인터페이스 개요

threat defense 디바이스에는 여러 모드를 설정할 수 있는 데이터 인터페이스와 관리/진단 인터페이스가 포함됩니다.

관리/진단 인터페이스

물리적 관리 인터페이스는 논리적 진단 인터페이스와 논리적 관리 인터페이스 간에 공유됩니다.

관리 인터페이스

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 management center에 설치하고 등록하는 데 사용됩니다. 고유 IP 주소 및 정적 라우팅을 사용합니다. **configure network** 명령을 사용해 CLI에서 설정을 구성할 수 있습니다. management center에 IP 주소를 추가한 뒤 CLI에서 IP 주소를 변경하는 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Devices(**디바이스**)** > **Management(**관리**)** 영역의 Secure Firewall Management Center에서 IP 주소를 일치시킬 수 있습니다.

관리 인터페이스 대신 데이터 인터페이스를 사용하여 threat defense를 관리할 수도 있습니다.

진단 인터페이스

논리적 진단 인터페이스는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** 화면에서 나머지 데이터 인터페이스와 함께 설정할 수 있습니다. 진단 인터페이스 사용은 선택 사항입니다(라우팅 및 투명 모드 구축 시나리오 참조). 진단 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다. SSH를 지원하지 않습니다. 데이터 인터페이스 또는 관리 인터페이스 사용 시에만 SSH를 사용할 수 있습니다. 진단 인터페이스는 SNMP 또는 시스템 로그 모니터링에 유용합니다.

참고 진단 및 관리 인터페이스는 물리적 포트를 공유하지만 동일한 네트워크의 각 인터페이스에 서로 다른 IP 주소를 할당해야 합니다.

인터페이스 모드 및 유형

일반 방화벽 모드와 IPS 전용 모드에서 threat defense 인터페이스를 구축할 수 있습니다. 동일한 디바이스에 방화벽 및 IPS 전용 인터페이스를 포함시킬 수 있습니다.

일반 방화벽 모드

방화벽 모드 인터페이스는 IP 및 TCP 레이어, IP 조각 모음, TCP 표준화에서 플로우 유지, 플로우 상태 추적 등의 방화벽 기능에 트래픽을 적용합니다. 필요한 경우 보안 정책에 따라 해당 트래픽에 대한 IPS 기능을 구성할 수도 있습니다.

구성할 수 있는 방화벽 인터페이스의 유형은 디바이스의 방화벽 모드 집합이 라우팅인지 투명 모드인지에 따라 달라집니다. 자세한 내용은 투명한 또는 라우팅된 방화벽 모드를 참조하십시오.

- 라우팅 모드 인터페이스(라우팅된 방화벽 모드 전용) - 서로 라우팅하려는 각 인터페이스가 다른 서브넷에 있습니다.
- 브리지 그룹 인터페이스(라우팅 및 투명 방화벽 모드 - 네트워크의 여러 인터페이스를 그룹화할 수 있고 Firepower Threat Defense 디바이스는 브리지 기술을 사용해 인터페이스 간 트래픽을 전달합니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 라우팅 모드에서 Firepower Threat Defense 디바이스는 BVI 및 일반 라우팅 인터페이스를 라우팅합니다. 투명 모드에서 의 각 브리지 그룹은 구분되며 서로 통신할 수 없습니다.

IPS 전용 모드

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. 인라인 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.

보안 영역 및 인터페이스 그룹

각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당될 수 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 하나 이상의 장치에 있는 "내부" 인터페이스를 "내부" 영역에 할당하고 "외부" 인터페이스를 "외부" 영역에 할당할 수 있습니다. 그런 다음 동일한 영역을 사용하는 모든 디바이스에 대해 트래픽이 내부 영역에서 외부 영역으로 이동할 수 있도록 액세스 제어 정책을 구성할 수 있습니다.

각 개체에 속한 인터페이스를 보려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 **Interface(**인터페이스**)**를 클릭합니다. 이 페이지에는 매니지드 디바이스에 구성된 보안 영역 및 인터페이스 그룹이 나열됩니다. 각 인터페이스 개체를 확장하여 각 인터페이스 개체의 인터페이스 유형을 볼 수 있습니다.

참고 모든 영역(전역 정책)에 적용되는 정책은 영역의 인터페이스 및 영역에 할당되지 않은 인터페이스에도 적용됩니다.

참고 진단/관리 인터페이스는 영역 또는 인터페이스 그룹에 속하지 않습니다.

보안 영역 및 인터페이스 그룹

인터페이스 개체의 유형은 두 가지입니다.

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹(및 하나의 보안 영역)에 속할 수 있습니다.

  NAT 정책, 사전 필터 정책 및 QoS 정책에서 인터페이스 그룹을 사용할 수 있으며, 시스템 로그 서버 또는 DNS 서버와 같이 인터페이스 이름을 직접 지정할 수 있는 기능도 사용할 수 있습니다.

일부 정책은 보안 영역만 지원하고 일부 정책은 영역 및 그룹을 지원합니다. 인터페이스 그룹에서 제공하는 기능이 필요한 경우가 아니면 보안 영역이 기본적으로 사용됩니다. 보안 영역은 모든 기능에서 지원되기 때문입니다.

인터페이스 그룹에 대한 기존의 보안 영역을 변경할 수 없으며 그 반대의 경우도 마찬가지입니다. 그 대신, 새 인터페이스 개체를 생성해야 합니다.

참고 터널 영역은 인터페이스 개체가 아니지만 특정 컨피그레이션에서는 보안 영역 대신 사용할 수 있습니다(터널 영역 및 사전 필터링 참조).

인터페이스 개체 유형

다음 인터페이스 개체 유형을 참조하십시오.

- Passive(패시브) - IPS 전용 패시브 또는 ERSPAN 인터페이스용입니다.
- Inline(인라인) - IPS 전용 인라인 집합 인터페이스용입니다.
- Switched(스위치드) - 일반 방화벽 브리지 그룹 인터페이스용입니다.
- Routed(라우팅됨) - 일반 방화벽 라우팅 인터페이스용입니다.
- ASA — (보안 영역만 해당) 레거시 ASA FirePOWER 디바이스 인터페이스용입니다.

인터페이스 개체의 모든 인터페이스는 모든 인라인, 수동, 스위칭, 라우팅이 동일한 유형이어야 합니다. 인터페이스 개체를 생성한 후에는 여기에 포함하는 인터페이스의 유형을 변경할 수 없습니다.

인터페이스 이름

인터페이스(또는 영역 이름) 자체는 보안 정책과 관련하여 어떤 기본 동작도 제공하지 않습니다. 향후 구성에서 실수를 방지하기 위해 자체 설명적인 이름을 사용하는 것이 좋습니다. 올바른 이름은 논리적 세그먼트 또는 트래픽 사양을 나타냅니다. 예를 들면 다음과 같습니다.

- 내부 인터페이스의 이름 - InsideV110, InsideV160, InsideV195
- DMZ 인터페이스의 이름 - DMZV11, DMZV12, DMZV-TEST
- 외부 인터페이스의 이름 - Outside-ASN78, Outside-ASN91

인터페이스 개체 및 멀티테넌시

다중 도메인 구축의 경우, 모든 수준에서 인터페이스 개체를 생성할 수 있습니다. 상위 도메인에 생성된 인터페이스 개체는 다른 도메인의 디바이스에 상주하는 인터페이스를 포함할 수 있습니다. 이 경우, 개체 관리자에서 상위 인터페이스 개체 구성을 보는 서브도메인 사용자는 해당 도메인에서 인터페이스만 볼 수 있습니다.

역할별로 제한하지 않는 한, 서브도메인 사용자는 상위 도메인에 생성된 인터페이스 개체를 보고 수정할 수 있습니다. 서브도메인 사용자는 이러한 인터페이스 개체에서 인터페이스를 추가하고 삭제할 수 있습니다. 그러나 인터페이스 개체를 삭제하거나 이름을 바꿀 수는 없습니다. 하위 도메인에 생성된 인터페이스 개체는 보거나 수정할 수 없습니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

인터페이스의 기본 설정

이 섹션에서는 인터페이스에 대한 기본 설정이 나열됩니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형에 따라 다릅니다.

- 물리적 인터페이스 - 비활성화됨. 초기 설정에 대해 활성화된 관리 인터페이스는 예외입니다.
- 이중 인터페이스 — 활성화되어 있습니다. 그러나 트래픽이 이중 인터페이스를 통과하려면 물리적 인터페이스 멤버도 활성화되어야 합니다.
- VLAN 하위 인터페이스 - 활성화됨, 그러나 트래픽이 하위 인터페이스를 통과하려면 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 - 채널 인터페이스(ISA 3000) - 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 - 채널 인터페이스(Firepower 및 Secure Firewall 모델) - 비활성화되어 있습니다.

참고 Firepower 4100/9300의 경우 관리를 위해 섀시와 management center에서 인터페이스를 활성화하거나 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 섀시와 management center를 일치시키지 않을 수 있습니다.

기본 속도와 양방향

기본적으로 구리(RJ-45) 인터페이스의 속도와 앙방향은 자동 협상이 이루어지도록 설정됩니다.

기본적으로 속도 및 듀플렉스(SFP) 인터페이스는 자동 협상이 활성화된 최대 속도로 설정됩니다.

Secure Firewall 3100의 경우, 속도는 설치된 SFP 속도를 탐지하도록 설정됩니다.

보안 영역 및 인터페이스 그룹 개체 생성

디바이스 인터페이스를 할당할 수 있는 보안 영역 및 인터페이스 그룹을 추가합니다.

팁 빈 인터페이스 개체를 만들고 여기에 인터페이스를 추가할 수 있습니다. 인터페이스를 추가하려면 인터페이스에 이름이 있어야 합니다. 인터페이스를 구성하는 동안 보안 영역(인터페이스 그룹은 제외)을 생성할 수도 있습니다.

시작하기 전에

각 인터페이스 개체 유형의 사용 요구 사항 및 제한 사항을 이해합니다. 보안 영역 및 인터페이스 그룹, 4 페이지을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Interface(**인터페이스**)**를 선택합니다.

단계 **3** **Add Security Zone(**보안 영역 추가**)** 또는 **Add** > **Interface Group(**추가 > 인터페이스 그룹**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Interface Type(**인터페이스 유형**)**을 선택합니다.

단계 **6** (선택 사항) **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 드롭다운 목록에서 추가할 인터페이스가 포함된 디바이스를 선택합니다.

이 화면에서는 인터페이스를 할당할 필요가 없습니다. 대신 인터페이스를 구성할 때 영역 또는 그룹에 인터페이스를 할당할 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

물리적 인터페이스 활성화 및 이더넷 설정 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화 기본적으로 물리적 인터페이스는 비활성화됩니다(진단 인터페이스의 경우는 제외).

- 특성 속도 및 양방향 설정 기본적으로 속도 및 양방향은 자동으로 설정되어 있습니다.

이 절차에서는 인터페이스 설정의 작은 하위 집합에 대해서만 설명합니다. 이 시점에서 다른 파라미터 설정은 하지 않는 것이 좋습니다. 예를 들면 EtherChannel 또는 이중 인터페이스의 일부로 사용하려는 인터페이스의 이름을 지정할 수 없습니다.

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

참고 Firepower 1010 스위치 포트에 대해서는 Firepower 1010 스위치 포트 구성의 내용을 참조하십시오.

Threat Defense 기능 기록**:**

- 7.3 - Secure Firewall 3100 고정 포트의 기본 FEC(전달 오류 수정)가 25GB+ SR, CSR 및 LR 트렌시버에 대해 조항 74 FC-FEC에서 조항 108 RS-FEC로 변경됨
- 7.2 - Firepower 2100, Secure Firewall 3100에 대한 LLDP 지원 Secure Firewall 3100에 대한 흐름 제어 지원
- 7.1- Secure Firewall 3100에 대한 전달 오류 수정 지원
- 7.1 - Secure Firewall 3100에 대한 SFP 기반 속도 설정 지원
- 7.1 - Firepower 1100에 대한 LLDP 지원
- 7.1- 이제 인터페이스 자동 협상이 속도 및 양방향과 독립적으로 설정되며, 인터페이스 동기화가 개선됨

시작하기 전에

management center에 추가한 후 디바이스의 물리적 인터페이스를 변경한 경우, **Interfaces(**인터페이스**)**의 왼쪽 상단에 있는 **Sync Interfaces from device(**디바이스의 인터페이스 동기화**)**를 클릭하여 인터페이스 목록을 새로 고쳐야 합니다. 핫 스왑을 지원하는 Secure Firewall 3100의 경우 디바이스에서 인터페이스를 변경하기 전에 Secure Firewall 3100용 네트워크 모듈 관리, 14 페이지 항목을 참고하십시오.

프로시저

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

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

단계 **3** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** (선택 사항) **Hardware Configuration(**하드웨어 구성**)** > **Speed(**속도**)**를 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**)** - **Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다. SFP 인터페이스는 전이중만 지원합니다.
- **Speed(**속도**)** — 속도를 선택합니다(모델에 따라 다름). (Secure Firewall 3100만 해당) 설치된 SFP 모듈의 속도를 탐지하고 적절한 속도를 사용하려면 **Detect SFP(SFP** 탐지**)**를 선택합니다. Duplex(듀플렉스)는 항상 Full(풀)이며 자동 협상은 항상 활성화되어 있습니다. 이 옵션은 나중에 네트워크 모듈을 다른 모델로 변경하고 속도를 자동으로 업데이트하려는 경우에 유용합니다.
- **Auto Negotiation(**자동 협상**)** - 속도, 링크 상태 및 흐름 제어를 협상하도록 인터페이스를 설정합니다.
- 전달 오류 수정 모드 - (Secure Firewall 3100만 해당) 25Gbps 이상의 인터페이스에서는 전달 오류 수정(FEC)을 활성화합니다. EtherChannel 멤버 인터페이스의 경우, 이를 EtherChannel에 추가하기 전에 전달 오류 수정을 구성해야 합니다. **Auto(**자동**)**를 사용할 때 선택하는 설정은 트랜시버 유형 및 인터페이스가 고정(내장) 또는 네트워크 모듈에 있는지 여부에 따라 달라집니다.

표 ***1:*** 자동 설정을 위한 기본 ***FEC***

트랜시버 유형	고정 포트 기본 **FEC(Ethernet 1/9~1/16)**	네트워크 모듈 기본 **FEC**
25G-SR	조항 108 RS-FEC	조항 108 RS-FEC
25G-LR	조항 108 RS-FEC	조항 108 RS-FEC
10/25G-CSR	조항 108 RS-FEC	조항 74 FC-FEC(25/50G)
25G-AOC*x*M	조항 74 FC-FEC	조항 74 FC-FEC
25G-CU2.5/3M	자동 협상	자동 협상
25G-CU4/5M	자동 협상	자동 협상

단계 **6** (선택 사항) (Firepower 1100, 2100, Secure Firewall 3100) **Hardware Configuration(**하드웨어 구성**)** > **Network Connectivity(**네트워크 연결**)**를 클릭하여 LLDP(Link Layer Discovery Protocol)를 활성화합니다.

- **Enable LLDP Receive(LLDP** 수신 활성화**)** — 방화벽이 피어에서 LLDP 패킷을 수신하도록 활성화합니다.
- **Enable LLDP Transmit(LLDP** 전송 활성화**)** — 방화벽이 LLDP 패킷을 피어로 전송하도록 활성화합니다.

단계 **7** (선택 사항) (Secure Firewall 3100) **Hardware Configuration(**하드웨어 구성**)** > **Network Connectivity(**네트워크 연결**)**를 클릭하고 **Flow Control Send(**플로우 제어 전송**)**를 선택하여 플로우 제어를 위한 일시 중지(XOFF) 프레임을 활성화합니다.

Flow control(흐름 제어)는 연결된 이더넷 포트를 활성화하여 혼잡한 노드가 다른 쪽 끝에서 링크 작업을 일시 중지하도록 허용하여 혼잡 중에 트래픽 속도를 제어합니다. Threat Defense 포트에 혼잡이 발생하고(내부 스위치의 대기 리소스가 소진된 경우) 더 이상 트래픽을 수신할 수 없는 경우, 해당 포트는 조건이 해결될 때까지 전송을 중지하도록 일시 중지 프레임을 전송하여 다른 포트에 알립니다. 일시 중지 프레임을 수신하면 전송 디바이스는 데이터 패킷 전송을 중지하여 혼잡 기간 동안 데이터 패킷이 손실되는 것을 방지합니다.

참고 threat defense는 원격 피어가 트래픽의 속도를 제어할 수 있도록 일시 중지 프레임 전송을 지원합니다.

그러나 일시 중지 프레임 수신은 지원되지 않습니다.

내부 스위치에는 각각 250 바이트의 8000 버퍼의 전역 풀이 있으며, 스위치는 각 포트에 동적으로 버퍼를 할당 합니다. 버퍼 사용량이 전역 최고 수위 표시(2MB(8000개 버퍼))를 초과하면 flowcontrol이 활성화된 모든 인터페이스에 일시 중지 프레임이 전송됩니다. 버퍼가 포트 최고 수위 표시 (0.3125MB(1250 버퍼))를 초과하면 일시 중지 프레임이 특정 인터페이스에서 전송됩니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위(전역 1.25 MB(5000 버퍼), .25 MB/port (1000 버퍼)) 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 연결 파트너가 XON 프레임을 받은 후 트래픽을 다시 시작할 수 있습니다.

802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.

단계 **8** 모드 드롭다운 목록에서 다음을 선택합니다.

- 없음 - 일반 방화벽 인터페이스 및 인라인 집합을 설정하려면 이 옵션을 선택합니다. 추가 설정에 따라 라우팅, 스위치, 인라인 모드로 자동 변경됩니다.
- 패시브 - 패시브 IPS 전용 인터페이스의 경우 이 설정을 선택합니다.
- **Erspan** - ERSPAN 패시브 IPS 전용 인터페이스의 경우 이 설정을 선택합니다.

단계 **9** **Priority(**우선순위**)** 필드에 0~65535 범위의 숫자를 입력합니다.

이 값은 정책 기반 라우팅 구성에서 사용됩니다. 우선순위는 여러 이그레스 인터페이스에서 트래픽을 분산할 방법을 결정하는 데 사용됩니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

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

단계 **12** 인터페이스 구성을 계속합니다.

- 일반 방화벽 인터페이스

- 인라인 집합 및 패시브 인터페이스

Management Center과 인터페이스 변경 사항 동기화

디바이스의 인터페이스 설정 변경은 management center과 디바이스의 동기화 오류를 발생시킬 수 있습니다. management center은 다음 방법 중 하나로 인터페이스 변경을 탐지할 수 있습니다.

- 디바이스에서 전송된 이벤트
- 에서 구축할 때 동기화 management center

  management center이 구축을 시도하지만 실패하는 경우 인터페이스 변경 사항을 탐지합니다. 먼저 인터페이스 변경 사항을 적용해야 합니다.
- 수동 동기화

management center 외부에서 수행되는 두 가지 유형의 인터페이스 변경은 동기화되어야 합니다.

- 물리적 인터페이스 추가 또는 삭제 - 새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 threat defense 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 threat defense 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다. 논리적 디바이스에 영향을 주거나 management center에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

  management center가 변경 사항을 탐지하는 경우 인터페이스 페이지는 각 인터페이스 왼쪽에 상태(제거, 변경, 추가)를 표시합니다.
- Management Center FMC 액세스 인터페이스 변경 - **configure network management-data-interface** 명령을 사용하여 management center 관리용 데이터 인터페이스를 구성하는 경우 management center에서 일치하는 구성 변경을 수동으로 수행한 다음 변경을 승인해야 합니다. 이러한 인터페이스 변경은 자동으로 수행할 수 없습니다.

이 절차는 필요한 경우 디바이스 변경 사항을 수동으로 동기화하는 방법과 탐지된 변경 사항을 인식하는 방법을 설명합니다. 디바이스가 임시로 변경되는 경우 management center에 변경 사항을 저장하지 말고 디바이스가 안정될 때까지 기다린 뒤 다시 동기화해야 합니다.

시작하기 전에

- 사용자 역할:
  - 관리자
  - 액세스 관리자
  - 네트워크 관리자

프로시저

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

단계 **2** 필요한 경우 인터페이스 왼쪽 상단의 디바이스 동기화를 클릭합니다.

단계 **3** 변경 사항이 탐지되면 다음 단계를 참조하십시오.

물리적 인터페이스 추가 또는 삭제

a) **Interfaces(**인터페이스**)**에 인터페이스 구성이 변경되었음을 나타내는 빨간색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 클릭하여 더 보기 링크를 클릭합니다.

b) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

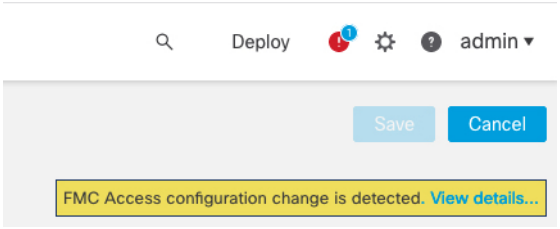
오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

c) **Save(**저장**)**를 클릭합니다.

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

FMC 액세스 인터페이스 변경

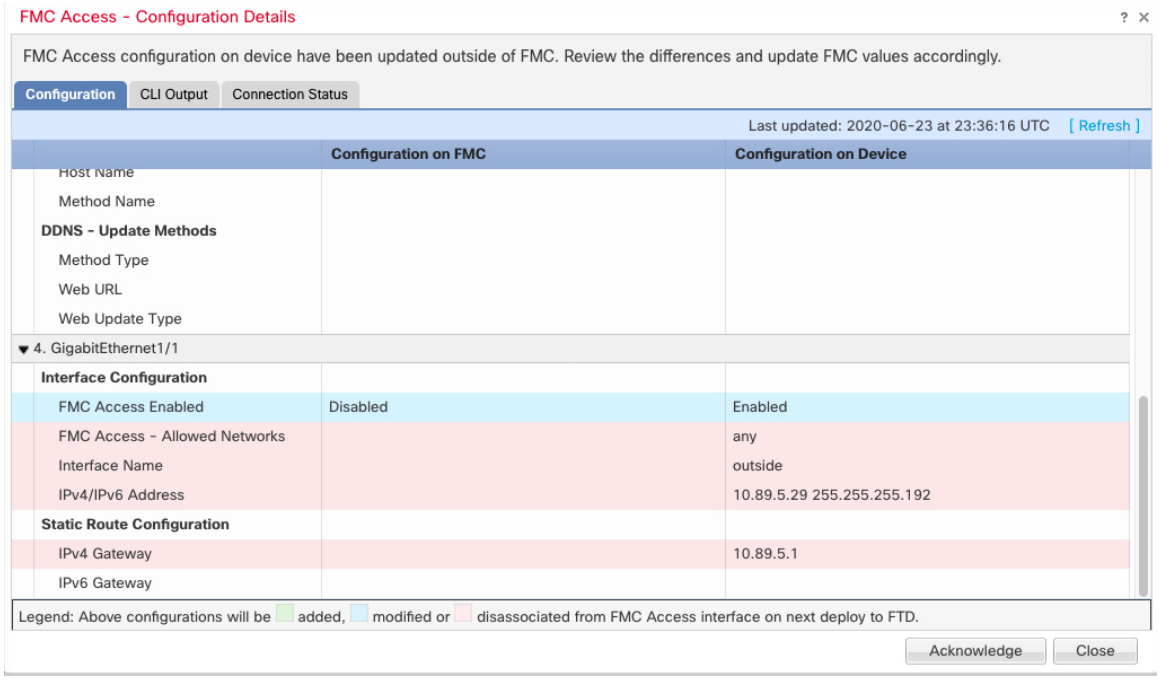
a) **Device(**디바이스**)** 페이지의 오른쪽 상단에 management center 액세스 구성이 변경되었음을 나타내는 노란색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 세부 정보 보기 링크를 클릭합니다.



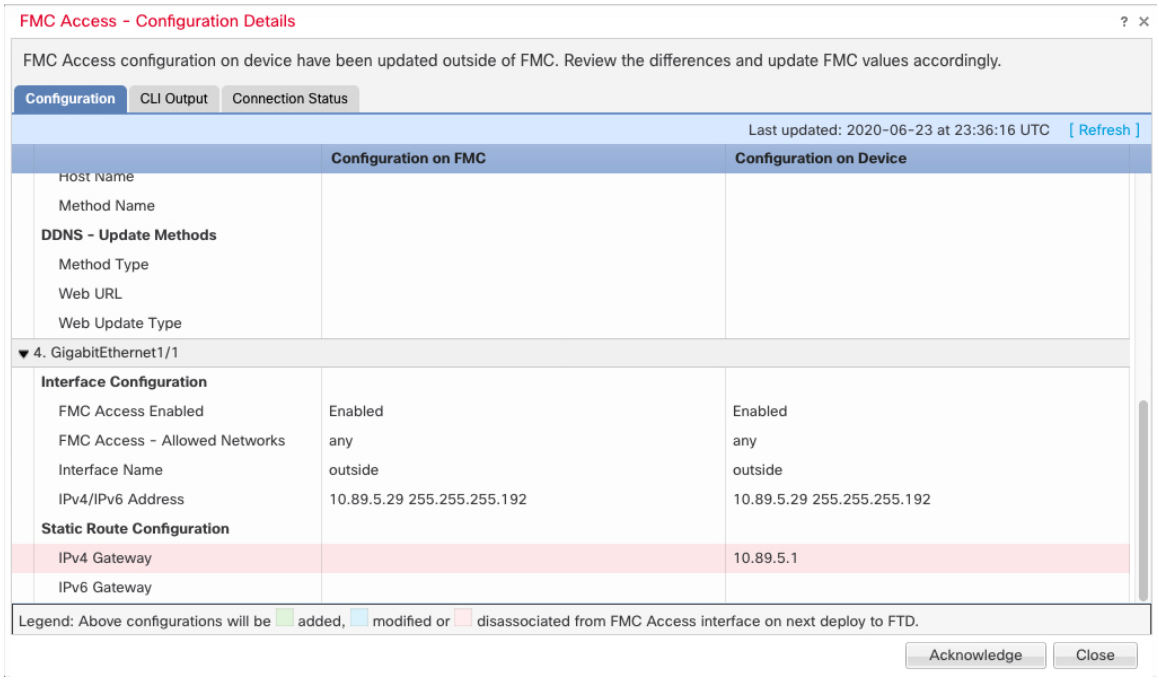
FMC Access - Configuration Details(FMC 액세스 - 구성 세부 정보**)** 대화 상자가 열립니다.

b) 강조 표시된 모든 구성, 특히 빨간색으로 강조 표시된 구성을 확인합니다. management center에서 수동으로 값을 구성하여 threat defense의 값을 일치시켜야 합니다.

예를 들어 아래의 분홍색 강조 표시는 threat defense에는 있지만 아직 management center에는 없는 구성을 보여줍니다.



다음 예는 management center에서 인터페이스를 구성한 후의 이 페이지를 보여줍니다. 인터페이스 설정이 일치하고 분홍색 강조 표시가 제거되었습니다.



c) **Acknowledge(**승인**)**를 클릭합니다.

management center 구성을 완료하고 구축 준비가 완료될 때까지 **Acknowledge(**승인**)**를 클릭하지 않는 것이 좋습니다. **Acknowledge(**승인**)**를 클릭하면 구축시 차단이 제거됩니다. 다음에 구축할

때 management center 구성은 threat defense의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 management center에서 구성을 수동으로 수정하는 것은 사용자의 책임입니다.

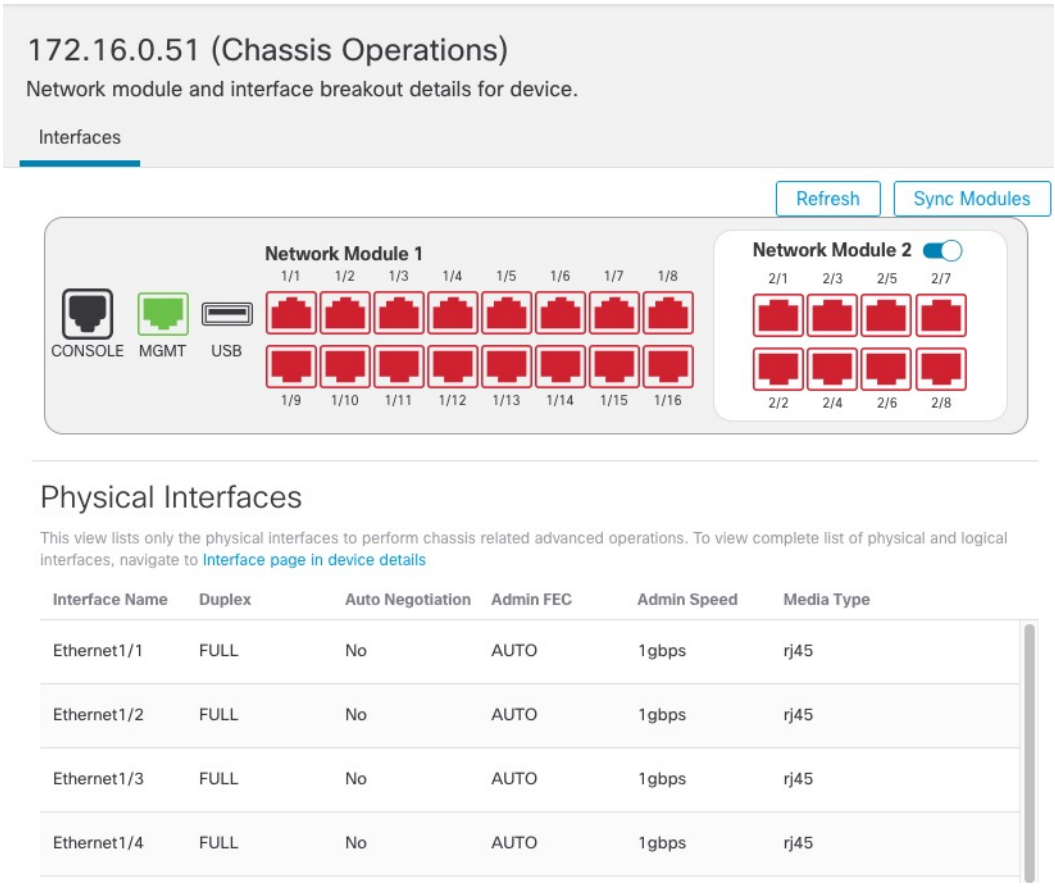
d) 이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다.

Secure Firewall 3100용 네트워크 모듈 관리

디바이스의 전원을 켜기 전에 네트워크 모듈을 설치하는 경우에는 별도의 작업이 필요하지 않습니다. 네트워크 모듈이 활성화되었으며 사용할 준비가 되었습니다.

디바이스에 대한 물리적 인터페이스 세부 정보를 보고 네트워크 모듈을 관리하려면 **Chassis Operations(**섀시 작업**)** 페이지를 엽니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성의 경우 이 옵션은 제어 노드/액티브 유닛에서만 사용할 수 있습니다. 디바이스의 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다.

그림 ***1:*** 섀시 작동



인터페이스 상태를 새로 고치려면 **Refresh(**새로 고침**)**를 클릭합니다. 탐지해야 하는 디바이스에서 하드웨어를 변경한 경우 **Sync Modules(**모듈 동기화**)**를 클릭합니다.

초기 부팅 후 네트워크 모듈 설치를 변경해야 하는 경우 다음 절차를 참조하십시오.

브레이크아웃 포트 구성

각 40GB 이상의 인터페이스에 대해 10GB 분할 포트를 구성할 수 있습니다. 이 절차에서는 포트를 분리하고 다시 조인하는 방법을 설명합니다. 브레이크아웃 포트는 EtherChannel에 추가되는 것을 포함하여 다른 물리적 이더넷 포트와 마찬가지로 사용할 수 있습니다.

변경 사항은 즉시 적용됩니다. 디바이스에 구축할 필요가 없습니다. 연결을 끊거나 다시 참가한 후에는 이전 인터페이스 상태로 롤백할 수 없습니다.

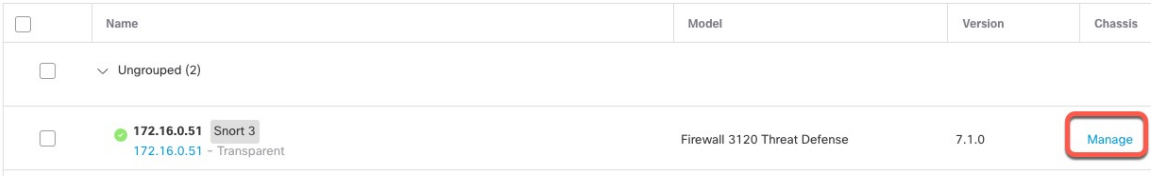
시작하기 전에

- 지원되는 브레이크아웃 케이블을 사용해야 합니다. 자세한 내용은 하드웨어 설치 가이드를 참조하십시오.
- 인터페이스를 분리하거나 다시 조인하기 전에 다음에 대해 인터페이스를 사용할 수 없습니다.
  - 페일오버 링크
  - 클러스터 제어 링크
  - 하위 인터페이스 보유
  - EtherChannel 멤버
  - BVI 멤버
  - 관리자 액세스 인터페이스
- 보안 정책에서 직접 사용되는 인터페이스는 구성에 영향을 줄 수 있습니다. 그러나 작업은 차단되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성(HA)의 경우 이 옵션은 노드/액티브 장치에 대해서만 사용할 수 있습니다. 네트워크 모듈 변경 사항은 모든 노드에 복제됩니다.

그림 ***2:*** 섀시 관리



디바이스에 대한 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다. 이 페이지에는 디바이스에 대한 물리적 인터페이스 세부 정보가 표시됩니다.

단계 **2** 40GB 이상의 인터페이스에서 10GB 포트를 분리합니다.

a) 인터페이스 오른쪽의 중단(↘)을 클릭합니다.

확인 대화 상자에서 **Yes(**예**)**를 클릭합니다. 인터페이스가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 브레이크아웃을 다시 시도할 수 있습니다.

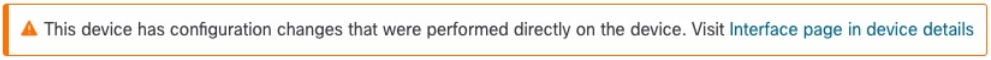
예를 들어 Ethernet2/1 40GB 인터페이스를 분리하기 위해 결과 하위 인터페이스는 Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 및 Ethernet2/1/4로 식별됩니다.

인터페이스 그래픽에서 분리된 포트의 모양은 다음과 같습니다.

그림 ***3:*** 브레이크아웃 포트

b) 화면 상단의 메시지 링크를 클릭하여 **Interfaces(**인터페이스**)** 페이지로 이동하여 인터페이스 변경 사항을 저장합니다.

그림 ***4: Interface(***인터페이스***)*** 페이지로 이동



c) **Interfaces(**인터페이스**)** 페이지 상단에서 **Click to know more(**자세한 내용을 보려면 클릭**)**를 클릭합니다. **Interface Changes(**인터페이스 변경 사항**)** 대화 상자가 열립니다.

그림 ***5:*** 인터페이스 변경 사항 보기

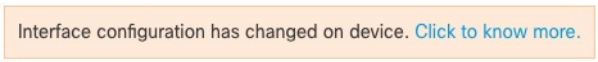
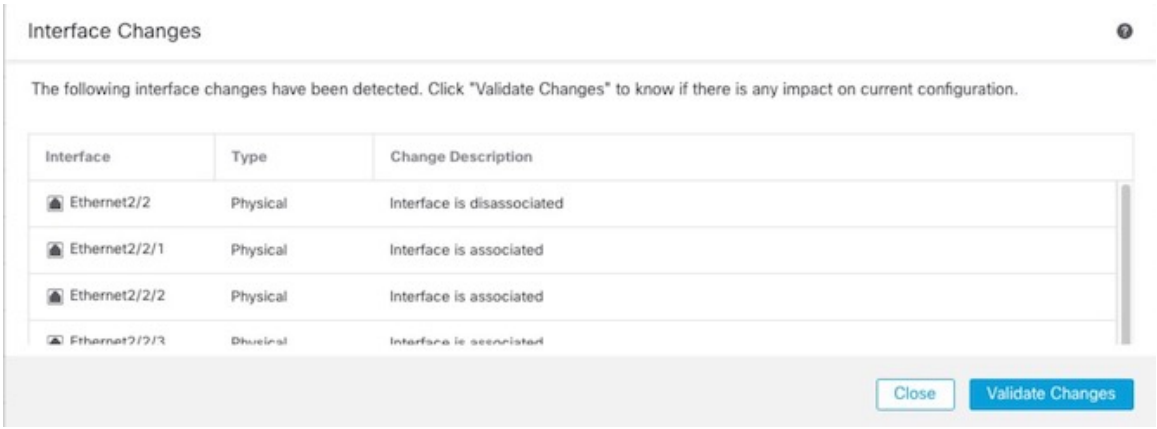


그림 ***6:*** 인터페이스 변경 사항



d) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

보안 정책에 사용되는 상위 인터페이스를 바꾸면 구성에 영향을 줄 수 있습니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다.

e) **Interfaces(**인터페이스**)** 페이지로 돌아가려면 **Close(**닫기**)**를 클릭합니다.

f) **Save(**저장**)**를 클릭하여 인터페이스 변경 사항을 방화벽에 저장합니다.

g) 구성을 변경해야 하는 경우 구축 > 구축으로 이동하여 정책을 구축합니다.

브레이크아웃 포트 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **3** 브레이크아웃 포트 다시 조인

인터페이스의 모든 하위 포트에 다시 조인해야 합니다.

a) 인터페이스 오른쪽에 있는 참가( )을 클릭합니다.

확인 대화 상자에서 **Yes(**예**)**를 클릭합니다. 하위 포트가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 다시 조인할 수 있습니다.

b) 화면 상단의 메시지 링크를 클릭하여 **Interfaces(**인터페이스**)** 페이지로 이동하여 인터페이스 변경 사항을 저장합니다.

그림 ***7: Interface(***인터페이스***)*** 페이지로 이동

c) **Interfaces(**인터페이스**)** 페이지 상단에서 **Click to know more(**자세한 내용을 보려면 클릭**)**를 클릭합니다. **Interface Changes(**인터페이스 변경 사항**)** 대화 상자가 열립니다.

그림 ***8:*** 인터페이스 변경 사항 보기

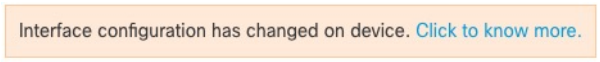
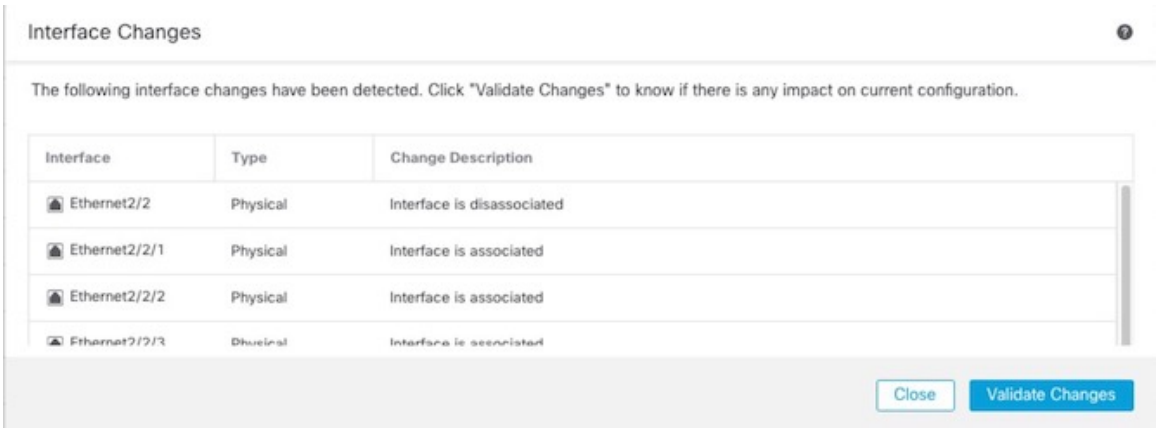


그림 *9:* 인터페이스 변경 사항



d) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

보안 정책에서 사용되는 하위 인터페이스를 교체하면 구성에 영향을 줄 수 있습니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다.

e) **Interfaces(**인터페이스**)** 페이지로 돌아가려면 **Close(**닫기**)**를 클릭합니다.

f) **Save(**저장**)**를 클릭하여 인터페이스 변경 사항을 방화벽에 저장합니다.

g) 구성을 변경해야 하는 경우 구축 > 구축으로 이동하여 정책을 구축합니다.

브레이크아웃 포트 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

네트워크 모듈 추가

초기 부팅 후 방화벽에 네트워크 모듈을 추가하려면 다음 단계를 수행합니다. 새 모듈을 추가하려면 재부팅해야 합니다.

프로시저

단계 **1** 하드웨어 설치 가이드에 따라 네트워크 모듈을 설치합니다.

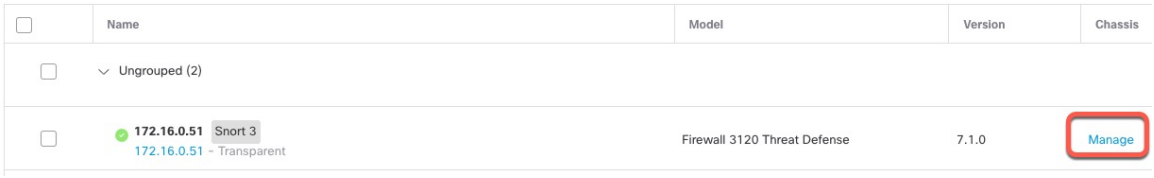
클러스터링 또는 고가용성의 경우 모든 노드에 네트워크 모듈을 설치합니다.

단계 **2** 방화벽을 재부팅합니다. 디바이스 종료 또는 재시작의 내용을 참조하십시오.

클러스터링 또는 고가용성의 경우 먼저 데이터 노드/스탠바이 유닛을 재부팅하고 다시 작동할 때까지 기다립니다. 그런 다음 제어 노드(제어 노드 변경 참조) 또는 액티브 유닛(Threat Defense 고가용성 쌍에서 활성 피어 전환 참조)을 변경하고 이전 제어 노드/액티브 유닛을 재부팅할 수 있습니다.

단계 **3** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성(HA)의 경우 이 옵션은 노드/액티브 장치에 대해서만 사용할 수 있습니다. 네트워크 모듈 변경 사항은 모든 노드에 복제됩니다.

그림 ***10:*** 섀시 관리

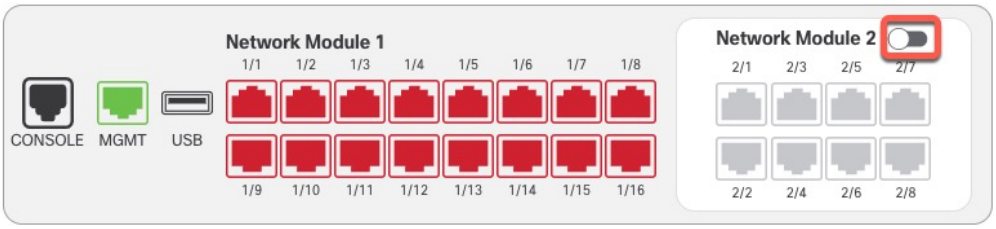


디바이스의 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다. 이 페이지에는 에 대한 물리적 인터페이스 세부 정보가 표시됩니다.

단계 **4** **Sync Modules(**모듈 동기화**)**를 클릭하여 새 네트워크 모듈 세부 정보로 페이지를 업데이트합니다.

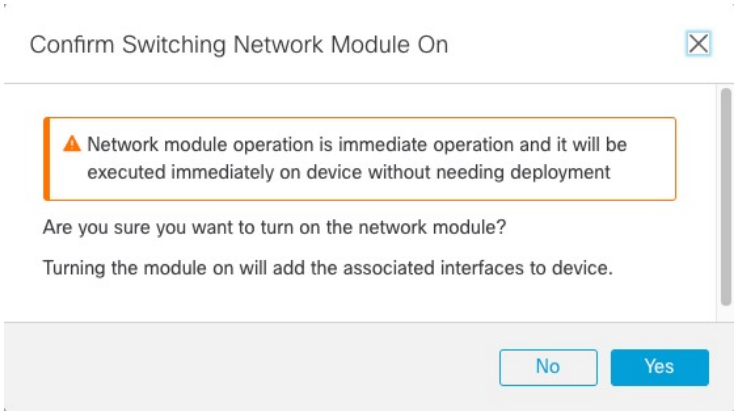
단계 **5** 인터페이스 그래픽에서 슬라이더 ( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 ***11:*** 네트워크 모듈 활성화



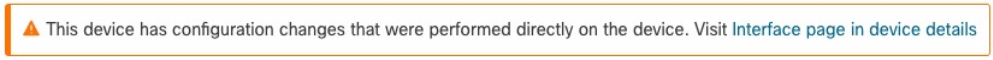
단계 **6** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***12:*** 사용 확인



단계 **7** 화면 상단에 메시지가 표시됩니다. 링크를 클릭하여 **Interfaces(**인터페이스**)** 페이지로 이동하여 인터페이스 변경 사항을 저장합니다.

그림 ***13: Interface(***인터페이스***)*** 페이지로 이동



단계 **8** (선택 사항) **Interfaces(**인터페이스**)** 페이지 상단에 인터페이스 구성이 변경되었다는 메시지가 표시됩니다. **Click to know more(**자세히 알아보려면 클릭**)**를 클릭하여 **Interface Changes(**인터페이스 변경 사항**)** 대화 상자를 열어 변경 사항을 볼 수 있습니다.

그림 ***14:*** 인터페이스 변경 사항 보기

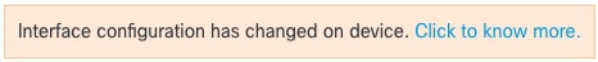
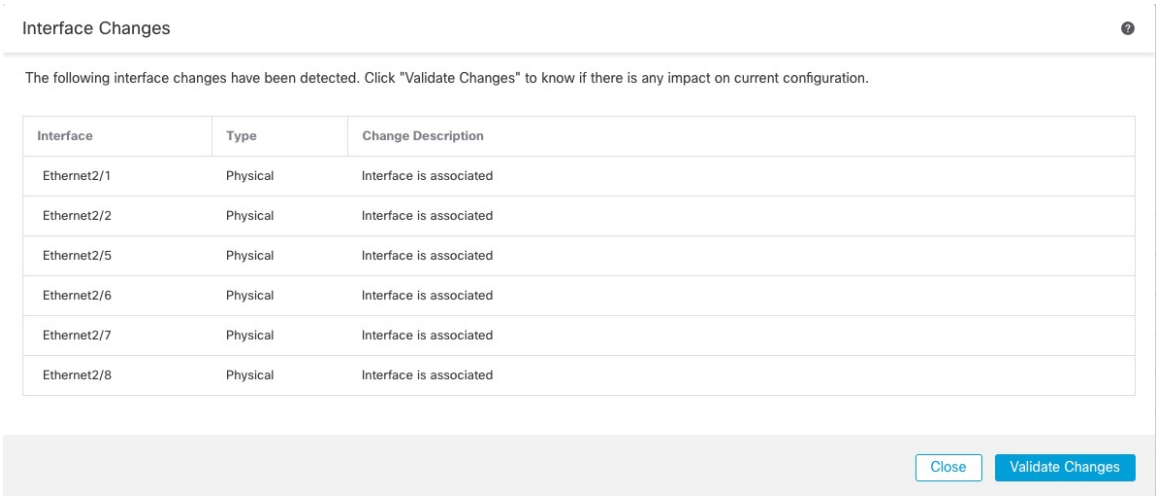


그림 ***15:*** 인터페이스 변경 사항



Interfaces(인터페이스**)** 페이지로 돌아가려면 **Close(**닫기**)**를 클릭합니다. (새 모듈을 추가하는 중이므로 구성에 영향을 미치지 않아야 하므로 **Validate Changes(**변경 사항 검증**)**를 클릭할 필요가 없습니다.)

단계 **9** **Save(**저장**)**를 클릭하여 인터페이스 변경 사항을 방화벽에 저장합니다.

네트워크 모듈 핫 스왑

재부팅할 필요 없이 네트워크 모듈을 동일한 유형의 새 모듈로 핫 스왑할 수 있습니다. 그러나 안전하게 제거하려면 현재 모듈을 종료해야 합니다. 이 절차에서는 기존 모듈을 종료하고 새 모듈을 설치하고 활성화하는 방법을 설명합니다.

클러스터링 또는 고가용성의 경우 제어 노드/액티브 유닛에서만 섀시 작업을 수행할 수 있습니다. 클러스터 제어 링크/페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다.

시작하기 전에

프로시저

단계 **1** 클러스터링 또는 고가용성의 경우 다음 단계를 수행합니다.

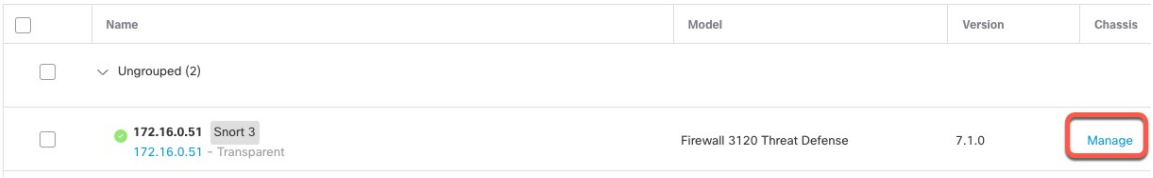
- 클러스터링 — 핫 스왑을 수행할 유닛이 데이터 노드인지 확인합니다(제어 노드 변경 참조). 그런 다음 노드를 분리하여 클러스터에 더 이상 존재하지 않도록 합니다. 노드 분리의 내용을 참조하십시오.

  핫 스왑을 수행한 후 노드를 클러스터에 다시 추가합니다. 또는 제어 노드에서 모든 작업을 수행할 수 있으며, 그러면 네트워크 모듈 변경 사항이 모든 데이터 노드에 동기화됩니다. 그러나 핫 스왑 중에는 모든 노드에서 이러한 인터페이스를 사용할 수 없게 됩니다.

- 고가용성 - 네트워크 모듈을 비활성화할 때 페일오버를 방지하려면 다음을 수행합니다.
  - 페일오버 링크가 네트워크 모듈에 있는 경우 고가용성을 해제해야 합니다. 고가용성 쌍 분리의 내용을 참조하십시오. 활성 페일오버 링크가 있는 네트워크 모듈을 비활성화하는 것은 허용되지 않습니다.
  - 네트워크 모듈의 인터페이스에 대한 인터페이스 모니터링을 비활성화합니다. 스탠바이 IP 주소 및 인터페이스 모니터링 구성의 내용을 참조하십시오.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성(HA)의 경우 이 옵션은 노드/액티브 장치에 대해서만 사용할 수 있습니다. 네트워크 모듈 변경 사항은 모든 노드에 복제됩니다.

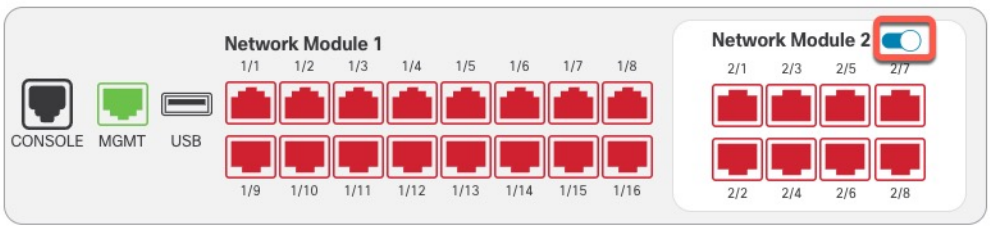
그림 ***16:*** 섀시 관리



디바이스의 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다. 이 페이지에는 에 대한 물리적 인터페이스 세부 정보가 표시됩니다.

단계 **3** 인터페이스 그래픽에서 슬라이더 ( )를 클릭하여 네트워크 모듈을 비활성화합니다.

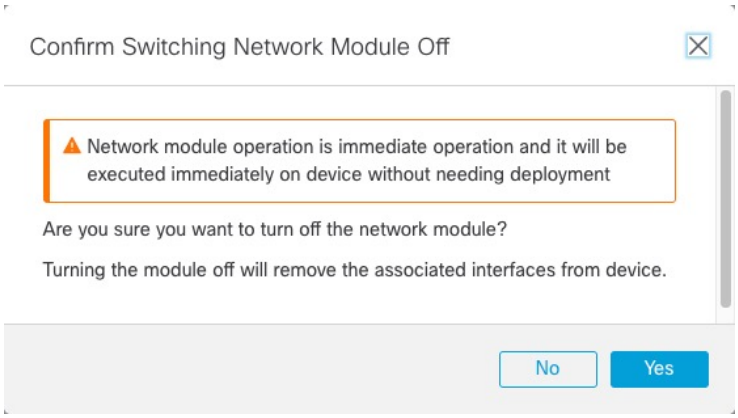
그림 ***17:*** 네트워크 모듈 비활성화



Interfaces(인터페이스**)** 페이지에서 변경 사항을 저장하지 마십시오. 네트워크 모듈을 교체하는 중이므로 기존 구성을 중단하지 않으려고 합니다.

단계 **4** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

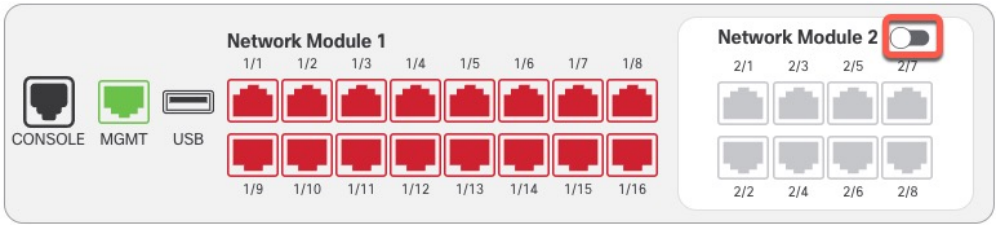
그림 ***18:*** 사용 안 함 확인



단계 **5** 디바이스에서 하드웨어 설치 가이드에 따라 기존 네트워크 모듈을 제거하고 새 네트워크 모듈로 교체합니다.

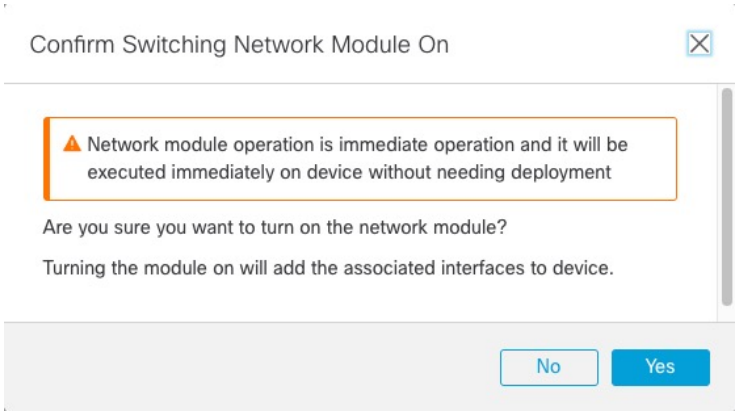
단계 **6** management center에서 슬라이더 ( )를 클릭하여 새 모듈을 활성화합니다.

그림 ***19:*** 네트워크 모듈 활성화



단계 **7** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***20:*** 사용 확인



단계 **8** 클러스터링 또는 고가용성의 경우 다음 단계를 수행합니다.

- 클러스터링 - 클러스터에 노드를 다시 추가합니다. 새 클러스터 노드 추가의 내용을 참조하십시오.
- 고가용성 -
  - 고가용성을 중단한 경우 고가용성을 다시 구성합니다. 고가용성 쌍 추가의 내용을 참조하십시오.
  - 네트워크 모듈의 인터페이스에 대한 인터페이스 모니터링을 다시 활성화합니다. 스탠바이 IP 주소 및 인터페이스 모니터링 구성의 내용을 참조하십시오.

네트워크 모듈을 다른 유형으로 교체

네트워크 모듈을 다른 유형으로 교체하는 경우 재부팅해야 합니다. 새 모듈에 이전 모듈보다 인터페이스가 더 적은 경우 더 이상 존재하지 않을 인터페이스와 관련된 모든 구성을 수동으로 제거해야 합니다.

클러스터링 또는 고가용성의 경우 제어 노드/액티브 유닛에서만 섀시 작업을 수행할 수 있습니다.

시작하기 전에

고가용성의 경우 페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다. 고가용성을 해제해야 합니다(고가용성 쌍 분리 참조). 즉, 액티브 유닛을 재부팅하면 다운타임이 발생합니다. 유닛 리부팅이 완료되면 고가용성을 재구성할 수 있습니다.

프로시저

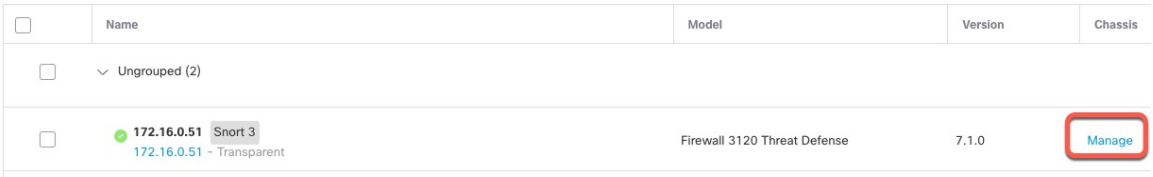
단계 **1** 클러스터링 또는 고가용성의 경우 다음 단계를 수행합니다.

- 클러스터링 — 다운타임을 방지하기 위해 네트워크 모듈 교체를 수행하는 동안 각 노드를 클러스터에 더 이상 포함하지 않도록 한 번에 하나씩 분리할 수 있습니다. 노드 분리의 내용을 참조하십시오.

  교체를 수행한 후 클러스터에 노드를 다시 추가합니다.
- 고가용성 — 네트워크 모듈을 교체할 때 페일오버를 방지하려면 네트워크 모듈에서 인터페이스에 대한 인터페이스 모니터링을 비활성화합니다. 스탠바이 IP 주소 및 인터페이스 모니터링 구성의 내용을 참조하십시오.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성(HA)의 경우 이 옵션은 노드/액티브 장치에 대해서만 사용할 수 있습니다. 네트워크 모듈 변경 사항은 모든 노드에 복제됩니다.

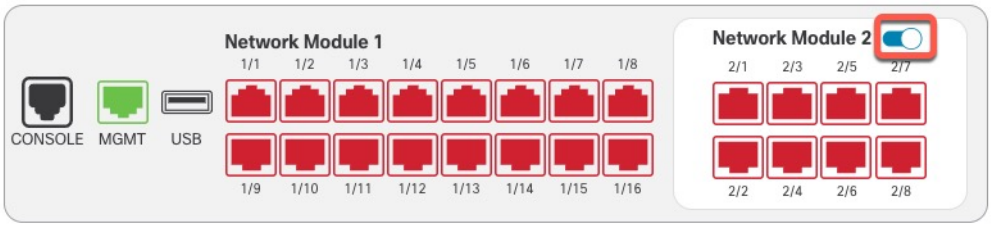
그림 *21:* 섀시 관리



디바이스의 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다. 이 페이지에는 에 대한 물리적 인터페이스 세부 정보가 표시됩니다.

단계 **3** 인터페이스 그래픽에서 슬라이더 ( )를 클릭하여 네트워크 모듈을 비활성화합니다.

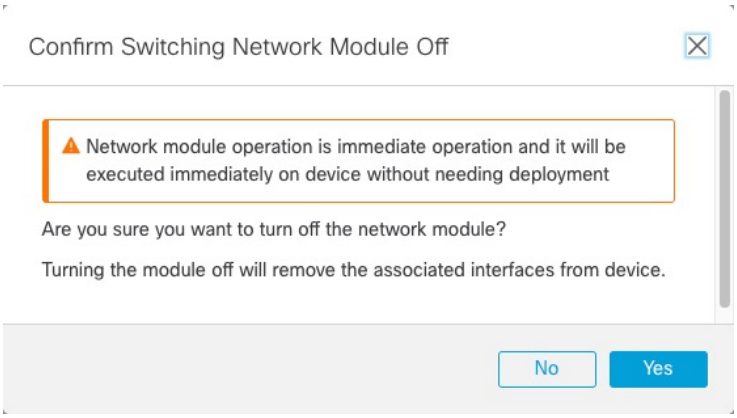
그림 *22:* 네트워크 모듈 비활성화



Interfaces(인터페이스**)** 페이지에서 변경 사항을 저장하지 마십시오. 네트워크 모듈을 교체하는 중이므로 기존 구성을 중단하지 않으려고 합니다.

단계 **4** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *23:* 사용 안 함 확인



단계 **5** 디바이스에서 하드웨어 설치 가이드에 따라 기존 네트워크 모듈을 제거하고 새 네트워크 모듈로 교체합니다.

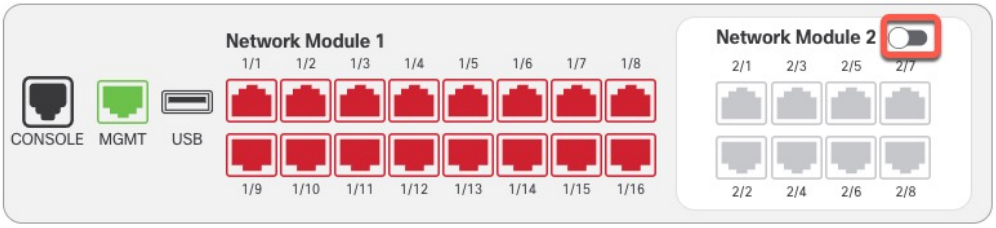
단계 **6** 방화벽을 재부팅합니다. 디바이스 종료 또는 재시작의 내용을 참조하십시오.

클러스터링 또는 고가용성의 경우 먼저 데이터 노드/스탠바이 유닛을 재부팅하고 다시 작동할 때까지 기다립니다. 그런 다음 제어 노드(제어 노드 변경 참조) 또는 액티브 유닛(Threat Defense 고가용성 쌍에서 활성 피어 전환 참조)을 변경하고 이전 제어 노드/액티브 유닛을 재부팅할 수 있습니다.

단계 **7** management center에서 **Sync Modules(**모듈 동기화**)**를 클릭하여 페이지를 새 네트워크 모듈 상세정보로 업데이트합니다.

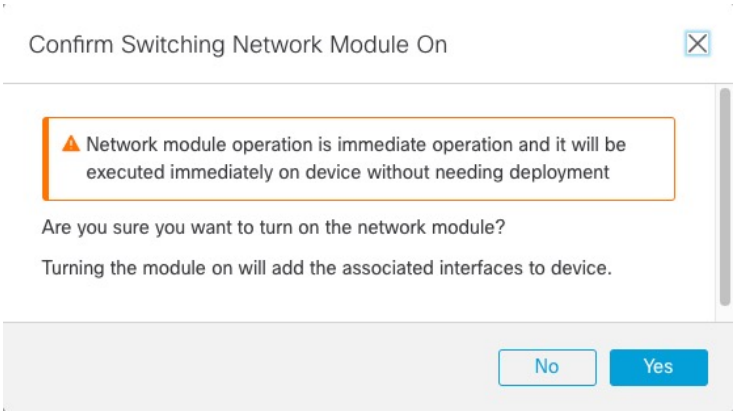
단계 **8** 슬라이더 ( )를 클릭하여 새 모듈을 활성화합니다.

그림 ***24:*** 네트워크 모듈 활성화



단계 **9** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***25:*** 사용 확인



단계 **10** 화면 상단의 메시지 링크를 클릭하여 **Interfaces(**인터페이스**)** 페이지로 이동하여 인터페이스 변경 사항을 저장합니다.

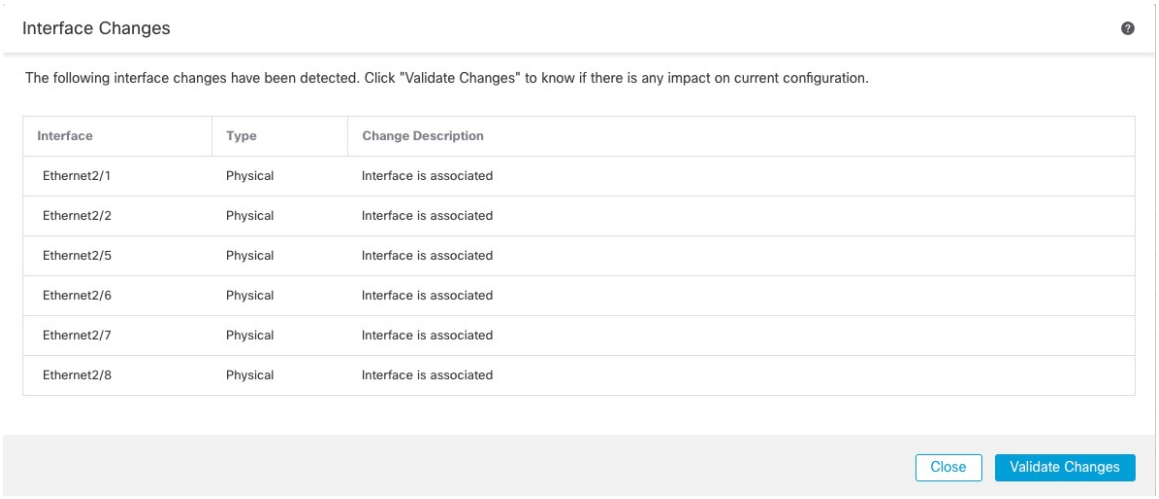
그림 ***26: Interface(***인터페이스***)*** 페이지로 이동

단계 **11** 네트워크 모듈의 인터페이스 수가 더 적은 경우:

a) **Interfaces(**인터페이스**)** 페이지 상단에서 **Click to know more(**자세한 내용을 보려면 클릭**)**를 클릭합니다. **Interface Changes(**인터페이스 변경 사항**)** 대화 상자가 열립니다.

그림 ***27:*** 인터페이스 변경 사항 보기

그림 *28:* 인터페이스 변경 사항



b) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칠 수 있습니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다.

c) **Interfaces(**인터페이스**)** 페이지로 돌아가려면 **Close(**닫기**)**를 클릭합니다.

단계 **12** 인터페이스 속도를 변경하려면 물리적 인터페이스 활성화 및 이더넷 설정 구성, 7 페이지의 내용을 참조하십시오.

기본 속도는 설치된 SFP에서 올바른 속도를 탐지하는 Detect SFP(SFP 탐지)로 설정됩니다. 수동으로 속도를 특정 값으로 설정하고 이제 새 속도가 필요한 경우에만 속도를 수정해야 합니다.

단계 **13** **Save(**저장**)**를 클릭하여 인터페이스 변경 사항을 방화벽에 저장합니다.

단계 **14** 구성을 변경해야 하는 경우 구축 > 구축으로 이동하여 정책을 구축합니다.

네트워크 모듈 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **15** 클러스터링 또는 고가용성의 경우 다음 단계를 수행합니다.

- 클러스터링 - 클러스터에 노드를 다시 추가합니다. 새 클러스터 노드 추가의 내용을 참조하십시오.
- 고가용성 — 네트워크 모듈의 인터페이스에 대한 인터페이스 모니터링을 다시 활성화합니다. 스탠바이 IP 주소 및 인터페이스 모니터링 구성의 내용을 참조하십시오.

네트워크 모듈 분리

네트워크 모듈을 영구적으로 제거하려면 다음 단계를 수행합니다. 네트워크 모듈을 제거하려면 재부팅해야 합니다.

클러스터링 또는 고가용성의 경우 제어 노드/액티브 유닛에서만 섀시 작업을 수행할 수 있습니다.

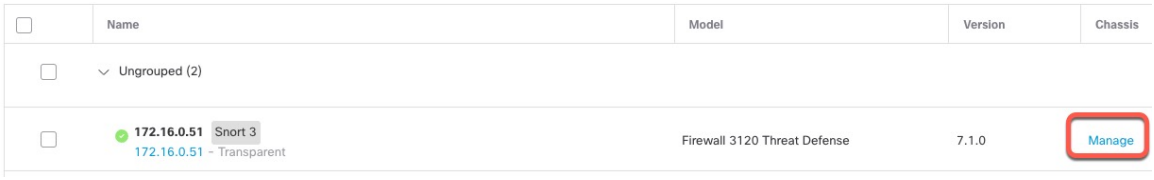
시작하기 전에

클러스터링 또는 고가용성의 경우 클러스터/페일오버 링크가 네트워크 모듈에 있지 않은지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 **Chassis(**섀시**)** 열의 **Manage(**관리**)**를 클릭합니다. 클러스터링 또는 고가용성(HA)의 경우 이 옵션은 노드/액티브 장치에 대해서만 사용할 수 있습니다. 네트워크 모듈 변경 사항은 모든 노드에 복제됩니다.

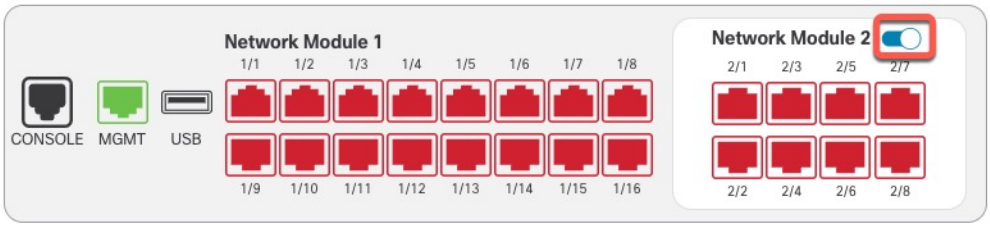
그림 ***29:*** 섀시 관리



디바이스의 **Chassis Operations(**섀시 작업**)** 페이지가 열립니다. 이 페이지에는 에 대한 물리적 인터페이스 세부 정보가 표시됩니다.

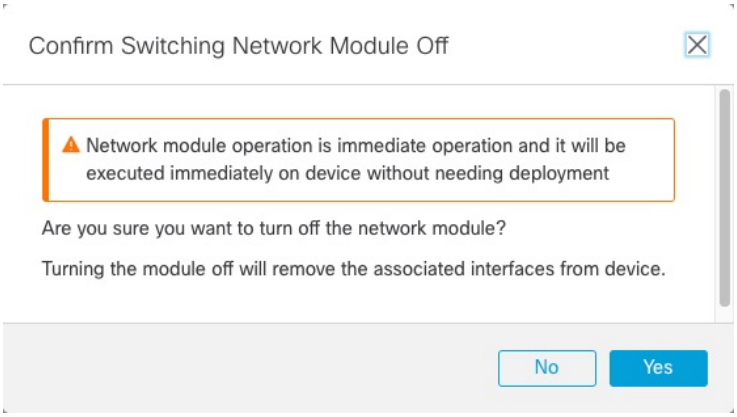
단계 **2** 인터페이스 그래픽에서 슬라이더 ( )를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 ***30:*** 네트워크 모듈 비활성화



단계 **3** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***31:*** 사용 안 함 확인

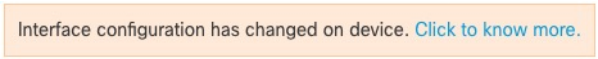


단계 **4** 화면 상단에 메시지가 표시됩니다. 링크를 클릭하여 **Interfaces(**인터페이스**)** 페이지로 이동하여 인터페이스 변경 사항을 저장합니다.

그림 ***32: Interface(***인터페이스***)*** 페이지로 이동

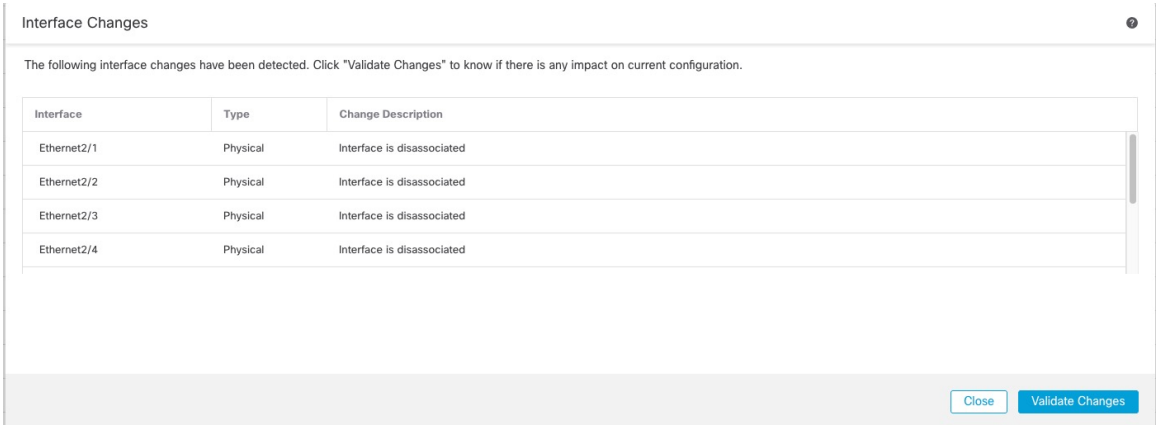
단계 **5** **Interfaces(**인터페이스**)** 페이지 상단에 인터페이스 구성이 변경되었다는 메시지가 표시됩니다.

그림 ***33:*** 인터페이스 변경 사항 보기



a) **Click to know more(**자세히 알아보려면 클릭**)**를 클릭하여 **Interface Changes(**인터페이스 변경 사항**)** 대화 상자를 열어 변경 사항을 확인합니다.

그림 ***34:*** 인터페이스 변경 사항



b) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칠 수 있습니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다.

c) **Interfaces(**인터페이스**)** 페이지로 돌아가려면 **Close(**닫기**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭하여 인터페이스 변경 사항을 방화벽에 저장합니다.

단계 **7** 구성을 변경해야 하는 경우 구축 > 구축으로 이동하여 정책을 구축합니다.

단계 **8** 방화벽을 재부팅합니다. 디바이스 종료 또는 재시작의 내용을 참조하십시오.

클러스터링 또는 고가용성의 경우 먼저 데이터 노드/스탠바이 유닛을 재부팅하고 다시 작동할 때까지 기다립니다. 그런 다음 제어 노드(제어 노드 변경 참조) 또는 액티브 유닛(Threat Defense 고가용성 쌍에서 활성 피어 전환 참조)을 변경하고 이전 제어 노드/액티브 유닛을 재부팅할 수 있습니다.

인터페이스 내역

기능	버전	세부정보
Secure Firewall 3100 고정 포트의 기본 FEC(전달 오류 수정)가 25GB+ SR, CSR 및 LR 트렌시버에 대해 조항 74 FC-FEC에서 조항 108 RS-FEC로 변경됨	7.3	Secure Firewall 3100 고정 포트에서 FEC를 Auto(자동)로 설정하면 이제 기본 유형이 25GB+ SR, CSR 및 LR 트렌시버에 대해 조항 74 FC-FEC 대신 조항 108 RS-FEC로 설정됩니다. 지원되는 플랫폼: Secure Firewall 3100
Firepower 2100, Secure Firewall 3100에 대한 LLDP 지원	7.2	Firepower 2100 및 Secure Firewall 3100 인터페이스에 대해 LLDP(Link Layer Discovery Protocol)를 활성화할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Hardware Configuration(**하드웨어 구성**)** > **Network Connectivity(**네트워크 연결**)** 신규/수정된 명령: **show lldp status, show lldp neighbors, show lldp statistics** 지원되는 플랫폼: Firepower 2100, Secure Firewall 3100
Secure Firewall 3100의 플로우 제어를 위한 프레임 일시 중지	7.2	트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Hardware Configuration(**하드웨어 구성**)** > **Network Connectivity(**네트워크 연결**)** 지원되는 플랫폼: Secure Firewall 3100

기능	버전	세부정보
Secure Firewall 3100에 대한 전달 오류 수정 지원	7.1	Secure Firewall 3100 25Gbps 인터페이스는 FEC(전달 오류 수정)를 지원합니다. FEC는 기본적으로 활성화되어 있으며 Auto(자동)로 설정되어 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** > **Hardware Configuration(**하드웨어 구성**)**
Secure Firewall 3100에 대한 SFP 기반 속도 설정 지원	7.1	Secure Firewall 3100은 설치된 SFP를 기반으로 인터페이스에 대한 속도 탐지를 지원합니다. Detect SFP(SFP 탐지)는 기본적으로 활성화되어 있습니다. 이 옵션은 나중에 네트워크 모듈을 다른 모델로 변경하고 속도를 자동으로 업데이트하려는 경우에 유용합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** > **Hardware Configuration(**하드웨어 구성**)**
Firepower 1100에 대한 LLDP 지원	7.1	Firepower 1100 인터페이스에 대해 LLDP(Link Layer Discovery Protocol)를 활성화할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Hardware Configuration(**하드웨어 구성**)** > **LLDP** 신규/수정된 명령: **show lldp status, show lldp neighbors, show lldp statistics** 지원되는 플랫폼: Firepower 1100
이제 인터페이스 자동 협상이 속도 및 양방향과 독립적으로 설정되며 인터페이스 동기화가 개선됨	7.1	이제 인터페이스 자동 협상이 속도 및 양방향과 독립적으로 설정됩니다. 또한 management center에서 인터페이스를 동기화하면 하드웨어 변경 사항이 더 효과적으로 탐지됩니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Hardware Configuration(**하드웨어 구성**)** > **Speed(**속도**)** 지원되는 플랫폼: Firepower 1000, 2100, Secure Firewall 3100
Firepower 1100/2100 Series 파이버 인터페이스에서 이제 자동 협상 비활성화 지원	6.7	이제 Flower 1100/2100 Series 파이버 인터페이스를 구성하여 플로우 제어 및 링크 상태 협상을 비활성화할 수 있습니다. 이전에는 이러한 디바이스에서 파이버 인터페이스 속도(1000 또는 10000Mbps)를 설정하면 플로우 제어 및 링크 상태 협상이 자동으로 활성화되었습니다. 이를 비활성화할 수 없습니다. 이제 **Auto-negotiation(**자동 협상**)**을 선택 취소하고 속도를 1000으로 설정하여 플로우 제어 및 링크 상태 협상을 비활성화할 수 있습니다. 10000Mbps에서는 협상을 비활성화할 수 없습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Hardware Configuration(**하드웨어 구성**)** > **Speed(**속도**)** 지원되는 플랫폼: Firepower 1100, 2100