IPS 디바이스 구축 및 구성

다음 주제는 IPS 구축에서 디바이스를 구성하는 방법을 설명합니다.

IPS 디바이스 구축 및 구성 소개

패시브 또는 인라인 IPS 구축에서 디바이스를 구성할 수 있습니다. 패시브 구축에서는 네트워크 트래픽 플로우 대역 외부에 시스템이 구축됩니다. 인라인 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에 투명하게 시스템을 구성합니다.

IPS 디바이스 구축 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

IPS 디바이스 구축 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf에 전달하는 고성능 고속 어플라이언스입니다.

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

수동 IPS 구축

패시브 IPS 구축에서 Firepower System은 스위치 SPAN 또는 미러 포트를 사용해 네트워크에서 이동하는 트래픽을 모니터링합니다. SPAN을 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않는 경우에도 네트워크 내의 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 패시브 인터페이스는 로컬 SPAN 및 원격 SPAN(RSPAN) 트래픽을 모두 지원합니다.

참고 아웃바운드 트래픽은 플로우 제어 패킷을 포함합니다. 따라서 어플라이언스의 패시브 인터페이스는 아웃바운드 트래픽을 표시할 수 있으며 컨피그레이션에 따라 이벤트를 생성할 수 있는데, 이는 자연스러운 동작입니다.

Firepower System의 패시브 인터페이스

관리되는 디바이스에서 하나 이상의 물리적 포트를 수동 인터페이스로 구성할 수 있습니다.

트래픽을 모니터링하기 위해 패시브 인터페이스를 활성화하면 구리 인터페이스에서만 사용 가능한 모드 및 MDI/MDIX 설정을 지정합니다. 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

패시브 인터페이스를 비활성화하면 보안 때문에 사용자가 액세스할 수 없습니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작를 참조하십시오.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위
Snort® 재시작 시나리오

패시브 인터페이스 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 패시브 인터페이스를 구성하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 패시브 인터페이스를 구성하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** 패시브를 클릭합니다.

단계 **5** 보안 영역 내 패시브 인터페이스를 연결하려면 다음 중 하나를 수행합니다.

- 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택합니다.
- 새 보안 영역을 추가하려면 새로 만들기를 선택합니다. 보안 영역 개체 생성를 참조하십시오.

단계 **6** **Enable(**활성화**)** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

단계 **7** 7000 및 8000 Series 전용: 모드 드롭다운 목록에서 링크 모드를 지정하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 지정합니다.

모드 설정은 구리 인터페이스에 대해서만 가능합니다.

8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

단계 **8** 7000 및 8000 Series 전용: **MDI/MDIX** 드롭다운 목록에서 인터페이스가 MDI(Medium Dependent Interface), MDIX(Medium Dependent Interface Crossover) 또는 Auto-MDIX로 구성될지 여부를 지정합니다.

MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 **9** **MTU** 필드에 최대 전송 단위(MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작를 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

인라인 IPS 구축

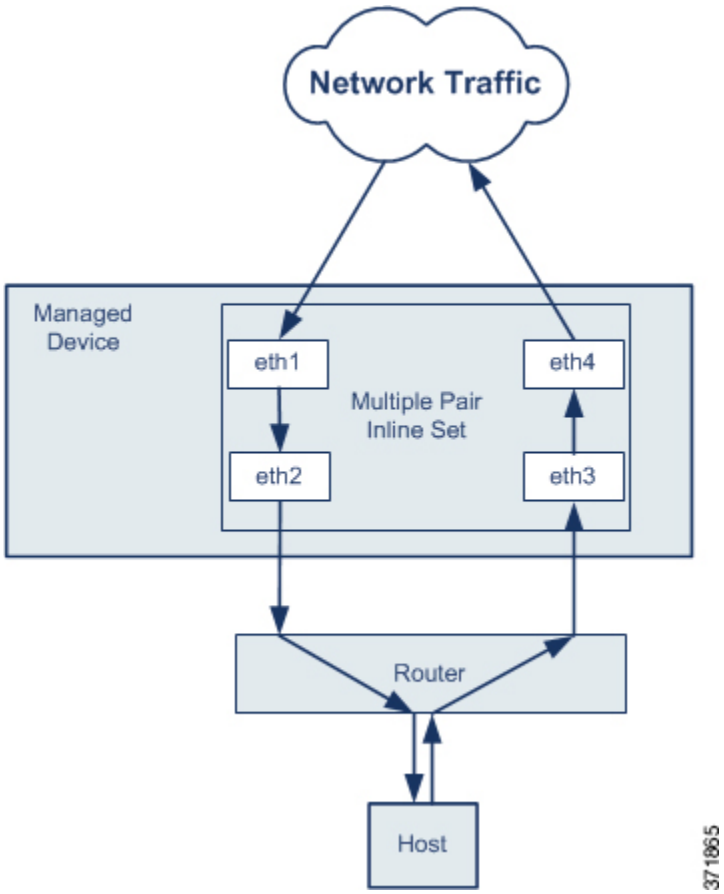
인라인 IPS 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에서 Firepower System을 투명하게 구성합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 구성 없이 네트워크 환경에 시스템을 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

참고 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

디바이스 트래픽이 인바운드인지 아웃바운드인지에 따라 서로 다른 인라인 인터페이스 쌍을 통해 네트워크의 호스트와 외부 호스트 간 트래픽을 라우팅하도록 관리되는 디바이스에서 인터페이스를 구성할 수 있습니다. 이는 비동기 라우팅 설정입니다. 비동기 라우팅을 구축하지만 인라인 집합에 인터페이스 쌍을 하나만 포함하려는 경우 트래픽이 절반만 표시되어 디바이스에서 네트워크 트래픽을 올바르게 분석하지 못할 수 있습니다.

동일한 인터페이스 집합에 여러 인라인 인터페이스 쌍을 추가하면 시스템은 동일한 트래픽 플로우의 일부로서 인바운드 및 아웃바운드 트래픽을 식별할 수 있습니다. 패시브 인터페이스에서는 인터페이스 쌍을 동일한 보안 영역에 포함해도 동일한 효과를 얻습니다.

시스템이 비동기 라우팅 컨피그레이션을 통과하는 트래픽에서 연결 이벤트를 생성하면, 해당 이벤트는 동일한 인터페이스 쌍에서 인그레스 및 이그레스 인터페이스를 식별할 수 있습니다. 예를 들어 다음 다이어그램의 설정은 **eth3**을 인그레스 인터페이스로, **eth2**를 이그레스 인터페이스로 식별하는 연결 이벤트를 생성합니다. 이 설정에서는 일반적인 동작입니다.



참고 여러 인터페이스 쌍을 단일 인라인 인터페이스 집합에 할당하여 중복 트래픽의 문제가 발생하는 경우 시스템이 패킷을 고유하게 식별하도록 다시 구성해야 합니다. 예를 들어 인라인 집합을 구별하도록 인터페이스 쌍을 다시 할당하거나 보안 영역을 수정할 수 있습니다.

인라인 집합이 있는 디바이스의 경우 디바이스를 다시 시작하면 소프트웨어 브리지가 패킷을 전송하도록 자동으로 다시 설정됩니다. 디바이스가 다시 시작 중이면 소프트웨어 브리지가 어디서도 실행되지 않습니다. 인라인 집합에서 우회 모드를 활성화하면 디바이스가 다시 시작되는 동안 하드웨어 우회로 들어갑니다. 이 경우 디바이스와의 링크 재협상 때문에, 시스템이 종료되었다가 다시 시작되면서 몇 초 분량의 패킷이 손실될 수 있습니다. 그러나 시스템은 Snort가 다시 시작되는 동안 트래픽을 전달합니다.

관련 항목

- 7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위
- Snort® 재시작 시나리오

Firepower System의 인라인 인터페이스

관리되는 디바이스에서 하나 이상의 물리적 포트를 인라인 인터페이스로 구성할 수 있습니다. 인라인 세트에 할당된 인라인 인터페이스 쌍에서만 인라인 구축의 트래픽을 처리할 수 있습니다.

참고:

- 시스템은 인라인 쌍의 인터페이스를 다른 속도로 설정하거나 인터페이스가 다른 속도로 협상하는 경우 경고를 표시합니다.
- 인터페이스를 인라인 인터페이스로 구성하는 경우 해당 NetMod의 인접 포트가 자동으로 인라인 인터페이스가 되어 쌍을 완성합니다.
- NGIPSv 디바이스에서 인라인 인터페이스를 구성하려면 인접 인터페이스를 사용하여 인라인 쌍을 생성해야 합니다.

인라인 인터페이스 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인터페이스를 구성하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 구성하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** 인라인을 클릭 합니다.

단계 **5** 보안 영역이 있는 페시브 인터페이스를 연결하려면 다음 중 하나를 수행합니다.

- 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택합니다.
- 새 보안 영역을 추가하려면 새로 만들기를 선택합니다. 보안 영역 개체 생성를 참조하십시오.

단계 **6** 인라인 집합 드롭다운 목록에서 기존 인라인 집합을 선택하거나 새로 만들기로 새 인라인 집합을 추가합니다.

참고 새 인라인 집합을 추가하는 경우 인라인 인터페이스를 설정한 후 구성해야 합니다. 인라인 집합 추가, 9 페이지을 참조하십시오.

단계 **7** **Enable(**활성화**)** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

단계 **8** 7000 및 8000 Series 전용: 모드 드롭다운 목록에서 링크 모드를 지정하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 지정합니다.

모드 설정은 구리 인터페이스에 대해서만 가능합니다.

8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

단계 **9** 7000 및 8000 Series 전용: **MDI/MDIX** 드롭다운 목록에서 인터페이스가 MDI(Medium Dependent Interface), MDIX(Medium Dependent Interface Crossover) 또는 Auto-MDIX로 구성될지 여부를 지정합니다.

MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

Firepower System의 인라인 집합

인라인 구축에서 인라인 인터페이스를 사용하려면 인라인 집합을 구성하고 여기에 인라인 인터페이스 쌍을 할당해야 합니다. 인라인 집합은 디바이스에 있는 하나 이상의 인라인 인터페이스 쌍을 그룹화한 것입니다. 한 인라인 인터페이스 쌍은 동시에 한 인라인 집합에만 속할 수 있습니다.

Device Management(디바이스 관리) 페이지의 **Inline Sets(**인라인 집합**)** 탭에는 디바이스에 구성한 모든 인라인 집합의 목록이 표시됩니다.

Device Management(디바이스 관리) 페이지의 **Inline Sets(**인라인 집합**)** 탭에서 인라인 집합을 추가하거나, 인라인 인터페이스를 구성할 때 인라인 집합을 추가할 수 있습니다.

인라인 인터페이스 쌍은 인라인 집합에만 할당할 수 있습니다. 매니지드 디바이스에서 인라인 인터페이스를 구성하기 전에 인라인 집합을 생성하려는 경우 빈 인라인 집합을 만들고 나중에 여기에 인터페이스를 추가할 수 있습니다. 인라인 집합의 이름을 입력할 때는 영숫자 및 공백을 사용할 수 있습니다.

참고 인라인 집합에서 인터페이스용 보안 영역을 추가하기 전에 인라인 집합을 생성합니다. 그렇지 않으면 보안 영역이 제거되므로 다시 추가해야 합니다.

이름

인라인 집합의 이름입니다.

Interfaces

인라인 집합에 할당된 모든 인라인 인터페이스 쌍의 목록입니다. Interfaces 탭에서 쌍의 두 인터페이스 중 하나를 비활성화하면 쌍을 사용할 수 없음

MTU

인라인 집합의 최대 전송 단위입니다. MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작를 참조하십시오.

Failsafe

트래픽이 탐지를 우회하고 디바이스를 계속 통과하도록 허용합니다. 매니지드 디바이스는 내부 트래픽 버퍼를 모니터링하고 버퍼가 꽉 차면 탐지를 우회합니다.

Bypass Mode(바이패스 모드**)**

Firepower 7000 또는 8000 Series에만 해당: 인라인 집합의 구성된 우회 모드입니다. 이 설정은 인터페이스에서 장애가 발생할 때 인라인 인터페이스의 릴레이가 어떻게 반응하는지를 결정합니다. 바이패스 모드에서는 트래픽이 인터페이스를 계속 통과할 수 있습니다. 바이패스 이외의 모드에서는 트래픽이 차단됩니다.

주의 우회 모드에서 어플라이언스를 재부팅하면 패킷이 약간 손실될 수 있습니다. 고가용성 쌍의 7000 또는 8000 Series 디바이스에 있는 인라인 집합, 8000 Series 디바이스에 있는 우회 이외의 NetMod 또는 Firepower 7115나 7125 디바이스의 SFP 모듈에 대해서는 우회 모드를 구성할 수 없습니다.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위
Snort® 재시작 시나리오

인라인 집합 보기

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 보려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

인라인 집합 추가

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 추가하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** **Add Inline Set(**인라인 집합 추가**)**를 클릭합니다.

단계 **5** **Name(**이름**)**을 입력합니다.

단계 **6** 인터페이스 옆에서 하나 이상의 인라인 인터페이스 쌍을 선택한 다음 **Add Selected(**선택 항목 추가**)**를 클릭합니다. 인라인 집합에 모든 인터페이스 쌍을 추가하려면 **Add All(**모두 추가**)**을 클릭합니다.

팁 인라인 집합에서 인라인 인터페이스를 제거하려면 하나 이상의 인라인 인터페이스 쌍을 선택하고 **Remove Selected(**선택 항목 제거**)**를 클릭합니다. 인라인 집합에서 모든 인터페이스 쌍을 제거하려면 **Remove All(**모두 제거**)**을 클릭합니다. 인터페이스에서 인터페이스 쌍의 인터페이스 중 하나를 비활성화하면 인터페이스 쌍이 제거됩니다.

단계 **7** **MTU** 필드에 최대 전송 단위(MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작를 참조하십시오.

단계 **8** 트래픽이 우회 탐지에서 허용되어 디바이스로 계속 진행하도록 하려는 경우 **Failsafe**를 선택합니다.

매니지드 디바이스는 내부 트래픽 버퍼를 모니터링하고 버퍼가 꽉 차면 탐지를 우회합니다.

단계 **9** (7000/8000 시리즈에만 해당) 우회 모드를 지정합니다.

- 트래픽이 인터페이스를 통과하도록 하려면 우회를 클릭합니다.
- 트래픽을 차단하려면 우회 안 함을 클릭합니다.

참고 고가용성 쌍의 7000 또는 8000 Series 디바이스에 있는 인라인 집합, NGIPSv 디바이스의 인라인 집합, 8000 Series 디바이스에 있는 우회 이외의 NetMod 또는 Firepower 7115나 7125 디바이스의 SFP 모듈에 대해서는 우회 모드를 구성할 수 없습니다.

단계 **10** 필요한 경우 고급 설정을 구성하려면 고급 인라인 설정 옵션, 10 페이지의 내용을 참조하십시오.

단계 **11** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위
Snort® 재시작 시나리오

고급 인라인 설정 옵션

인라인 집합을 구성할 때 고려해야 할 몇 가지 고급 옵션이 있습니다.

탭 모드

탭 모드는 7000 및 8000 Series 디바이스에서 인라인 또는 fail-open 인터페이스를 포함하는 인라인 집합을 생성할 때 사용 가능합니다.

탭 모드에서는 디바이스가 인라인으로 구축되지만, 패킷 플로우가 디바이스를 통과하는 대신 각 패킷의 복사본이 디바이스로 전송되며 네트워크 트래픽 플로우가 방해받지 않습니다. 패킷 자체가 아니라 패킷의 복사본으로 작업하므로 삭제하도록 설정한 규칙 및 교체 키워드를 사용하는 규칙은 패킷 흐름에 영향을 주지 않습니다. 그러나 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다.

인라인으로 구축된 디바이스에서 탭 모드를 사용하는 데에는 몇 가지 이점이 있습니다. 예를 들어 디바이스가 인라인 상태인 것처럼 디바이스와 네트워크 간에 케이블링을 설정할 수 있으며 디바이스가 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. 디바이스를 인라인으로 구축할 준비가 되면, 디바이스와 네트워크 간 케이블링을 다시 구성하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽의 삭제를 시작할 수 있습니다.

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

링크 상태 전파

참고 가상 디바이스에서는 링크 상태 전파가 지원되지 않습니다. 7000 및 8000 Series 디바이스만 링크 상태 전파를 지원합니다.

링크 상태 전파는 인라인 집합의 두 쌍이 상태를 추적하도록 우회 모드 및 비 우회 모드에서 구성되는 인라인 집합의 기능입니다. 링크 상태 전파는 구리 및 파이버 구성 가능 우회 인터페이스에서 모두 사용할 수 있습니다.

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 어플라이언스는 변경 사항을 감지하고 다른 인터페이스의 링크 상태가 일치하도록 업데이트합니다. 어플라이언스가 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.

고가용성 쌍 내 7000 및 8000 Series 디바이스에 구성된 인라인 집합에 대한 링크 상태 전파를 비활성화할 수 없습니다.

투명 인라인 모드

투명 인라인 모드 옵션은 디바이스가 "bump in the wire" 역할을 수행하도록 합니다. 즉 디바이스는 소스 및 대상과 관계없이 발견되는 모든 네트워크 트래픽을 전달합니다. 7000 및 8000 Series디바이스에서는 이 옵션을 비활성화할 수 없습니다.

엄격한 **TCP** 시행

참고 가상 디바이스에서는 엄격한 TCP 시행이 지원되지 않습니다. 7000 및 8000 Series 디바이스만 이 옵션을 지원합니다. 또한 동일한 인라인 집합에서 이 옵션 및 탭 모드를 활성화할 수 없습니다.

TCP 보안을 극대화하기 위해 엄격한 시행을 활성화할 수 있으며 3방향 핸드셰이크가 완료되지 않은 연결이 차단됩니다. 엄격한 시행은 다음 항목도 차단합니다.

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

고급 인라인 집합 옵션 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 편집하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** 편집하려는 인라인 집합 옆에 있는 수정( )을 클릭합니다.

단계 **5** **Advanced(**고급**)**를 클릭합니다.

단계 **6** 고급 인라인 설정 옵션, 10 페이지의 설명에 따라 옵션을 구성합니다.

참고 가상 디바이스에서는 링크 상태 전파 및 엄격한 TCP 시행이 지원되지 않습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

인라인 집합 삭제

인라인 집합을 삭제할 때 그 집합에 지정되었던 모든 인라인 인터페이스는 다른 집합에 포함될 수 있게 됩니다. 인터페이스가 삭제되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 인라인 집합을 삭제하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** 삭제하려는 인라인 집합 옆에 있는 삭제( )을 클릭합니다.

단계 **5** 확인 메시지가 표시되면 인라인 집합 삭제를 확인합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.