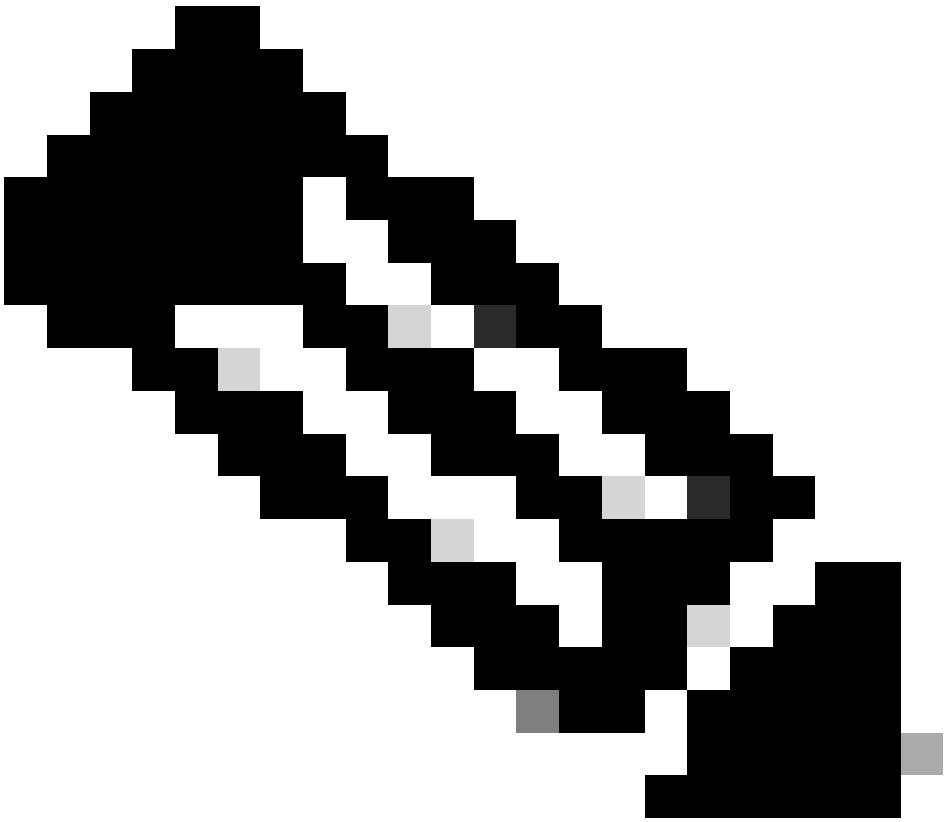
하드웨어 바이패스

기능 및 제한 사항

- 하드웨어 우회는 정전이 발생하는 동안 인라인 인터페이스 쌍 간에 트래픽이 계속 흐르도록

보장합니다. 이 기능은 소프트웨어 또는 하드웨어 장애 시 네트워크 연결을 유지하는 데 사용할 수 있습니다.

- 하드웨어 바이패스 포트는 인라인 집합에 대해서만 지원됩니다.
- 고가용성 모드에서는 하드웨어 우회가 지원되지 않습니다.
- 하드웨어 바이패스 모드:
  - DISABLED(비활성화됨) - 지원되는 인터페이스에서 바이패스를 비활성화합니다. 지원되지 않는 인터페이스에 대한 기본 모드입니다.
  - STANDBY - 대기 상태에서는 트리거 이벤트가 발생할 때까지 인터페이스가 정상 작동 상태로 유지됩니다.
  - BYPASS FORCE - 수동으로 인터페이스 쌍을 검사를 우회하도록 강제합니다.



참고: FTD 인터페이스 유형 및 하드웨어 바이패스에 대한 정보

Snort Fail Open vs 하드웨어 바이패스

- 하드웨어 바이패스 기능을 사용하면 완벽한 정전 및 특정 제한된 소프트웨어 장애를 포함하여 하드웨어 장애 중에 트래픽이 이동할 수 있습니다.
- Snort Fail Open을 트리거하는 소프트웨어 오류는 하드웨어 우회를 트리거하지 않습니다.

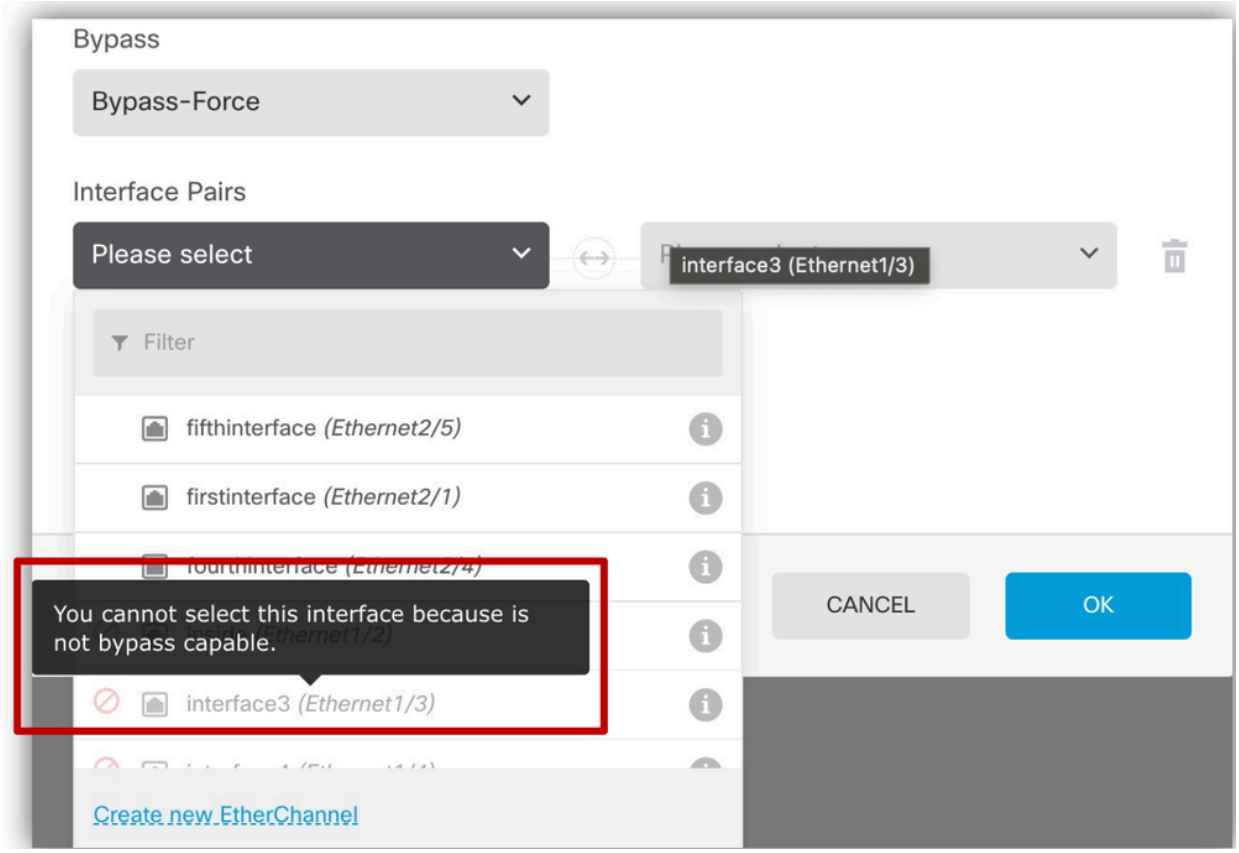
하드웨어 바이패스 트리거

하드웨어 우회는 다음 시나리오에서 트리거될 수 있습니다.

- 애플리케이션 충돌
- 애플리케이션 재부팅
- 디바이스 충돌
- 디바이스 재부팅 또는 업그레이드
- 장치 전력 손실
- 수동 트리거

하드웨어 우회를 지원하는 인터페이스를 보려면

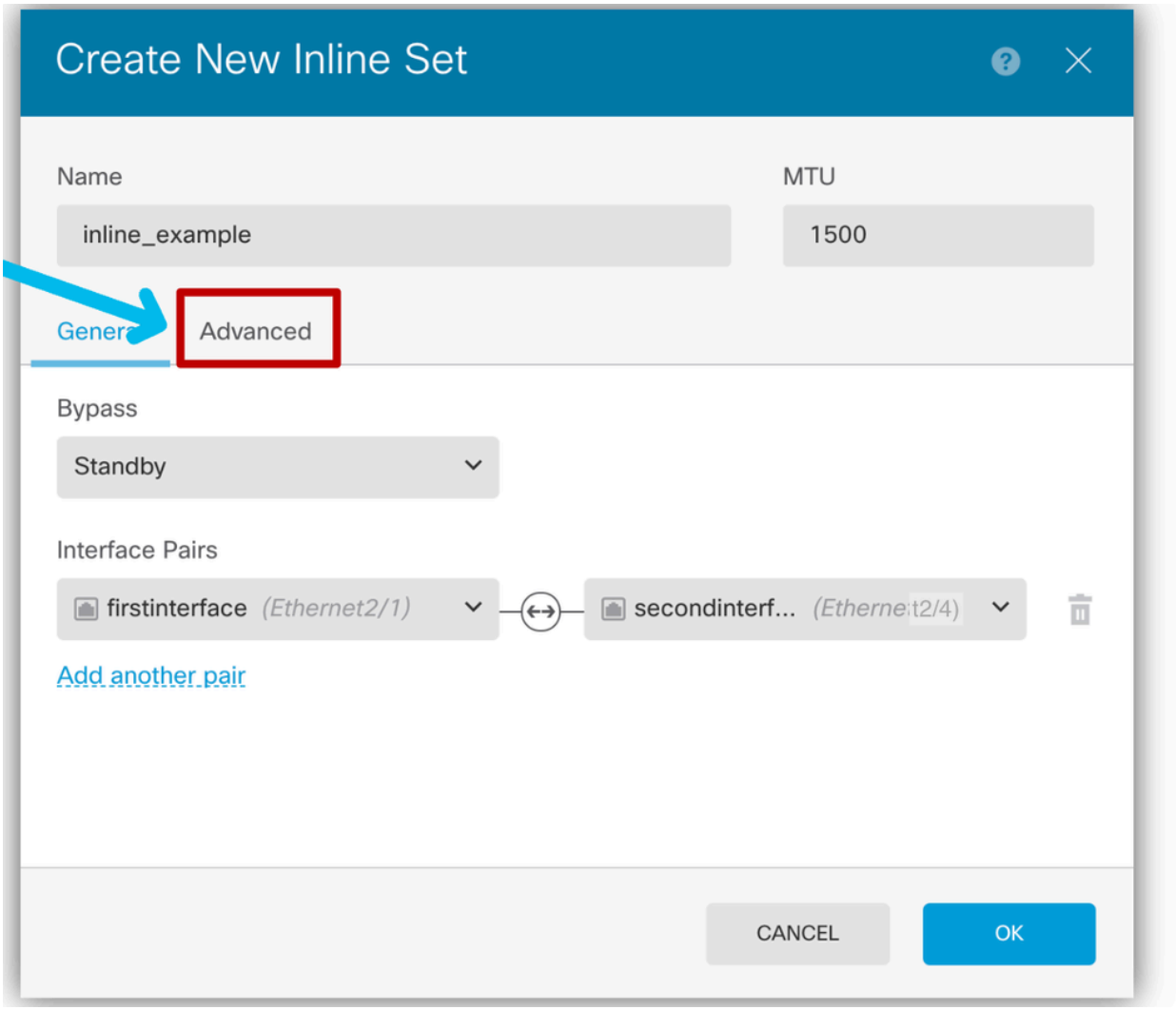
- FDM GUI에서 Bypass(우회)를 선택한 경우 다음을 수행합니다.
  - 이를 지원하는 인터페이스는 선택할 수 있습니다.
  - 지원되지 않는 인터페이스는 회색으로 표시됩니다.
  - 이 예에서 Ethernet1/3은 다음 그림에서 회색으로 표시됩니다.



하드웨어 바이패스 지원 확인

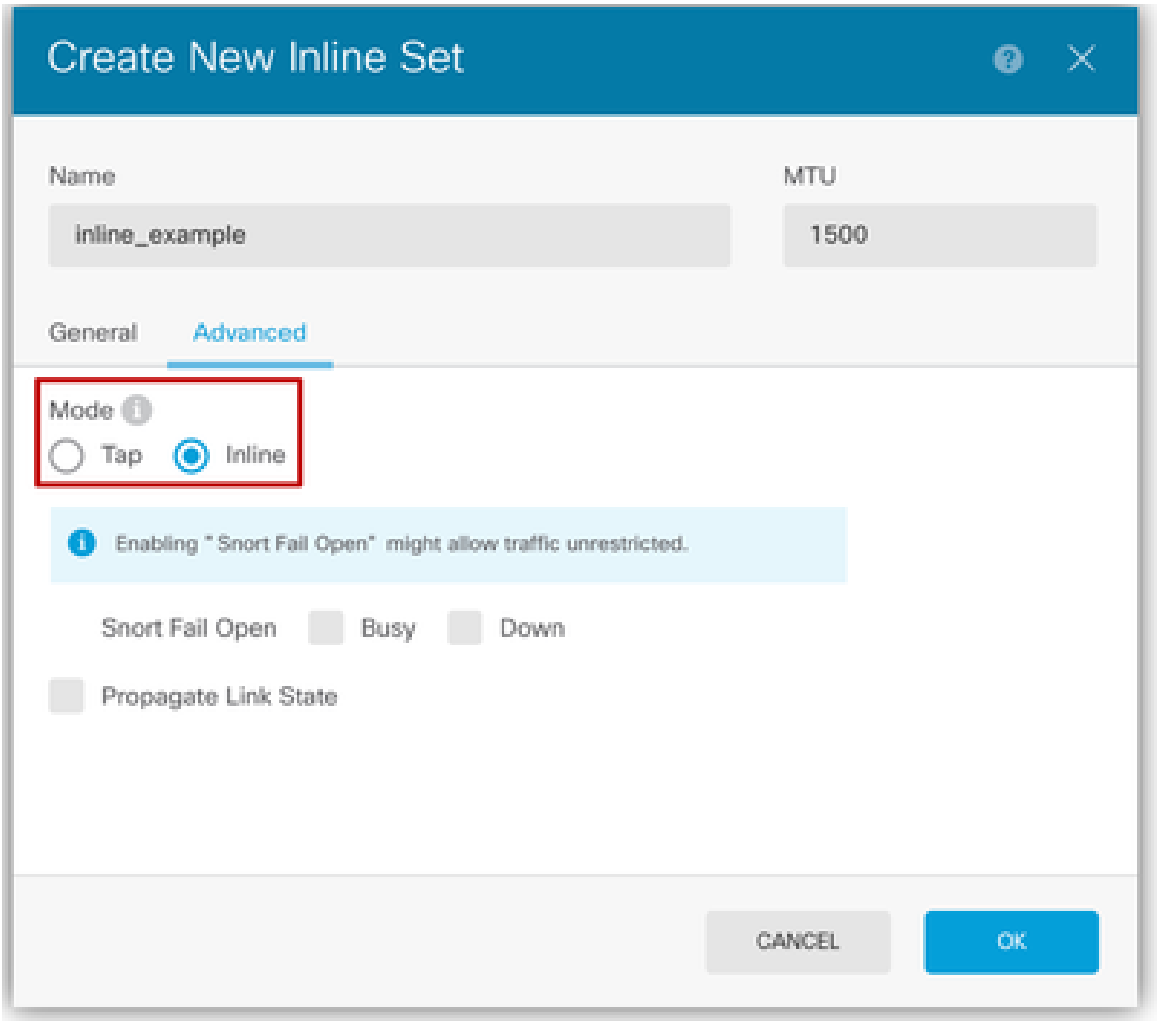
3단계: 인라인 집합 고급 설정을 구성합니다.

- Device(디바이스) > Interfaces(인터페이스) > Inline sets(인라인 집합) 탭으로 이동하거나 이미 생성된 인라인 집합을 수정합니다.
- 고급 탭으로 이동합니다.
  - Advanced(고급) 탭에서는 Inline Sets(인라인 집합)에 대한 옵션 설정을 구성할 수 있습니다.
  - Advanced(고급) 탭을 클릭합니다.



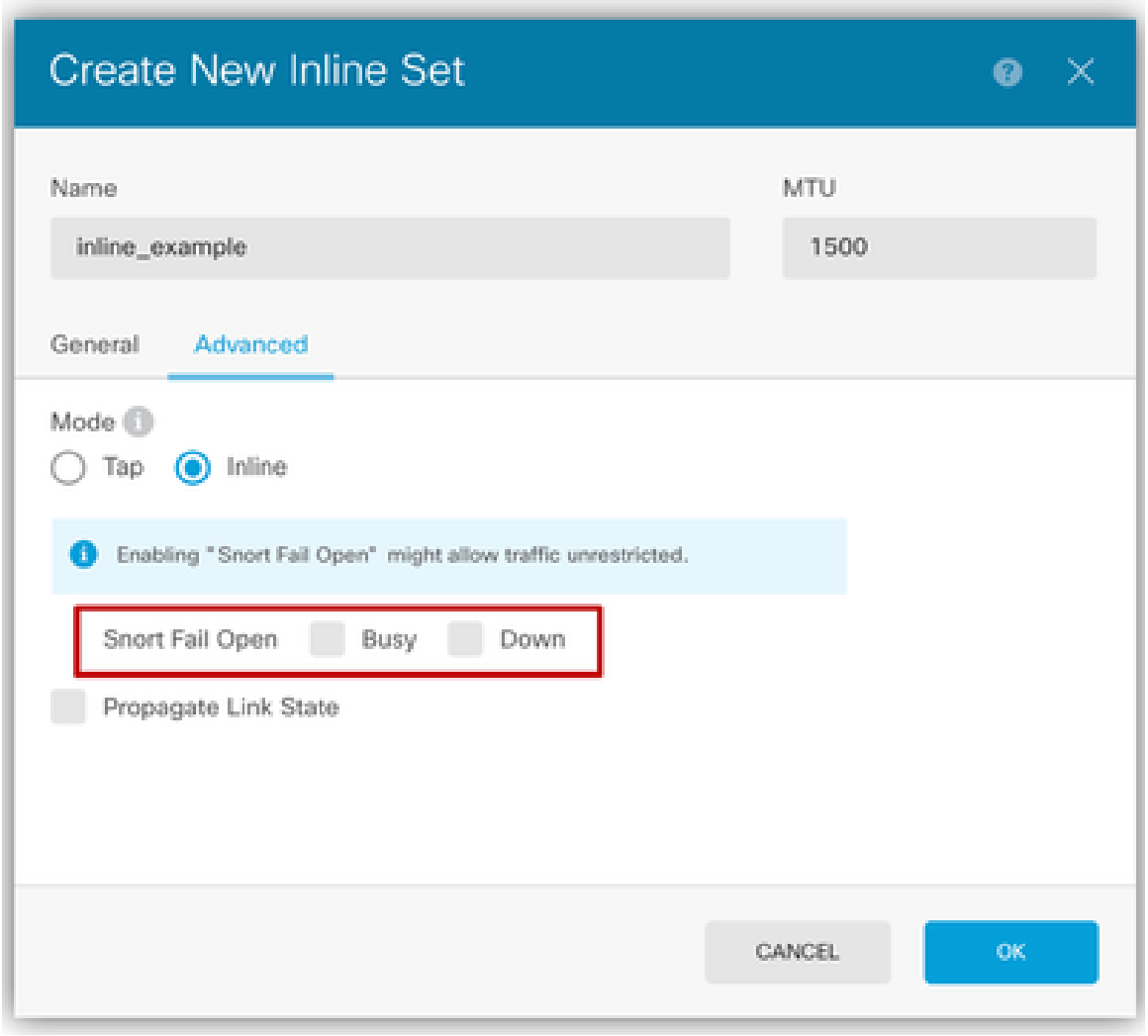
인라인 집합 구성

- 모드로 들어갑니다
  - 탭: 인라인 탭 모드로 설정합니다. 탭 모드가 활성화된 경우 Snort Fail Open이 비활성화됩니다.
  - 인라인



모드 선택

- Snort 실패 열기 설정
  - 원하는 Snort Fail Open 설정을 선택합니다.
  - 없음, 하나 또는 둘 다. Busy 및 Down 옵션을 설정할 수 있습니다.
  - Snort Fail Open을 사용하면 Snort 프로세스가 사용 중이거나 중단된 경우 검사 없이 신규 및 기존 트래픽을 통과(활성화)하거나 삭제(비활성화)할 수 있습니다.

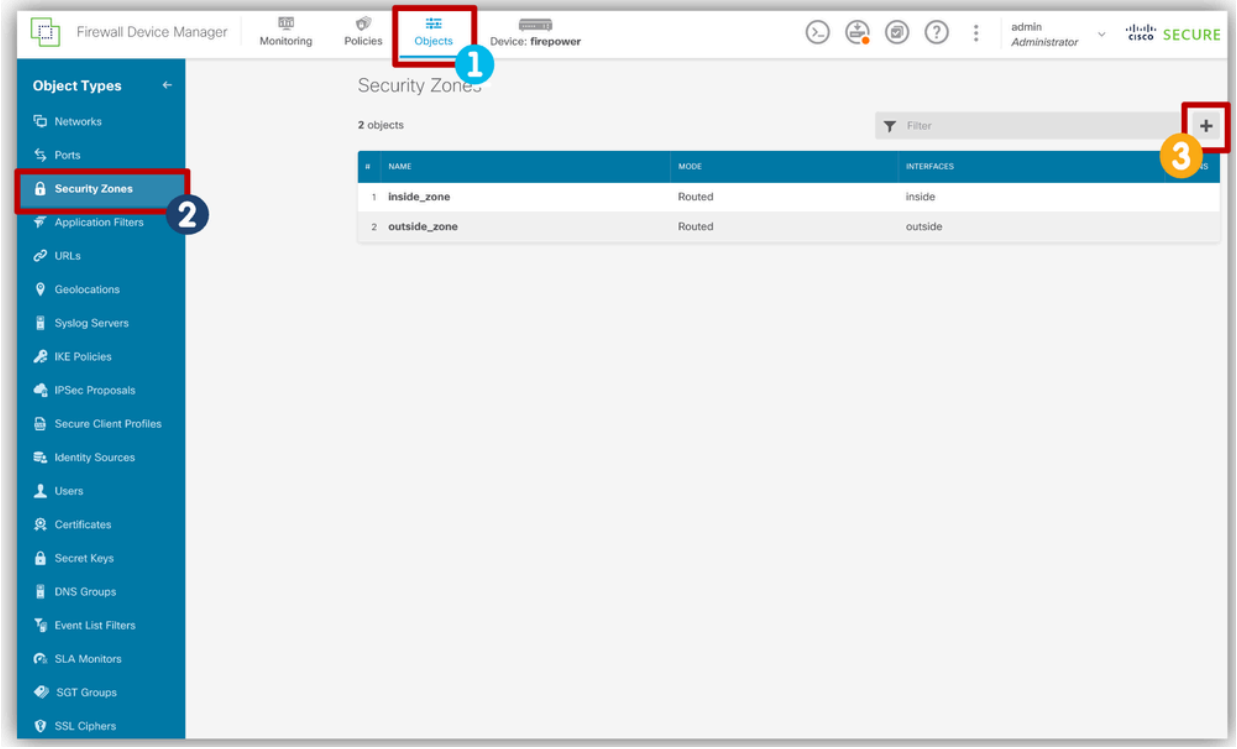


Snort Fail Open 및 Propagate 링크 상태

- 링크 상태 전파
  - Propagate Link State(링크 상태 전파)는 인터페이스 중 하나가 다운되면 인라인 쌍에서 두 번째 인터페이스를 자동으로 다운합니다. 다운된 인터페이스가 복구되면 두 번째 인터페이스도 자동으로 복구됩니다.
- 인라인 세트를 생성하려면 OK를 클릭합니다.

4단계: Security Zone(보안 영역)에 적용합니다(선택 사항).

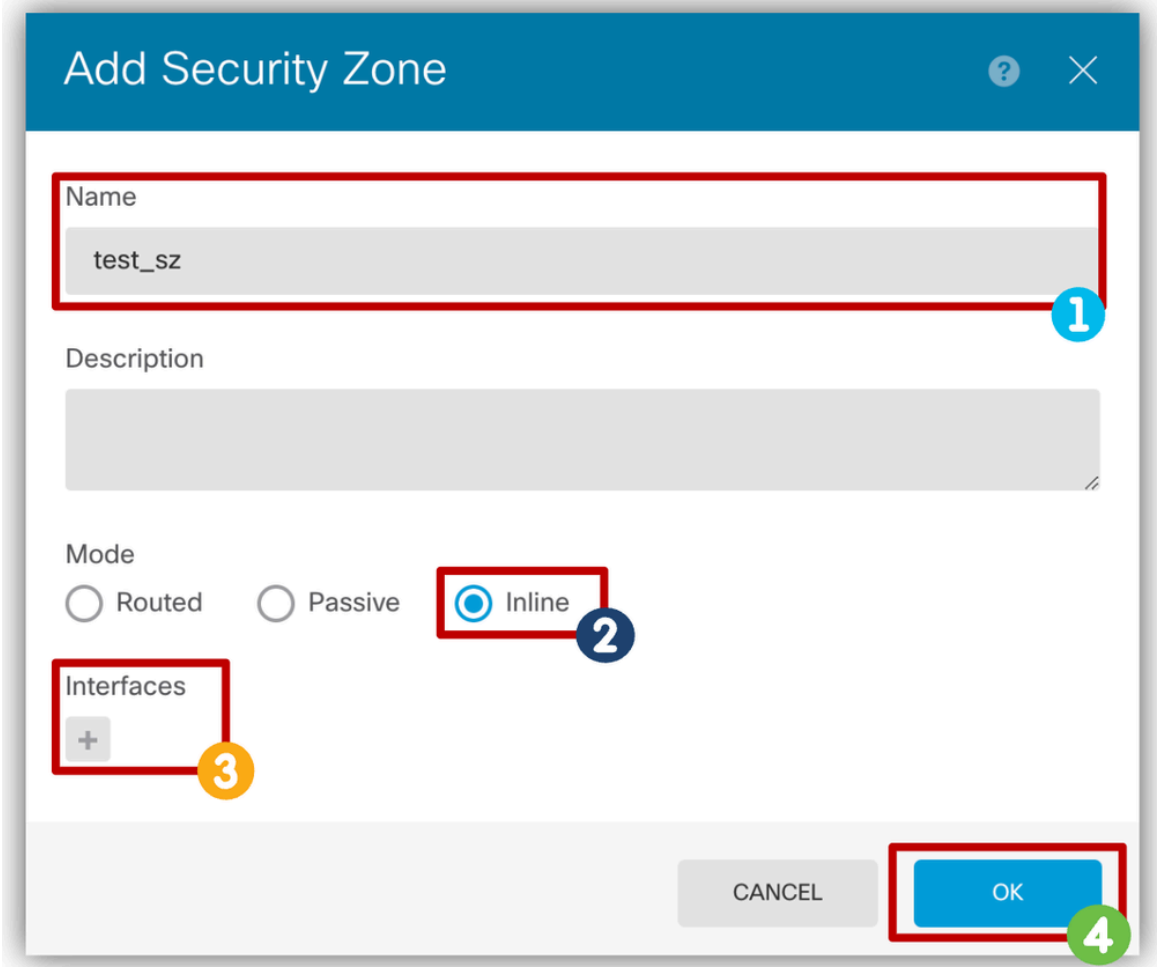
1. 위쪽 탐색 모음에서 Objects(개체)로 이동합니다.
2. 왼쪽 탐색에서 보안 영역 선택:
   - 보안 영역을 추가하려면 +를 클릭합니다.



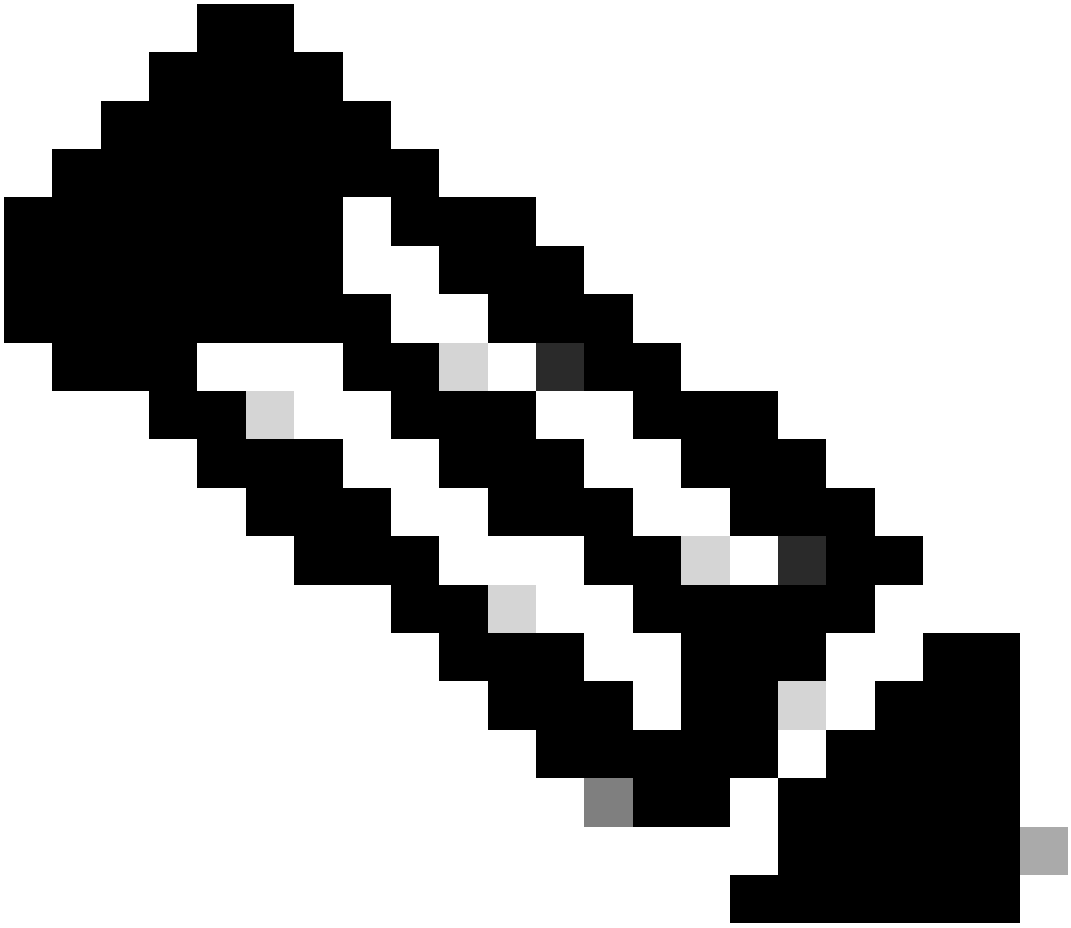
보안 영역 추가

보안 영역 구성(선택 사항)

1. 보안 영역의 이름을 지정합니다.
2. Inline Mode를 선택합니다.
   보안 영역 및 인터페이스는 동일한 모드를 가져야 합니다.
3. 인라인 집합의 일부인 Interfaces를 선택합니다.
4. OK(확인)를 클릭합니다.


Add Security Zone
Name
test_sz
1
Description
Mode
Routed
Passive
Inline
2
Interfaces
+
3
CANCEL
OK
4

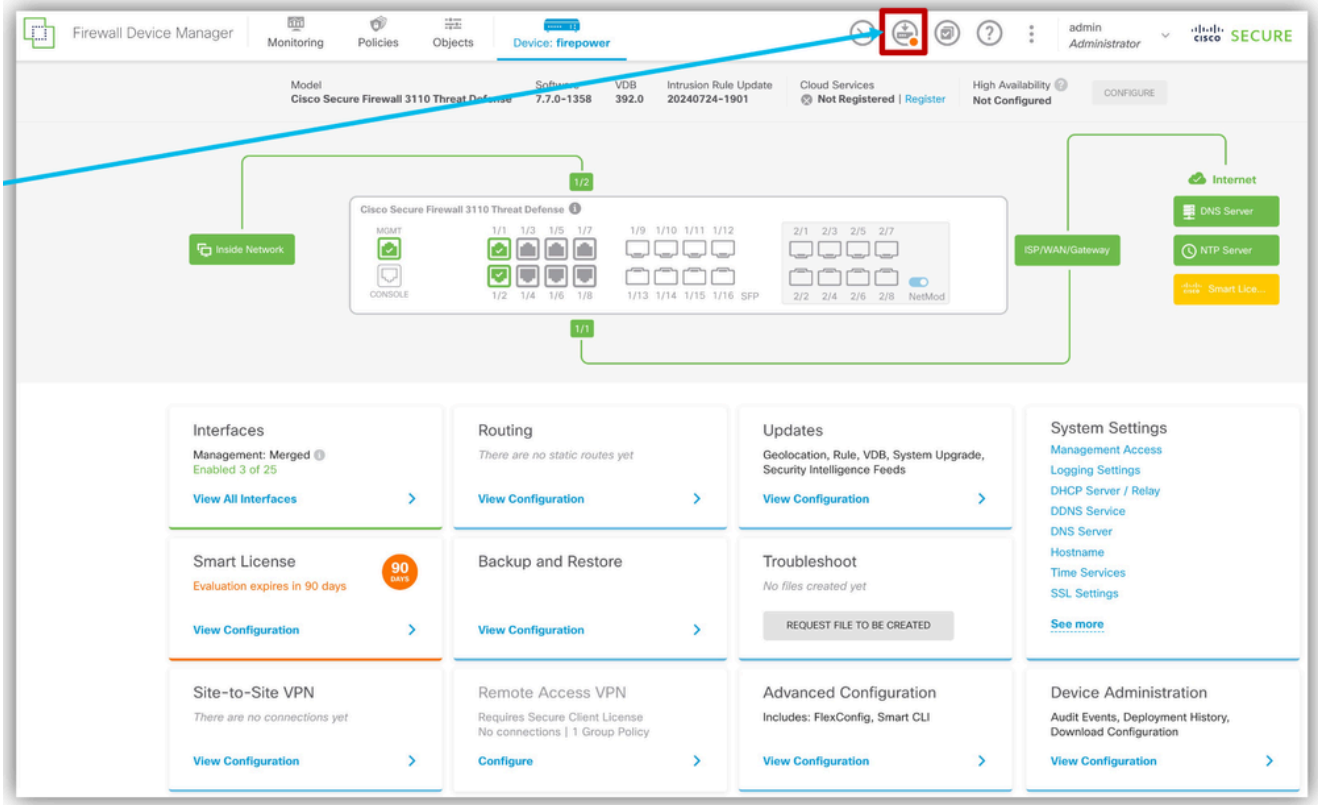
보안 영역 구성



참고: 인터페이스의 경우, 인라인 쌍에 인터페이스가 추가된 후 모드가 자동으로 인라인으로 변경됩니다.

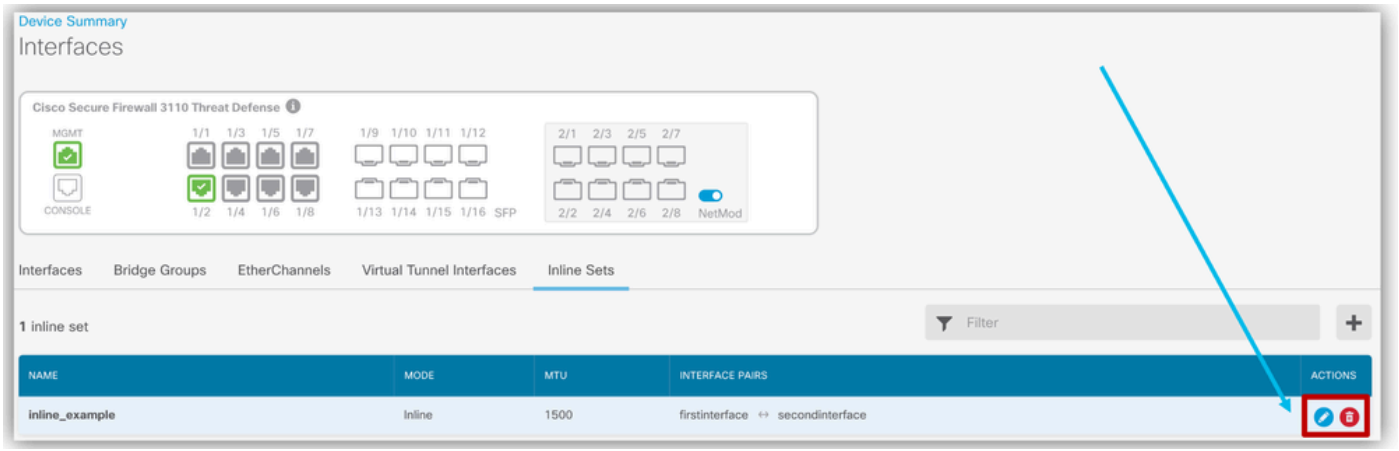
4단계: 구축

- Deployment(구축) 탭으로 이동하여 구축합니다.



변경 사항 배포

- 인라인 집합을 수정 및 삭제합니다.
  - Device(디바이스) > Interfaces(인터페이스) > Inline sets(인라인 집합) 탭으로 이동합니다.
  - Edit(수정) 및 Delete(삭제) 버튼은 인라인 집합에 사용할 수 있습니다.



인라인 집합 편집 및 삭제

FDM 장치 REST API

REST API 엔드포인트

- 가져오기: /devices/default/inlinesets

모든 기존 인라인 집합의 목록을 가져옵니다.

- GET :/devices/default/inlinesets/{objID}
  ID로 특정 인라인 집합 개체를 가져옵니다.
- POST: /devices/default/inlinesets
  새 인라인 집합을 만듭니다.
- PUT: /devices/default/inlinesets/{objID}
  ID로 기존 인라인 집합 개체를 업데이트합니다.
- 삭제:/devices/default/inlinesets/{objID}
  ID로 기존 인라인 집합 개체를 삭제합니다.
- GET :/operational/interfaceinfo/{objID}
  모든 InterfaceInfoentities 목록을 가져옵니다.
- 하드웨어 우회를 지원하기 위해 InterfaceInfo API에 새 필드가 추가되었습니다.

인터페이스 정보 REST API 모델

- 하드웨어 바이패스 통합을 지원하기 위해 새 field bypassInterfacePeerIdid가 추가되었습니다
  .
- 이 필드는 현재 인터페이스에 대한 하드웨어 바이패스 인터페이스 쌍의 ID를 나타냅니다.
- 값:
  - Null - 인터페이스가 우회를 지원하지 않습니다.
  - ID - 인터페이스에서 바이패스를 지원합니다.

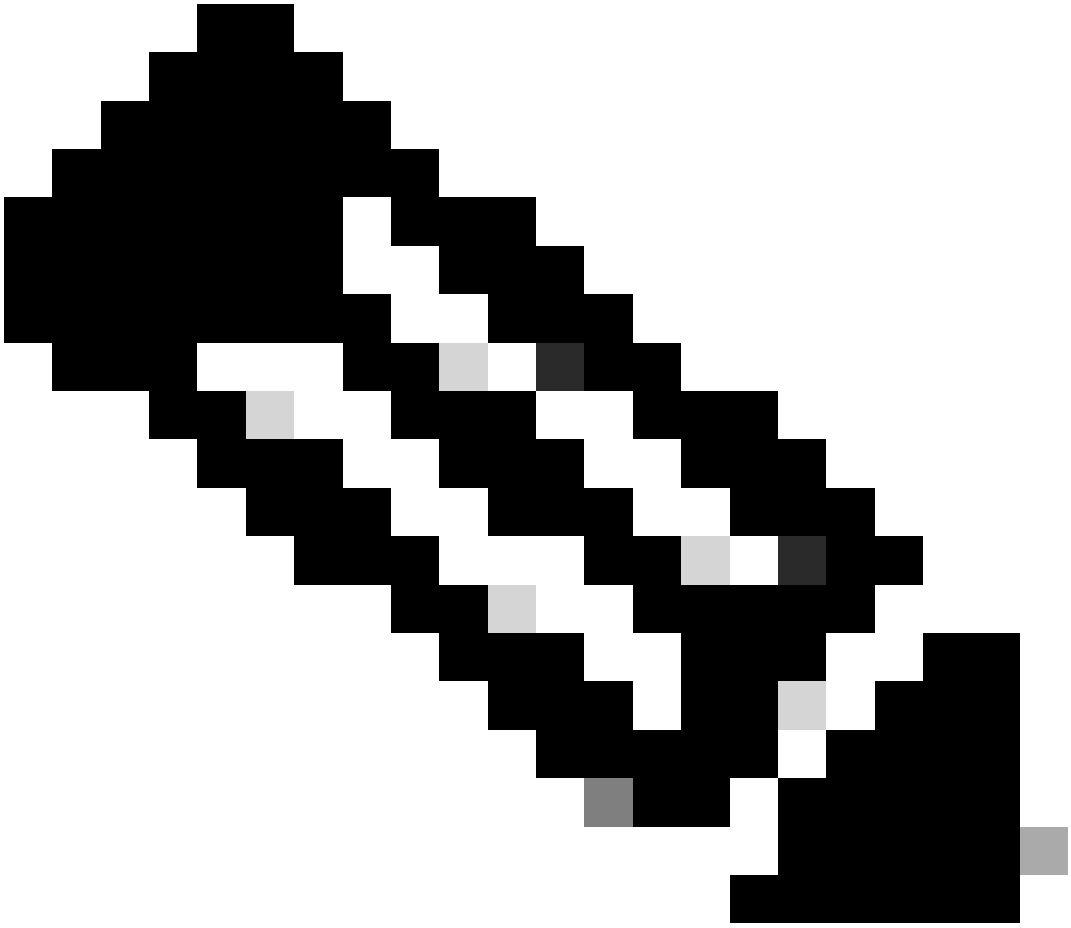
인터페이스 정보 REST API

인터페이스 정보 REST API 예

- 인터페이스 정보 REST API 예입니다.
  - Interface without Hardware Bypass support(Ethernet 1/4).
  - 하드웨어 바이패스 지원이 포함된 인터페이스 쌍(Ethernet2/1 및 Ethernet 2/2).

```
{ "interfaceInfoList": [
    {
        "interfaceId": "da9edc2d-58ba-11ef-b764-ffea0b8d9fa2",
        "hardwareName": "Ethernet1/4",
        "bypassInterfacePeerId": null,
        ...
    },
    {
        "interfaceId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
        "hardwareName": "Ethernet2/1",
        "bypassInterfacePeerId": "dc74fbc3-58ba-11ef-b764-11d423dbcbd7",
        ...
    },
    {
        "interfaceId": "dc74fbc3-58ba-11ef-b764-11d423dbcbd7",
        "hardwareName": "Ethernet2/2",
        "bypassInterfacePeerId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
        ...
    }],
  "id": "default",
  "type": "interfaceinfo",
  "links": { "self": "https://u90c04p02-
vrouter.cisco.com:25455/api/fdm/v6/operational/interfaceinfo/1/default"
    }
}
```


인터페이스 정보 REST API 예



참고: 크기 때문에 전체 호출의 코드 조각입니다.

인라인 집합 REST API 모델

- 인라인 집합 모델은 다음으로 구성됩니다.
  - 유형
  - 이름
  - 탭 모드
  - MTU
  - 링크 상태 전파
  - Fail Open Snort 사용 중
  - 우회 값: DISABLED, STANDBY, BYPASS_FORCE

인라인 집합 REST API

인라인 집합 REST API 예

- 다음과 같은 기본 인라인 집합의 예:

- 인라인 쌍 1개
- 대기 모드 우회

```
{
  "name": "inline_set_example",
  "type": "inlineset",
  "tapMode": false,
  "mtu": 1500,
  "propagateLinkState": false,
  "failOpenSnortBusy": false,
  "failOpenSnortDown": true,
  "bypass": "STANDBY",
  "inlinePairs": [
    {
      "first": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "second": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "type": "inlinesetpair"
    }
  ]
}
```

2. 인라인 집합을 만듭니다(페이로드 예는 API 탐색기 참조).

POST/디바이스/기본/인라인 세트
3. 보안 영역 만들기(페이로드 예제는 API 탐색기 참조)(선택 사항).
POST/object/security 영역
4. 장치에 구축(페이로드 예제는 API 탐색기 참조).
사후/운영/구축

하드웨어 바이패스로 인라인 집합 구성 및 구축

1. 인터페이스 ID 및 하드웨어 바이패스 인터페이스 쌍에 대한 정보를 가져옵니다(페이로드 예는 API 탐색기 참조).
GET/operational/interfaceinfo/{objId}
2. 인라인 집합을 만듭니다(페이로드 예는 API 탐색기 참조).
POST/디바이스/기본/인라인 세트
3. 보안 영역 만들기(페이로드 예제는 API 탐색기 참조)(선택 사항).
POST/object/security 영역
4. 장치에 구축(페이로드 예제는 API 탐색기 참조).
사후/운영/구축

인라인 집합 편집

1. 인터페이스 ID를 가져옵니다(페이로드 예는 API 탐색기 참조).
GET/디바이스/기본/인터페이스
2. 인라인 집합을 가져옵니다.
GET/장치/기본/인라인 집합
3. 인라인 집합을 편집합니다(페이로드 예는 API 탐색기 참조).
PUT/devices/default/inlinesets/{objId}
4. 장치에 배포합니다(페이로드 예는 API 탐색기 참조).
사후/운영/구축

다음을 확인합니다.

<#root>

> show running-config inline-set

```
inline-set test_inline_0
    interface-pair test2 test1
inline-set test_inline_1
```

hardware-bypass standby

```
    interface-pair test27 test28
```

```
inline-set test_inline_2
    hardware-bypass bypass
    interface-pair test26 test25
```

> show inline-set

```
 Inline-set test_inline_0
   Mtuis 1600 bytes
   Fail-open for snort down is off
   Fail-open for snort busy is off
   Tap mode is off
   Propagate-link-state option is off
```

hardware-bypass mode is disabled

```
   Interface-Pair[1]:
     Interface: Ethernet1/3 "test1"
       Current-Status: DOWN
     Interface: Ethernet1/4 "test2"
       Current-Status: DOWN
     Bridge Group ID: 519
```

> show inline-set

```
Inline-set test_inline_1
Mtuis 1500 bytes
Fail-open for snort down is off
Fail-open for snort busy is off
Tap mode is off
Propagate-link-state option is off
hardware-bypass mode is standby
Interface-Pair[1]:
Interface: Ethernet2/7 "test27"
Current-Status: DOWN
Interface: Ethernet2/8 "test28"
Current-Status: DOWN
Bridge Group ID: 618
```

> show inline-set

```
Inline-set test_inline_1
Mtuis 1500 bytes
Fail-open for snort down is off
Fail-open for snort busy is off
Tap mode is off
Propagate-link-state option is off
```

hardware-bypass mode is bypass

```
Interface-Pair[1]:
Interface: Ethernet2/6 "test26"
Current-Status: DOWN
Interface: Ethernet2/5 "test25"
Current-Status: DOWN
Bridge Group ID: 610
```

```
> show interface


...
Interface Ethernet1/7 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Available but not configured via nameif

...
Interface Ethernet2/7 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Hardware bypass is supported with interface Ethernet2/8


Available but not configured via nameif

...
Interface Ethernet2/8 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Hardware bypass is supported with interface Ethernet2/7


Available but not configured via nameif
```

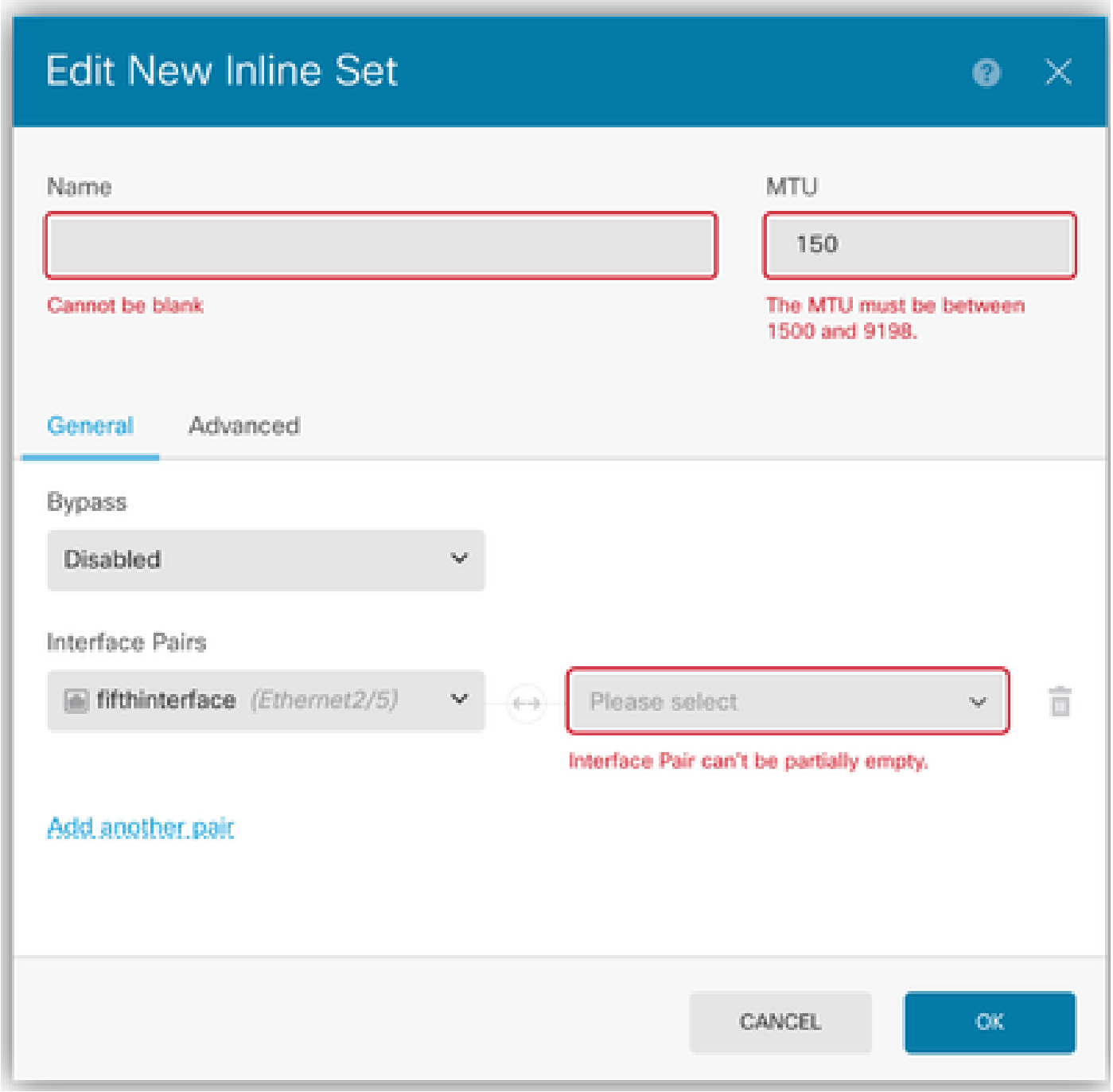
문제 해결

명령

- show running-config inline-set
- 인라인 집합 표시
- 인터페이스 표시
- 시스템 지원 추적

인라인 집합 - 생성 시 검증

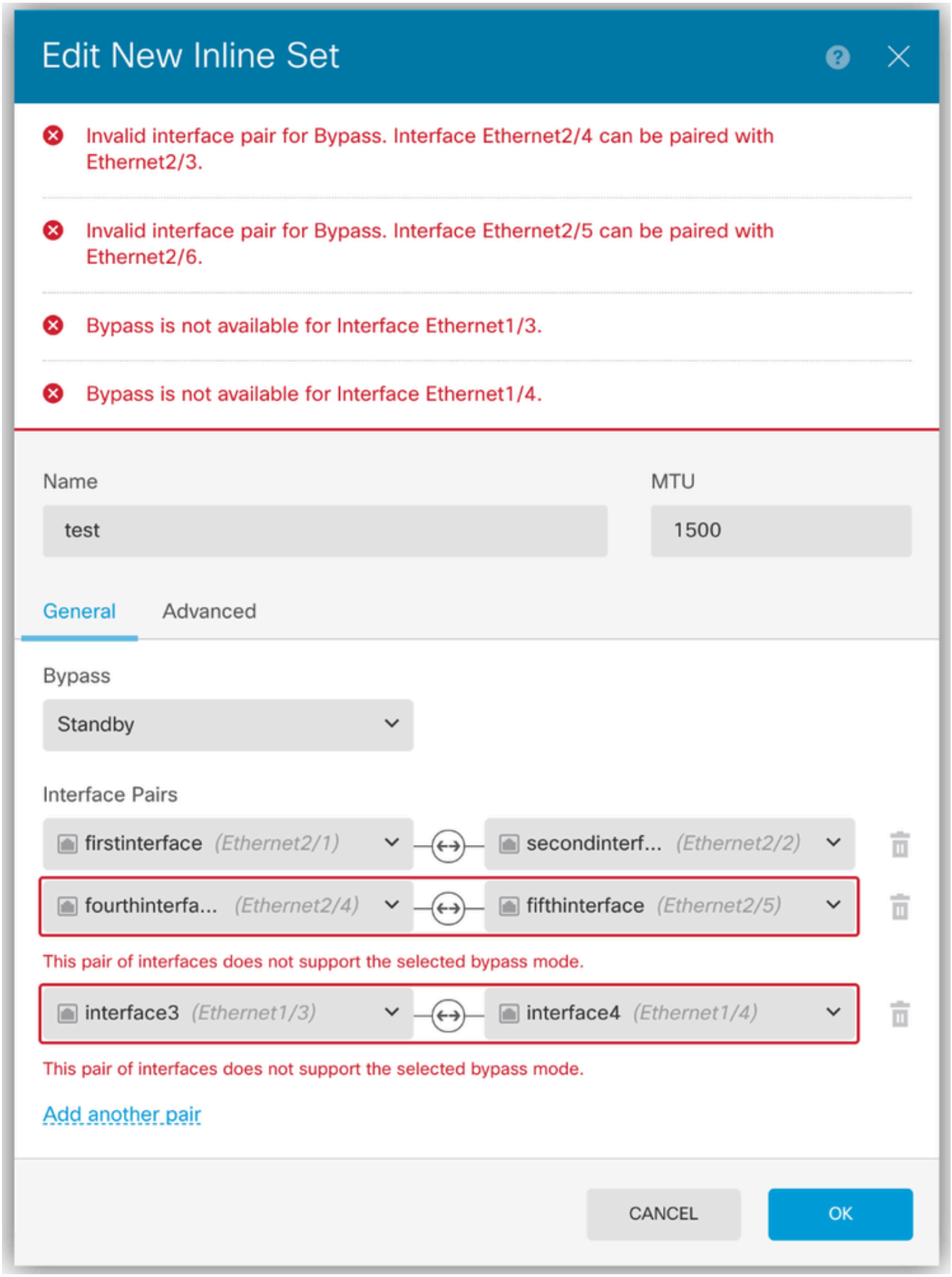
- 각 필드의 GUI에 오류가 표시됩니다.
  - 이름을 입력해야 합니다.
  - MTU 크기는 1500 이상이어야 합니다.
  - 쌍의 두 인터페이스를 모두 선택해야 합니다.



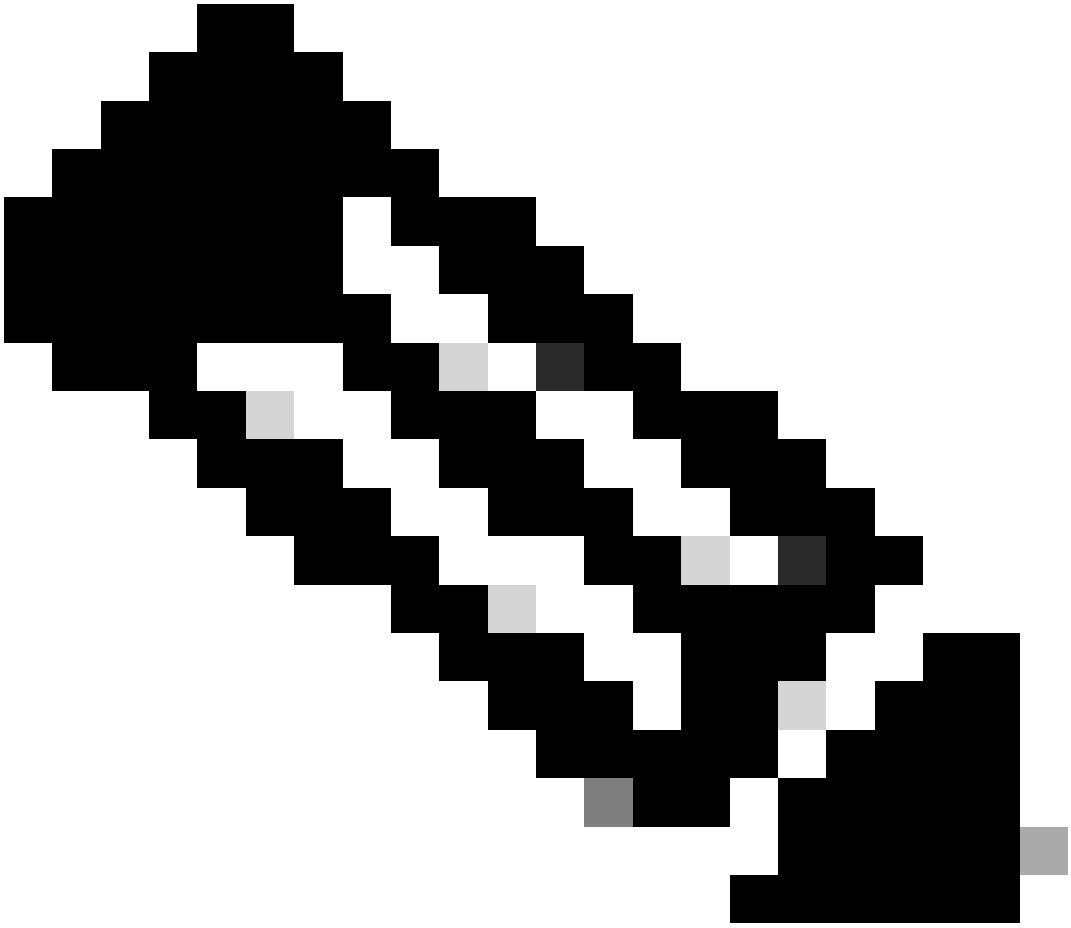
MTU 크기

하드웨어 바이패스 - 생성 시 검증

- Bypass가 활성화된 경우 각 필드의 GUI에 새로운 오류가 표시됩니다.
  - 모든 인터페이스는 Bypass를 지원해야 합니다.
    - 지원되지 않는 인터페이스를 표시하는 오류가 발생했습니다.
  - 모든 쌍은 미리 정해진 인터페이스 쌍을 사용해야 합니다.
    - 사용 가능한 바이패스 인터페이스 쌍에 대한 오류 메시지 설명입니다.


Edit New Inline Set
Invalid interface pair for Bypass. Interface Ethernet2/4 can be paired with Ethernet2/3.
Invalid interface pair for Bypass. Interface Ethernet2/5 can be paired with Ethernet2/6.
Bypass is not available for Interface Ethernet1/3.
Bypass is not available for Interface Ethernet1/4.
Name
test
MTU
1500
General
Advanced
Bypass
Standby
Interface Pairs
firstinterface (Ethernet2/1)
secondinterf... (Ethernet2/2)
fourthinterfa... (Ethernet2/4)
fifthinterface (Ethernet2/5)
This pair of interfaces does not support the selected bypass mode.
interface3 (Ethernet1/3)
interface4 (Ethernet1/4)
This pair of interfaces does not support the selected bypass mode.
Add another pair
CANCEL
OK

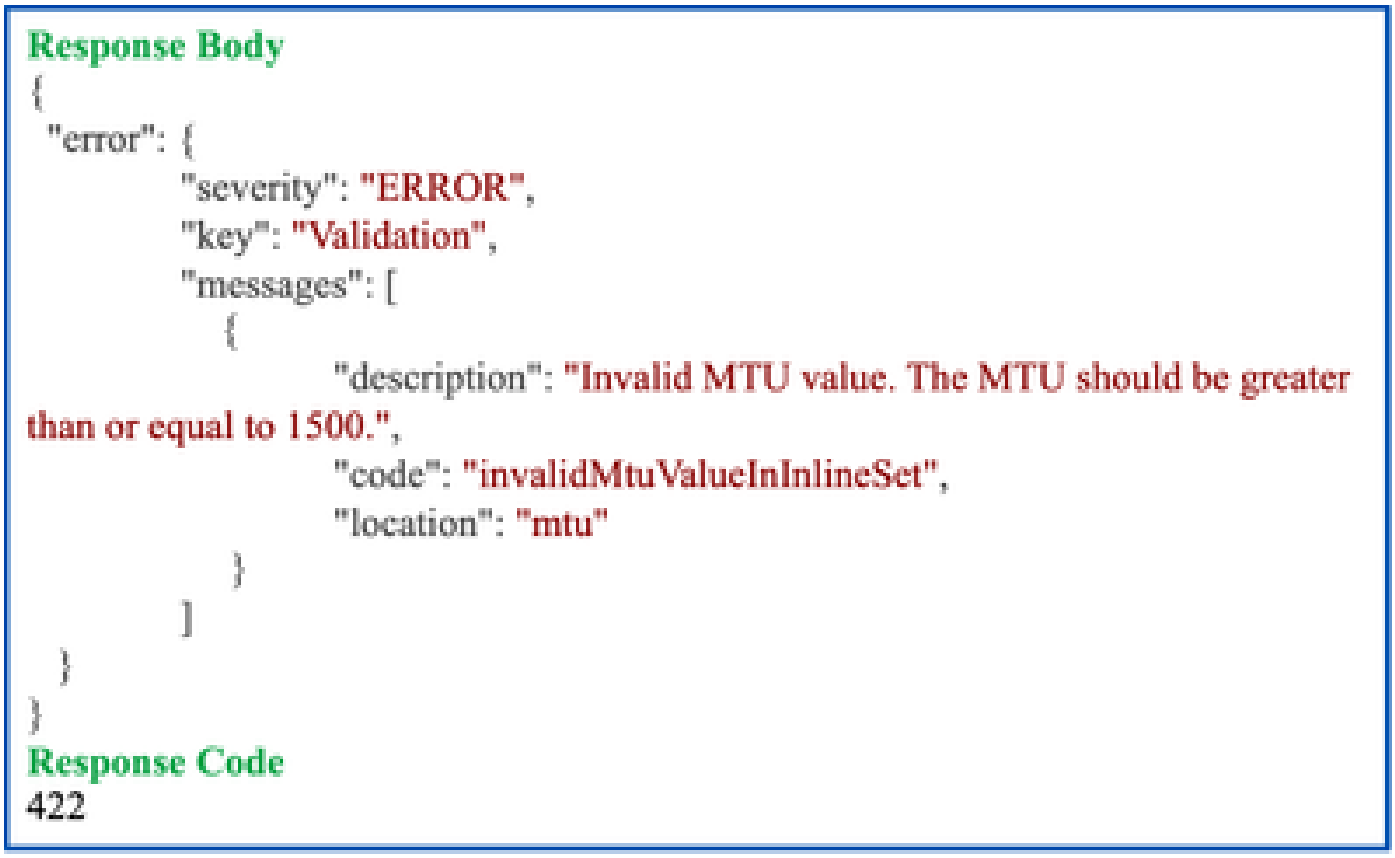
GUI 검증



참고: 첫 번째 쌍(Ethernet2/1-Ethernet2/2)이 유효합니다.

REST API 응답에서 오류 표시

- 오류는 REST API 응답에 표시됩니다.
  - 여기서 MTU 값이 잘못되었습니다.



REST API 검증

이 릴리스의 구현 제한 사항

- 인라인 집합: 물리적 인터페이스 및 EtherChannel에서만 작동합니다.
- 하드웨어 바이패스가 있는 인라인 집합: 물리적 인터페이스에서만 작동하며 네트워크 모듈이 필요합니다.

인라인 인터페이스에서 지원되지 않는 방화벽 기능

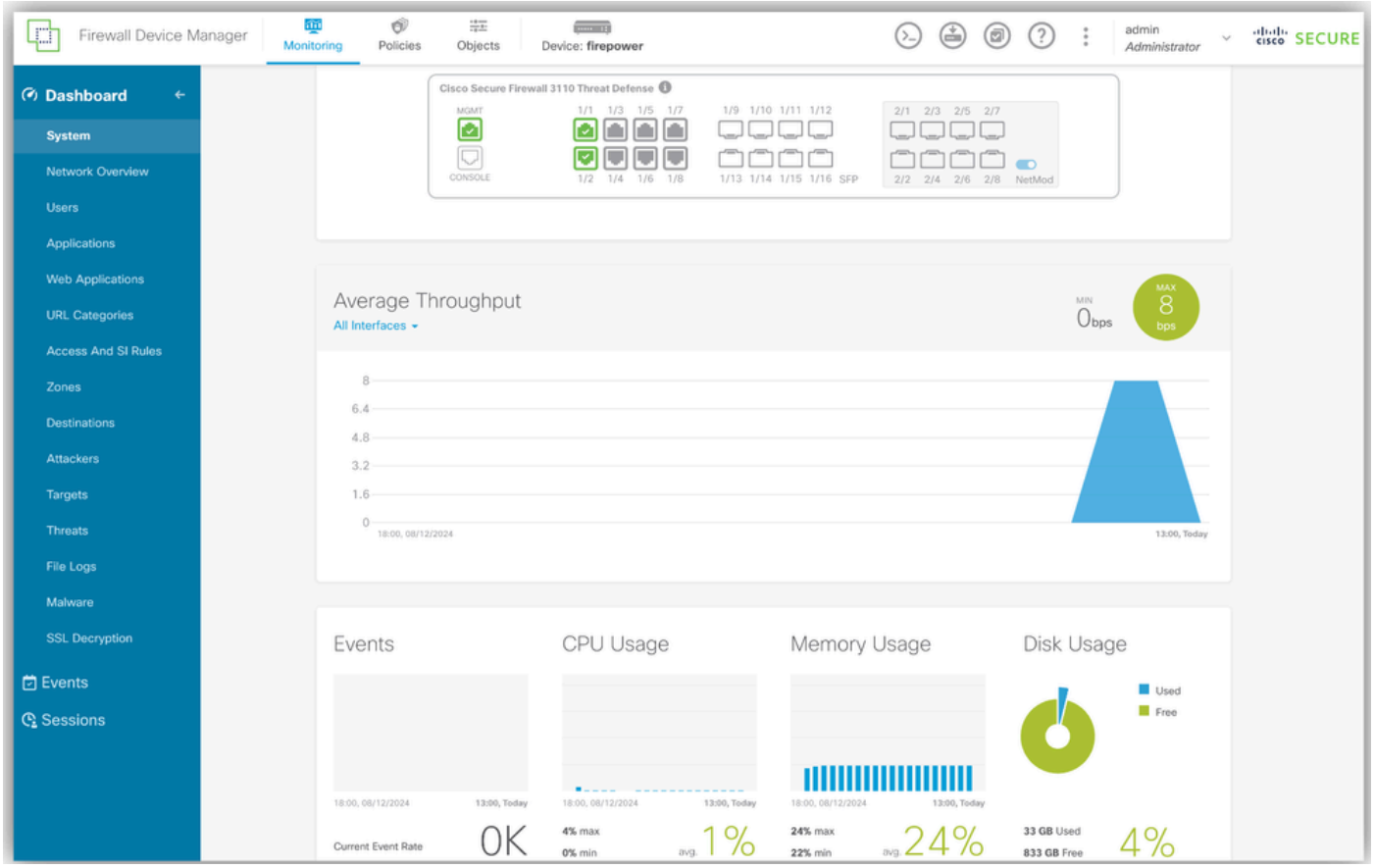
- DHCP 서버
- DHCP 릴레이
- DHCP 클라이언트
- TCP 가로채기
- 라우팅
- NAT
- VPN
- 애플리케이션
- 검사
- QoS
- Netflow

CLI에서 로그 확인

- 로깅.
  - 로그는 /ngfw/var/log/cisco/ngfw-onbox.log에서 찾을 수 있습니다.
  - 인라인 집합을 검색합니다.
  - 로그에서 발견된 가능한 오류의 예:
    - 두 인터페이스는 바이패스를 지원하지 않습니다.
    - 두 인터페이스가 올바른 바이패스 쌍이 아닙니다.

```
root@FPR-3110-Pair:/home/admin# cd /ngfw/var/log/cisco/

root@FPR-3110-Pair:/ngfw/var/log/cisco# cat ngfw-onbox.log | grep "InlineSet"

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator: 548 - Invalid

interface pair for Bypass. Interface Ethernet2/4 can be paired with Ethernet2/3.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:548 - Invalid

interface pair for Bypass. Interface Ethernet2/5 can be paired with Ethernet2/6.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass

is not available for Interface Ethernet1/3.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass

is not available for Interface
```

- GUI에서 트래픽을 확인합니다.
  - 이벤트는 GUI에서 표시됩니다.
  - 트래픽 흐름의 정확성은 여기에서 모니터링할 수 있습니다.
  - Monitoring(모니터링) > System(시스템)으로 이동합니다.



FDM 모니터링

- CLI에서 트래픽 정확성을 확인합니다.

<#root>

```
> system support trace
Enable firewall-engine-debug too? [n]:
Please specify an IP protocol: ICMP
Please specify a client IP address:
Please specify a server IP address:
Monitoring packet tracer debug messages
```

[packets show up here]

FAQ

Q: FDM의 인라인 집합에서 HA가 지원됩니까?
A: Bypass가 없는 인라인 집합이 지원됩니다.
  Bypass가 있는 인라인 집합은 지원되지 않습니다.
Q: 스패닝 트리 BPDU가 인라인 집합 쌍에서 차단됩니까?
A : 아니요, 차단되어 있지 않습니다.
Q: 3100에서 FTW 카드가 지원됩니까?

A : 예. FTW netmod는 3100 Series가 7.1/9.17로 도입된 이후 지원되었습니다. 하드웨어 우회는 7.7.0부터 사용할 수 있습니다.
Q: 3100 FTW 카드의 경우 FMC에서 Disabled, Standby, Bypass-Force 등의 Bypass 모드가 지원됩니까?
A : 하드웨어 우회는 FTW 카드가 장착된 3100 디바이스에서 7.7.0부터 사용할 수 있습니다.
Q: 포트 채널 전체에서 트래픽이 비대칭인 경우 포트 채널이 있는 인라인 집합이 지원됩니까?
A : PortChannel 구성 속도에 대해서는 검증이 수행되지 않으므로 FTD에서 지원하는 한 반드시 지원해야 합니다.
Q: Snort가 검사에 실패할 경우 failopen이 지원됩니까?
A : Firepower Management Center 컨피그레이션 가이드의 이 설정에 대한 설명서를 참조하십시오.

관련 정보

- 인라인 쌍 모드에서 FTD 인터페이스 구성
- Firepower Management Center 컨피그레이션 가이드, 버전 6.3
- Cisco Secure Firewall 3100 Series 하드웨어 설치 가이드
- Cisco Secure Firewall 3100 Series 데이터 시트

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.