Secure Firewall 3100에서 멀티 인스턴스 모드 사용

초판: 2023년 12월 13일

최종 변경: 2024년 7월 17일

Secure Firewall 3100에 대한 멀티 인스턴스 모드 사용

Secure Firewall 3100을 단일 디바이스(어플라이언스 모드) 또는 여러 컨테이너 인스턴스(멀티 인스턴스 모드)로 구축할 수 있습니다. 이 장에서는 멀티 인스턴스 모드에서 디바이스를 구축하는 방법을 설명합니다.

참고 이 문서에서는 최신 버전의 기능에 대해 설명합니다. 기능 변경에 대한 자세한 내용은 멀티 인스턴스 모드 기록, 68 페이지를 참조하십시오. 이전 버전이 설치되어 있는 경우 사용자 버전에 맞는 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 절차를 참조하십시오.

멀티 인스턴스 모드 정보

멀티 인스턴스 모드에서는 완전히 독립적인 디바이스 역할을 하는 단일 섀시에 여러 컨테이너 인스턴스를 구축할 수 있습니다.

멀티 인스턴스 모드와 어플라이언스 모드 비교

멀티 인스턴스 모드 또는 어플라이언스 모드에서 디바이스를 실행할 수 있습니다.

어플라이언스 모드

어플라이언스 모드가 기본값입니다. 디바이스는 네이티브 threat defense 이미지를 실행하며 단일 디바이스로 작동합니다. 섀시 관리자 페이지에서 사용 가능한 유일한 섀시 레벨 컨피그레이션은 네트워크 모듈 관리(브레이크 아웃 포트 또는 네트워크 모듈 활성화/비활성화)를 위한 것입니다.

멀티 인스턴스 모드

멀티 인스턴스 모드로 변경할 경우 디바이스는 섀시에서 Secure Firewall eXtensible Operating System (FXOS)를 실행하는 반면, 각 인스턴스는 별도의 threat defense 이미지를 실행합니다. FXOS CLI를 사용하여 모드를 구성할 수 있습니다.

여러 인스턴스가 동일한 섀시에서 실행되므로 다음 항목에 대해 섀시 레벨의 관리를 수행해야 합니다.

- 리소스 프로파일을 사용하는 CPU 및 메모리 리소스.
- 인터페이스 설정 및 할당
- 인스턴스의 구축 및 모니터링.

멀티 인스턴스 디바이스의 경우, 섀시를 management center 에 추가하고 섀시 관리자 페이지에서 섀시 레벨 설정을 구성합니다.

섀시 관리 인터페이스

섀시 관리

섀시는 디바이스의 전용 관리 인터페이스를 사용합니다. 멀티 인스턴스 모드는 섀시 관리를 위한 데이터 인터페이스 사용 또는 관리 인터페이스에 대한 DHCP 주소 지정을 지원하지 않습니다.

threat defense CLI(초기 설정 시) 또는 (멀티 인스턴스 모드로 변환한 후) FXOS CLI에서만 섀시 관리 인터페이스를 구성할 수 있습니다. 초기 설정은 멀티 인스턴스 모드 활성화, 19 페이지을 참조하십시오. 멀티 인스턴스 모드에서 관리 인터페이스 설정을 변경하려면 FXOS CLI에서 섀시 관리 설정 변경, 62 페이지 을(를) 참조하십시오.

참고 기본적으로 SSH 서버 및 SSH 액세스 목록을 활성화하지 않는 한 멀티 인스턴스 모드에서 이 인터페이스에 대한 SSH가 허용되지 않습니다. 이러한 차이로 인해 SSH를 사용하여 애플리케이션 모드 Threat Defense Management 인터페이스에 연결할 수 있지만 멀티 인스턴스 모드로 변환한 후에는 기본적으로 SSH를 사용하여 더 이상 연결할 수 없습니다. SSH 및 SSH 액세스 목록 구성, 48 페이지의 내용을 참조하십시오.

인스턴스 관리

모든 인스턴스는 섀시 관리 인터페이스를 공유하며 각 인스턴스는 관리 네트워크에서 고유한 IP 주소를 갖습니다. 인스턴스를 추가하고 IP 주소를 지정한 후에는 threat defense CLI에서 네트워크 설정을 변경할 수 있습니다.

인스턴스 관리 IP 주소는 기본적으로 SSH를 허용합니다.

인스턴스 인터페이스

인스턴스에 대해 물리적 인터페이스를 유연하게 사용할 수 있도록 섀시에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스(VLAN 또는 물리적)를 공유할 수 있습니다. 공유 인터페이스 확장성, 5 페이지 및 하위 인터페이스 구성, 32 페이지를 참조하십시오.

참고 이 장에서는 섀시 VLAN 하위 인터페이스에 대해서만 설명합니다. threat defense 인스턴스 내에서 별도로 하위 인터페이스를 만들 수 있습니다. 자세한 내용은 섀시 인터페이스와 인스턴스 인터페이스 비교, 3 페이지를 참조하십시오.

인터페이스 유형

물리적 인터페이스, VLAN 하위 인터페이스 및 EtherChannel 인터페이스는 다음 유형 중 하나가 될 수 있습니다.

- 데이터 - 일반 데이터 또는 장애 조치 링크에 사용합니다. 데이터 인터페이스는 인스턴스 간에 공유할 수 없으며, 인스턴스는 백플레인을 통해 다른 인스턴스와 통신할 수 없습니다. 데이터 인터페이스 트래픽의 경우, 모든 트래픽은 하나의 인터페이스에서 섀시를 종료하고 다른 인터페이스로 돌아가서 다른 인스턴스에 연결해야 합니다. 데이터 인터페이스에 VLAN 하위 인터페이스를 추가하여 고가용성 쌍별로 별도의 장애 조치 링크를 제공할 수 있습니다.
- Data-sharing(데이터 공유) - 일반 데이터에 사용합니다. 이러한 데이터 인터페이스는 하나 이상의 인스턴스에서 공유할 수 있습니다. 각 인스턴스는 이 인터페이스를 공유하는 다른 모든 인스턴스와 백플레인을 통해 통신할 수 있습니다. 공유 인터페이스는 구축할 수 있는 인스턴스 수에 영향을 줄 수 있습니다. 브리지 그룹 멤버 인터페이스(투명 모드 또는 라우팅 모드), 인라인 집합, 패시브 인터페이스, 또는 페일오버 링크에 대해서는 공유 인터페이스가 지원되지 않습니다.

섀시 인터페이스와 인스턴스 인터페이스 비교

섀시 수준에서 물리적 인터페이스, 인스턴스의 VLAN 하위 인터페이스 및 EtherChannel 인터페이스의 기본 이더넷 설정을 관리합니다. 인스턴스 내에서는 상위 레벨 설정을 구성합니다. 예를 들어, 섀시에서는 EtherChannel만 생성할 수 있습니다. 그러나 인스턴스 내의 EtherChannel에 IP 주소를 할당할 수 있습니다.

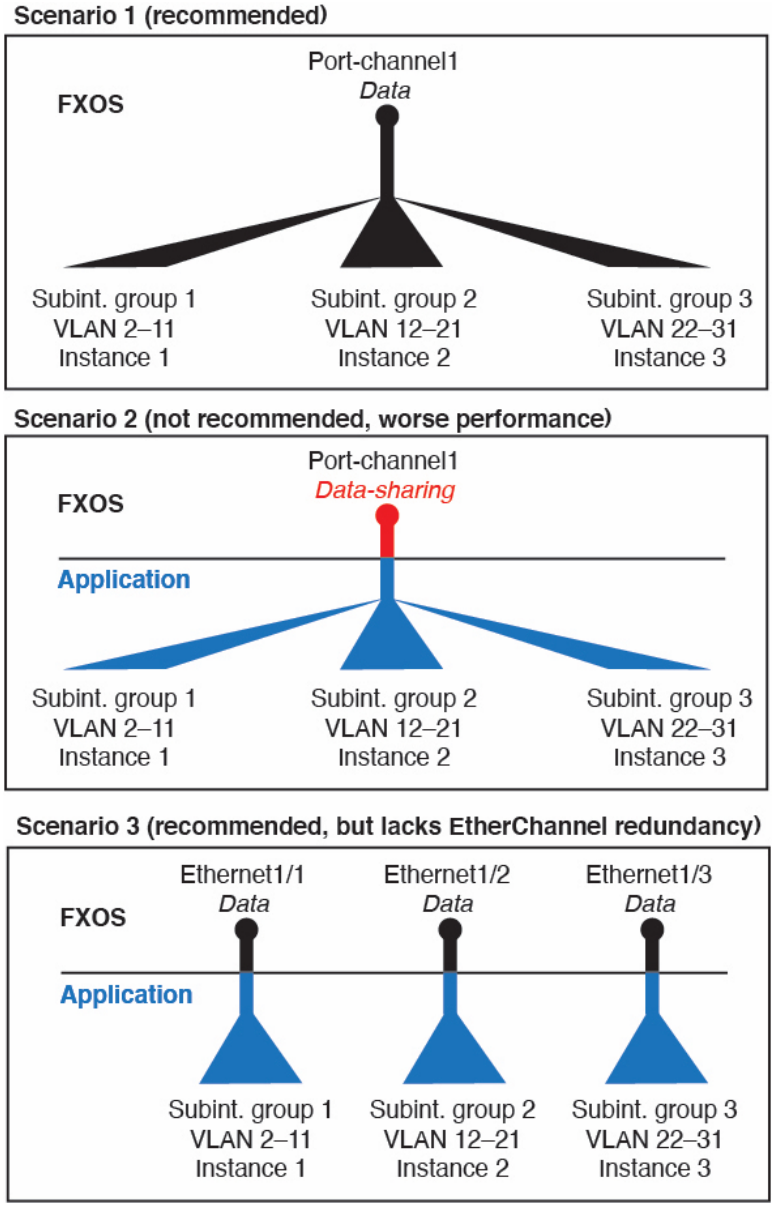
다음 섹션에서는 섀시와 인터페이스에 대한 인스턴스 간의 상호 작용에 대해 설명합니다.

VLAN 하위 인터페이스

다른 디바이스와 마찬가지로 인스턴스 내에서 VLAN 하위 인터페이스를 생성할 수 있습니다.

섀시에서 VLAN 하위 인터페이스를 생성할 수도 있습니다. 인스턴스 정의 하위 인터페이스는 섀시 제한에 영향을 받지 않습니다. 네트워크 구축 및 개인 환경 설정에 따라 하위 인터페이스를 생성할 위치를 선택합니다. 예를 들어, 하위 인터페이스를 공유하려면 섀시에서 하위 인터페이스를 생성해야 합니다. 섀시 하위 인터페이스를 이용하는 또 다른 시나리오는 단일 인터페이스에서 별도의 하위 인터페이스 그룹을 여러 인스턴스에 할당하는 것입니다. 인스턴스 A에는 VLAN 2~11이, 인스턴스 B에는 VLAN 12~21, 인스턴스 C에는 VLAN 22~31이 있는 Port-channel1을 사용하려는 경우를 예로 들어 보겠습니다. 인스턴스 내에서 이러한 하위 인터페이스를 생성하는 경우에는 섀시에서 상위 인터페이스를 공유해야 하는데, 이러한 방식은 효율적이지 않을 수 있습니다. 다음 그림에서 이 시나리오를 수행할 수 있는 세 가지 방법을 참조하십시오.

그림 *1:* 섀시 및 인스턴스의 ***VLAN*** 비교



섀시와 인스턴스의 독립 인터페이스 상태

관리를 위해 섀시와 인스턴스에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 위치에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로, 섀시와 인스턴스를 일치시키지 않을 수 있습니다.

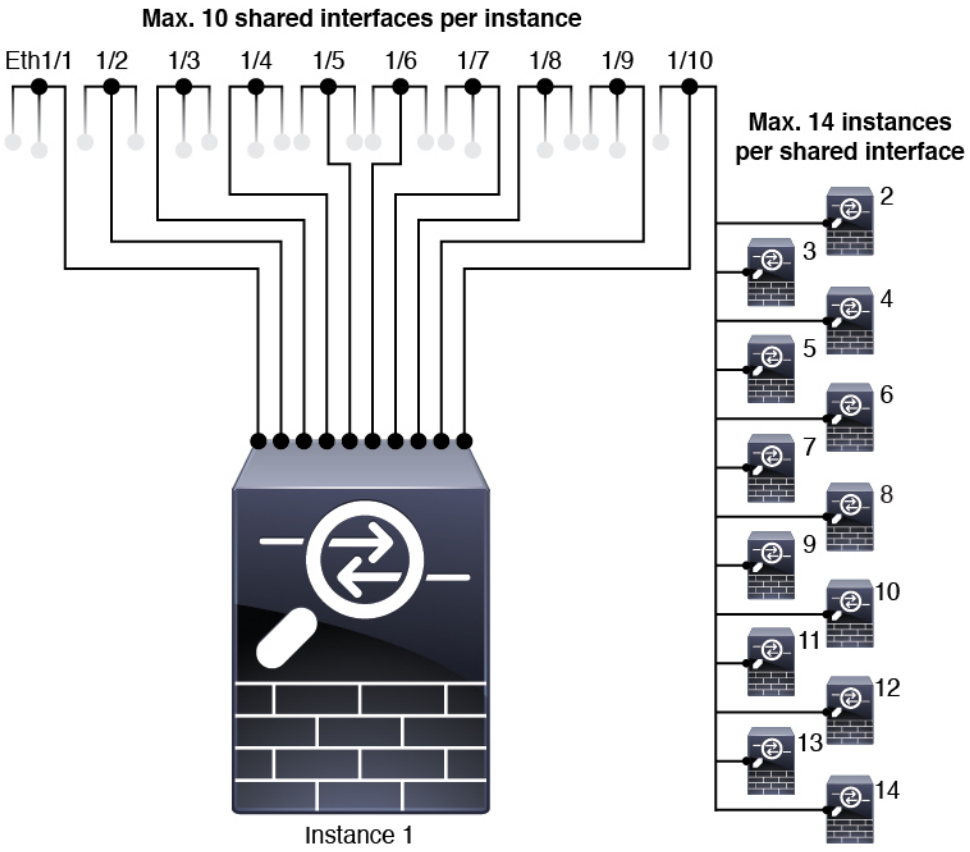
인스턴스 내의 인터페이스 기본 상태는 인터페이스 유형에 따라 달라집니다. 예를 들어, 물리적 인터페이스 또는 EtherChannel은 인스턴스 내에서 기본적으로 비활성화되지만 하위 인터페이스는 기본적으로 활성화됩니다.

공유 인터페이스 확장성

인스턴스는 데이터 공유 유형 인터페이스를 공유할 수 있습니다. 이 기능을 통해 물리적 인터페이스 사용량을 절약하면서 유연한 네트워킹 구축도 지원할 수 있습니다. 인터페이스를 공유할 때 섀시는 고유한 MAC 주소를 사용하여 올바른 인스턴스로 트래픽을 포워딩합니다. 그러나 공유 인터페이스로 인해 섀시 내에 전체 메시 토폴로지가 필요해져서 포워딩 테이블이 커질 수 있습니다. 모든 인스턴스가 동일한 인터페이스를 공유하는 다른 모든 인스턴스와 통신할 수 있어야 하기 때문입니다. 따라서 공유할 수 있는 인터페이스 수에는 제한이 있습니다.

섀시는 포워딩 테이블 외에 VLAN 하위 인터페이스 포워딩용 VLAN 그룹 테이블도 유지합니다.최대 500개의 VLAN 하위 인터페이스를 생성할 수 있습니다.

공유 인터페이스 할당과 관련한 다음 제한을 참조하십시오.



공유 인터페이스 모범 사례

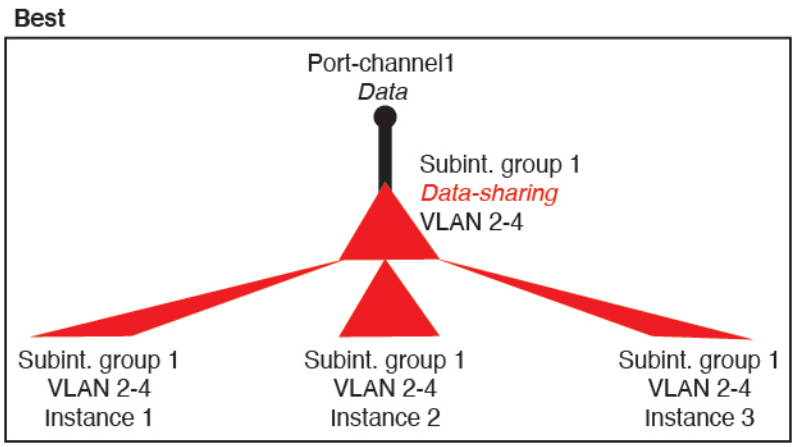
포워딩 테이블의 최적의 확장성을 위해 최대한 적은 수의 인터페이스를 공유합니다. 대신, 하나 이상의 물리적 인터페이스에서 최대 500개의 VLAN 하위 인터페이스를 생성하고 컨테이너 인스턴스 사이에 VLAN을 나눌 수 있습니다.

인터페이스 공유 시에는 다음 사례를 확장성이 높은 방식부터 차례로 따르십시오.

1. 최고 - 단일 상위 인터페이스에 속한 하위 인터페이스를 공유하고 동일한 인스턴스 그룹과 동일한 하위 인터페이스 집합을 사용합니다.

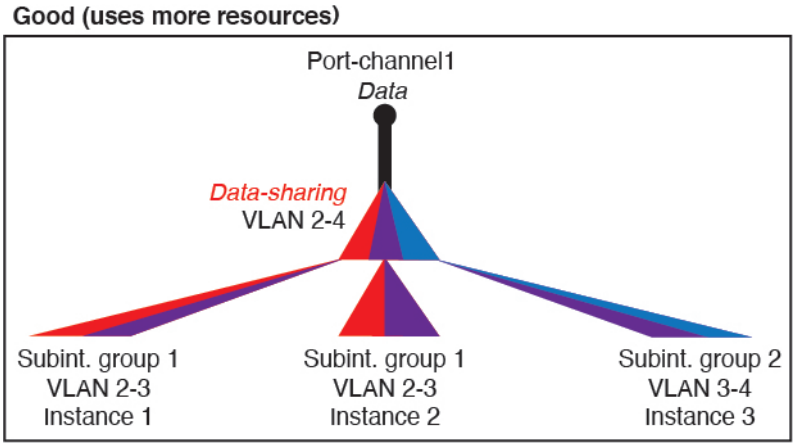
예를 들어 대규모 EtherChannel 하나를 생성해 유사한 종류의 모든 인터페이스를 함께 번들로 묶은 다음 해당 EtherChannel의 하위 인터페이스를 공유합니다. 즉, Port-Channel2, Port-Channel3 및 Port-Channel4를 공유하는 대신 Port-Channel1.2, 3 및 4를 공유합니다. 단일 상위 인터페이스의 하위 인터페이스를 공유하면 상위 인터페이스 전체에서 하위 인터페이스를 공유하거나 물리적/EtherChannel 인터페이스를 공유할 때 VLAN 그룹 테이블이 전달 테이블보다 더 잘 확장됩니다.

그림 ***2:*** 최고 **:** 하나의 상위에 있는 공유 하위 인터페이스 그룹



인스턴스의 그룹과 동일한 하위 인터페이스 집합을 공유하지 않는 경우 구성으로 인해 더 많은 리소스 사용량(더 많은 VLAN 그룹)이 발생할 수 있습니다. Port-Channel1.3 및 4를 인스턴스 3(2개의 VLAN 그룹)과 공유하는 동안 Port-Channel1.2 및 3을 인스턴스 1 및 2와 공유하는 대신 Port-Channel1.2, 3 및 4를 인스턴스 1, 2 및 3(1개의 VLAN 그룹)과 공유하는 경우를 예로 들 수 있습니다.

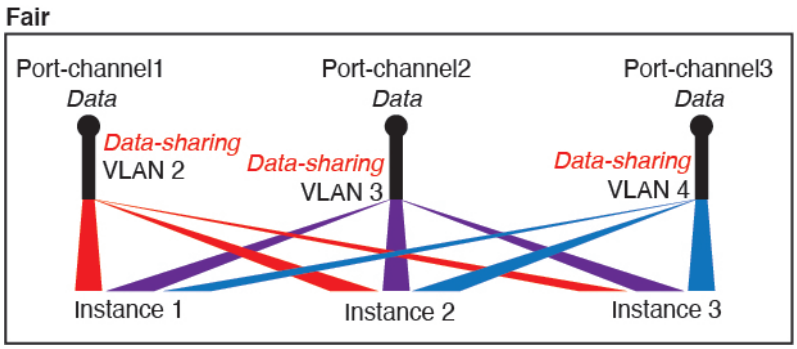
그림 ***3:*** 좋음 **:** 하나의 상위에서 여러 하위 인터페이스 그룹 공유



2. 양호 - 여러 상위 인터페이스 간에 하위 인터페이스를 공유합니다.

   예를 들어 Port-Channel2, Port-Channel4 및 Port-Channel4 대신 Port-Channel1.2, Port-Channel2.3 및 Port-Channel3.4를 공유합니다. 이러한 사용 방법은 동일한 상위 인터페이스에서 하위 인터페이스만 공유하는 것만큼 효율적이지는 않지만 여전히 VLAN 그룹의 장점을 활용합니다.

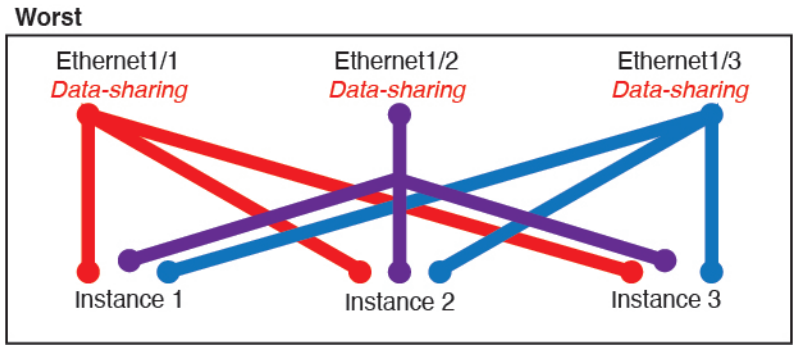
그림 4: 보통 : 개별 상위의 공유 하위 인터페이스



3. 최악 - 개별 상위 인터페이스(물리적 또는 EtherChannel)를 공유합니다.

   이 방법에서는 대부분의 전달 테이블 항목을 사용합니다.

   그림 5: 최악 : 공유 상위 인터페이스



새시가 패킷을 분류하는 방법

새시에 들어오는 각 패킷은 분류되어야 합니다. 그러면 새시에서 어떤 인스턴스에 패킷을 보낼지 판단할 수 있습니다.

- 고유 인터페이스 - 단 하나의 인스턴스가 인그레스 인터페이스와 연결된 경우 새시는 해당 패킷을 해당 인스턴스로 분류합니다. 투명 모드 또는 라우티드 모드의 브리지 그룹 멤버 인터페이스, 인라인 집합 또는 패시브 인터페이스의 경우에는 항상 이 방법을 사용하여 패킷을 분류합니다.
- 고유 MAC 주소 - 새시가 공유 인터페이스를 포함한 모든 인터페이스에 대해 고유한 MAC 주소를 자동으로 생성합니다. 여러 인스턴스가 인터페이스 하나를 공유하는 경우 분류자는 각 인스턴스의 인터페이스에 할당된 고유 MAC 주소를 사용합니다. 업스트림 라우터는 고유 MAC 주소가 없으면 인스턴스로 직접 라우팅할 수 없습니다. 또한 애플리케이션 내에서 각 인터페이스를 구성할 때 수동으로 MAC 주소를 설정할 수도 있습니다.

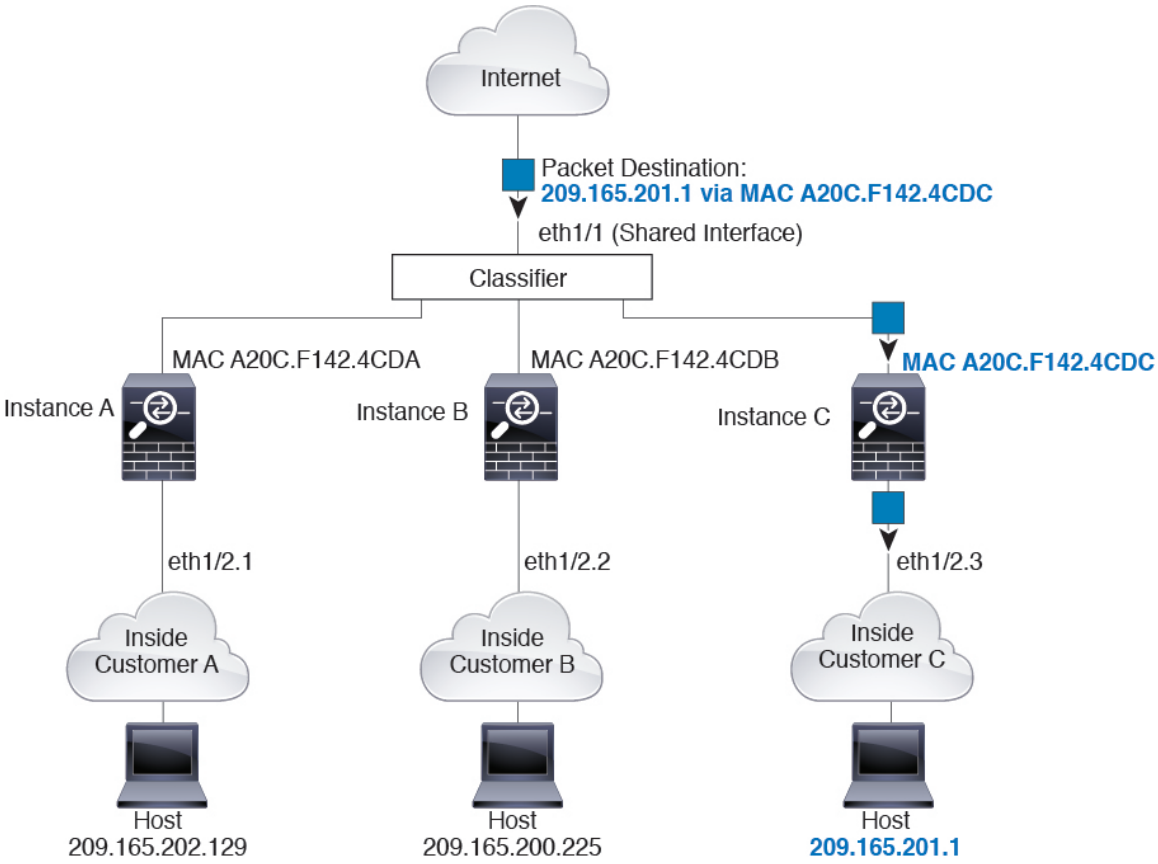
참고 대상 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 인스턴스에 배포됩니다.

분류의 예

MAC 주소를 사용하는 공유 인터페이스를 통한 패킷 분류

다음 그림은 외부 인터페이스를 공유하는 여러 인스턴스를 보여 줍니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 라우터에서 패킷을 보내는 MAC 주소가 인스턴스 C에 포함되어 있기 때문입니다.

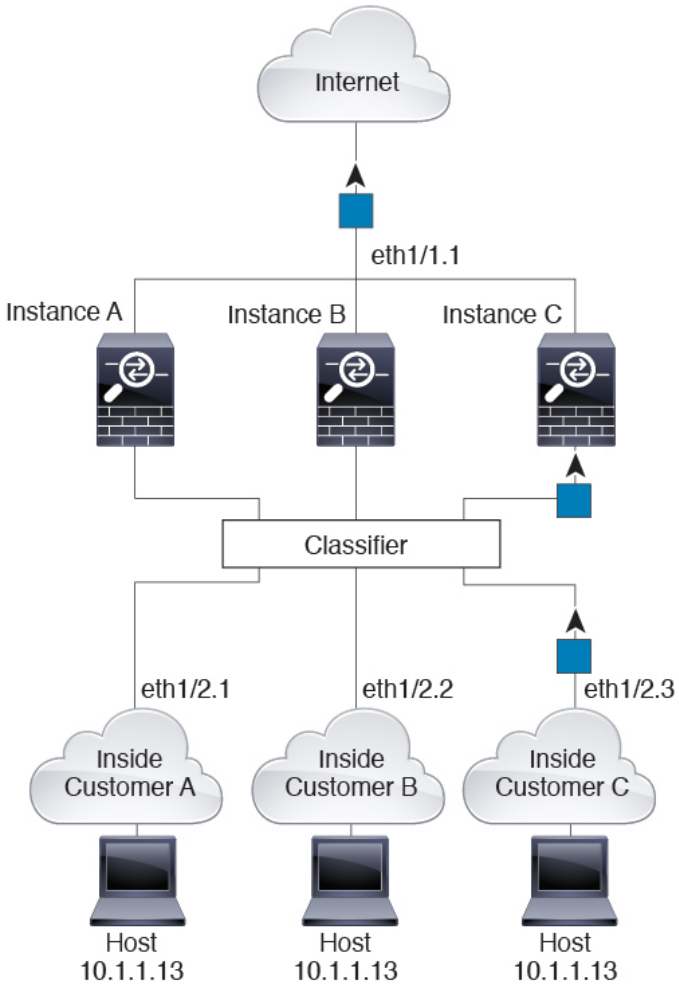
그림 ***6: MAC*** 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



내부 네트워크로부터 수신하는 트래픽

내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 다음 그림에는 인터넷에 액세스하는 네트워크 내의 인스턴스 C에 있는 호스트가 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/2.3이기 때문입니다.

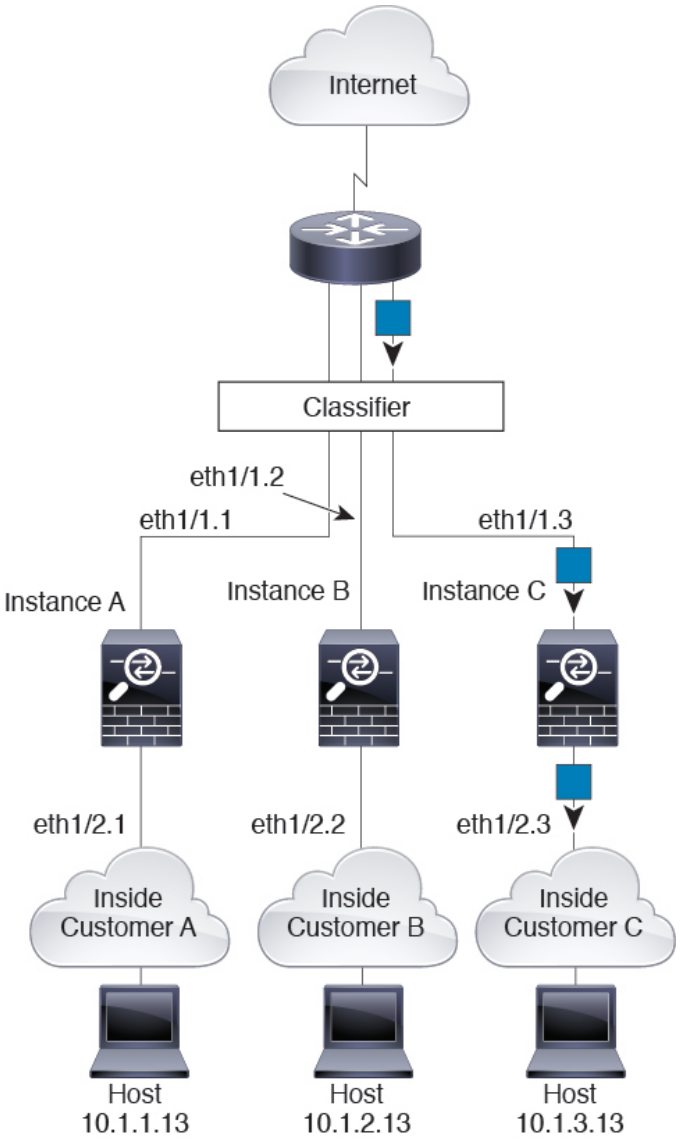
그림 *7:* 내부 네트워크로부터 수신하는 트래픽



투명 방화벽 인스턴스

투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 다음 그림에는 인터넷의 네트워크 내 인스턴스 C에 있는 호스트로 전송되는 패킷이 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/2.3이기 때문입니다.

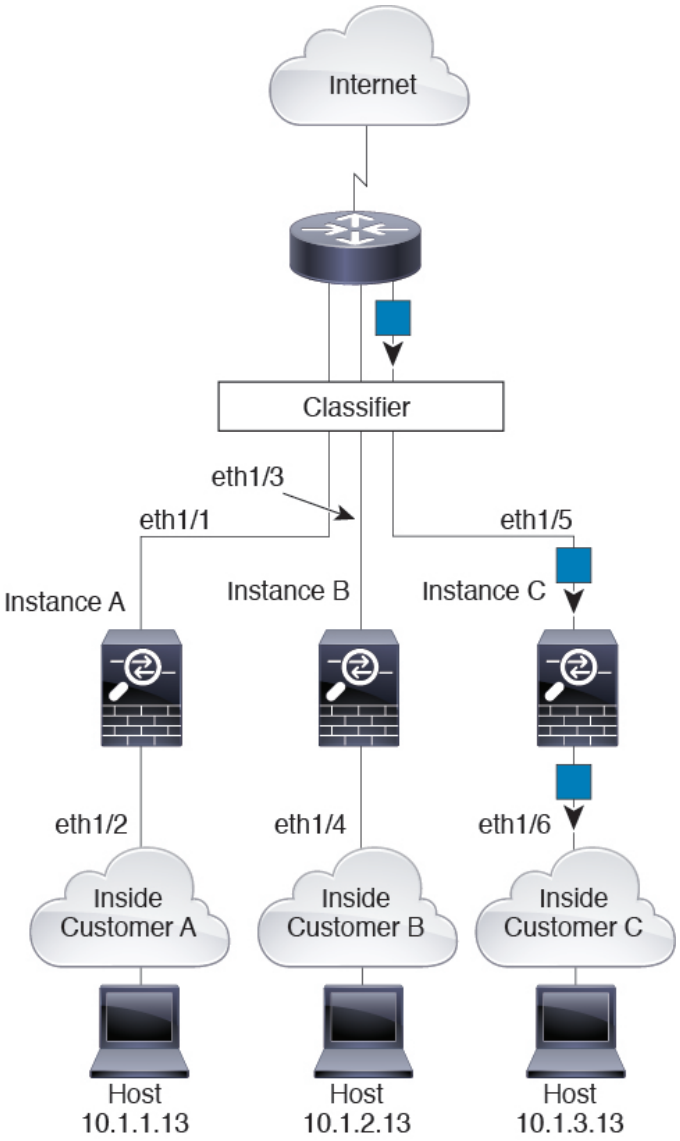
그림 *8:* 투명 방화벽 인스턴스



인라인 세트

인라인 집합의 경우에는 고유 인터페이스를 사용해야 하며, 해당 인터페이스는 물리적 인터페이스 또는 EtherChannel이어야 합니다. 다음 그림에는 인터넷의 네트워크 내 인스턴스 C에 있는 호스트로 전송되는 패킷이 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/5이기 때문입니다.

그림 *9:* 인라인 세트

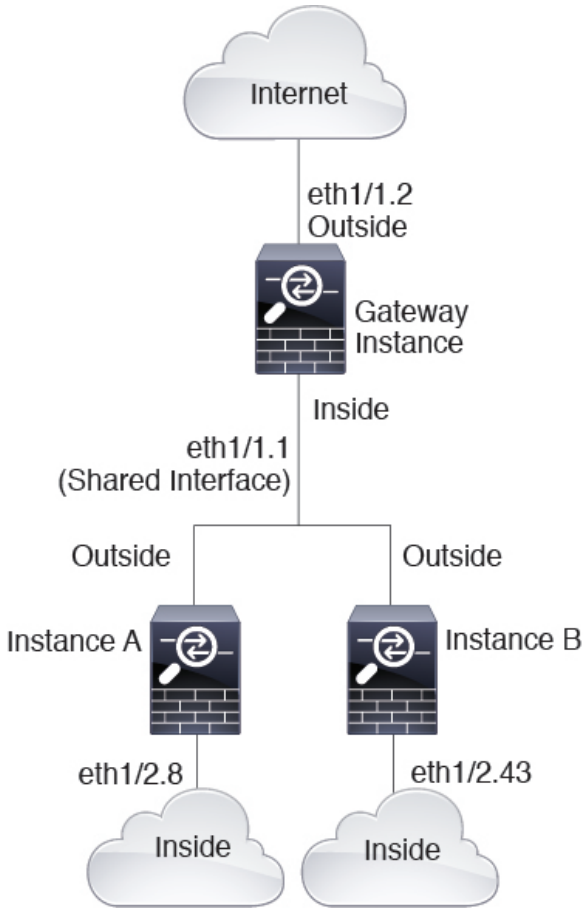


연속 인스턴스

다른 인스턴스 바로 앞에 인스턴스를 배치하는 것을 연속 컨테이너 인스턴스라고 합니다. 하나의 인스턴스의 외부 인터페이스는 다른 인스턴스의 내부 인터페이스와 동일한 인터페이스입니다. 최상위 인스턴스에서 공유 파라미터를 구성함으로써 일부 인스턴스의 구성을 간소화하고 싶다면 인스턴스 캐스케이딩이 유용할 수 있습니다.

다음 그림에는 게이트웨이 뒤에 인스턴스가 2개 있는 게이트웨이 인스턴스가 나와 있습니다.

그림 *10:* 연속 인스턴스



참고 고가용성에 연속 인스턴스(공유 인터페이스 사용)를 사용하지 마십시오. 페일오버가 수행되고 스탠바이 유닛이 다시 조인한 후에는 MAC 주소가 일시적으로 중복되어 중단이 발생할 수 있습니다. 대신 게이트웨이 인스턴스와 외부 스위치를 사용하는 내부 인스턴스에 고유한 인터페이스를 사용하여 인스턴스 간에 트래픽을 전달해야 합니다.

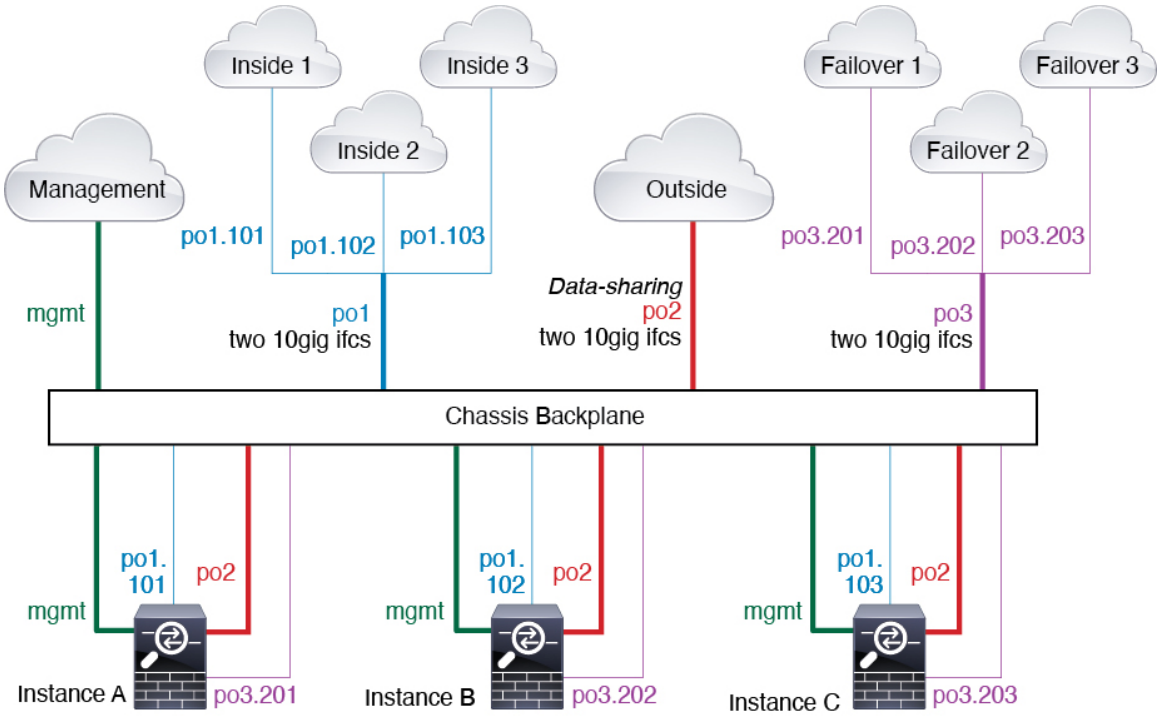
일반적인 멀티 인스턴스 구축

다음 예에는 라우팅된 방화벽 모드의 컨테이너 인스턴스 3개가 포함되어 있습니다. 이러한 컨테이너 인스턴스는 다음 인터페이스를 포함합니다.

- Management(관리) - 모든 인스턴스와 섀시에서 전용 관리 인터페이스를 사용합니다. 각 인스턴스 및 섀시 내에서 인터페이스는 동일한 관리 네트워크의 고유 IP 주소를 사용합니다.
- Inside(내부) - 각 인스턴스가 Port-Channel1(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.

- Outside(외부) - 모든 인스턴스가 Port-Channel2 인터페이스(데이터 공유 유형)를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 애플리케이션 내에서 인터페이스는 동일한 외부 네트워크의 고유 IP 주소를 사용합니다.
- Failover(페일오버) - 각 인스턴스가 Port-Channel3(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.

그림 *11:* 일반적인 멀티 인스턴스 구축



인스턴스 인터페이스용 자동 **MAC** 주소

섀시는 인스턴스 인터페이스용 MAC 주소를 자동으로 생성하며 각 인스턴스의 공유 인터페이스가 고유한 MAC 주소를 사용하도록 보장합니다.

인스턴스 내의 공유 인터페이스에 직접 MAC 주소를 할당하는 경우 직접 할당한 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 삭제할 경우 자동 생성 주소가 사용됩니다. 드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 인스턴스 내에서 인터페이스의 MAC 주소를 직접 설정하는 것이 좋습니다.

자동 생성 주소는 A2로 시작하기 때문에, 주소가 겹칠 위험이 있으므로 수동 MAC 주소를 A2로 시작해서는 안 됩니다.

섀시는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx.yyzz.zzzz*

여기서 *xx.yy*는 사용자 정의 접두사 또는 시스템 정의 접두사이고 *zz.zzzz*는 섀시에서 생성되는 내부 카운터입니다. 시스템 정의 접두사는 IDPROM에 프로그래밍되는 번인된 MAC 주소 풀의 첫 번째 MAC 주소의 하위 2바이트와 일치합니다. MAC 주소 풀을 확인하려면 **connect fxos**, **show module**을 차례로 사용합니다. 예를 들어 모듈 1에 대해 표시되는 MAC 주소 범위가 b0aa.772f.f0b0~b0aa.772f.f0bf이면 시스템 접두사는 f0b0입니다.

사용자 정의 접두사는 16진수로 변환되는 정수입니다. 사용자 정의 접두사가 어떻게 사용되는지 예를 들어 설명하자면, 접두사를 77로 설정하는 경우 섀시에서는 77을 16진수 값 004D(*yyxx*)로 변환합니다. 접두사가 MAC 주소에서 쓰일 때는 섀시 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A2**4D.00***zz.zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

멀티 인스턴스 모드의 성능 확장 요인

플랫폼의 최대 처리량(연결, VPN 세션)은 어플라이언스 모드 디바이스의 메모리 및 CPU 사용에 대해 계산됩니다. 이 값은 **show resource usage**에 표시됩니다. 멀티 인스턴스를 사용하는 경우 처리량은 인스턴스에 할당하는 CPU 코어의 비율을 기준으로 계산해야 합니다. 예를 들어, 코어가 50%인 인스턴스를 사용하는 경우, 처음에는 처리량의 50%를 계산해야 합니다. 또한 인스턴스에서 사용할 수 있는 처리량은 어플라이언스에서 사용할 수 있는 처리량보다 적을 수 있습니다로 줄여야 합니다.

인스턴스의 처리량 계산에 대한 자세한 지침은 https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html의 내용을 참조하십시오.

인스턴스 및 고가용성

2개의 개별 섀시에서 인스턴스를 사용하여 고가용성을 사용할 수 있습니다. 예를 들어, 각각 인스턴스가 10개인 섀시가 2개 있으면 고가용성 쌍 10개를 생성할 수 있습니다. 또한 고가용성 인스턴스와 동일한 섀시에 독립형 인스턴스를 포함할 수 있습니다. 자세한 요구 사항은 인스턴스의 요구 사항 및 사전 요건, 15 페이지의 내용을 참조하십시오.

참고 클러스터링은 지원되지 않습니다.

인스턴스용 라이선스

모든 라이선스는 인스턴스 단위가 아닌 섀시 단위로 사용됩니다. 자세한 내용은 다음을 참조하십시오.

- Essentials 라이선스는 섀시당 하나씩 섀시에 할당됩니다.
- 기능 라이선스는 각 인스턴스에 할당되지만, 섀시당 기능별 하나의 라이선스만 사용합니다.

인스턴스의 요구 사항 및 사전 요건

모델 지원

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140

참고 Secure Firewall 3105는 지원되지 않습니다.

모델당 최대 컨테이너 인스턴스 및 리소스

각 컨테이너 인스턴스에 대해 인스턴스에 할당할 CPU 코어(또는 더 구체적으로 스레드) 수를 지정할 수 있습니다. 다양한 하드웨어 아키텍처를 설명하기 위해 일반적으로 "코어"라는 용어를 사용합니다. 코어 수에 따라 RAM은 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다.

표 *1:* 모델당 최대 컨테이너 인스턴스 및 리소스

모델	최대 컨테이너 인스턴스 수	사용 가능한 **CPU** 코어**(**스레드**)**
Secure Firewall 3110	3	22
Secure Firewall 3120	5	30
Secure Firewall 3130	7	46
Secure Firewall 3140	10	62

소프트웨어 요구 사항

섀시에서 실행 중인 FXOS 버전과 모두 호환되는 한, 각 인스턴스에서 서로 다른 threat defense 소프트웨어 버전을 실행할 수 있습니다.

고가용성 요구 사항

- 고가용성 구성의 두 인스턴스는 다음과 같아야 합니다.
  - 독립된 섀시에 있어야 합니다.
  - 같은 모델이어야 합니다.

- 같은 인터페이스가 할당되어야 합니다. 고가용성을 활성화하기 전에 모든 인터페이스가 FXOS와 동일하게 사전 설정되어야 합니다.
- 동일한 리소스 프로파일 속성을 사용해야 합니다. 프로파일 이름은 다를 수 있지만 정의는 일치해야 합니다.

Management Center 필수조건

라이선싱 구현으로 인해 섀시 관리 및 섀시의 모든 인스턴스에 동일한 management center를 사용해야 합니다.

인스턴스 지침 및 제한 사항

일반 지침

- 단일 management center 는 섀시의 모든 인스턴스와 섀시 자체를 관리해야 합니다.
- 인스턴스의 경우에는 다음 기능이 지원되지 않습니다.
  - TLS 암호화 가속
  - 클러스터링
  - Management Center UCAPL/CC 모드
  - 하드웨어로의 플로우 오프로드
- CDO 클라우드 제공 management center 에 의한 섀시의 기본 관리 및 온프레미스 management center 에 의한 섀시의 별도 분석 전용 관리는 지원되지 않습니다. 그러나 CDO 관리 인스턴스를 분석 전용 온프레미스 management center에 추가할 수 있습니다.

관리 인터페이스

- 섀시 관리를 위한 데이터 인터페이스가 지원되지 않습니다. 전용 관리 인터페이스만 사용 가능합니다.
- 관리 인터페이스에 대한 DHCP 주소 지정 없음

VLAN 하위 인터페이스

- 이 문서에서는 섀시 VLAN 하위 인터페이스에 대해서만 설명합니다. 인스턴스 내에서 별도로 하위 인터페이스를 만들 수 있습니다.
- 인스턴스에 상위 인터페이스를 할당하는 경우에는 태그가 지정되지 않은(비 VLAN) 트래픽만 전달합니다. 태그가 지정되지 않은 트래픽을 전달하려는 경우가 아니라면 상위 인터페이스를 할당하지 마십시오.
- 하위 인터페이스는 데이터 또는 데이터 공유 유형 인터페이스와에서 지원됩니다..

- VLAN ID는 최대 500개까지 생성할 수 있습니다.
- 하위 인터페이스를 인라인 집합용으로 또는 패시브 인터페이스로 사용할 수는 없습니다.
- 페일오버 링크용으로 하위 인터페이스를 사용하는 경우에는 해당 상위 인터페이스의 모든 하위 인터페이스와 상위 인터페이스 자체가 페일오버 링크로 사용되도록 제한됩니다. 페일오버 링크로 사용할 수 없는 하위 인터페이스도 있고, 일반 데이터 인터페이스로 사용할 수 없는 하위 인터페이스도 있습니다.

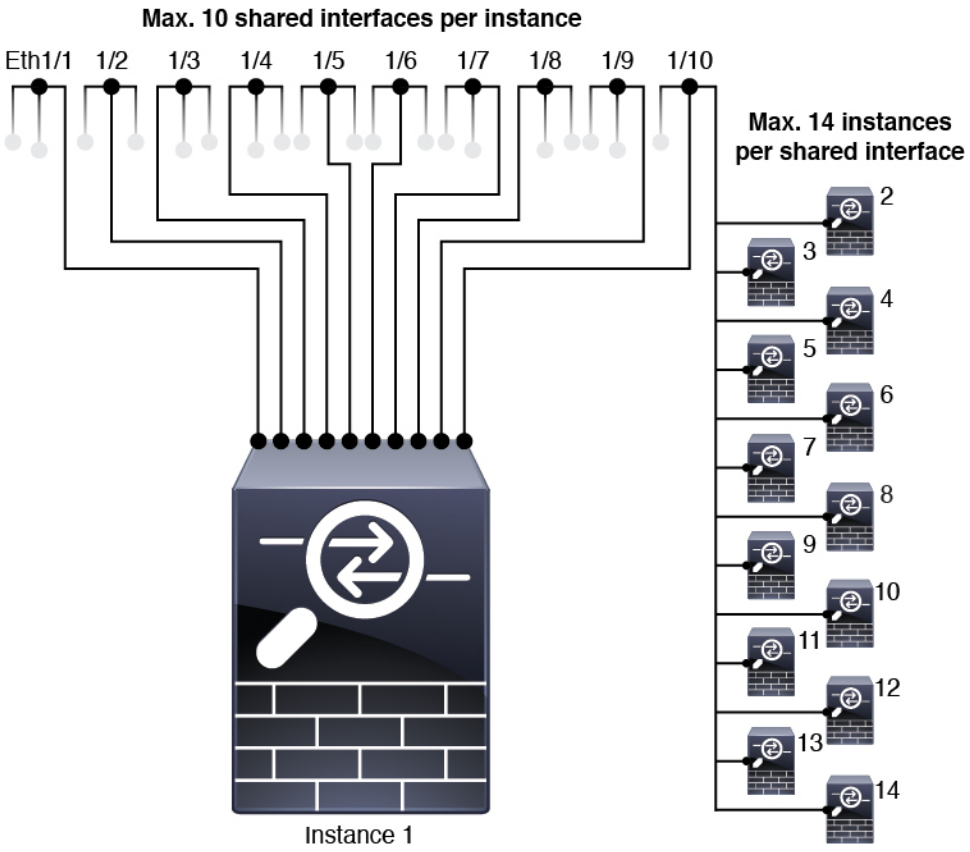
EtherChannel

- 물리적 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
- EtherChannel에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다.
- EtherChannel의 모든 인터페이스는 미디어 유형 및 속도 용량이 동일해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 **Detect SFP(SFP** 탐지**)**로 설정되어 있는 한 대용량 인터페이스에서 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. 이 경우 다른 인터페이스 용량을 사용할 수 있으며 최저 공통 속도가 사용됩니다.
- 섀시에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, 섀시에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다.
- 15.1(1)S2 이전 Cisco IOS 소프트웨어 버전에서는 섀시가 EtherChannel과 스위치 스택 간의 연결을 지원하지 않았습니다. 기본 스위치 설정으로 섀시 EtherChannel이 교차 스택에 연결되어 있는 상태에서 기본 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.

데이터 공유 인터페이스

- 공유 인터페이스당 최대 인스턴스 수는 14개입니다. 예를 들어 Instance1~Instance14에 Ethernet1/1을 할당할 수 있습니다.

  인스턴스당 최대 공유 인터페이스 수는 10개입니다. 예를 들어 Instance1에 Ethernet1/1.1~Ethernet1/1.10을 할당할 수 있습니다.



- 데이터 공유 인터페이스는 투명 방화벽 모드 인스턴스에서 사용할 수 없습니다.
- 데이터 공유 인터페이스는 인라인 집합 또는 패시브 인터페이스와 함께 사용할 수 없습니다.
- 데이터 공유 인터페이스는 페일오버 링크용으로 사용할 수 없습니다.

기본 MAC 주소

- 모든 인터페이스의 MAC 주소를 MAC 주소 풀에서 가져옵니다. 하위 인터페이스의 경우에는 MAC 주소를 수동으로 구성할 때 적절한 분류를 위해 동일한 상위 인터페이스의 모든 하위 인터페이스에 대해 고유한 MAC 주소를 사용해야 합니다. 인스턴스 인터페이스용 자동 MAC 주소, 13 페이지의 내용을 참조하십시오.

인스턴스 구성

인스턴스를 구성하기 전에 멀티 인스턴스 모드를 활성화하고, 새시를 management center에 추가한 다음 새시 인터페이스를 구성합니다. 새시 설정을 사용자 지정할 수도 있습니다.

멀티 인스턴스 모드 활성화

멀티 인스턴스 모드를 활성화하려면 콘솔 포트에서 threat defense CLI에 연결해야 합니다. 모드를 구성한 후 management center에 추가할 수 있습니다.

참고 관리 포트에서 SSH에 연결할 수 있지만, 여러 번 연결이 끊어지는 것을 방지하기 위해 콘솔 포트를 사용하는 것이 좋습니다. 이 절차에서는 콘솔 포트에 대해 설명합니다.

프로시저

단계 **1** 새시 콘솔 포트에 연결합니다.

콘솔 포트는 FXOS CLI에 연결됩니다.

단계 **2** 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

FXOS에 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다.

참고 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야합니다. 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

예제:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

단계 **3** 현재 모드(네이티브 또는 컨테이너)를 확인하십시오. 모드가 네이티브인 경우 이 절차를 계속 진행하여 멀티 인스턴스(컨테이너) 모드로 변환할 수 있습니다.

show system detail

예제:

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
```

```
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

단계 **4** threat defense CLI에 연결합니다.

connect ftd

예제**:**

```
firepower# connect ftd
>
```

단계 **5** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

설정 스크립트를 사용하여 관리 인터페이스 IP 주소 및 기타 설정을 지정할 수 있습니다. 그러나 멀티 인스턴스 모드로 전환하는 경우 다음과 같은 설정만 유지됩니다.

- 관리자 비밀번호(최초 로그인 시 설정)
- DNS 서버
- 검색 도메인

멀티 인스턴스 모드 명령의 일부로 관리 IP 주소 및 게이트웨이를 재설정하게 됩니다. 멀티 인스턴스 모드로 전환한 후 FXOS CLI에서 관리 설정을 변경할 수 있습니다. FXOS CLI에서 섀시 관리 설정 변경, 62 페이지의 내용을 참조하십시오.

단계 **6** 멀티 인스턴스 모드를 활성화하고, 섀시 관리 인터페이스 설정을 지정한 다음, management center를 식별합니다. IPv4 및/또는 IPv6 고정 주소를 사용할 수 있습니다. DHCP는 지원되지 않습니다. 명령을 입력한 후에는 구성을 지우고 재부팅하라는 메시지가 표시됩니다. **ERASE** (모두 대문자)를 입력합니다. 모드 변경의 일환으로 시스템이 재부팅되고 명령에 설정한 관리 네트워크 설정 및 관리자 비밀번호를 제외하고 컨피그레이션이 지워집니다. 섀시 호스트 이름은 "firepower-*model*"로 설정됩니다.

IPv4:

configure multi-instance network ipv4 *ip_address network_mask gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv4_address* | **DONTRESOLVE**} *registration_key nat_id*

IPv6:

configure multi-instance network ipv6 *ipv6_address prefix_length gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv6_address* | **DONTRESOLVE**} *registration_key nat_id*

다음 **manager** 구성 요소를 참고하십시오.

- {*hostname* | *ipv4_address* | **DONTRESOLVE**}—management center의 FQDN 또는 IP 주소를 지정합니다. 하나 이상의 디바이스(management center 또는 섀시)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 관리자 호스

트 이름 또는 IP 주소를 지정하지 않으면 **DONTRESOLVE**를 입력합니다. 이 경우 섀시에 연결 가능한 IP 주소 또는 호스트 이름이 있어야 하며 *nat_id*를 지정해야 합니다.

- *reg_key* — 섀시 등록 시 management center에 지정할 일회용 등록 키를 입력합니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.
- *nat_id* — 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 섀시를 등록할 때 management center에 지정할 고유한 일회용 문자열을 지정합니다. 이는 관리자 주소 또는 호스트 이름을 지정하지 않은 경우 필요하지만, 호스트 이름 또는 IP 주소를 지정하는 경우에도 항상 NAT ID를 설정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다.

모드를 다시 어플라이언스 모드로 변경하려면 FXOS CLI를 사용하여 **scope system** 및 **set deploymode native**를 입력해야 합니다. FXOS CLI에서 섀시 관리 설정 변경, 62 페이지의 내용을 참조하십시오.

예제:

```
> configure multi-instance network ipv4 172.16.0.104 255.255.255.0 172.16.0.1 manager
fmc1 172.16.0.103 impala67 winchester1
WARNING: This command will discard any FTD configuration (except admin's credentials).
Make sure you backup your content. All previous content will be lost. System is going to
be re-initialized.
Type ERASE to confirm:ERASE
Exit...
>
```

에 멀티 인스턴스 섀시 추가Management Center

멀티 인스턴스 섀시를 management center에 추가합니다. Management Center와 섀시는 섀시 MGMT 인터페이스를 사용하여 별도의 관리 연결을 공유합니다.

management center 를 사용하여 모든 섀시 설정과 인스턴스를 구성할 수 있습니다. FXOS CLI에서의 Secure Firewall 섀시 관리자 또는 구성은 지원되지 않습니다.

시작하기 전에

섀시를 멀티 인스턴스 모드로 변환합니다. 멀티 인스턴스 모드 활성화, 19 페이지을 참조하십시오.

프로시저

단계 **1** management center에서 섀시 관리 IP 주소 또는 호스트 이름을 사용하여 섀시를 추가합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 **Add(**추가**)** > **Chassis(**섀시**)**를 선택합니다.

그림 *12:* 섀시 추가

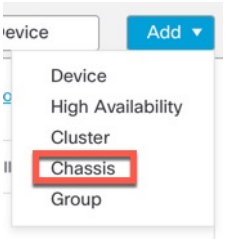
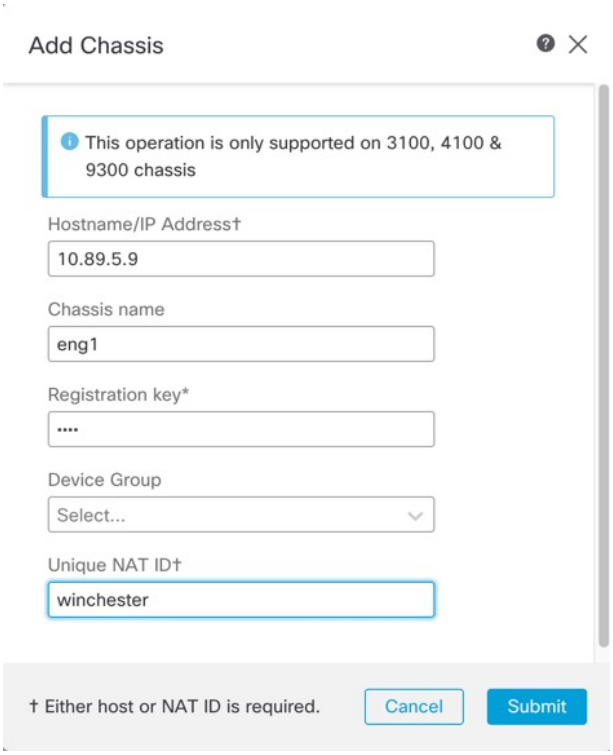


그림 *13:* 섀시 추가



b) **Hostname/IP Address(**호스트 이름**/IP** 주소**)** 필드에 추가할 섀시의 IP 주소 또는 호스트 이름을 입력합니다.

   호스트 이름 또는 IP 주소를 모르는 경우 이 필드를 비워두고 고유 **NAT ID**를 지정할 수 있습니다.

c) management center에 표시할 섀시의 이름을 **Chassis Name(**섀시 이름**)** 필드에 입력합니다.

d) management center로 관리할 섀시를 구성할 때 사용한 것과 동일한 등록 키를 **Registration Key(**등록 키**)** 필드에 입력합니다.

   등록 키는 일회용 공유 암호입니다. 키는 영숫자 및 하이픈(-)을 포함할 수 있습니다.

e) 다중 도메인 구축에서는 현재 도메인과 상관없이 섀시를 리프 도메인으로 할당합니다.

   현재 도메인이 리프 도메인인 경우 섀시는 자동으로 현재 도메인에 추가됩니다. 현재 도메인이 리프 도메인이 아닌 경우나 이후 재등록을 한 경우라면 리프 도메인으로 전환하여 섀시를 구성합니다. 섀시는 하나의 도메인에만 속할 수 있습니다.

f) (선택 사항) **Device Group(**디바이스 그룹**)**에 섀시를 추가합니다.

g) 섀시 설정 중에 NAT ID를 사용한 경우 고유 **NAT ID** 필드에 동일한 NAT ID를 입력합니다.

NAT ID는 영숫자 및 하이픈(-)을 포함할 수 있습니다.

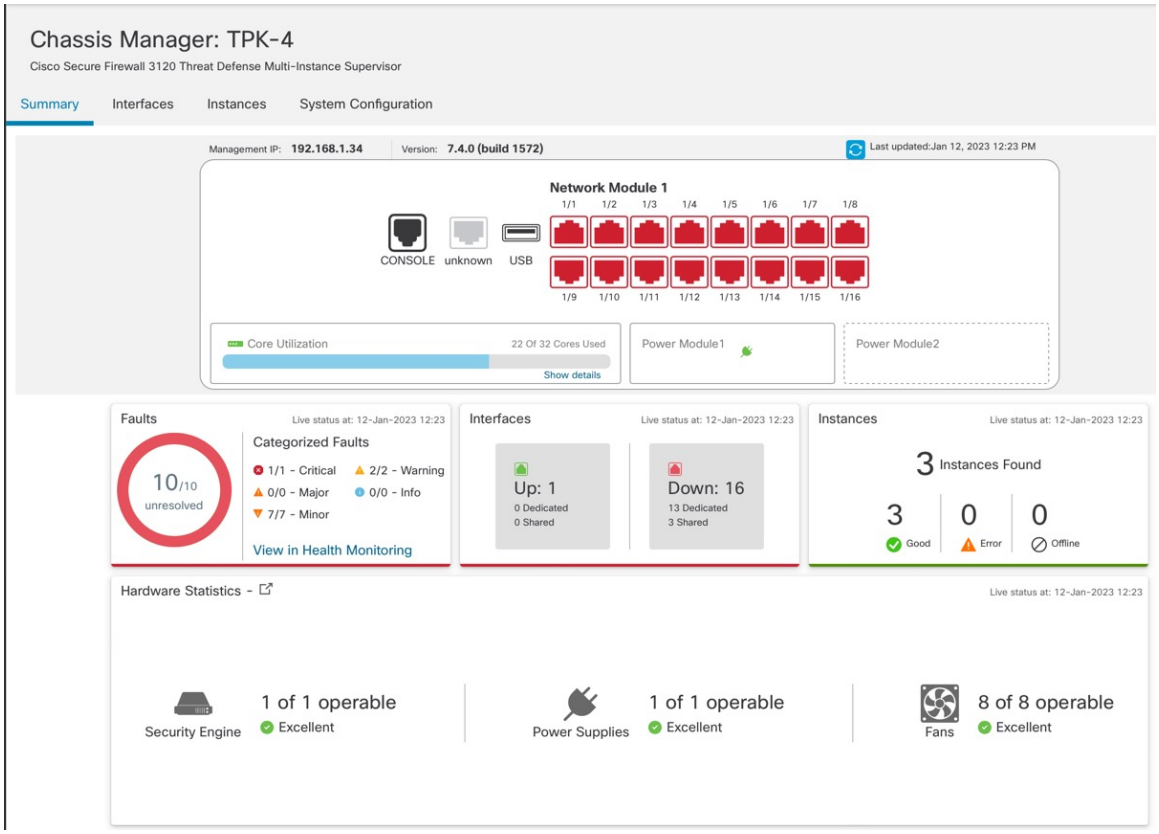
h) **Submit(**제출**)**을 클릭합니다.

Device(디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에 섀시가 추가됩니다.

단계 **2** 섀시를 보고 구성하려면 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)을 클릭합니다.

섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

그림 ***14:*** 섀시 요약



섀시 인터페이스 구성

섀시 수준에서 물리적 인터페이스, 인스턴스의 VLAN 하위 인터페이스 및 EtherChannel 인터페이스의 기본 이더넷 설정을 구성합니다. 기본적으로 물리적 인터페이스는 비활성화되어 있습니다.

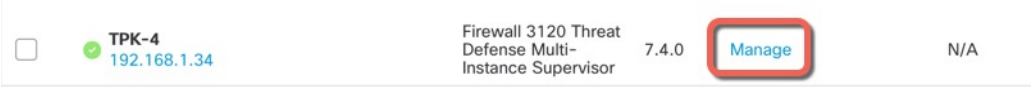
실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스와 기타 하드웨어 설정을 지정할 수 있습니다. 인터페이스를 사용하려면 섀시에 대해 인터페이스를 물리적으로 활성화하고 인스턴스에서 논리적으로 활성화해야 합니다. 기본적으로 물리적 인터페이스는 비활성화되어 있습니다. VLAN 하위 인터페이스의 경우 관리 상태는 상위 인터페이스에서 상속됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

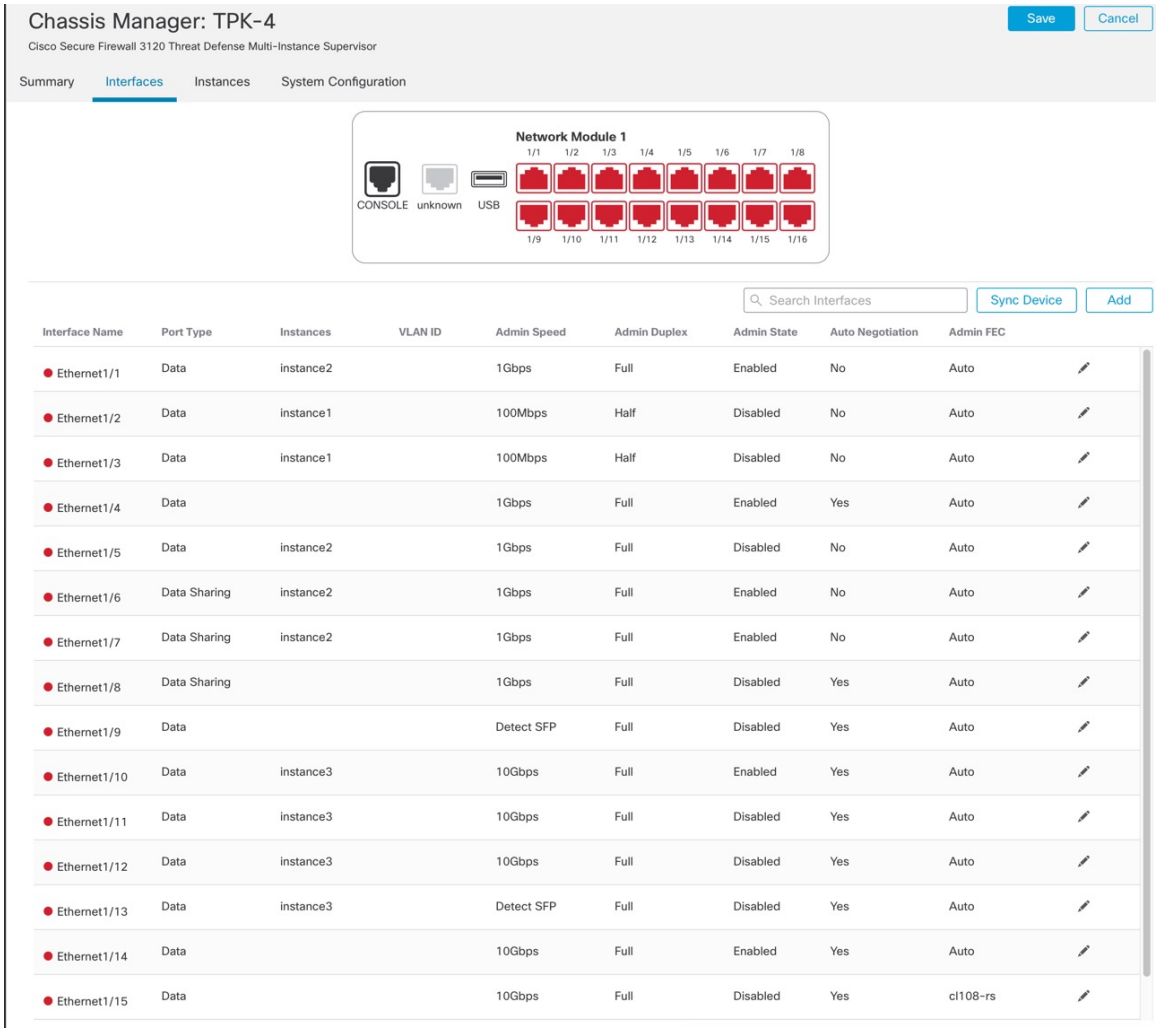
그림 ***15:*** 섀시 관리



섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

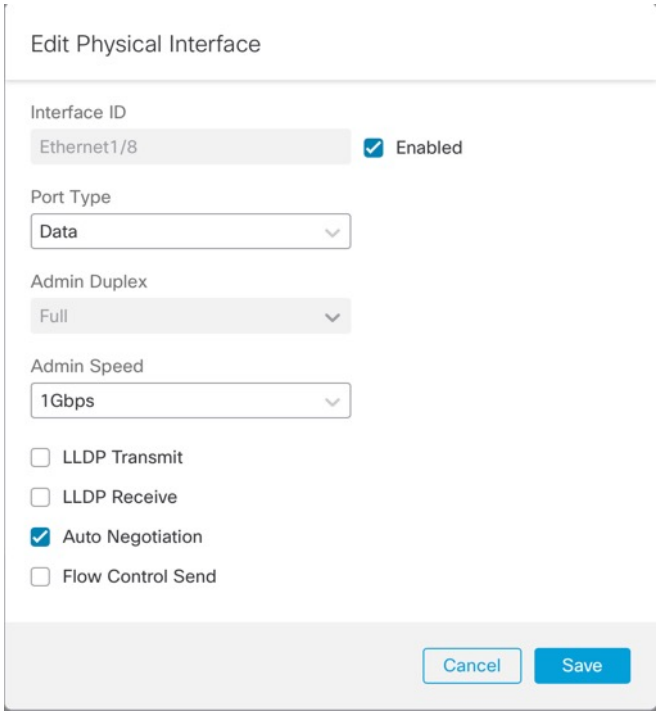
단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

그림 *16:* 인터페이스



단계 **3** 수정할 인터페이스의 편집 (✎)을 클릭합니다.

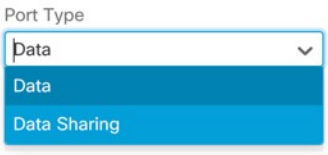
그림 *17:* 물리적 인터페이스 편집



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

단계 **5** 포트 유형에 대해 데이터 또는 데이터 공유를 선택합니다.

그림 *18:* 포트 유형



단계 **6** 관리 듀플렉스로 설정합니다.

1Gbps 이상의 속도는 풀 듀플렉스만 지원합니다. SFP 인터페이스는 풀 듀플렉스만 지원합니다.

단계 **7** **Admin Speed**(관리 속도)를 설정합니다.

SFP의 경우 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.

단계 **8** (선택 사항) **LLDP** 전송 및/또는 **LLDP** 수신 을 선택하여 LLDP(Link Layer Discovery Protocol) 패킷을 활성화합니다.

단계 **9** (선택 사항) **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 **10** (선택 사항) **Auto Negotiation(**자동 협상**)**을 선택하여 속도, 링크 상태 및 플로우 제어를 협상하도록 인터페이스를 설정합니다. 1Gbps 미만의 속도에서는 이 설정을 편집할 수 없습니다. SFP 인터페이스의 경우 속도가 1Gbps로 설정된 경우에만 자동 협상을 비활성화할 수 있습니다.

단계 **11** **Save(**저장**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 페이지의 오른쪽 상단에서 **Save(**저장**)**를 클릭합니다.

이제 정책을 섀시에 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

EtherChannel 구성

EtherChannel(포트 채널로 알려짐)은 동일한 미디어 유형 및 용량의 멤버 인터페이스를 최대 8개까지 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 **Detect SFP(SFP** 탐지**)**로 설정되어 있는 한 대용량 인터페이스에서 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. 이 경우 다른 인터페이스 용량을 사용할 수 있으며 최저 공통 속도가 사용됩니다.

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다. LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

섀시에서 EtherChannel을 생성하면 물리적 링크가 가동 중이더라도 EtherChannel은 논리적 디바이스에 할당될 때까지 Active LACP(액티브 LACP) 모드인 경우 **Suspended(**일시 중단**)** 상태로, On LACP(LACP 켜짐) 모드인 경우 **Down(**중단**)** 상태로 유지됩니다. EtherChannel은 인스턴스에 추가될 때 **Suspended** (일시 중단) 상태에서 해제됩니다.

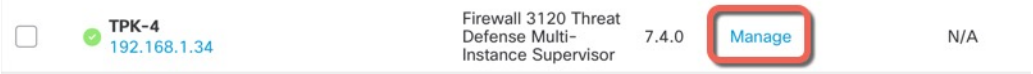
시작하기 전에

물리적 인터페이스를 활성화하고 하드웨어 매개변수를 설정합니다. 실제 인터페이스 구성, 24 페이지을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

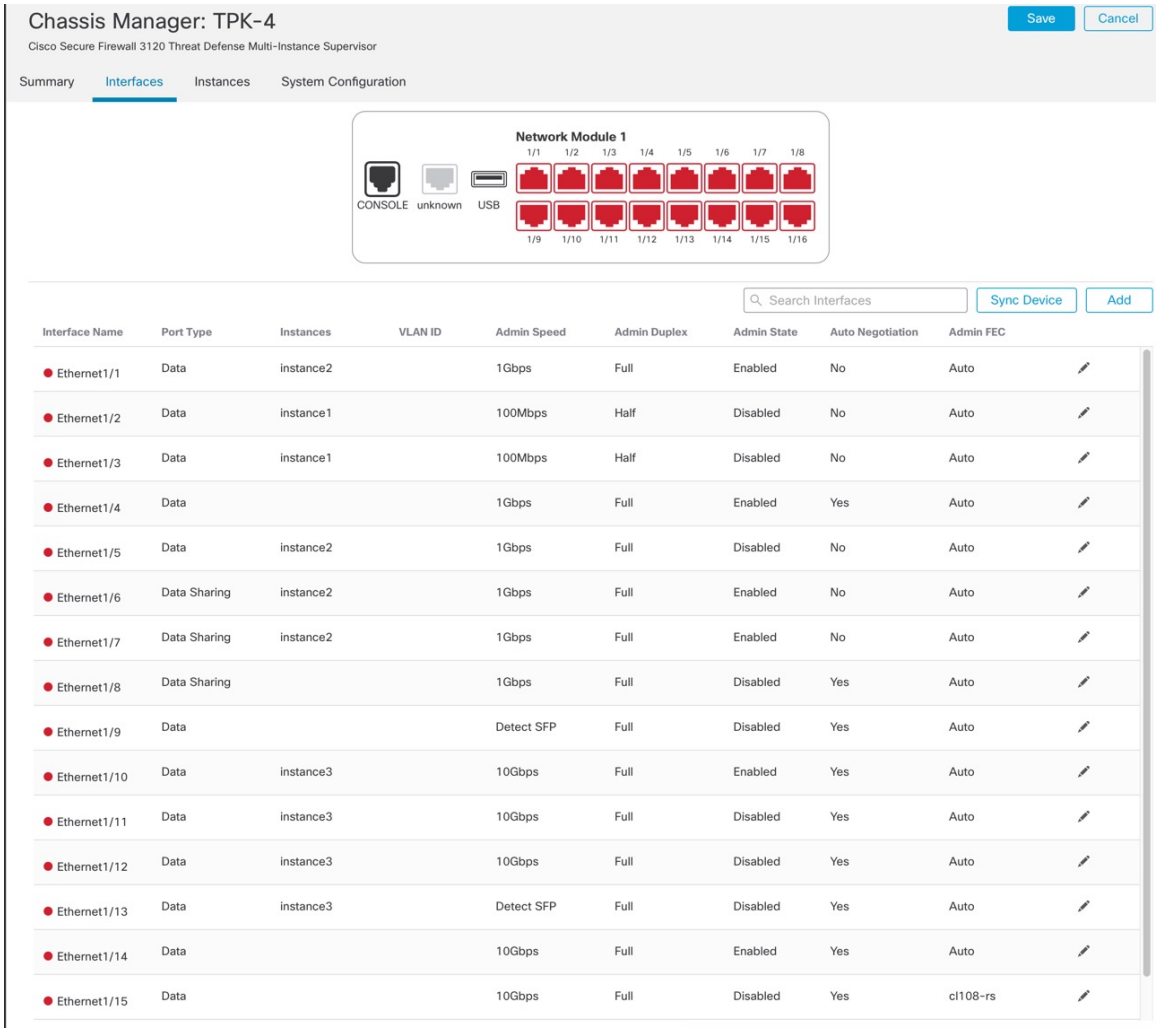
그림 ***19:*** 섀시 관리



섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

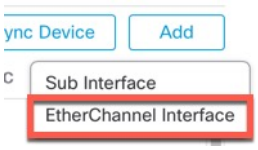
단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

그림 *20:* 인터페이스



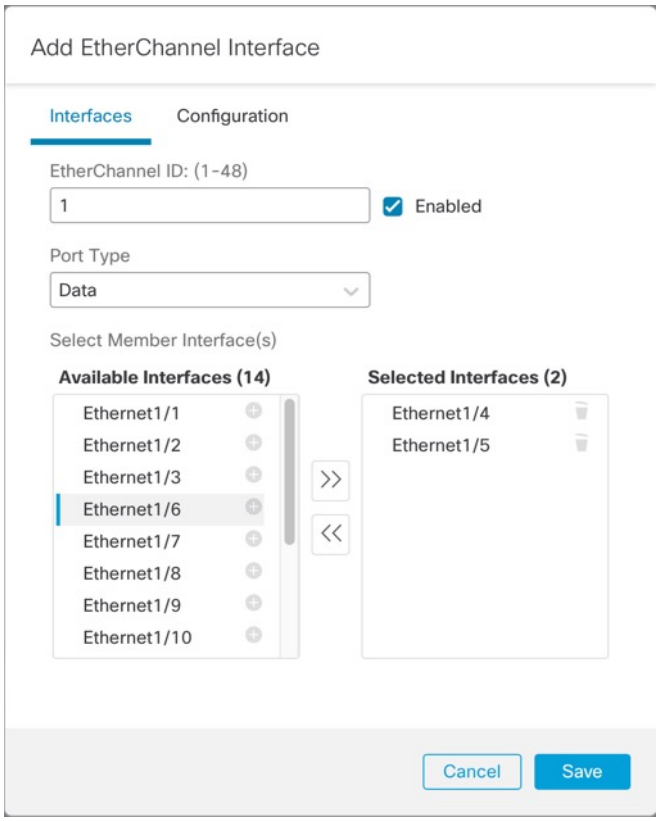
단계 **3** **Add(**추가**)** > **EtherChannel Interface(EtherChannel** 인터페이스**)**를 클릭합니다.

그림 *21: EtherChannel* 추가



단계 **4** 다음 **Interfaces(**인터페이스**)** 매개변수를 설정합니다.

그림 22: 인터페이스 설정



a) **EtherChannel ID**에 대해 1~48의 ID를 지정합니다.
b) **Enable(**활성화**)**를 선택합니다.
c) 포트 유형에 대해 데이터 또는 데이터 공유를 선택합니다.

   포트 유형에 대한 자세한 내용은 인터페이스 유형, 3 페이지를 참조하십시오.

d) EtherChannel에 물리적 인터페이스를 추가하려면 **Available Interfaces** (사용 가능한 인터페이스) 목록에서 **Add(**추가**)** (⊕) 를 클릭하여 **Selected Interfaces** (선택한 인터페이스) 목록으로 이동합니다.

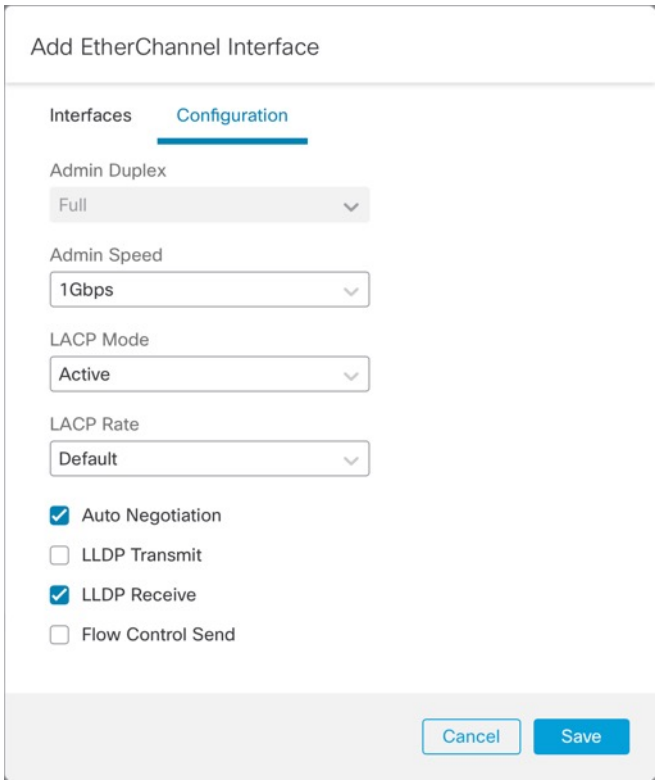
   모든 인터페이스를 추가하거나 제거하려면 이중 화살표 버튼을 클릭합니다.

   참고 이미 인스턴스에 할당된 인터페이스는 추가할 수 없습니다.

단계 **5** (선택 사항) 다음 **Configuration(**구성**)** 매개변수를 설정합니다.

이러한 설정 중 다수(LACP 설정 제외)는 EtherChannel에 포함할 인터페이스의 요구 사항을 설정합니다. 멤버 인터페이스의 설정을 재정의하지 않습니다. 따라서 예를 들어 **LLDP** 전송을 선택하는 경우 해당 설정이 있는 인터페이스만 추가해야 합니다. **Admin Speed** (관리 속도)를 1Gbps로 설정하는 경우 1Gbps 인터페이스만 포함할 수 있습니다.

그림 *23:* 구성 설정



a) 멤버 인터페이스에 대해 필요한 **Admin Duplex(**관리 듀플렉스**)**, **Full Duplex(**풀 듀플렉스**)** 또는 **Half Duplex(**하프 듀플렉스**)**를 선택합니다.

지정된 듀플렉스로 설정된 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

b) 드롭다운 목록에서 멤버 인터페이스에 대해 필요한 **Admin Speed(**관리 속도**)**를 선택합니다.

지정된 속도가 아닌 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

c) **LACP Mode(LACP** 모드) 를 **Active** (액티브) 또는 **On**(켜기)으로 선택합니다.

- **Active(**액티브**)** - LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- **On(**켜짐**)** — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

참고 On에서 활성화, 또는 활성화에서 On으로 모드를 변경하는 경우 EtherChannel가 작동하는 데 최대 3분이 걸립니다.

d) **LACP Rate**(LACP 속도), **Default**(기본값), **Fast**(빠름) 또는 **Normal**(일반)을 선택합니다.

기본값은 **Fast**입니다.

e) **LLDP Transmit** (LLDP 전송) 및/또는 **LLDP Receive**(LLDP 수신)를 선택하여 멤버 인터페이스에 필요한 LLDP(Link Layer Discovery Protocol) 설정을 선택합니다.

f) 멤버 인터페이스에 필요한 **Flow Control Send** (플로우 제어 전송) 설정을 확인합니다.

단계 **6** **Save(**저장**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 페이지의 오른쪽 상단에서 **Save(**저장**)**를 클릭합니다.

이제 정책을 섀시에 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

하위 인터페이스 구성

섀시에는 하위 인터페이스를 500 개까지 추가할 수 있습니다.

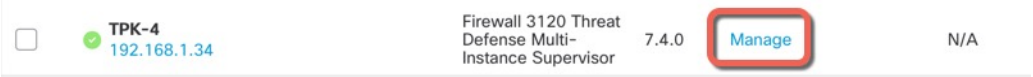
인터페이스당 VLAN ID는 고유해야 하며 인스턴스 내에서 VLAN ID는 모든 할당된 인터페이스에 대해 고유해야 합니다. VLAN ID가 다른 인스턴스에 할당되었다면 별도의 인터페이스에서 해당 VLAN ID를 재사용할 수 있습니다. 그러나 동일한 ID를 사용하더라도 계속해서 각 하위 인터페이스에는 이제한이 적용됩니다.

이 섹션에서는 *FXOS* VLAN 하위 인터페이스에 대해서만 설명합니다. 인스턴스 내에서 별도로 하위 인터페이스를 만들 수 있습니다. 섀시 인터페이스와 인스턴스 인터페이스 비교, 3 페이지을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

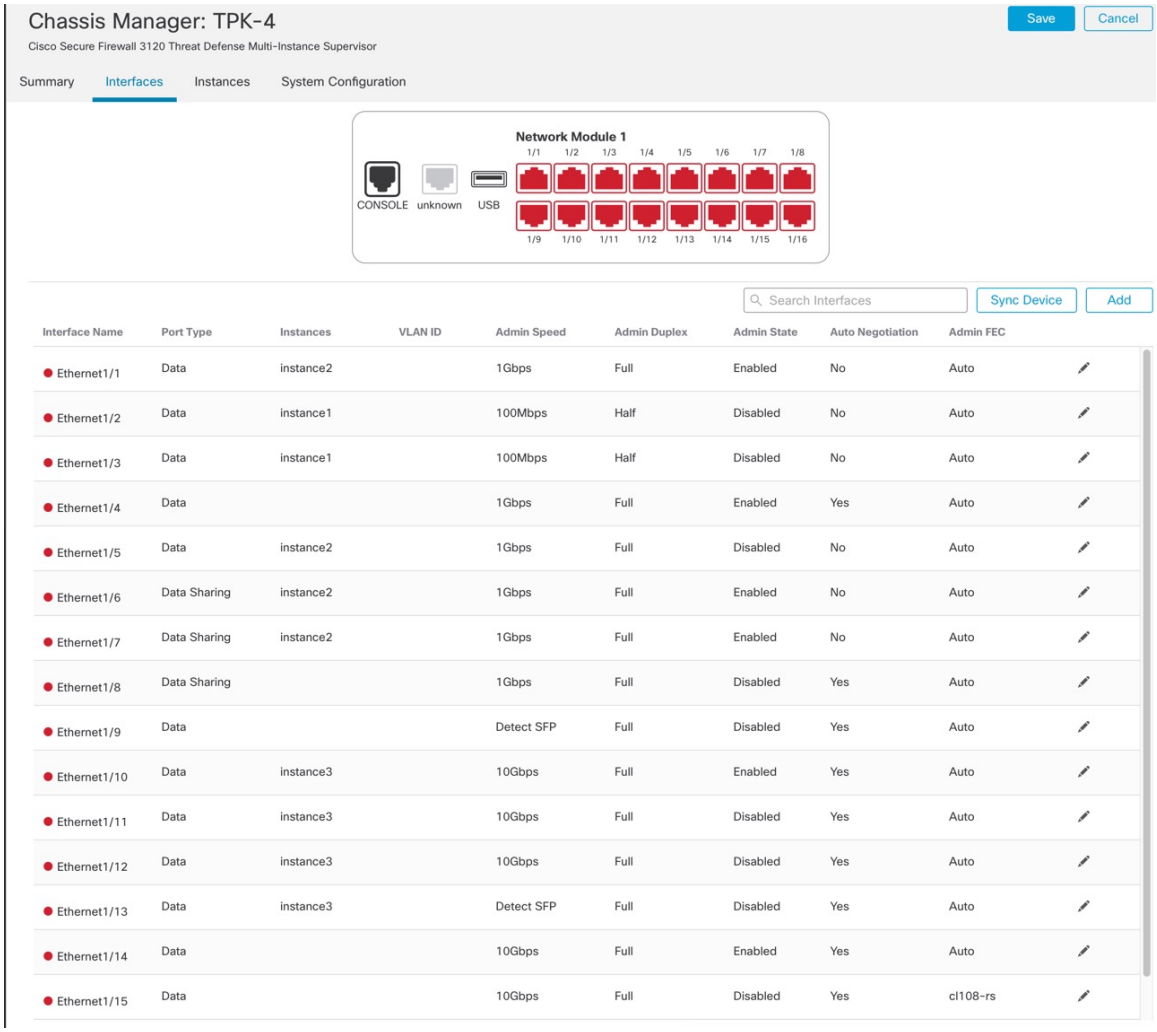
그림 ***24:*** 섀시 관리



섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

그림 *25:* 인터페이스

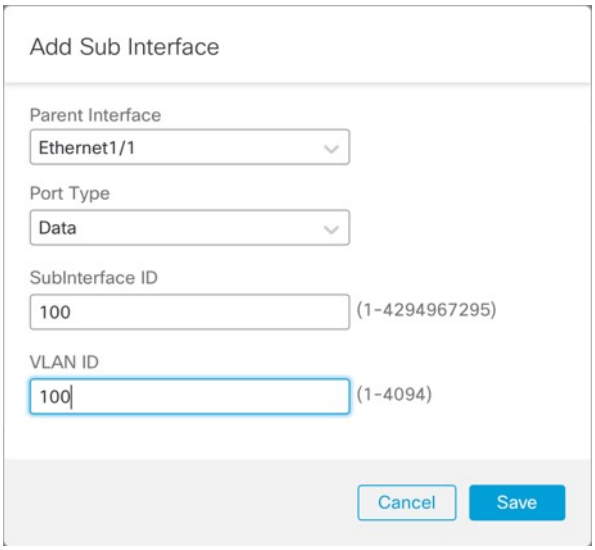


단계 **3** **Add(**추가**)** > **Subinterface(**하위 인터페이스**)**를 클릭합니다.

그림 *26: SubInterface* 추가

단계 **4** 다음 매개변수를 설정합니다.

그림 *27:* 하위 인터페이스 설정



a)

단계 **5** **Save(**저장**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 페이지의 오른쪽 상단에서 **Save(**저장**)**를 클릭합니다.

이제 정책을 섀시에 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

인스턴스 추가

멀티 인스턴스 모드에서 섀시에 하나 이상의 인스턴스를 추가할 수 있습니다. 지원되는 인스턴스 수는 모델에 따라 다릅니다. 인스턴스의 요구 사항 및 사전 요건, 15 페이지를 참조하십시오.

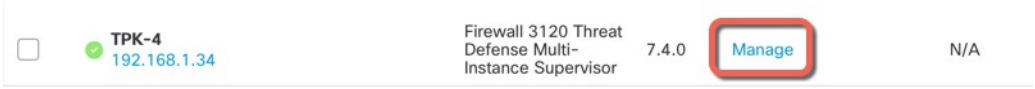
시작하기 전에

멀티 인스턴스 모드 활성화, 19 페이지 및 에 멀티 인스턴스 섀시 추가Management Center, 21 페이지.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

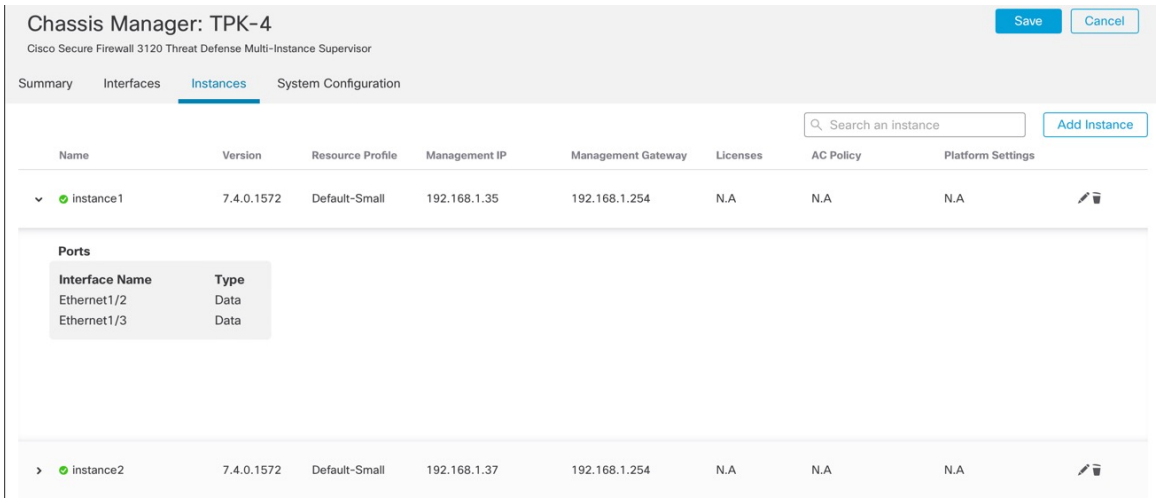
그림 *28:* 섀시 관리



섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

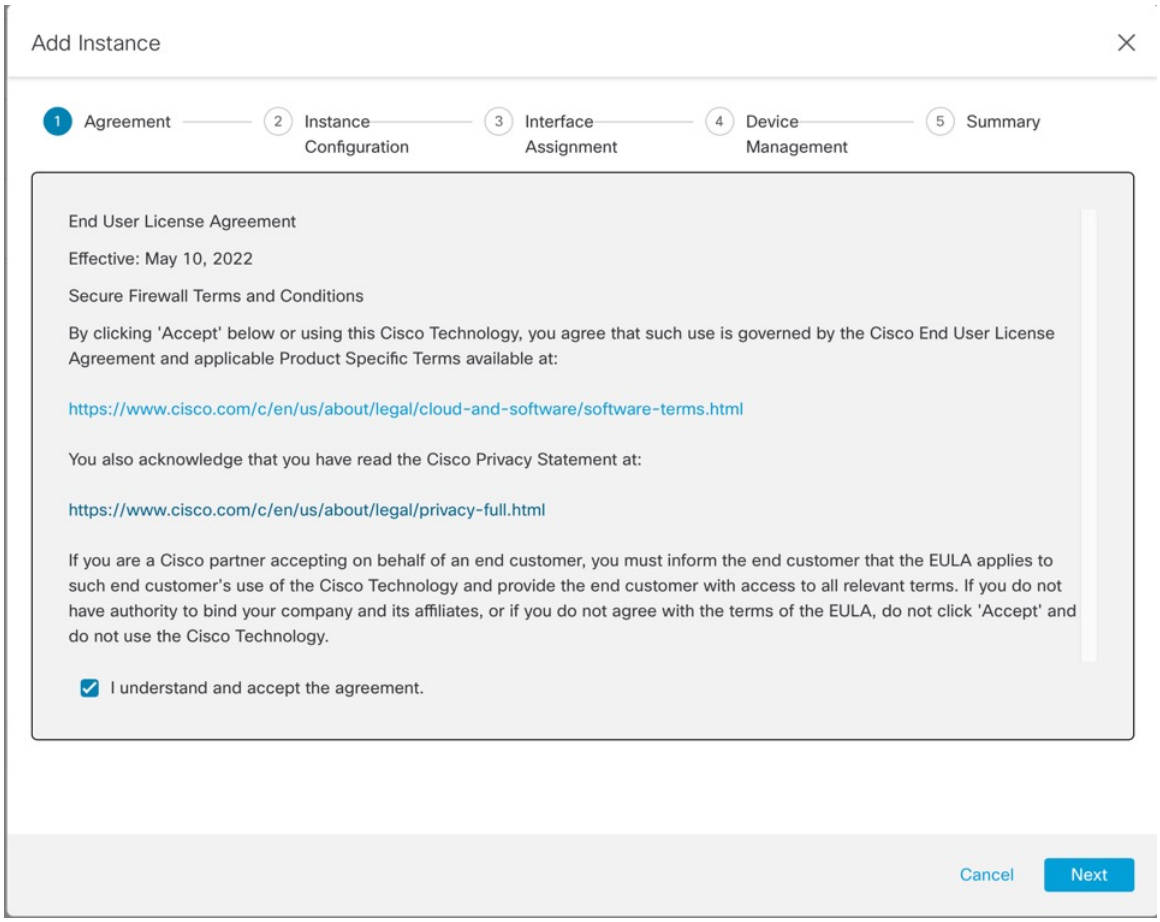
단계 **2** **Instances**(인스턴스) 를 클릭하고 **Add Instance**(인스턴스 추가)를 클릭합니다.

그림 ***29:*** 인스턴스



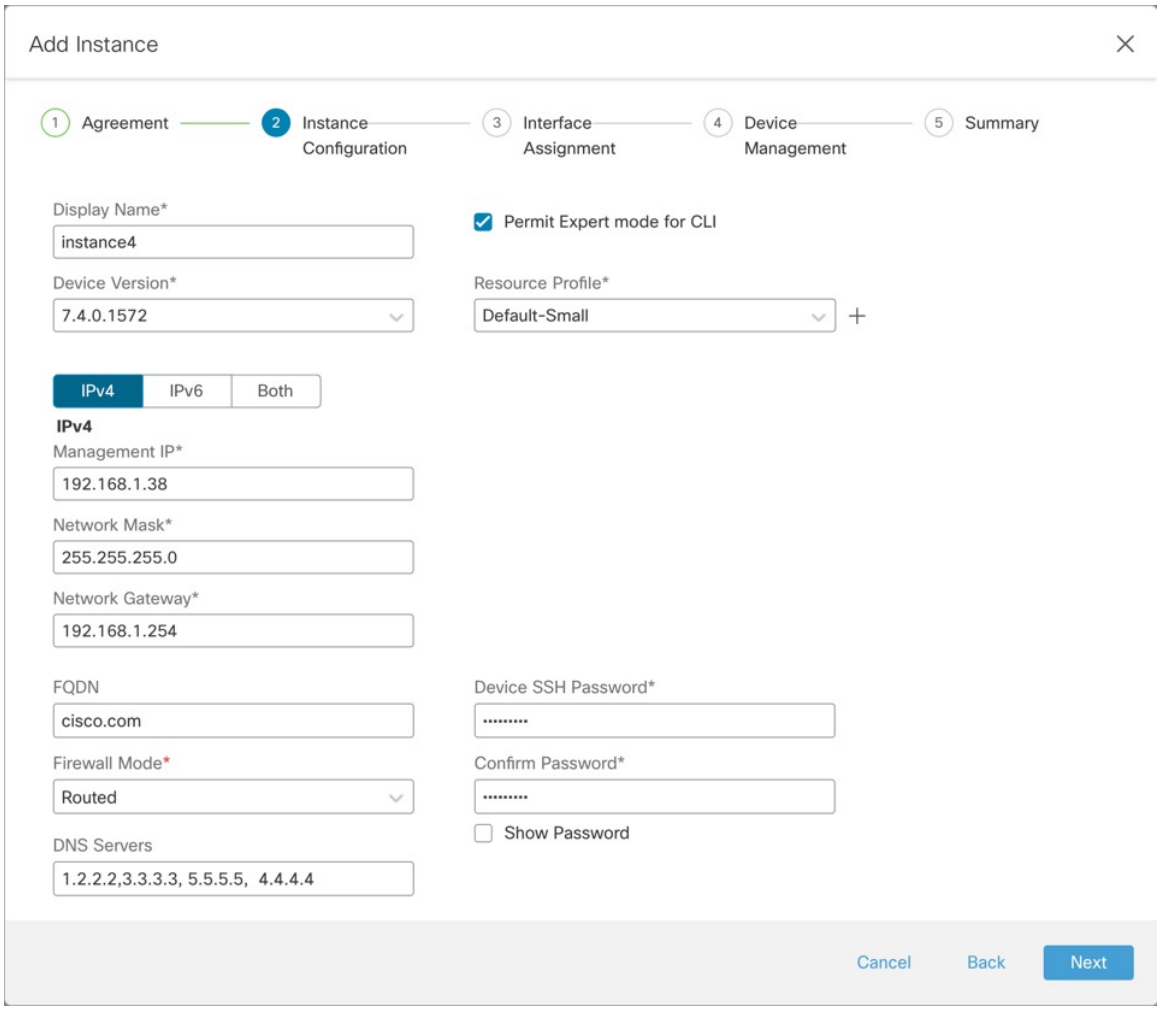
단계 **3** **Agreement**(계약) 에서 **I agree and accept the Agreement(**계약을 이해하고 동의합니다)를 선택하고 **Next**(다음)를 클릭합니다.

그림 *30:* 계약



단계 **4** **Instance Configuration**(인스턴스 구성)에서 인스턴스 파라미터를 설정하고 **Next**(다음)를 클릭합니다.

그림 *31:* 인스턴스 구성



- 표시 이름
- **Device Version**(디바이스 버전) - 나열된 버전은 현재 섀시에 다운로드된 패키지입니다. 새 패키지로 업그레이드하려면 **Devices(**장치**)** > **Chassis Upgrade(**섀시 업그레이드**)**를 참조하십시오. 업그레이드하면 이전 버전과 새 버전이 메뉴에 나열됩니다. 이전 패키지를 다운로드하려면 FXOS CLI를 사용해야 합니다. Cisco Firepower 1000/2100 및 Firepower Threat Defense 기능이 있는 Threat Defense 3100/4200용 Cisco FXOS 문제 해결 가이드을 참조하십시오.
- **IPv4**, **IPv6**또는 둘 다 - 섀시 관리 인터페이스와 동일한 네트워크에서 관리 **IP** 주소를 설정합니다. 네트워크 마스크 및 게이트웨이(섀시와 동일한 게이트웨이일 수 있음)를 설정합니다. 섀시 관리 인터페이스는 각 인스턴스와 공유되며, 각 인스턴스는 네트워크에서 고유한 IP 주소를 갖습니다. 기본적으로 이 IP 주소에 SSH로 연결하여 threat defense CLI에 연결할 수 있습니다.
- (선택 사항) **FQDN**
- 방화벽 모드 - 라우팅 또는 투명.
- **DNS Servers**(DNS 서버) - 관리 트래픽에만 사용할 쉼표로 구분된 DNS 서버 목록을 입력합니다.

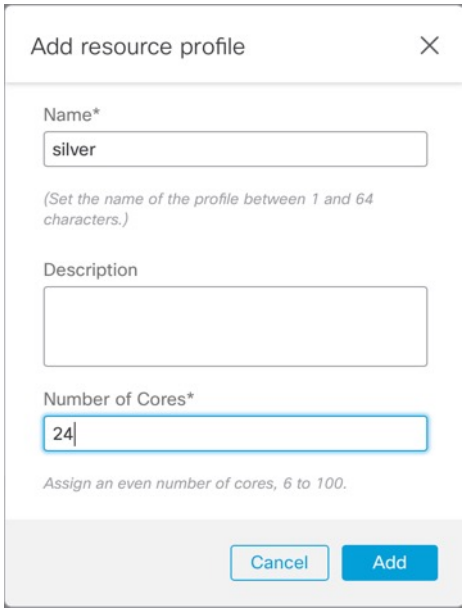
- (선택 사항) **Permit Expert Mode for CLI(CLI**에 대한 전문가 모드 허용**)** - 전문가 모드는 고급 문제 해결을 위해 threat defense 쉘(shell) 액세스를 제공합니다.

  이 옵션을 활성화하면 SSH 세션에서 인스턴스에 직접 액세스하는 사용자가 전문가 모드를 시작할 수 있습니다. 비활성화하는 경우 FXOS CLI에서 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리하려면 이 옵션을 비활성화하는 것이 좋습니다.

  문서에 설명되어 있는 절차에 따라 Expert 모드가 필요하다고 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 요청하는 경우에만 Expert 모드를 사용합니다. 이 모드를 설정하려면 threat defense CLI에서 **expert** 명령을 사용합니다.

- **Resource Profile(**리소스 프로파일**)** - 리소스 프로파일은 CPU 코어 수를 설정합니다. RAM은 코어 수에 따라 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다. 섀시에는 기본 리소스 프로파일인 Default-Small, Default-Medium 및 Default-Large가 포함되어 있습니다. **Add(**추가**)** (+)를 클릭하여 이 섀시용으로 다른 프로파일을 추가할 수 있습니다. 나중에 리소스 프로필을 수정할 수 없습니다.

  그림 ***32:*** 리소스 프로파일 추가



  - 최소 코어 수는 6입니다.

    참고 코어 수가 적은 인스턴스는 코어 수가 더 많은 CPU 사용률보다 CPU 사용률이 상대적으로 높아질 수 있습니다. 코어 수가 적은 인스턴스는 트래픽 로드 변경에 더욱 민감합니다. 트래픽 삭제를 경험하는 경우 더 많은 코어를 할당해 보십시오.

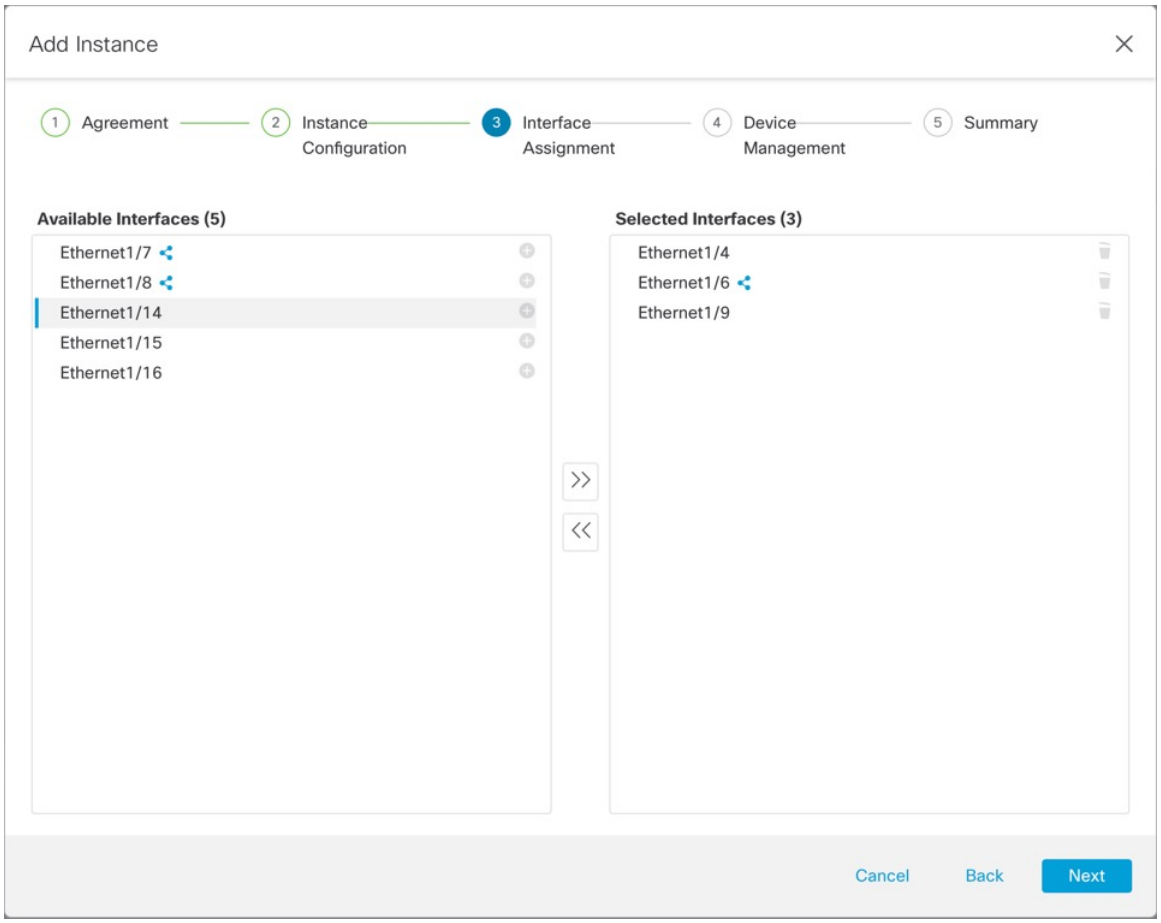
  - 코어는 최대값까지 짝수(6, 8, 10, 12, 14 등)로 할당할 수 있습니다.
  - 사용 가능한 코어의 최대 수는 모델에 따라 달라집니다. 인스턴스의 요구 사항 및 사전 요건, 15 페이지의 내용을 참조하십시오.

나중에 다른 리소스 프로파일을 할당하는 경우 인스턴스가 다시 로드됩니다. 다시 로드는 5분 정도 걸릴 수 있습니다. 설정된 고가용성 쌍에 대해 크기가 다른 리소스 프로파일을 할당하는 경우에는 최대한 빠른 시간 내에 모든 멤버를 같은 크기로 설정해야 합니다.

- **Device SSH Password**(디바이스 SSH 비밀번호) - CLI 액세스(SSH 또는 콘솔)를 위한 threat defense 관리자 사용자 비밀번호를 설정합니다. **Confirm Password(**비밀번호 확인**)** 필드에 비밀번호를 다시 입력합니다.

단계 **5** **Interface Assignment**(인터페이스 할당)에서 인스턴스에 새시 인터페이스를 할당하고 **Next**(다음)를 클릭합니다.

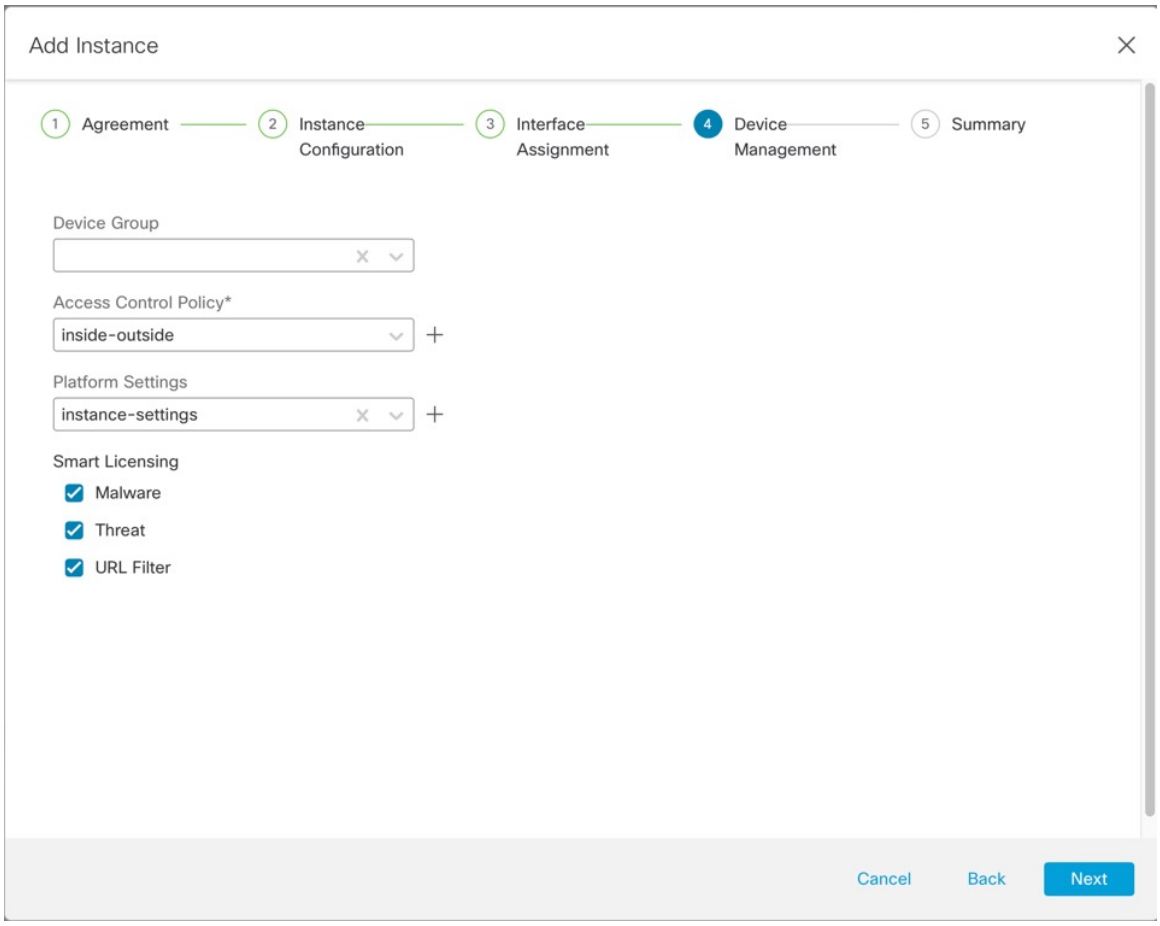
그림 ***33:*** 인터페이스 할당



공유 인터페이스는 공유 아이콘( )을 표시합니다.

단계 **6** 디바이스 관리에서 디바이스 관련 설정을 지정하고 **Next**(다음)를 클릭합니다.

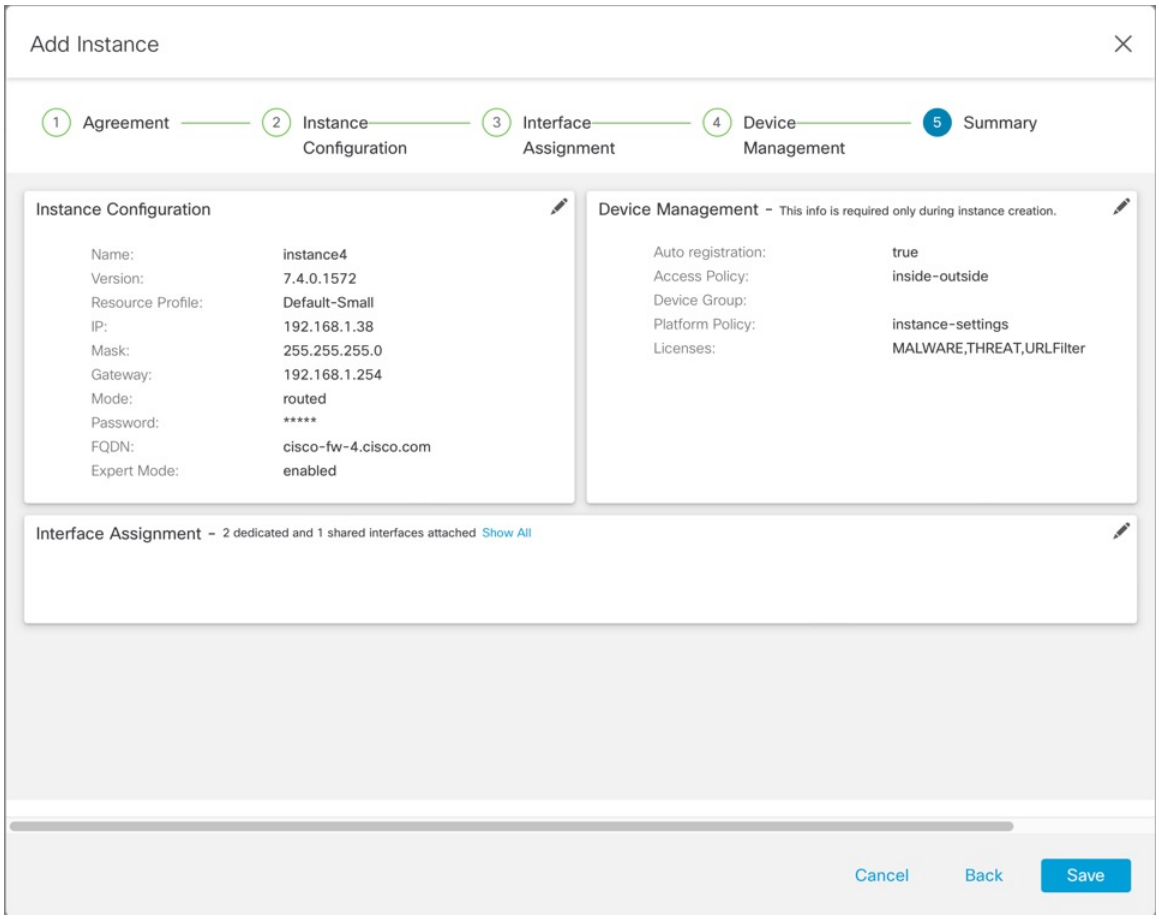
그림 *34:* 디바이스 관리



- 디바이스 그룹
- **Access Control Policy**(액세스 제어 정책) - 기존 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.
- **Platform Settings(**플랫폼 설정**)** - 기존 플랫폼 설정 정책을 선택하거나 새 정책을 만듭니다.
- 스마트 라이선싱

단계 **7** **Summary**(요약)에서 설정을 확인하고 **Save**(저장)를 클릭합니다.

그림 *35:* 요약



인스턴스를 저장하기 전에 이 화면에서 설정을 수정할 수 있습니다. 저장하면 인스턴스가 **Instances(**인스턴스**)** 화면에 추가됩니다.

단계 **8** **Instances(**인스턴스**)** 화면에서 **Save(**저장**)**를 클릭합니다.

단계 **9** 섀시 구성을 구축합니다.

구축이 끝나면 디바이스 관리 페이지에 인스턴스가 디바이스로 추가됩니다.

시스템 구성 사용자 지정

SNMP와 같은 섀시 레벨 설정을 구성할 수 있습니다. 섀시 FXOS 구성을 가져오거나 내보낼 수도 있습니다.

SNMP 구성

섀시 시스템 구성에서 지정하는 인스턴스 중 하나의 데이터 인터페이스를 통해 섀시 레벨 MIB에 액세스할 수 있습니다. 섀시 SNMP 정보에 이 인스턴스만 사용할 수 있습니다. 섀시 관리 인터페이스를 통해 SNMP에 액세스할 수 없습니다.

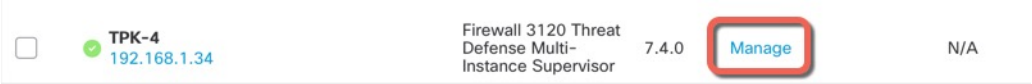
시작하기 전에

인스턴스 중 하나에 대해 SNMP를 구성합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

그림 ***36:*** 섀시 관리

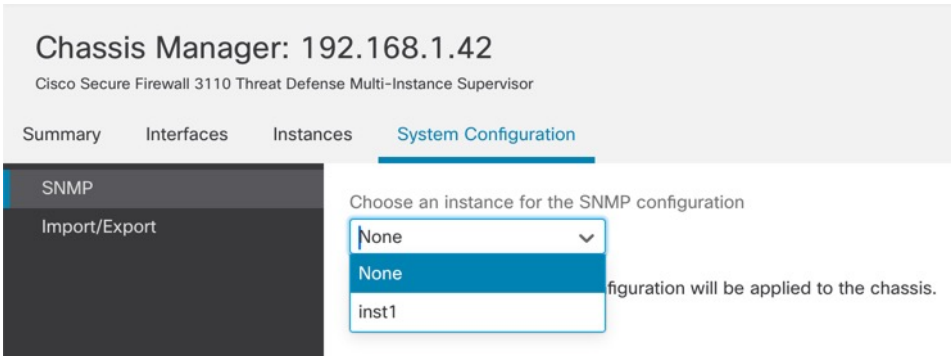


섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

단계 **2** 시스템 구성을 클릭합니다.

단계 **3** **SNMP**를 클릭하고 드롭다운 목록에서 인스턴스를 선택합니다.

그림 ***37: SNMP***



선택한 인스턴스에서 섀시의 SNMP에 액세스할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 섀시 구성을 구축합니다.

섀시 구성 가져오기 또는 내보내기

구성 내보내기 기능을 사용하여 섀시 구성 설정이 들어 있는 XML 파일을 로컬 컴퓨터로 내보낼 수 있습니다. 나중에 해당 구성 파일을 가져와서 구성 설정을 섀시에 빠르게 적용하여, 알려진 정상적인

구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다. 사전 요건이 충족되는 경우, 섀시 구성을 새 섀시로 가져올 수도 있습니다(예: RMA).

내보내는 경우 섀시 구성만 내보냅니다. 인스턴스 구성 설정은 내보내지지 않습니다. 디바이스 백업/복원 기능을 사용하여 인스턴스를 별도로 백업해야 합니다.

가져오면 섀시의 모든 기존 컨피그레이션이 가져오기 파일의 구성으로 교체됩니다.

시작하기 전에

구성을 가져오려는 섀시의 경우 다음 특성이 일치해야 합니다.

- 동일한 섀시 소프트웨어 버전
- 동일한 threat defense 인스턴스 이미지
- 동일한 네트워크 모듈

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**의 **Chassis(**섀시**)** 열에서 **Manage(**관리**)**를 클릭하거나 편집 (✎)를 클릭합니다.

그림 ***38:*** 섀시 관리

섀시에 대한 **Chassis Manager(**섀시 관리자**)** 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

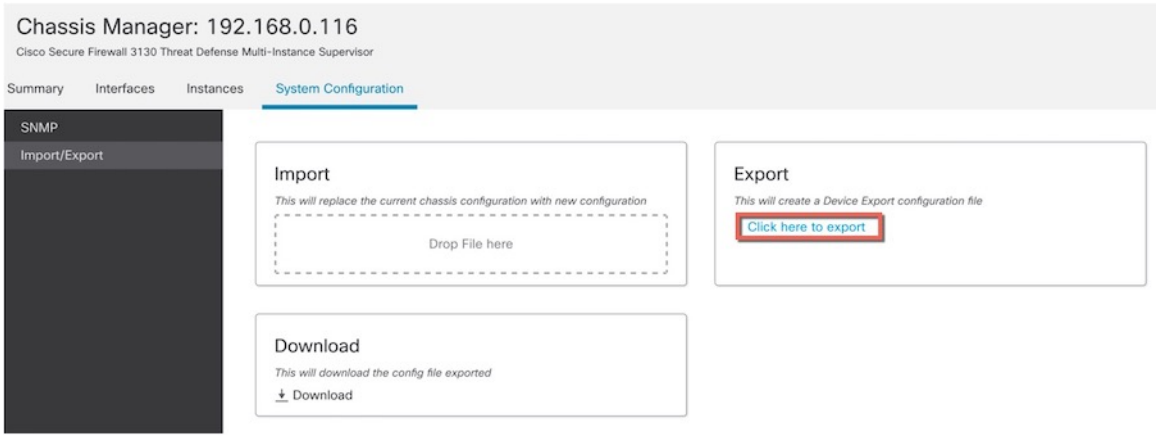
단계 **2** 시스템 구성을 클릭합니다.

단계 **3** **Import/Export(**가져오기/내보내기**)**를 클릭합니다.

단계 **4** 구성을 내보내려면 다음 단계를 수행합니다.

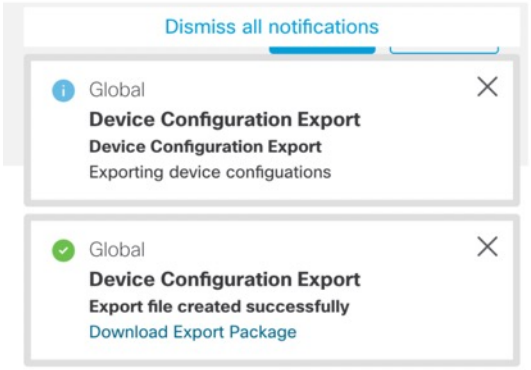
a) **Export** (내보내기) 영역에서 **Click here to export**(내보내려면 여기를 클릭)를 클릭합니다.

그림 ***39:*** 내보내기 파일 생성



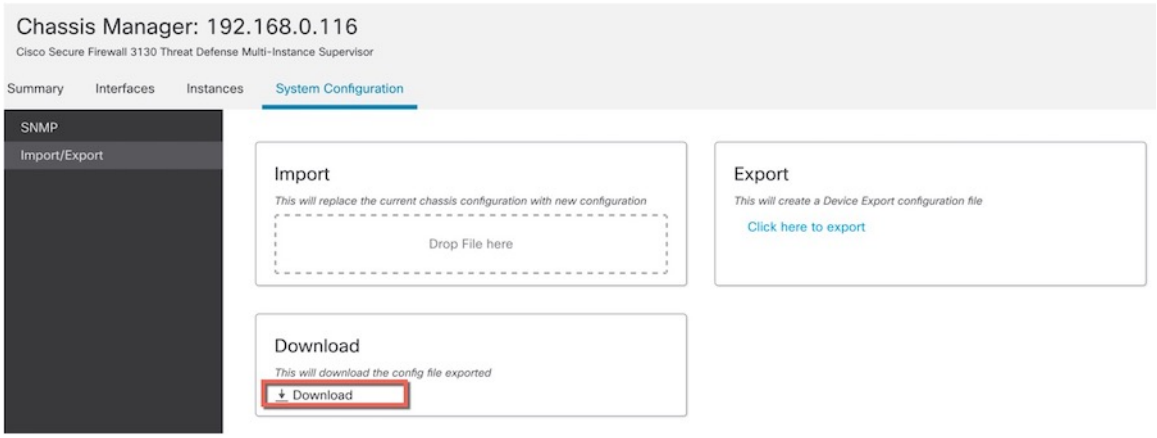
b) **Export file created successfully** 메시지에 대한 알림을 모니터링합니다.

그림 ***40:*** 내보내기 파일 생성 성공



c) 알림 메시지(**Download Export Package**(내보내기 패키지 다운로드))를 클릭하거나 Download(다운로드) 를 클릭하여 내보내기 파일을 다운로드합니다.

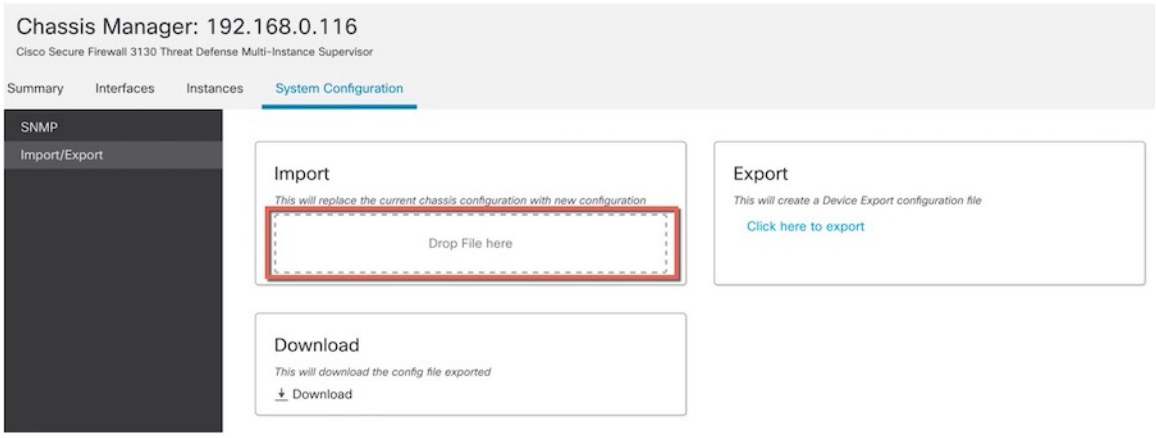
그림 ***41:*** 다운로드



파일은 **.sfo** 확장자로 저장됩니다.

단계 **5** 구성을 가져오려면 **.sfo** 파일을 **Import(**가져오기**)** > **Drop File here(**여기로 파일 끌어다놓기**)** 영역으로 끌어옵니다.

그림 *42:* 가져오기



섀시 플랫폼 설정 구성

섀시 플랫폼 설정에서는 섀시 관리를 위한 다양한 기능을 구성합니다. 여러 섀시 간에 정책을 공유할 수 있습니다. 섀시마다 다른 설정을 원하는 경우에는 여러 정책을 생성해야 합니다.

섀시 플랫폼 설정 정책 생성

플랫폼 설정 정책을 관리하려면 **Platform Settings(**플랫폼 설정**)** 페이지(**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**)를 사용합니다. 이 페이지는 각 정책에 대한 디바이스 유형을 나타냅니다. **Status(**상태**)** 열에는 정책에 대한 디바이스 대상이 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택합니다.

단계 **2** 기존 정책의 경우, **Copy(**복사**)** ( ), 편집 ( ) 또는 **Delete(**삭제**)** ( ) 정책을 사용할 수 있습니다.

주의 대상 디바이스에 마지막으로 구축한 정책은 최신 상태가 아니더라도 삭제할 수 없습니다. 정책을 완전히 삭제하기 전에 다른 정책을 해당 대상에 구축하는 것이 좋습니다.

단계 **3** 새 정책을 생성하려면 **New Policy(**새 정책**)**를 클릭합니다.

a) 드롭다운 목록에서 **Chassis Platform Settings** (섀시 플랫폼 설정)를 선택합니다.

b) 새 정책의 이름을 입력하고 선택적으로 설명을 입력합니다.

c) 필요에 따라 정책을 적용할 **Available Chassis(**사용 가능한 섀시**)**를 선택하고 **Add(**추가**)**를 클릭하거나 드래그 앤 드롭하여 선택한 섀시를 추가합니다. **Search(**검색**)** 필드에 검색 문자열을 입력하여 섀시 목록을 좁힐 수 있습니다.

d) **Save(**저장**)**를 클릭합니다.

시스템이 정책을 생성하고 편집을 위해 엽니다.

단계 **4** 정책의 대상 섀시를 변경하려면 편집할 플랫폼 설정 정책 옆의 편집 ( )을 클릭합니다

a) **Policy Assignment(**정책 할당**)**를 클릭합니다.

b) 정책에 섀시를 할당하려면 **Available Chassis** (사용 가능한 섀시) 목록에서 섀시를 선택하고 **Add**(추가)를 클릭합니다. 아니면 끌어서 놓을 수도 있습니다.

c) 섀시 할당을 제거하려면 **Selected Chassis** (선택한 섀시) 목록의 섀시 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

d) **OK(**확인**)**를 클릭합니다.

DNS 구성

섀시에서 호스트 이름의 IP 주소를 확인해야 하는 경우 DNS 서버를 지정해야 합니다. 이러한 섀시 DNS 설정은 디바이스 플랫폼 설정에서 설정되는 인스턴스별 DNS 설정과는 별개입니다.

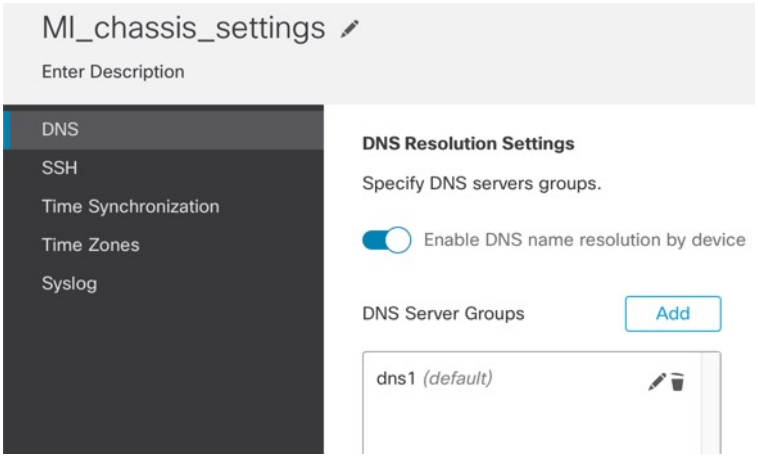
여러 DNS 서버를 구성할 때 섀시는 임의의 순서로 서버를 사용합니다. 4개의 DNS 서버 그룹에 최대 4개의 서버를 설정할 수 있습니다. 예를 들어 단일 서버 그룹을 4개의 서버로 구성하거나 4개의 서버 그룹을 각각 한 개씩 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 섀시 정책을 생성하거나 편집합니다.

단계 **2** **DNS**를 선택합니다.

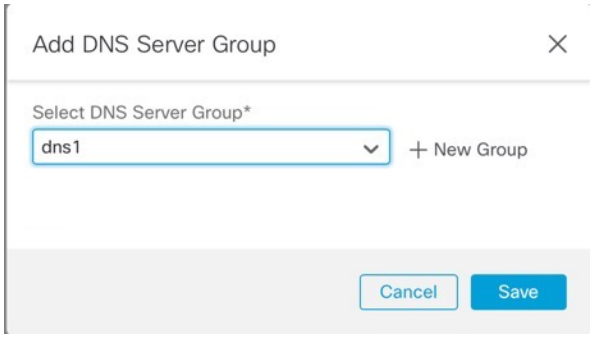
그림 ***43: DNS***



단계 **3** **Enable DNS name resolution by device(**디바이스로 **DNS** 이름 확인 활성화**)** 슬라이더를 활성화합니다.

단계 **4** **Add(**추가**)**를 클릭하여 DNS 서버 그룹을 추가합니다.

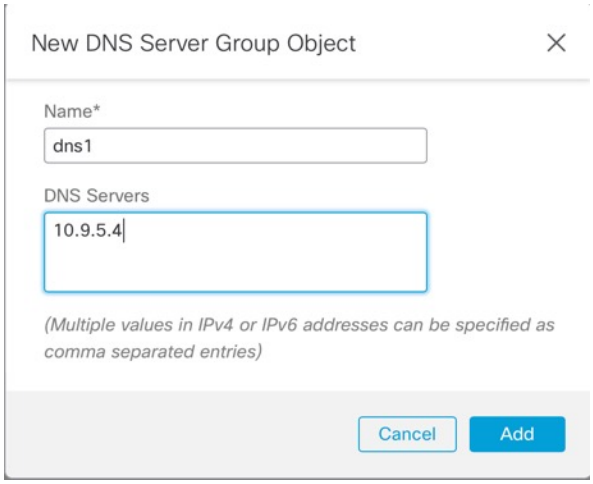
그림 ***44: DNS*** 서버 그룹 추가



단계 **5** 기존 DNS 서버 그룹을 선택하거나(DNS 서버 그룹 개체 생성참조) + 새 그룹을 클릭합니다.

새 그룹을 추가하는 경우, 다음 대화 상자가 표시됩니다. 이름과 최대 4개의 DNS 서버 IP 주소를 쉼표로 구분된 값으로 제공하고 **Add**(추가)를 클릭합니다.

그림 ***45:*** 새로운 ***DNS*** 서버 그룹 개체



단계 **6** **Save**(저장)를 클릭하여 DNS 서버를 목록에 추가합니다.

단계 **7** 이 단계를 반복하여 서버 그룹을 추가합니다.

모든 그룹을 합해 최대 4개의 DNS 서버만 식별합니다.

단계 **8** **Save(**저장**)**를 클릭하여 정책의 변경 사항을 모두 저장합니다.

SSH 및 SSH 액세스 목록 구성

관리 인터페이스에서 섀시로의 SSH 세션을 허용하려면 SSH 서버를 활성화하고 허용되는 네트워크를 구성합니다.

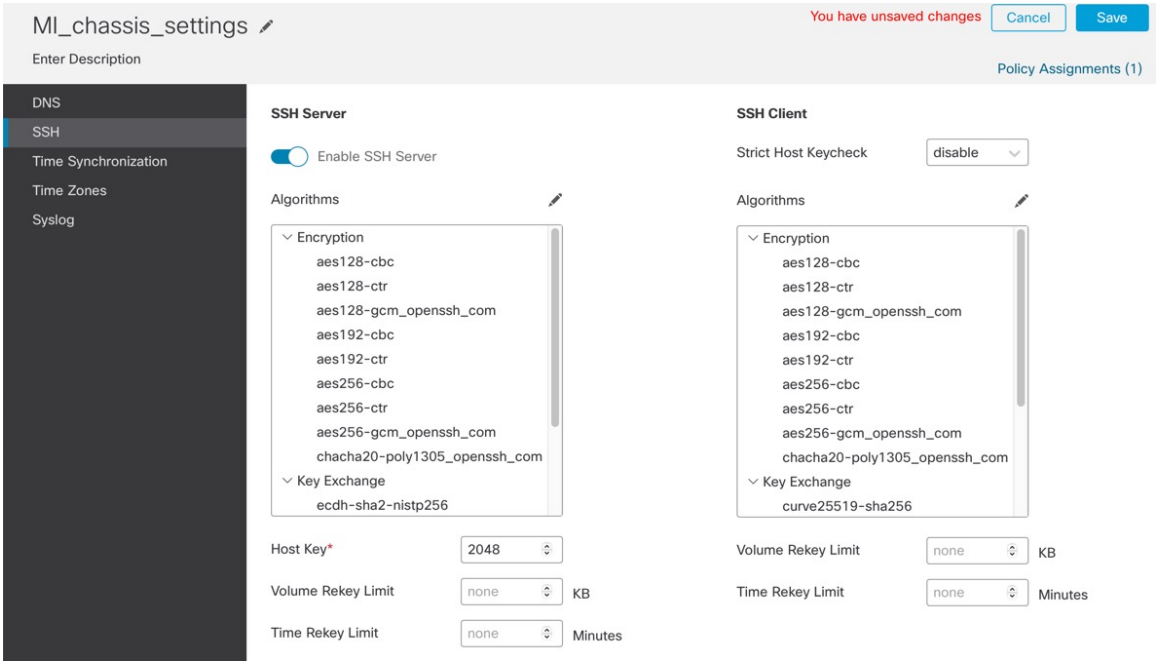
프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 섀시 정책을 생성하거나 편집합니다.

단계 2 **SSH**를 선택합니다.

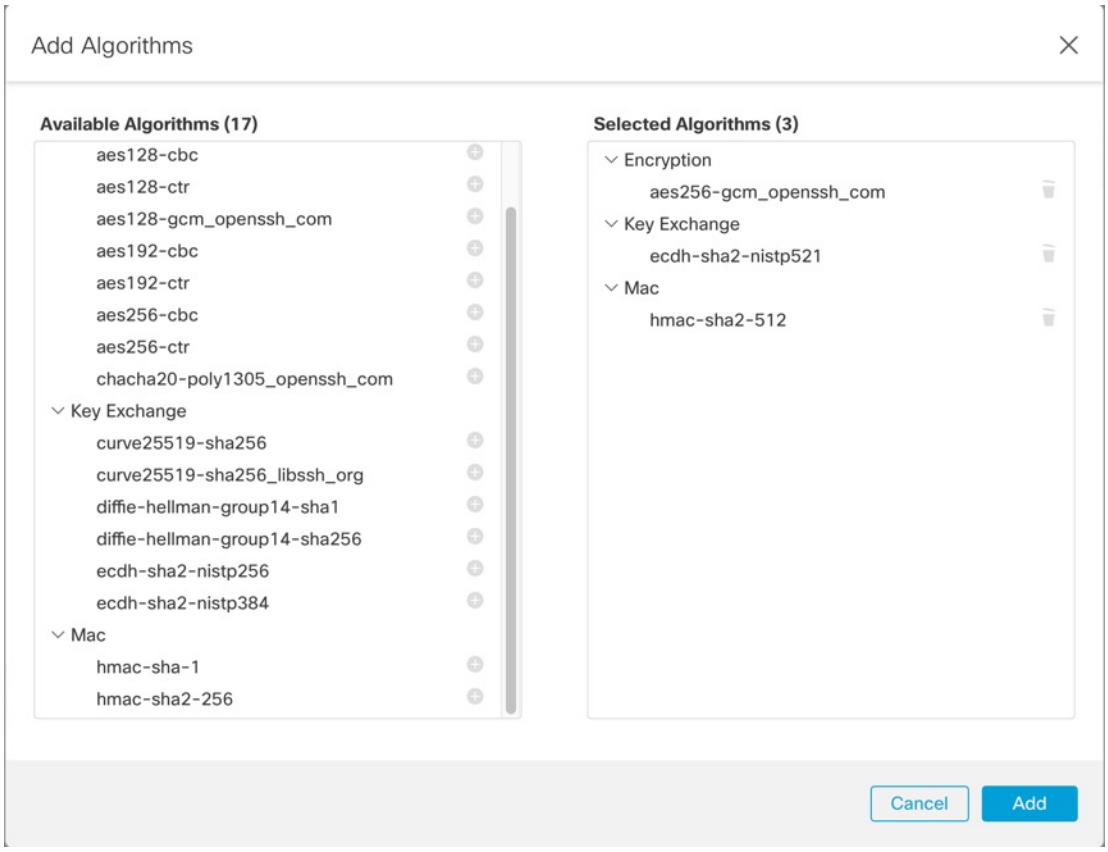
단계 3 섀시에 대한 SSH 액세스를 활성화하려면 **Enable SSH Server(SSH** 서버 활성화**)** 슬라이더를 선택합니다.

그림 ***46: SSH***



단계 4 허용되는 알고리즘을 설정하려면 편집 (✎)를 클릭합니다.

그림 47: □알고리즘추가



a) 암호화 알고리즘을 선택합니다.
b) 키 교환 알고리즘을 선택합니다.

   키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 수행합니다. 이 키 교환 방식은 명시적 서버 인증을 수행합니다.

c) **Mac** 무결성 알고리즘을 선택합니다.

단계 **5** **Host Key(**호스트 키**)**에 대해 RSA 키 쌍에 대한 모듈러스 크기를 입력합니다.

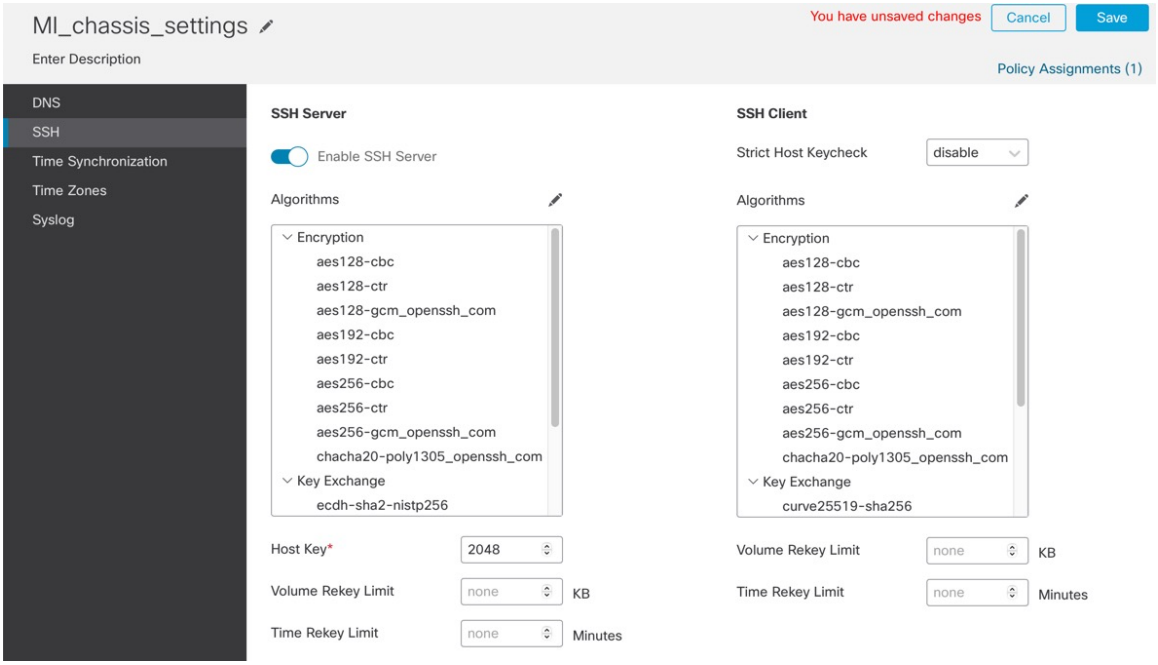
모듈러스 값(비트 단위)은 1024~2048 범위의 8의 배수입니다. 지정하는 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 오래 걸립니다. 권장되는 값은 2048입니다.

단계 **6** 서버의 **Volume Rekey Limit(**볼륨 재생성 제한**)**에 대해 FXOS가 세션에서 연결을 해제하기 전에 연결을 통해 허용되는 트래픽 양(KB 단위)을 설정합니다.

단계 **7** 서버의 **Time Rekey Limit(**시간 키 재생성 제한**)**에 대해 FXOS가 세션에서 연결을 해제하기 전에 SSH 세션이 유휴 상태가 될 수 있는 시간(분 단위)을 설정합니다.

단계 **8** **SSH Client(SSH** 클라이언트**)**에 대해 다음 설정을 구성합니다.

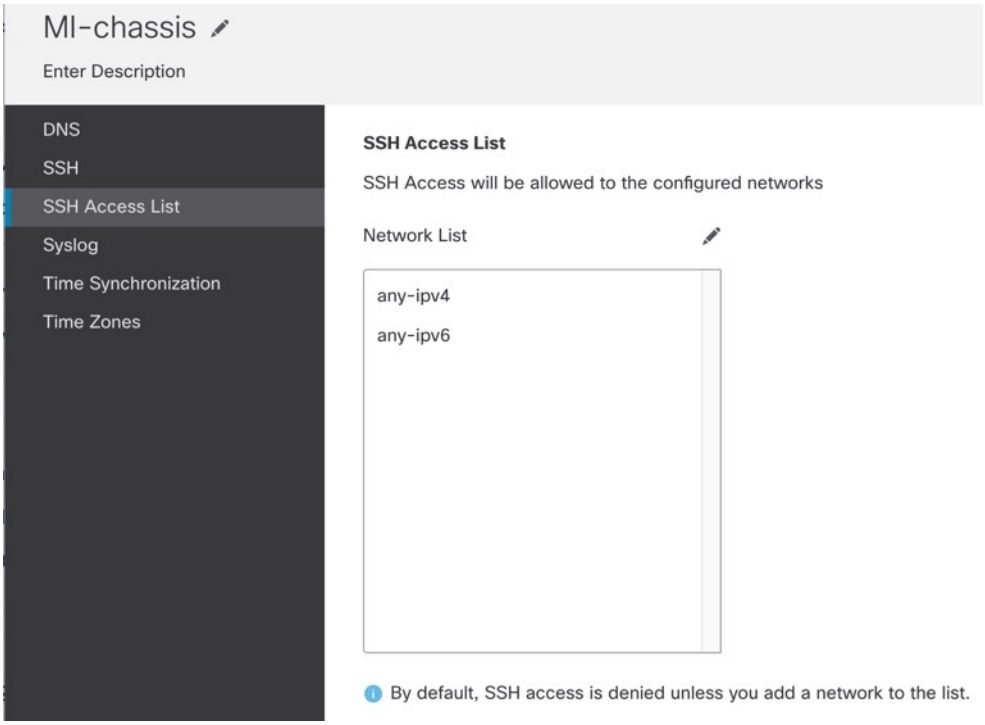
그림 *48: SSH*



- **Strict Host Keycheck(**엄격한 호스트 키 확인**) - enable(**활성화**)**, **disable(**비활성화**)** 또는 **prompt(**프롬프트**)**를 선택하여 SSH 호스트 키 확인을 제어합니다.
  - **enable(**활성화**)** — 호스트 키가 FXOS의 알려진 호스트 파일에 없는 경우 연결이 거부됩니다. 시스템/서비스 범위에서 **enter ssh-host** 명령을 사용하여 FXOS CLI에서 호스트를 수동으로 추가해야 합니다.
  - **prompt(**프롬프트**)** — 호스트 키가 섀시에 저장되어 있지 않은 경우 호스트 키를 수락하거나 거부하라는 프롬프트가 표시됩니다.
  - **disable(**비활성화**)** - (기본값) 이전에 저장한 호스트 키가 없는 경우 섀시가 호스트 키를 자동으로 수락합니다.
- 알고리즘 - 편집 (✎)를 클릭한 다음 **Encryption(**암호화**)** , **Key Exchange(**키 교환**)** 및 **Mac** 알고리즘을 선택합니다.
- **Volume Rekey Limit(**볼륨 키 재생성 제한**)** - FXOS가 세션에서 연결을 해제하기 전에 연결을 통해 허용되는 트래픽 양(KB 단위)을 설정합니다.
- **Time Rekey Limit(**시간 키 재생성 제한**)** - FXOS가 세션에서 연결을 해제하기 전에 SSH 세션이 유휴 상태가 될 수 있는 시간(분 단위)을 설정합니다.

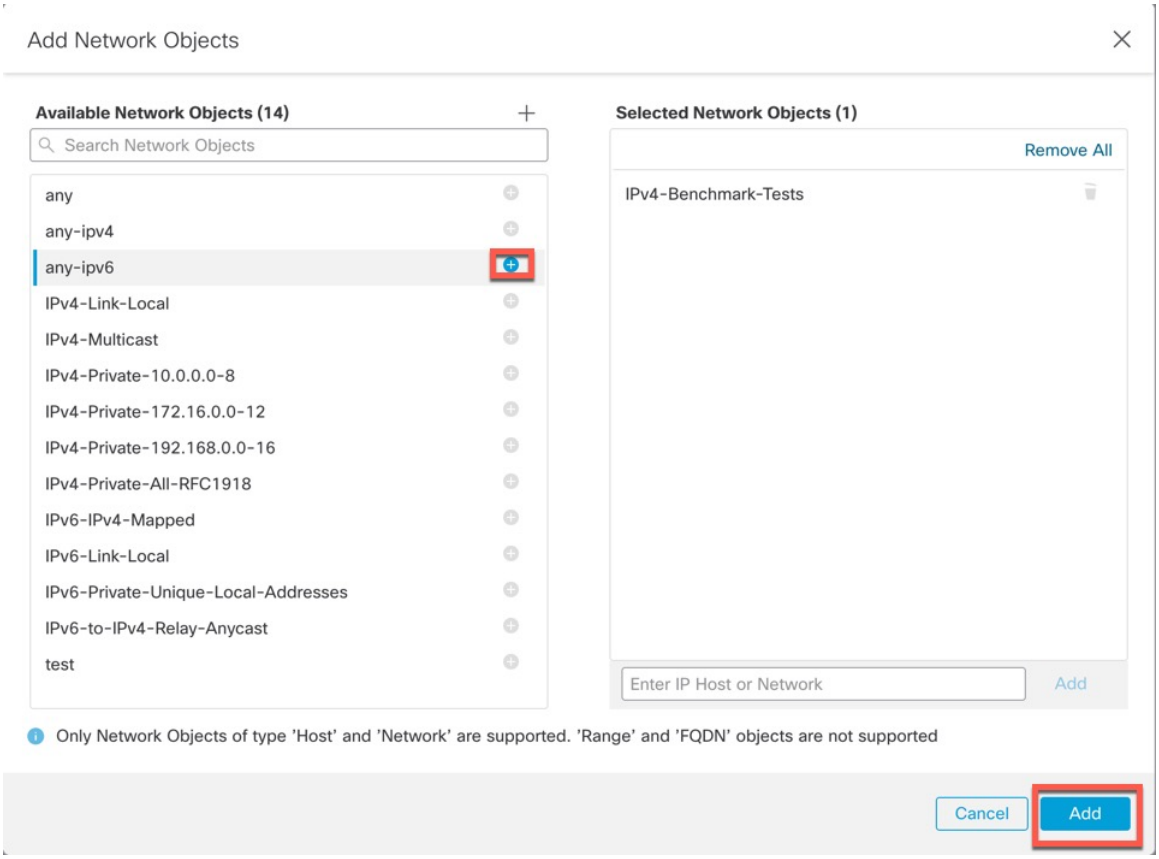
단계 **9** **SSH Access List(SSH** 액세스 목록**)**를 선택합니다. SSH를 사용하려면 IP 주소 또는 네트워크에 대한 액세스를 허용해야 합니다.

그림 *49: SSH* 액세스 목록



단계 **10** 편집 (✎)를 클릭하여 네트워크 개체를 추가하고 **Save(**저장**)**를 클릭합니다. 수동으로 IP 주소를 입력할 수도 있습니다.

그림 50: 네트워크 개체



단계 **11** **Save(**저장**)**를 클릭하여 정책의 변경 사항을 모두 저장합니다.

Syslog 설정

새시에서 syslog를 활성화할 수 있습니다. 이러한 시스템 로그는 새시의 FXOS 운영 체제에서 제공됩니다.

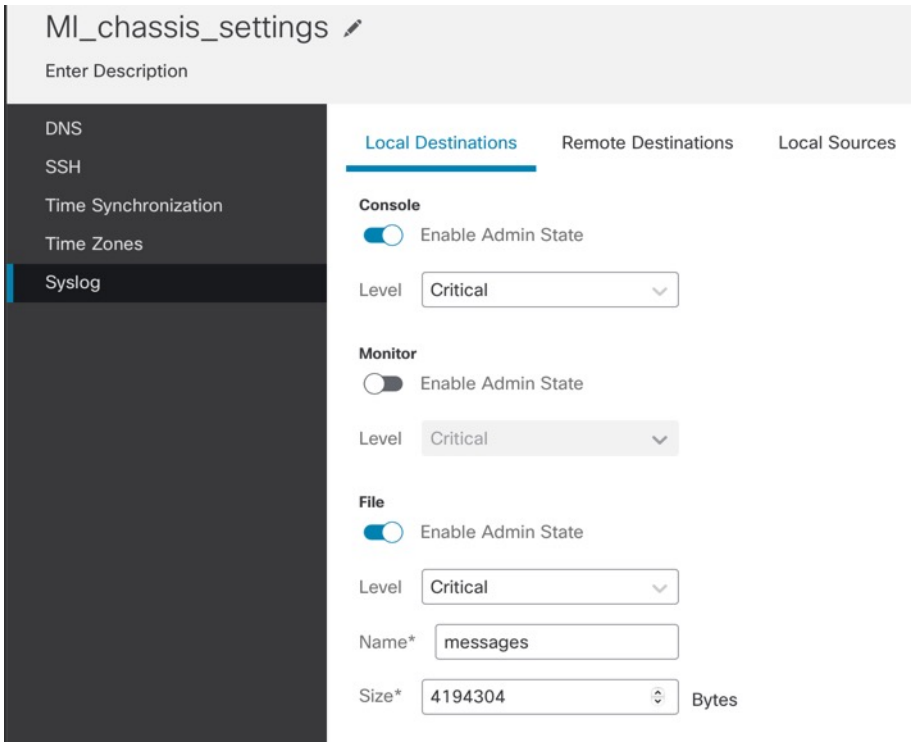
프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 새시 정책을 생성하거나 편집합니다.

단계 **2** **Syslog(**시스템 로그**)**를 선택합니다.

단계 **3** **Local Destinations(**로컬 대상**)** 탭을 클릭하고 다음 필드를 입력합니다.

그림 ***51:*** 시스템 로그 로컬 대상

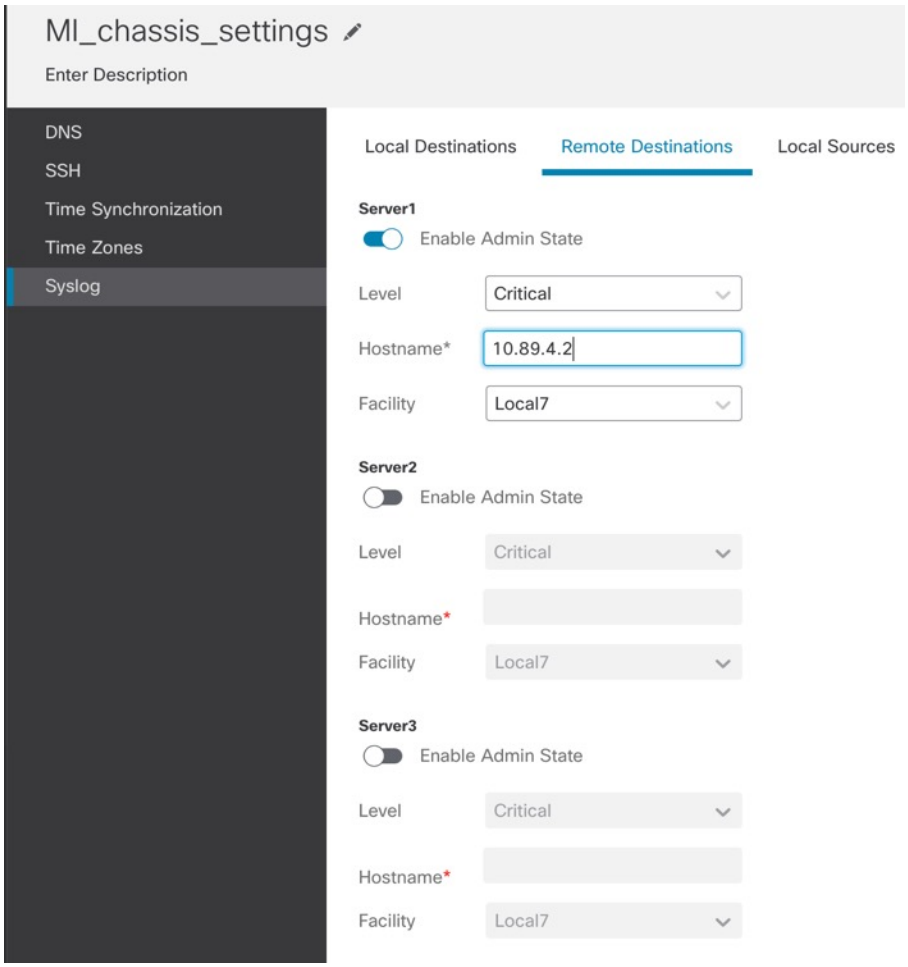


이름	설명
Console(콘솔**)** 섹션	
Admin State(관리 상태**)** 필드	섀시가 콘솔에 syslog 메시지를 표시하는지 여부. 콘솔에 syslog 메시지를 표시하고 로그에 추가하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다. **Enable(**활성화**)** 확인란이 선택되지 않은 경우, syslog 메시지는 로그에 추가되지만 콘솔에 표시되지 않습니다.
Level(레벨**)** 필드	**Console - Admin State(**콘솔 **-** 관리 상태**)**의 **Enable(**활성화**)** 확인란을 선택한 경우, 콘솔에 표시할 가장 낮은 메시지 수준을 선택합니다. 섀시가 콘솔에 해당 레벨 이상의 메시지를 표시합니다. 다음 중 하나일 수 있습니다. • **Emergencies** • **Alerts** • **Critical**
Monitor(모니터**)** 섹션	

이름	설명
Admin State(관리 상태**)** 필드	섀시가 모니터에 syslog 메시지를 표시하는지 여부. 모니터에 syslog 메시지를 표시하고 로그에 추가하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다. **Enable(**활성화**)** 확인란이 선택되지 않은 경우, syslog 메시지는 로그에 추가되지만 모니터에 표시되지 않습니다.
Level(수준**)** 드롭다운 목록	**Monitor - Admin State(**모니터 - 관리 상태**)**의 **Enable(**활성화**)** 확인란을 선택한 경우, 모니터에 표시할 가장 낮은 메시지 수준을 선택합니다. Firepower 섀시는 모니터에 해당 수준 이상의 메시지를 표시합니다. 다음 중 하나일 수 있습니다. • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information(**정보**)** • **Debugging**

단계 **4** **Remote Destination(**원격 대상**)** 탭에서, 섀시에서 생성된 메시지를 저장할 수 있는 최대 3개의 외부 로그에 대해 다음 필드를 입력합니다.

그림 52: 시스템 로그 원격 대상



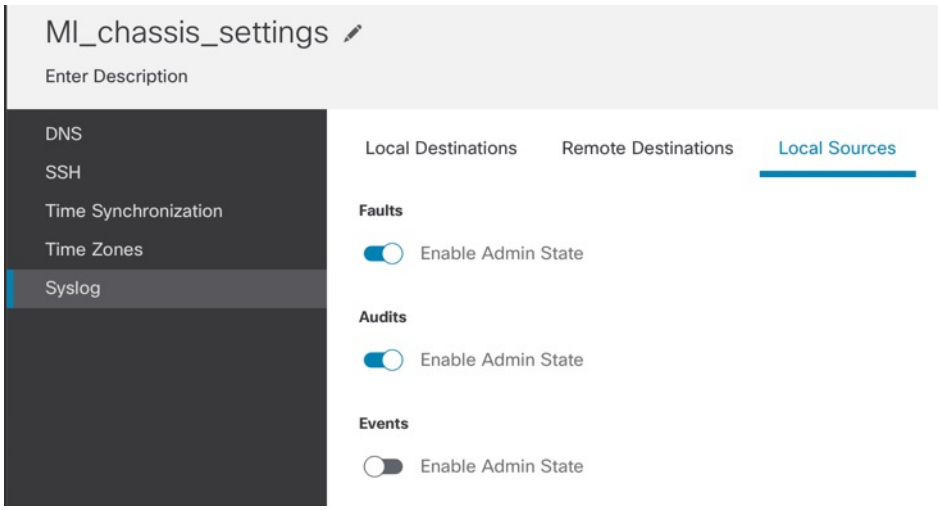
원격 대상에 syslog 메시지를 전송하여 외부 syslog 서버의 사용 가능한 디스크 공간에 따라 메시지를 보관할 수 있으며, 저장한 후에 로그 데이터를 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

이름	설명
Admin State(관리 상태**)** 필드	원격 로그 파일에 syslog 메시지를 저장하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다.

이름	설명
Level(수준**)** 드롭다운 목록	시스템에서 저장할 가장 낮은 메시지 수준을 선택합니다. 시스템은 원격 파일에 해당 수준 이상의 메시지를 저장합니다. 다음 중 하나일 수 있습니다. • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information(**정보**)** • **Debugging**
Hostname/IP Address(호스트 이름**/IP** 주소**)** 필드	원격 로그 파일이 있는 호스트 이름 또는 IP 주소입니다. 참고 IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.
Facility(기능**)** 드롭다운 목록	파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다. 다음 중 하나일 수 있습니다. • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

단계 **5** **Local Sources(**로컬 소스**)** 탭을 클릭하고 다음 필드를 입력합니다.

그림 **53:** 시스템 로그 로컬 소스



이름	설명
Faults(결함**)** > **Enable Admin State(**관리 상태 활성화**)**	시스템 결함 로깅을 활성화합니다.
Audits(감사**)** > **Enable Admin State(**관리 상태 활성화**)**	감사 로그를 활성화합니다.
Events(이벤트**)** > **Enable Admin State(**관리 상태 활성화**)**	시스템 이벤트 로깅을 활성화합니다.

단계 **6** **Save(**저장**)**를 클릭하여 정책의 변경 사항을 모두 저장합니다.

시간 동기화 구성

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용합니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다. 최대 4개까지 NTP 서버를 구성할 수 있습니다.

참고

- FXOS는 NTP 버전 3을 사용합니다.
- 외부 NTP 서버의 stratum 값이 13 이상인 경우 애플리케이션 인스턴스는 FXOS 섀시의 NTP 서버와 동기화할 수 없습니다. NTP 클라이언트가 NTP 서버와 동기화될 때마다 stratum 값이 1씩 증가합니다.

  자체 NTP 서버를 설정한 경우, 서버의 /etc/ntp.conf 파일에서 해당 계층 값을 찾을 수 있습니다. NTP 서버의 stratum 값이 13 이상인 경우 ntp.conf 파일에서 stratum 값을 변경하고 서버를 다시 시작하거나 다른 NTP 서버(예: pool.ntp.org)를 사용할 수 있습니다.

시작하기 전에

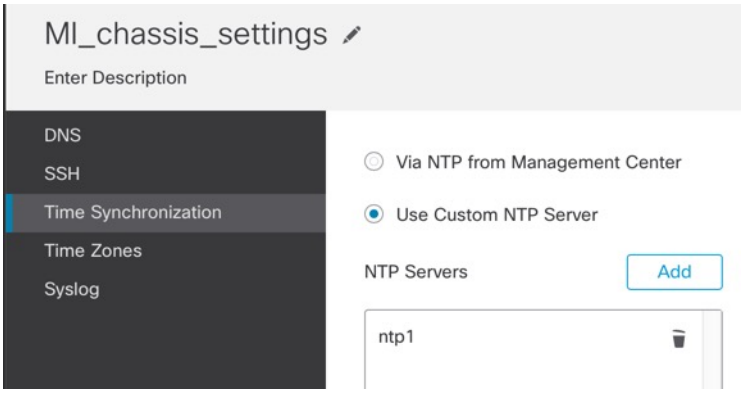
NTP 서버의 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다. DNS 구성, 46 페이지를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 새시 정책을 생성하거나 편집합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 선택합니다.

그림 ***54:*** 시간 동기화



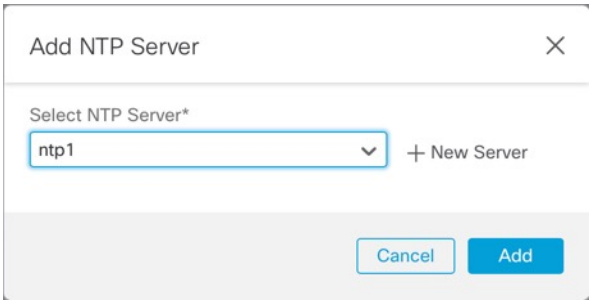
단계 **3** management center에서 시간을 가져 오려면 **Via NTP from Management Center(Management Center**에서 **NTP**를 통해)를 클릭합니다.

이 옵션을 사용하면 와 새시의 management center 모두 같은 시간을 가질 수 있습니다.

단계 **4** 외부 NTP 서버를 사용 하려면 **Use Custom NTP Server**(맞춤형 NTP 서버 사용) 를 클릭합니다.

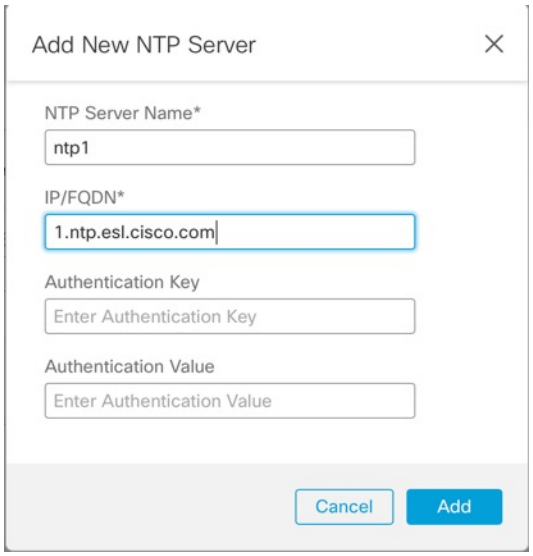
a) **Add(**추가**)**를 클릭하여 서버를 추가합니다.

그림 ***55: NTP*** 서버 추가



b) 드롭다운 메뉴에서 이미 정의된 서버를 선택하고 Add(추가) 를 클릭하거나 + **New Server** (새 서버)를 클릭하여 새 서버를 추가합니다.

그림 *56:* 새 *NTP* 서버 추가



c) 새 서버의 경우 다음 필드를 입력하고 **Add**(추가)를 클릭합니다.

- **NTP** 서버 이름— 이 서버를 식별하기 위한 이름입니다.
- **IP/FQDN** - 서버의 IP 주소 또는 호스트 이름입니다.
- 인증 키 및 인증 값- NTP 서버에서 키 ID와 값을 가져옵니다. 예를 들어 OpenSSL이 설치된 NTP 서버 버전 4.2.8p8 이상에서 SHA1 키를 생성하려면 **ntp-keygen -M** 명령을 입력한 다음 ntp.keys 파일에서 키 ID 및 값을 확인합니다. message digest를 계산할 때 어떤 키 값을 사용할지를 클라이언트 및 서버에 알려줄 때 키 ID가 사용됩니다.

  NTP 서버 인증에는 SHA1만 지원됩니다.

단계 **5** **Save(**저장**)**를 클릭하여 정책의 변경 사항을 모두 저장합니다.

표준 시간대 구성

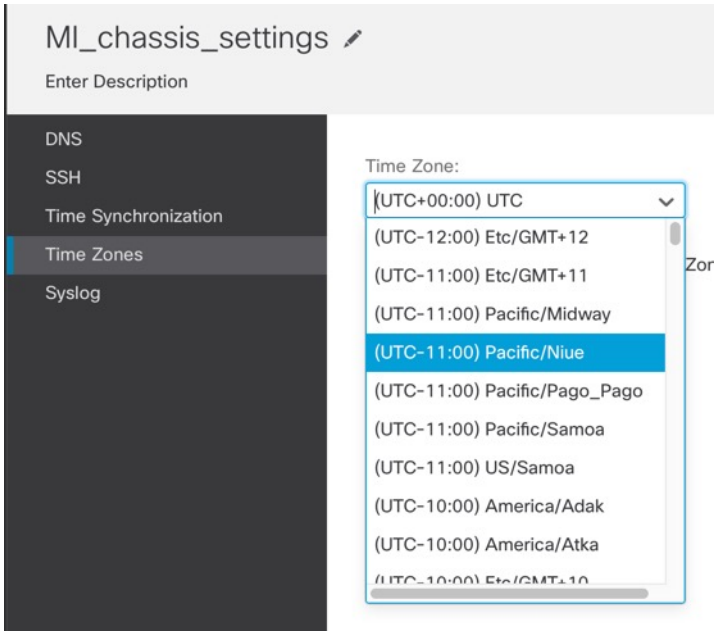
새시의 표준 시간대를 설정합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 새시 정책을 생성하거나 편집합니다.

단계 **2** 표준 시간대를 선택합니다.

그림 *57:* 표준 시간대



단계 **3** 드롭다운 메뉴에서 **Time Zone(**표준 시간대**)**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭하여 정책의 변경 사항을 모두 저장합니다.

멀티 인스턴스 모드 관리

이 섹션에서는 FXOS CLI에서 설정 변경 또는 섀시에 할당된 인터페이스 변경 등 일반적이지 않은 작업에 대해 설명합니다.

인스턴스에 할당된 인터페이스 변경

인스턴스에 인터페이스를 할당 또는 할당 해제할 수 있습니다. 새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 인스턴스 구성에 미치는 영향은 아주 적습니다. 인스턴스에 영향을 주지 않고 할당된 EtherChannel의 멤버십을 편집할 수도 있습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다.

액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 인스턴스 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다.

보안 영역을 참조하는 정책은 영향을 받지 않습니다.

참고 고가용성을 위해 다른 유닛에 대해 동일한 인터페이스를 변경해야 합니다. 그렇지 않으면 고가용성이 올바르게 작동하지 않을 수 있습니다.

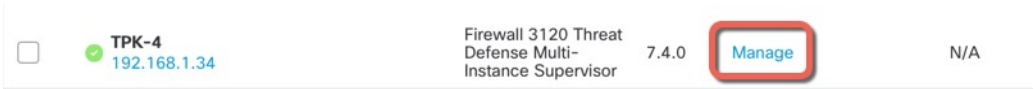
시작하기 전에

- 인스턴스 구성, 18 페이지에 따라 인터페이스를 구성합니다.
- 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 인스턴스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 인스턴스에 EtherChannel을 할당할 수 있습니다.

프로시저

단계 **1** **Devices**(디바이스) > **Device Management**(디바이스 관리)의 **Chassis**(섀시) 열에서 **Manage**(관리)를 클릭하거나 편집 (✎)를 클릭합니다.

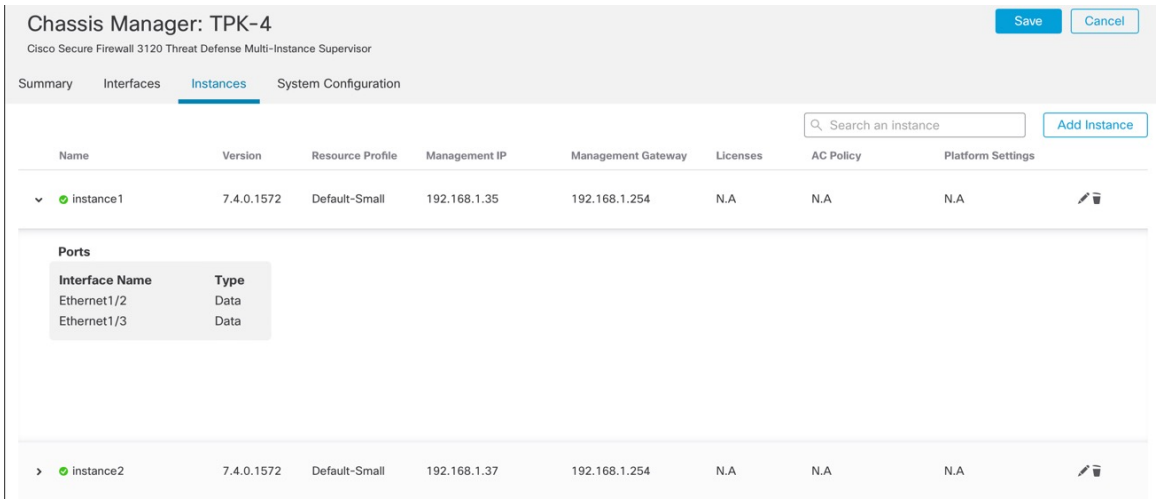
그림 ***58:*** 섀시 관리



섀시에 대한 **Chassis Manager**(섀시 관리자) 페이지가 열리고 **Summary**(요약) 페이지가 표시됩니다.

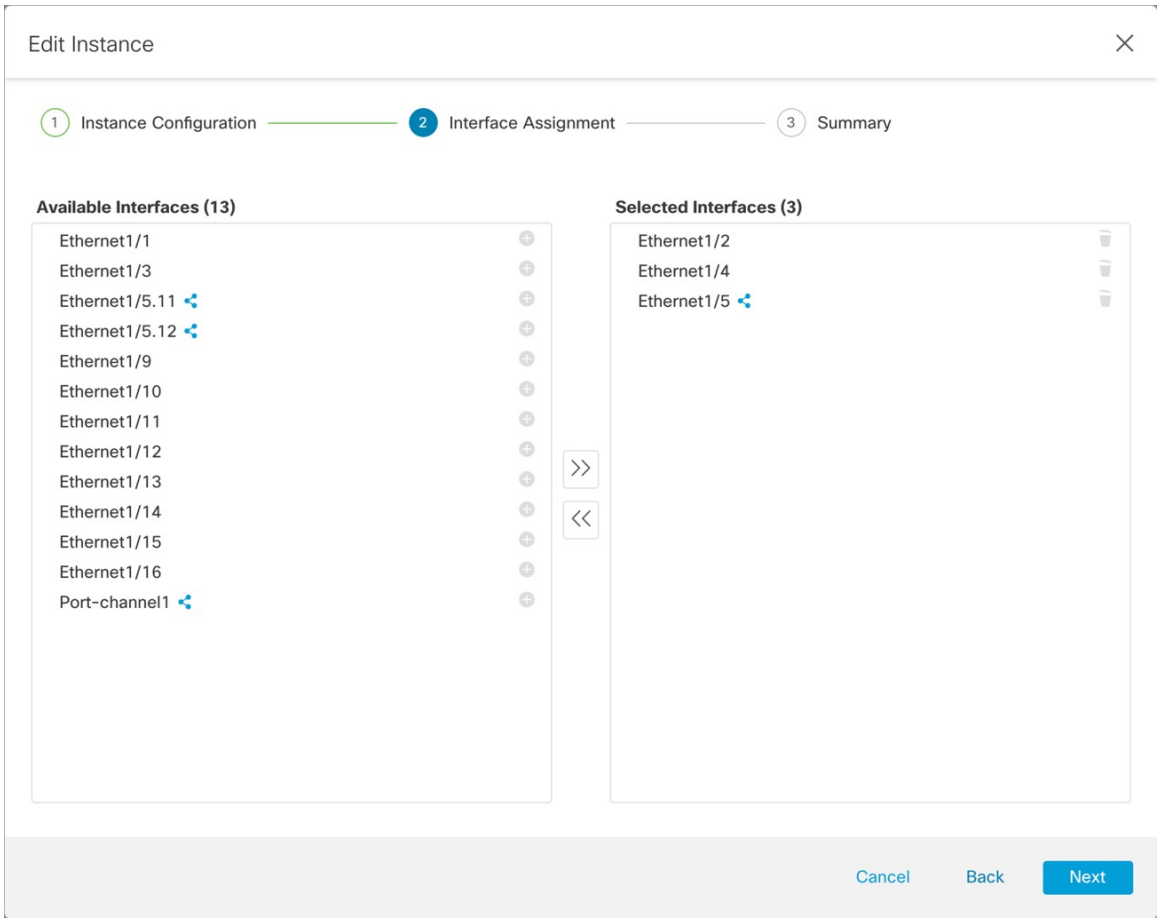
단계 **2** **Instances**(인스턴스)를 클릭하고 인터페이스를 변경할 인스턴스 옆에 있는 편집 (✎) 를 클릭합니다.

그림 ***59:*** 인스턴스



단계 **3** **Interface Assignment** (인터페이스 할당) 화면이 표시될 때까지 **Next** (다음)를 클릭합니다.

그림 60: 인터페이스 할당



공유 인터페이스는 공유 아이콘( )을 표시합니다.

단계 4 인터페이스를 변경하고 **Next**(다음)를 클릭합니다.

단계 5 **Summary**(요약) 화면에서 **Save**(저장)를 클릭합니다.

단계 6 고가용성을 위해 다른 유닛에 대해 동일한 인터페이스를 변경해야 합니다. 그렇지 않으면 고가용성이 올바르게 작동하지 않을 수 있습니다.

FXOS CLI에서 섀시 관리 설정 변경

섀시 관리 인터페이스 IP 주소 및 게이트웨이를 변경하거나, 새 관리자로 management center를 변경하거나, 관리자 비밀번호를 변경하거나, 멀티 인스턴스 모드를 비활성화하려는 경우 FXOS CLI를 사용하면 됩니다.

프로시저

단계 1 섀시 콘솔 포트에 연결합니다.

콘솔 포트는 FXOS CLI에 연결됩니다.

참고 콘솔 포트를 사용하는 것이 좋습니다. management center의 섀시 플랫폼 설정에서 구성한 경우 SSH를 사용하여 관리 인터페이스에 연결할 수도 있습니다. 그러나 관리 IP 주소를 변경할 경우 연결이 끊어집니다.

단계 **2** 초기 설정 시 사용자 이름 **admin**과 비밀번호를 사용해 로그인합니다.

단계 **3** 관리 IP 주소를 변경합니다. 고정 IPv4 또는 IPv6 주소를 사용할 수 있습니다.

IPv4:

scope fabric-interconnect

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

IPv6:

scope fabric-interconnect

scope ipv6-config

set out-of-band static ipv6 *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

예제**:**

IPv4:

```
firepower-3110# scope fabric-interconnect
firepower-3110 /fabric-interconnect # set out-of-band static ip 10.5.23.8 netmask
255.255.255.0
gw 10.5.23.1
```

IPv6:

```
firepower-3110# scope fabric-interconnect
firepower-3110 / fabric-interconnect # scope ipv6-config
firepower-3110 / fabric-interconnect /ipv6-config # set out-of-band static ipv6 2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

단계 **4** management center를 변경합니다.

먼저 현재 management center에서 섀시의 등록을 해제해야 합니다.

enter device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

등록 키를 입력하라는 메시지가 표시됩니다.

모든 범위에서 이 명령을 입력할 수 있습니다.

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—management center의 FQDN 또는 IP 주소를 지정합니다. 하나 이상의 디바이스(management center 또는 섀시)에는 두 디바이스 간 양방향 TLS-1.3 암호화 커뮤니케이션 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. **hostname**을 지정하지 않으면 섀시에 연결 가능한 IP 주소 또는 호스트 이름이 있어야 하며 **nat-id**를 지정해야 합니다.

- **nat-id** *nat_id* — 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 섀시를 등록할 때 management center에 지정할 고유한 일회용 문자열을 지정합니다. 이는 **hostname**을 지정하지 않은 경우 필요하지만, 호스트 이름 또는 IP 주소를 지정하는 경우에도 항상 NAT ID를 설정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다.
- **Registration Key:** *reg_key*—섀시를 등록할 때 management center에 지정할 일회용 등록 키를 입력하라는 메시지가 표시됩니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.

예제:

```
firepower-3110# enter device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

단계 **5** 관리자 비밀번호 변경합니다.

scope security

set password

비밀번호를 입력합니다. *password*

비밀번호를 확인합니다. *password*

예제:

```
firepower-3110# scope security
firepower-3110 /security # set password
Enter new password: Sw@nsong67
Confirm new password: Sw@nsong67
firepower-3110 /security #
```

단계 **6** 멀티 인스턴스 모드를 비활성화하고 시스템을 어플라이언스 모드로 다시 설정합니다.

scope system

set deploymode native

재부팅하라는 메시지가 나타납니다.

예제:

```
firepower-3110# scope system
firepower-3110 /system # set deploymode native
All configuration and bootable images will be lost and system will reboot.
If there was out of band upgrade, it might reboot with the base version and
need to re-image to get the expected running version.
Do you still want to change deploy mode? (yes/no):yes
firepower-3110 /system #
```

모드를 다시 멀티 인스턴스 모드로 변경하려면 **set deploymode container**를 입력합니다. **show system detail** 명령을 사용하면 현재 모드를 확인할 수 있습니다.

멀티 인스턴스 모드 모니터링

이 섹션은 멀티 인스턴스 모드 새시 및 인스턴스의 문제를 해결하고 진단하는 데 도움이 됩니다.

멀티 인스턴스 구성 모니터링

시스템 세부 사항 표시

이 FXOS 명령은 현재 모드(네이티브 또는 컨테이너)를 표시합니다. 모드가 네이티브(어플라이언스 모드라고도 함)인 경우 멀티 인스턴스(컨테이너) 모드로 변환할 수 있습니다. 멀티 인스턴스 모드의 프롬프트/이름은 일반적인 "firepower-<model> " 반면 어플라이언스 모드의 프롬프트는 threat defense에 대해 설정한 호스트 이름입니다(기본값은 "firepower").

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

scope system > show

이 FXOS 명령은 현재 모드를 테이블 형식으로 표시합니다. 멀티 인스턴스 모드의 프롬프트/이름은 일반적인 "firepower-<model> " 반면 어플라이언스 모드의 프롬프트는 threat defense에 대해 설정한 호스트네임입니다.

```
firepower-3110# scope system
firepower-3110 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
    firepower-3110
               Stand Alone Container   10.89.5.42        ::


3110-1# scope system
3110-1 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
```

```
    ---------- ----------- ----------- ----------------- -------------------
    3110-1     Stand Alone Native      10.89.5.41        ::
3110-1 /system #
```

인스턴스 인터페이스 모니터링

show portmanager switch forward-rules hardware mac-filter

이 명령은 각 인스턴스에 전용 물리적 인터페이스가 할당된 두 인스턴스에 대한 내부 전환 전달 규칙을 보여줍니다. 이더넷 1/2는 ftd1에 할당되고 이더넷 1/1은 ftd2에 할당됩니다.

ECMP 그룹 1540은 ftd1에 할당되고 ECMP 그룹 1541은 ftd2에 할당됩니다.

```
secfw-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19       29164  0:0:0:0:0:0
2        0         19       0       19         17       67588  0:0:0:0:0:0
3        0          1       0      101       1541           0  a2:5b:83:0:0:15
4        0          1       0      101       1541        8181  ff:ff:ff:ff:ff:ff
5        0          2       0      102       1540           0  a2:5b:83:0:0:18
6        0          2       0      102       1540         431  ff:ff:ff:ff:ff:ff
7        0         17       0        0          0       11133  0:0:0:0:0:0
8        0         17       0        0          0           0  0:0:0:0:0:0
```

이 명령은 공유 물리적 인터페이스가 두 인스턴스에 할당된 상태로 인스턴스 2개에 대한 내부 전환 전달 규칙을 표시합니다. 이더넷 1/1은 ftd1과 ftd2 간에 공유됩니다.

ECMP 그룹 1540은 ftd1에 할당되고 ECMP 그룹 1541은 ftd2에 할당됩니다.

MCAST 그룹 4096은 ftd1과 ftd2 간의 브로드캐스트 트래픽을 복제하는 데 사용됩니다.

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19        2268  0:0:0:0:0:0
2        0         19       0       19         17        4844  0:0:0:0:0:0
3        0          1       0      101       1541           0  a2:5b:83:0:0:9
4        0          1       0      101       4096         546  ff:ff:ff:ff:ff:ff
5        0          1       0      101       1540           0  a2:5b:83:0:0:c
6        0         17       0        0          0        1263  0:0:0:0:0:0
7        0         17       0        0          0           0  0:0:0:0:0:0
```

이 명령은 공유 하위 인터페이스가 두 인스턴스 모두에 할당된 두 인스턴스에 대한 내부 전환 전달 규칙을 표시합니다. 이더넷 1/1.2452는 ftd1과 ftd2 간에 공유됩니다.

ECMP 그룹 1540은 ftd1에 할당되고 ECMP 그룹 1541은 ftd2에 할당됩니다.

MCAST 그룹 4097은 ftd1과 ftd2 간의 브로드캐스트 트래픽을 복제하는 데 사용됩니다.

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19       21305  0:0:0:0:0:0
2        0         19       0       19         17       50976  0:0:0:0:0:0
3     2452          1       0      101       1541         430  a2:5b:83:0:0:f
4     2452          1       0      101       4097           0  ff:ff:ff:ff:ff:ff
5     2452          1       0      101       1540           0  a2:5b:83:0:0:12
6        0         17       0        0          0       11038  0:0:0:0:0:0
7        0         17       0        0          0           0  0:0:0:0:0:0
```

show portmanager switch ecmp-groups 세부 정보

이 명령을 사용하여 각 인스턴스 Ecmp-Vport-Physical 포트 매핑 세부 정보를 나열합니다.

참고 Physical-Port 18은 내부 스위치와 인스턴스 간의 백플레인 업링크 인터페이스입니다.

```
firepower-3140(local-mgmt)# show portmanager switch ecmp-groups detail
       ECMP-GROUP  VPORT      PHYSICAL-PORT
1      1536        256        18
2      1537        257        18
3      1538        258        18
4      1539        259        18
5      1540        260        18
6      1541        261        18
7      1542        262        18
8      1543        263        18
9      1544        264        18
10     1545        265        18
```

show portmanager switch mcast-groups 세부 정보

MCAST 그룹 멤버십 세부 정보를 나열하려면 이 명령을 사용합니다.

```
firepower-3140(local-mgmt)# show portmanager switch mcast-groups detail
       MCAST-GROUP
1      4096
       Member-ports
       Ethernet 1/1
       ECMP-ID 1541
       ECMP-ID 1540
```

show portmanager counters mcast-groups

이 명령을 사용하여 MCAST 그룹 패킷 카운터를 확인합니다.

```
firepower-3140(local-mgmt)# show portmanager counters mcast-group 4096
PKT_CNT: 8106
```

portmanager counters ecmp 표시

ECMP 그룹 패킷 카운터를 확인하려면 이 명령을 사용합니다.

```
firepower-3140(local-mgmt)# show portmanager counters ecmp 1541
PKT_CNT: 430
```

멀티 인스턴스 모드 기록

표 *2:*

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Secure Firewall 3100의 멀티 인스턴스 모드.	7.4.1	7.4.1	Secure Firewall 3100을 단일 디바이스(어플라이언스 모드) 또는 여러 컨테이너 인스턴스(멀티 인스턴스 모드)로 구축할 수 있습니다. 멀티 인스턴스 모드에서는 완전히 독립적인 디바이스 역할을 하는 단일 섀시에 여러 컨테이너 인스턴스를 구축할 수 있습니다. 멀티 인스턴스 모드에서는 컨테이너 인스턴스(*Threat Defense* 업그레이드)와 별도로 운영 체제 및 펌웨어를 업그레이드합니다(섀시 업그레이드). 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Add(**추가**)** > **Chassis(**섀시**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Chassis Manager(**섀시 관리자**)** • **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **New Policy(**새 정책**)** > **Chassis Platform Settings(**섀시 플랫폼 설정**)** • **Devices(**디바이스**)** > **Chassis Upgrade(**섀시 업그레이드**)** 신규/수정된 Threat Defense CLI 명령: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** 신규/수정된 FXOS CLI 명령: **create device-manager**, **set deploymode** 플랫폼 제한: Secure Firewall 3105에서 지원되지 않습니다. 참조: Secure Firewall 3100의 멀티 인스턴스 모드 및 Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드