# 인라인 집합 및 패시브 인터페이스

IPS 전용 패시브 인터페이스, 패시브 ERSPAN 인터페이스 및 인라인 집합을 구성할 수 있습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.


- IPS 인터페이스, 1 페이지
- 인라인 집합의 요구 사항 및 사전 요건, 4 페이지
- 인라인 집합 및 패시브 인터페이스 가이드라인, 5 페이지
- 패시브 인터페이스 구성, 6 페이지
- 인라인 집합 구성, 8 페이지
- 인라인 집합 및 패시브 인터페이스 히스토리, 12 페이지


## IPS 인터페이스

이 섹션에서는 IPS 인터페이스에 대해 설명합니다.

### IPS 인터페이스 유형

IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다.

IPS 전용 인터페이스는 다음과 같은 유형으로 구축할 수 있습니다.

- 필요에 따라 탭 모드가 가능한 인라인 집합 - 인라인 집합은 비활성 엔드포인트(bump in the wire)처럼 작동하며 두 인터페이스를 슬롯에 포함해 기존 네트워크에 바인딩합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 설정 없이 네트워크 환경에 FTD를 설치할 수 있습니다. 인라

인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

탭 모드에서는 FTD가 인라인으로 구축되지만, 네트워크 트래픽 플로우는 방해받지 않습니다. 대신 FTD는 패킷을 분석할 수 있도록 각 패킷의 복사본을 만듭니다. 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며, 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다. 인라인으로 구축된 FTD에서 탭 모드를 사용하는 데는 몇 가지 이점이 있습니다. 예를 들어, 디바이스가 인라인 상태인 것처럼 FTD와 네트워크 간에 케이블링을 설정할 수 있으며 FTD가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. FTD를 인라인으로 구축할 준비가 되면 FTD와 네트워크 간 케이블링을 다시 설정하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽을 삭제할 수 있습니다.

참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

참고 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 투명 방화벽 모드 또는 방화벽 유형 인터페이스와는 관련이 없습니다.

- 패시브 또는 ERSPAN 패시브 - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용해 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 패시브 구축으로 FTD를 설정한 경우, FTD에서 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며, 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 인터페이스는 여러 스위치를 통해 배포되는 소스 포트의 트래픽을 모니터링하고 GRE를 사용해 트래픽을 캡슐화합니다. ERSPAN 인터페이스는 FTD가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

참고 NGFWv에서 SR-IOV 인터페이스를 패시브 인터페이스로 사용하는 것은 무차별 모드 제한으로 인해 SR-IOV 드라이버를 사용하는 일부 Intel 네트워크 어댑터(예: Intel X710 또는 82599)에서 지원되지 않습니다. 이 경우 이 기능을 지원하는 네트워크 어댑터를 사용하십시오. Intel 네트워크 어댑터에 대한 자세한 내용은 Intel 이더넷 제품을 참조하십시오.

# 인라인 집합용 하드웨어 바이패스 정보

지원되는 모델의 특정 인터페이스의 경우(인라인 집합의 요구 사항 및 사전 요건, 4 페이지 참조) 하드웨어 바이패스 기능을 활성화할 수 있습니다. 하드웨어 바이패스는 트래픽이 정전 중에 1개의 인라인 인터페이스 쌍 사이에서 이동하도록 해 줍니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다.

## 하드웨어 바이패스 트리거

하드웨어 바이패스 다음 시나리오에서 트리거될 수 있습니다.

- FTD 애플리케이션 충돌
- FTD 애플리케이션 재부팅
- 보안 모듈 재부팅
- 화력 섀시 충돌
- Firepower 섀시의 재부팅 또는 업그레이드
- 수동 트리거
- Firepower 섀시 전력 손실
- 보안 모듈 전력 손실

참고 하드웨어 우회는 계획되지 않은/예기치 않은 장애 시나리오를 위한 것이며, 계획된 소프트웨어 업그레이드 중에 자동으로 트리거되지 않습니다. 하드웨어 우회는 FTD 애플리케이션이 재부팅될 때 계획된 업그레이드 프로세스가 끝날 때만 사용됩니다.

## 하드웨어 우회 전환

정상 작동 상태에서 하드웨어 우회로 전환하거나 그 반대로 전환하는 경우에는 몇 초 동안 트래픽 전송이 중단될 수 있습니다. 구리 포트 자동 협상이나 파트너가 링크 결함 및 디바운스 타이밍을 처리하는 방식 등 광학 링크 파트너의 활동, STP(Spanning Tree Protocol) 컨버전스, 동적 라우팅 프로토콜 컨버전스 등 여러 가지 요인이 이 중단 시간에 영향을 줄 수 있습니다. 이 시간 동안에는 연결이 끊길 수 있습니다.

일반 작업으로 돌아온 이후 연결 미드스트림을 분석할 때 애플리케이션 식별 오류 때문에 연결 중단이 발생할 수도 있습니다.

## Snort Fail Open vs.하드웨어 바이패스

탭 모드의 인라인 집합이 아닌 경우 Snort 프로세스가 바쁘거나 중단된 경우 검사 없이 트래픽을 삭제하거나 허용하려고 할 때 Snort Fail Open 옵션을 사용할 수 있습니다. Snort Fail Open는 하드웨어 바이패스을 지원하는 인터페이스만이 아니라 탭 모드가 아닌 모든 인라인 집합에서 지원합니다.

하드웨어 바이패스 기능을 사용하면 전원 완전 차단을 포함한 하드웨어 오류와 일부 한정 소프트웨어 오류가 발생한 경우에도 트래픽이 전송됩니다. Snort Fail Open을 트리거하는 소프트웨어 오류는 하드웨어 바이패스을 트리거하지 않습니다.

## 하드웨어 바이패스 **Status(상태)**

시스템에 전원이 있는 경우 우회 LED는 하드웨어 바이패스 상태를 나타냅니다. LED 설명에 대해서는 Firepower 섀시 하드웨어 설치 가이드를 참조하십시오.

# 인라인 집합의 요구 사항 및 사전 요건

모델 지원

FTD

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

하드웨어 바이패스 지원

FTD는 다음 모델에서 특정 네트워크 모듈의 인터페이스 쌍에 대해 하드웨어 바이패스를 지원합니다.

- Firepower 9300
- Firepower 4100
- Firepower 2130 및 2140

참고 ISA 3000에는 하드웨어 우회에 대한 별도의 구현이 있으며, FlexConfig만 사용하여 활성화할 수 있습니다 (FlexConfig 정책 참조). ISA 3000 하드웨어 우회를 구성하는 데 이 장을 사용하지 마십시오.

이러한 모델에 대해 지원되는 하드웨어 바이패스 네트워크 모듈은 다음과 같습니다.

- Firepower 4100
  - Firepower 6포트 1G SX FTW 네트워크 모듈 싱글 와이드(FPR4K-NM-6X1SX-F)
  - Firepower 6포트 10G SR FTW 네트워크 모듈 싱글 와이드(FPR4K-NM-6X10SR-F)
  - Firepower 6포트 10G LR FTW 네트워크 모듈 싱글 와이드(FPR4K-NM-6X10LR-F)

- Firepower 2 포트 40G SR FTW 네트워크 모듈 싱글 와이드(FPR4K-NM-2X40G-F)
- Firepower 8 포트 1G Copper FTW 네트워크 모듈 싱글 와이드(FPR4K-NM-8X1G-F)

- Firepower 9300:
  - Firepower 6 포트 10G SR FTW 네트워크 모듈 싱글 와이드(FPR9K-NM-6X10SR-F)
  - Firepower 6 포트 10G LR FTW 네트워크 모듈 싱글 와이드(FPR9K-NM-6X10LR-F)
  - Firepower 2 포트 40G SR FTW 네트워크 모듈 싱글 와이드(FPR9K-NM-2X40G-F)

- Firepower 2130 및 2140:
  - Firepower 6포트 1G SX FTW 네트워크 모듈 싱글 와이드(FPR2K-NM-6X1SX-F)
  - Firepower 6포트 10G SR FTW 네트워크 모듈 싱글 와이드(FPR2K-NM-6X10SR-F)
  - Firepower 6포트 10G LR FTW 네트워크 모듈 싱글 와이드(FPR2K-NM-6X10LR-F)

하드웨어 바이패스는 다음 포트 쌍만 사용할 수 있습니다.

- 1 및 2
- 3 및 4
- 5 및 6
- 7 및 8

# 인라인 집합 및 패시브 인터페이스 가이드라인

방화벽 모드

- ERSPAN 인터페이스는 디바이스가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

일반 지침

- 인라인 집합 및 패시브 인터페이스는 물리적 인터페이스 및 EtherChannel만 지원하며 이중 인터페이스, VLAN 등을 사용할 수 없습니다. Firepower 4100/9300 하위 인터페이스는 또한 IPS 전용 인터페이스를 지원하지 않습니다.
- 인라인 집합 및 패시브 인터페이스는 섀시 내 및 섀시 간 클러스터링에서 지원됩니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 인라인 집합을 사용할 때 FTD을 통과할 수 없습니다. BFD를 실행하는 FTD의 양쪽 측면에 두 개의 네이버가 있는 경우, FTD는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

- 인라인 집합 및 패시브 인터페이스의 경우, FTD는 패킷에서 최대 2개의 802.1Q 헤더(Q-in-Q 지원이라고도 함)를 지원합니다. 단, 하나의 802.1Q 헤더만 지원하는 Firepower 4100/9300은 예외입니다. 참고**:** 방화벽 유형 인터페이스는 Q-in-Q를 지원하지 않으며, 802.1Q 헤더를 하나만 지원합니다.

하드웨어 바이패스 지침

- 하드웨어 바이패스 포트는 인라인 집합에만 지원됩니다.
- 하드웨어 바이패스 포트는 EtherChannel의 일부가 될 수 없습니다.
- 섀시 내 클러스터링에 지원됩니다. 포트는 섀시의 마지막 유닛에 오류가 발생하는 경우 하드웨어 바이패스 모드에 배치됩니다. 섀시 간 클러스터링은 지원 되지 않습니다.
- 클러스터의 모든 유닛에 오류가 발생하는 경우 하드웨어 바이패스은 최종 유닛에서 트리거되고 트래픽은 계속 전달됩니다. 유닛이 복구되면 하드웨어 바이패스은 스탠바이 모드로 돌아갑니다. 그러나 애플리케이션 트래픽과 일치하는 규칙을 사용하면 이 연결이 삭제되어 다시 설정해야 할 수 있습니다. 클러스터 유닛에 상태 정보가 보존되지 않으므로 연결이 삭제되고 유닛은 허용된 애플리케이션에 속한 트래픽을 식별하지 못합니다. 트래픽 삭제를 방지하려면 애플리케이션 기반 규칙 대신 구축에 적합한 경우 포트 기반 규칙을 사용합니다.
- 하드웨어 바이패스 는 고가용성 모드에서 지원되지 않습니다.

**IPS** 인터페이스에서 지원되지 않는 방화벽 기능

- DHCP 서버
- DHCP 릴레이
- DHCP 클라이언트
- TCP 인터셉트
- 라우팅
- NAT
- VPN
- 애플리케이션 검사
- QoS
- NetFlow
- VXLAN

# 패시브 인터페이스 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 인터페이스를 활성화합니다. 기본적으로 인터페이스는 비활성화되어 있습니다.
- 인터페이스 모드를 패시브 또는 ERSPAN으로 설정합니다. ERSPAN 인터페이스의 경우 ERSPAN 파라미터와 IP 주소를 설정할 수 있습니다.
- MTU를 변경합니다. 기본적으로 MTU는 1500 바이트로 설정됩니다. MTU에 대한 자세한 내용은 MTU 정보을 참조하십시오.
- 특정 속도 및 양방향 설정(제공되는 경우) 기본적으로 속도 및 양방향은 자동으로 설정되어 있습니다.

참고 FXOS 섀시의 Firepower Threat Defense의 경우 Firepower 4100/9300에서 기본 인터페이스 설정을 구성합니다. 자세한 내용은 실제 인터페이스 구성를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Mode(**모드**)** 드롭다운 목록에서 **Passive(**패시브**)** 또는 **ERSPAN**을 선택합니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

단계 **6** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

단계 **7** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **8** (선택 사항) 일반에서 64와 9198바이트 사이의 **MTU**를 설정하십시오. Firepower Threat Defense Virtual과 FXOS 섀시의 Firepower Threat Defense의 경우 9000바이트가 최대입니다.

기본값은 1500바이트입니다.

단계 **9** ERSPAN 인터페이스에 대한 다음 파라미터를 설정합니다.

- 플로우 **ID** - ERSPAN 트래픽을 식별하기 위해 소스 및 대상 세션에서 사용하는 ID를 구성하며 그 값은 1에서 1023 사이입니다. 이 ID 값은 ERSPAN 대상 세션에도 입력해야 합니다.
- 소스 **IP** - ERSPAN 트래픽 소스로 사용되는 IP 주소를 구성합니다.

단계 **10** ERSPAN 인터페이스의 경우 **IPv4**에서 IPv4 주소 및 마스크를 설정합니다.

단계 **11** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

정확한 속도 및 듀플렉스 옵션은 하드웨어에 따라 달라집니다.

- **Duplex(**듀플렉스**) - Full(**풀 듀플렉스**), Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.
- **Speed(**속도**) - 10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

# 인라인 집합 구성

이 섹션에서는 인라인 집합에 추가할 수 있는 물리적 인터페이스 2개를 활성화하고 이름을 지정합니다. 원하는 경우 지원되는 인터페이스 쌍에 대해 하드웨어 바이패스를 활성화할 수도 있습니다.

참고 Firepower 4100/9300의 경우 기본 인터페이스 설정을 섀시의 FXOS에서 구성합니다. 자세한 내용은 실제 인터페이스 구성를 참조하십시오.

시작하기 전에

- FTD 인라인 쌍 인터페이스에 연결하는 STP 활성화 스위치에 대해 STP PortFast를 구성하는 것이 좋습니다. 이 설정은 하드웨어 바이패스 구성에 특히 유용하며, 우회 시간을 줄일 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

인라인 집합에 이 인터페이스를 추가하고 나면 이 필드에 모드로 Inline(인라인)이 표시됩니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

보안 구역은 아직 설정하지 마십시오. 이 절차 후반에서 인라인 모음을 생성한 다음에 설정해야 합니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **7** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

정확한 속도 및 듀플렉스 옵션은 하드웨어에 따라 달라집니다.

- **Duplex(**듀플렉스**) - Full(**풀 듀플렉스**)**, **Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.
- **Speed(**속도**) - 10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

이 인터페이스에 대한 다른 설정은 지정하지 마십시오.

단계 **9** 인라인 집합에 추가할 두 번째 인터페이스에 대해 **Edit(**수정**)** ( )을 클릭합니다.

단계 **10** 첫 번째 인터페이스에 대한 설정을 구성합니다.

단계 **11** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **12** **Add Inline Set(**인라인 집합 추가**)**를 클릭합니다.
**General(**일반**)**이 선택된 상태로 **Add Inline Set(**인라인 집합 추가**)** 대화 상자가 나타납니다.

단계 **13** **Name(**이름**)** 필드에 집합의 이름을 입력합니다.

단계 **14** (선택 사항) 점보 프레임을 활성화하려면 **MTU**를 변경합니다.

인라인 집합의 경우, MTU 설정이 사용되지 않습니다. 그러나 점보 프레임 설정은 인라인 집합과 관련이 있으며 점보 프레임은 최대 9000바이트까지 패킷을 수신하도록 인라인 인터페이스를 활성화합니다. 점보 프레임을 활성화하려면 1500바이트 이상인 디바이스에서 모든 인터페이스의 MTU를 설정해야 합니다.

단계 **15** 하드웨어 바이패스을 구성합니다.

a) **Bypass(**바이패스**)** 모드의 경우 다음 옵션 중 하나를 선택합니다.

- **Disabled(**비활성화됨**)** - 하드웨어 바이패스가 지원되는 인터페이스에 대해 하드웨어 바이패스를 비활성화하거나, 하드웨어 바이패스가 지원되지 않는 인터페이스를 사용합니다.
- **Standby(**스탠바이**)** - 지원되는 인터페이스에서 하드웨어 바이패스를 스탠바이 상태로 설정합니다. 하드웨어 바이패스 인터페이스 쌍만 표시됩니다. 스탠바이 상태에서 인터페이스는 트리거 이벤트가 발생할 때까지 정상 작동 상태로 유지됩니다.
- **Bypass-Force(**바이패스-강제**)** - 인터페이스 쌍이 바이패스 상태가 되도록 수동으로 강제 지정합니다. **Inline Sets(**인라인 집합**)**에서 Bypass-Force(바이패스-강제) 모드인 모든 인터페이스 쌍에 대해 **Yes(**예**)**가 표시됩니다.

b) **Available Interfaces Pairs(**사용 가능한 인터페이스 쌍**)** 영역에서 쌍을 클릭한 다음 **Add(**추가**)**를 클릭하여 해당 쌍을 **Selected Interface Pair(**선택한 인터페이스 쌍**)** 영역으로 이동합니다.

모드가 None(없음)으로 설정된 명명된 인터페이스와 활성화된 인터페이스 간에 가능한 모든 쌍이 이 영역에 표시됩니다.

단계 **16** (선택 사항) **Advanced(**고급**)**를 클릭하여 다음의 선택적 파라미터를 설정합니다.

- **Tap Mode(**탭 모드**)** - 인라인 탭 모드로 설정합니다.

동일한 인라인 집합에서 이 옵션 및 Strict TCP Enforcement를 활성화할 수 없습니다.

참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

- **Propagate Link State(**링크 상태 전파**)** - 링크 상태 전파를 구성합니다.

  링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 한 인터페이스의 링크 상태가 변경되면 디바이스가 변경사항을 감지하고 다른 인터페이스의 링크 상태도 일치하도록 업데이트합니다. 디바이스가 링크 상태 변경사항을 전파하려면 최대 4초가 걸립니다. 링크 상태 전파는 라우터가 장애 상태인 네트워크 디바이스를 우회해 트래픽을 자동으로 다시 라우팅하도록 구성된 탄력적인 네트워크 환경에서 특히 유용합니다.

- **Strict TCP Enforcement(**엄격한 **TCP** 시행**)** - TCP 보안을 극대화하기 위해 엄격한 시행을 활성화할 수 있습니다. 그러면 3방향 핸드셰이크가 완료되지 않은 연결이 차단됩니다.

  엄격한 시행은 다음 항목도 차단합니다.

  - 3방향 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
  - TCP 연결의 Responder가 SYN-ACK를 보내기 전에 이니시에이터가 보낸 비 SYN/RST 패킷
  - TCP 연결에서 SYN 이후/세션이 설정되기 전에 Responder가 보낸 비 SYN-ACK/RST 패킷
  - 설정된 TCP 연결에서 이니시에이터 또는 Responder가 보낸 SYN 패킷

- **Snort Fail-Open** - Snort 프로세스가 사용 중이거나 중단될 때 새 트래픽과 기존 트래픽을 검사 없이 통과할지(활성화됨) 아니면 삭제할지(비활성화됨)에 따라 **Busy(**사용 중**)** 및 **Down(**중단**)** 옵션 중 하나 또는 둘 다를 활성화하거나 비활성화합니다.

  기본적으로 Snort 프로세스가 중단되면 트래픽이 검사 없이 통과되고, Snort 프로세스가 사용 중이면 트래픽이 삭제됩니다.

  Snort 프로세스의 상태별 속성은 다음과 같습니다.

  - Busy(사용 중) - 디바이스가 처리할 수 있는 양보다 트래픽이 더 많아서 트래픽 버퍼가 꽉 차거나 다른 소프트웨어 리소스 문제가 있어서 Snort 프로세스가 트래픽을 충분히 빠르게 처리할 수 없습니다.
  - Down(중단) - Snort 프로세스를 재시작해야 하는 컨피그레이션을 구축했으므로 프로세스가 재시작됩니다. 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션의 내용을 참조하십시오.

    Snort 프로세스는 중단되었다가 다시 작동할 때 새 연결을 검사합니다. 오탐(False Positive) 및 미탐(False Negative)을 방지하기 위해 Snort 프로세스는 인라인, 라우팅 또는 Transparent 인터페이스의 기존 연결을 검사하지 않습니다. 프로세스가 중단된 동안 초기 세션 정보가 손실되었을 수 있기 때문입니다.

참고 Snort가 열리지 않으면 Snort 프로세스를 사용하는 기능이 작동하지 않습니다. 이러한 기능에는 애플리케이션 제어 및 심층 검사가 포함됩니다. 시스템은 단순하며 쉽게 확인 가능한 전송 및 네트워크 계층 특성을 사용하여 기본적인 액세스 제어만 수행합니다.

단계 **17** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **18** 구성원 인터페이스 중 하나에 대한 아이콘(**Edit(**수정**)** ( ))을 클릭합니다.

단계 **19** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

인라인 집합에 인터페이스를 추가한 후에만 영역을 설정할 수 있습니다. 인라인 집합에 영역을 추가하면 모드가 Inline(인라인)으로 구성되며, 인라인 유형 보안 영역을 선택할 수 있습니다.

단계 **20** **OK(**확인**)**를 클릭합니다.

단계 **21** 두 번째 인터페이스의 보안 영역을 설정합니다.

단계 **22** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

# 인라인 집합 및 패시브 인터페이스 히스토리

| 기능 | 버전 | 세부 사항 |
|---|---|---|
| FTD 작동 링크 상태와 Firepower 4100/9300의 물리적 링크 상태 간 동기화 | 6.7 | 이제 Firepower 4100/9300 섀시는 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다.<br>참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 데코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다.<br>신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)**<br>신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail**<br>지원되는 플랫폼: Firepower 4100/9300 |

| 기능 | 버전 | 세부 사항 |
| --- | --- | --- |
| 지원되는 네트워크 모듈용 Firepower 2100 및 2140에 대한 하드웨어 우회 지원 | 6.3.0 | Firepower 2130 및 2140은 이제 하드웨어 우회 네트워크를 사용할 때 하드웨어 우회 기능을 지원합니다.<br>신규/수정된 화면:<br>**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)**<br>지원되는 플랫폼: Firepower 2130 및 2140 |
| FTD 인라인 집합에서 EtherChannel 지원 | 6.2.0 | 이제 FTD 인라인 집합에서 EtherChannel을 사용할 수 있습니다.<br>지원되는 플랫폼: Firepower 4100/9300, Firepower 2100(6.2.1 이상) |
| 지원되는 네트워크 모듈용 Firepower 4100/9300에 대한 하드웨어 우회 지원 | 6.1.0 | Hardware Bypass는 정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다.<br>신규/수정된 화면:<br>**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)**<br>지원되는 플랫폼: Firepower 4100/9300 |
| 인라인 집합 링크 상태 전파 지원 FTD | 6.1.0 | FTD 애플리케이션에서 인라인 집합을 구성하고 링크 상태 전파를 활성화하면 FTD에서 FXOS 섀시로 인라인 집합 멤버십을 전송합니다. 링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다.<br>신규/수정된 FXOS 명령: **show fault \|grep link-down**, **show interface detail**<br>지원되는 플랫폼: Firepower 4100/9300, Firepower 2100(6.2.1 이상) |