



논리적 디바이스

- 논리적 디바이스 정보, 1 페이지
- 논리적 디바이스의 요구 사항 및 사전 요구 사항, 10 페이지
- 논리적 디바이스 관련 지침 및 제한 사항, 19 페이지
- 독립형 논리적 디바이스 추가, 25 페이지
- 고가용성 쌍 추가, 38 페이지
- 클러스터 추가, 39 페이지
- Radware DefensePro 구성, 63 페이지
- TLS 암호화 가속화 구성, 69 페이지
- FTD 링크 상태 동기화를 활성화합니다., 72 페이지
- 논리적 디바이스 관리, 73 페이지
- 논리적 디바이스 페이지, 84 페이지
- 사이트 간 클러스터링 예시, 87 페이지
- 논리적 디바이스의 기록, 91 페이지

논리적 디바이스 정보

논리적 디바이스를 사용하면 애플리케이션 인스턴스 하나(ASA 또는 FTD)와 선택적 데코레이터 애플리케이션(Radware DefensePro)을 실행하여 서비스 체인을 만들 수 있습니다.

논리적 디바이스를 추가할 때는 애플리케이션 인스턴스 유형 및 버전 정의, 인터페이스 할당, 애플리케이션 구성으로 푸시되는 부트스트랩 설정 작업도 수행합니다.



참고 Firepower 9300의 경우 새시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

독립형 논리적 디바이스와 클러스터형 논리적 디바이스

다음의 논리적 디바이스 유형을 추가할 수 있습니다.

- 독립형 — 독립형 유닛으로 또는 고가용성 쌍의 유닛으로 작동하는 독립형 논리적 디바이스입니다.
- 클러스터 — 클러스터형 논리적 디바이스에서는 여러 유닛을 함께 그룹화할 수 있으므로 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. Firepower 9300과 같은 다중 모듈 디바이스는 인트라 새시 클러스터링(intra-chassis clustering)을 지원합니다. Firepower 9300의 경우 세 개 모듈 모두가 네이티브와 컨테이너 인스턴스 모두에 대해 클러스터에 참여해야 합니다. FDM에서는 클러스터링을 지원하지 않습니다.

논리적 디바이스 애플리케이션 인스턴스: 컨테이너 및 기본

다음 구축 유형으로 애플리케이션 인스턴스가 실행됩니다.

- 기본 인스턴스 — 기본 인스턴스는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다.
- 컨테이너 인스턴스 — 컨테이너 인스턴스는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다. 다중 인스턴스 기능은 FMC를 사용하는 FTD에 대해서만 지원되며, ASA 또는 FDM를 사용하는 FTD에 대해서는 지원되지 않습니다.



참고 다중 인스턴스 기능은 ASA 다중 컨텍스트 모드와 비슷하지만 구현은 서로 다릅니다. 다중 컨텍스트 모드에서는 단일 애플리케이션 인스턴스를 분할하는 반면 다중 인스턴스 기능 사용 시에는 독립적인 컨테이너 인스턴스를 사용할 수 있습니다. 컨테이너 인스턴스에서는 하드 리소스 분리, 별도의 구성 관리/다시 로드/소프트웨어 업데이트가 허용되며 전체 FTD 기능이 지원됩니다. 다중 컨텍스트 모드에서는 리소스가 공유되므로 지정된 플랫폼에서 더 많은 컨텍스트가 지원됩니다. FTD에서는 다중 상황 모드를 사용할 수 없습니다.

Firepower 9300의 경우 일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다.

컨테이너 인스턴스 인터페이스

컨테이너 인스턴스에 대해 물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스(VLAN 또는 물리적)를 공유할 수 있습니다. 기본 인스턴스는 VLAN 하위 인터페이스 또는 공유 인터페이스를 사용할 수 없습니다. 멀티 인스턴스 클러스터는 VLAN 하위 인터페이스 또는 공유된 인터페이스를 사용할 수 없습니다. 클러스터 EtherChannel의 하위 인터페이스를 사용할 수 있는 클러스터 제어 링크는 예외입니다. [공유 인터페이스 확장성](#) 및 [컨테이너 인스턴스에 VLAN 하위 인터페이스 추가](#)를 참조하십시오.



참고 이 문서에서는 *FXOS VLAN* 하위 인터페이스에 대해서만 설명합니다. FTD 애플리케이션 내에 하위 인터페이스를 추가할 수 있습니다. 자세한 내용은 [FXOS 인터페이스와 애플리케이션 인터페이스 비교](#)를 참조하십시오.

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 라우터드 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.

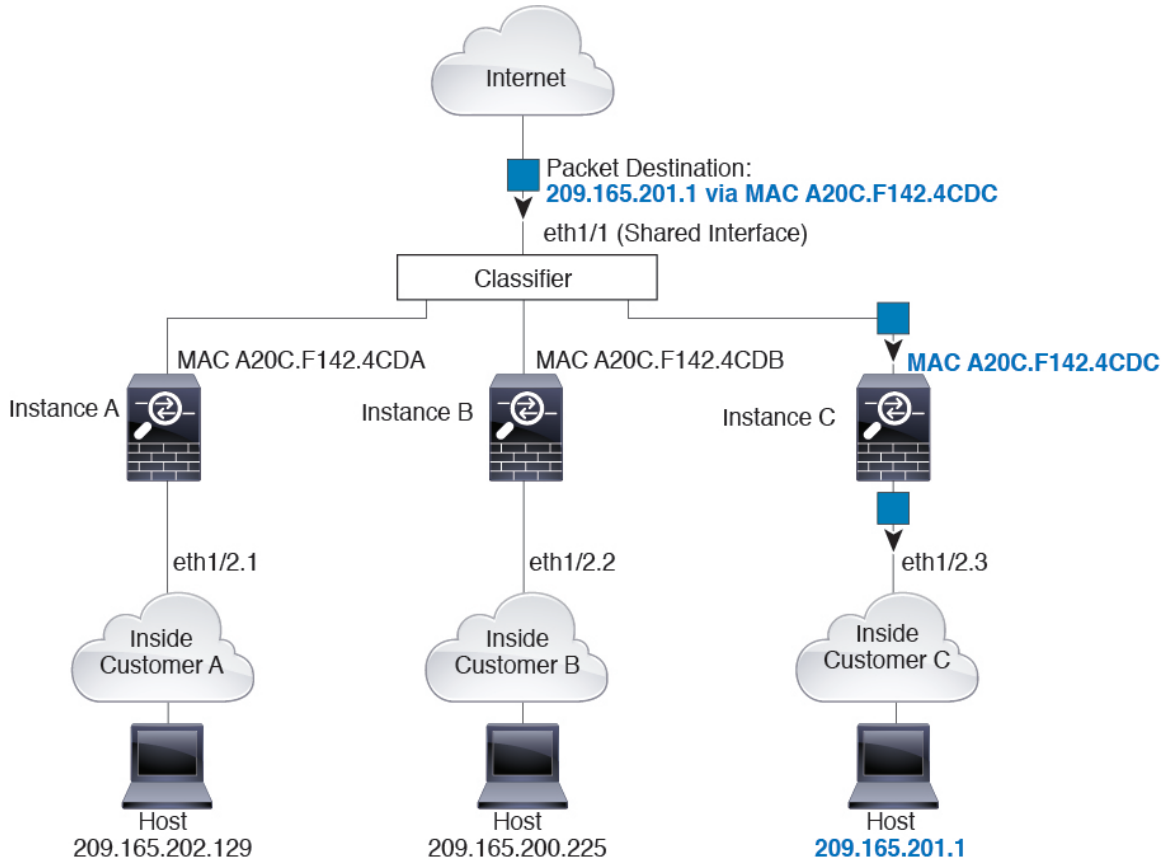


참고 대상 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 인스턴스에 배포됩니다.

분류의 예

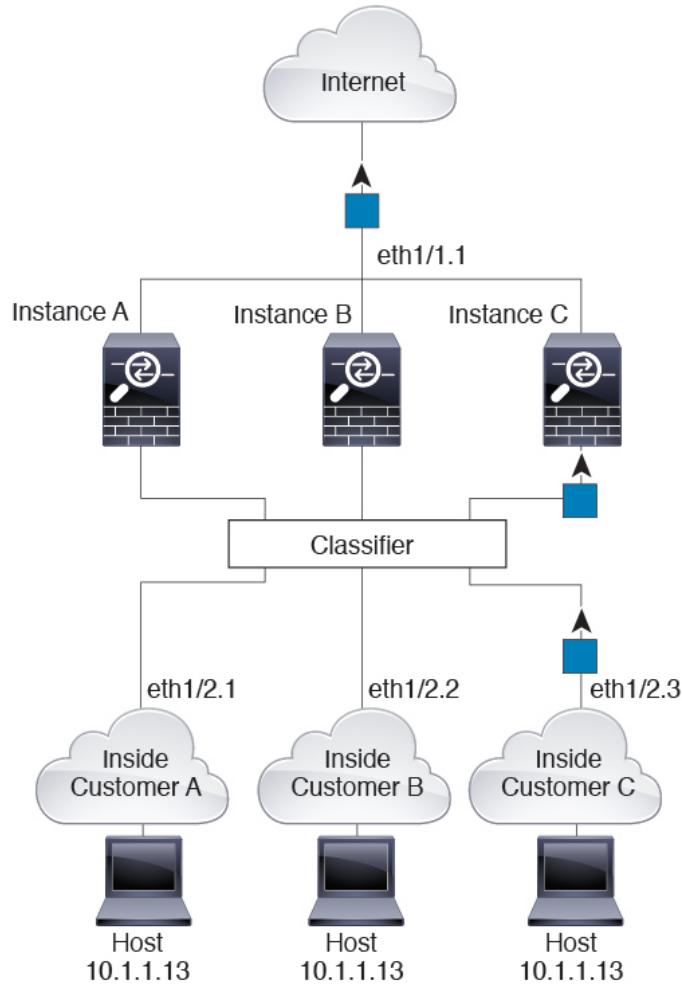
다음 그림은 외부 인터페이스를 공유하는 여러 인스턴스를 보여 줍니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 라우터에서 패킷을 보내는 MAC 주소가 인스턴스 C에 포함되어 있기 때문입니다.

그림 1: MAC 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



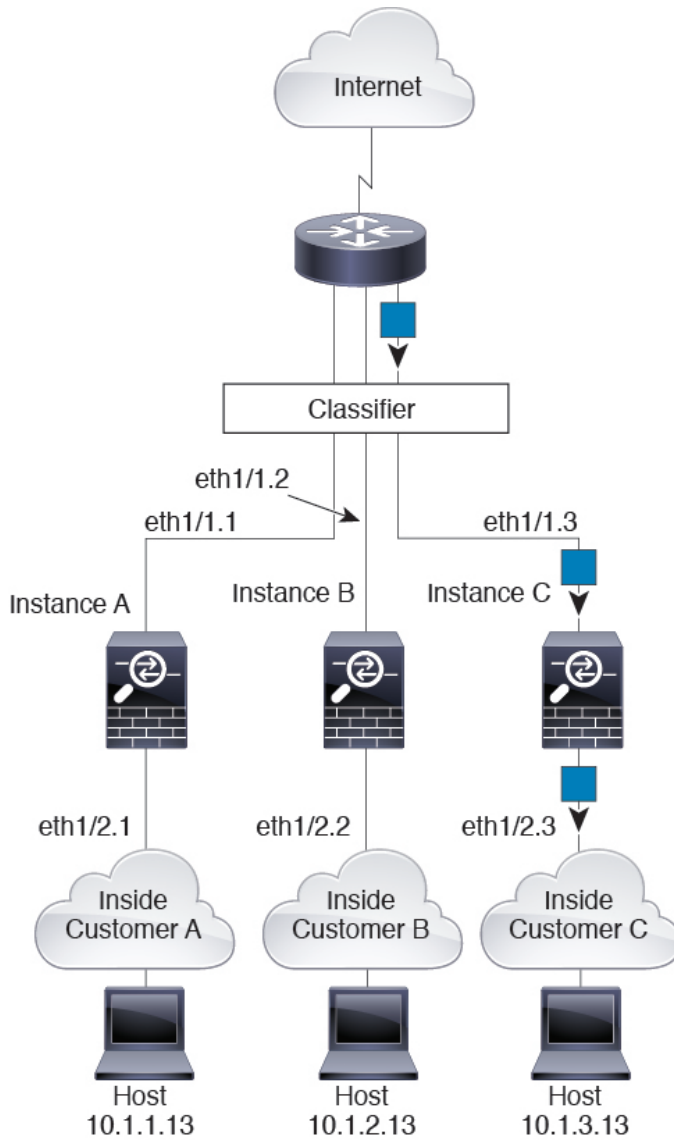
내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 다음 그림에는 인터넷에 액세스하는 네트워크 내의 인스턴스 C에 있는 호스트가 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/2.3이기 때문입니다.

그림 2: 내부 네트워크로부터 수신하는 트래픽



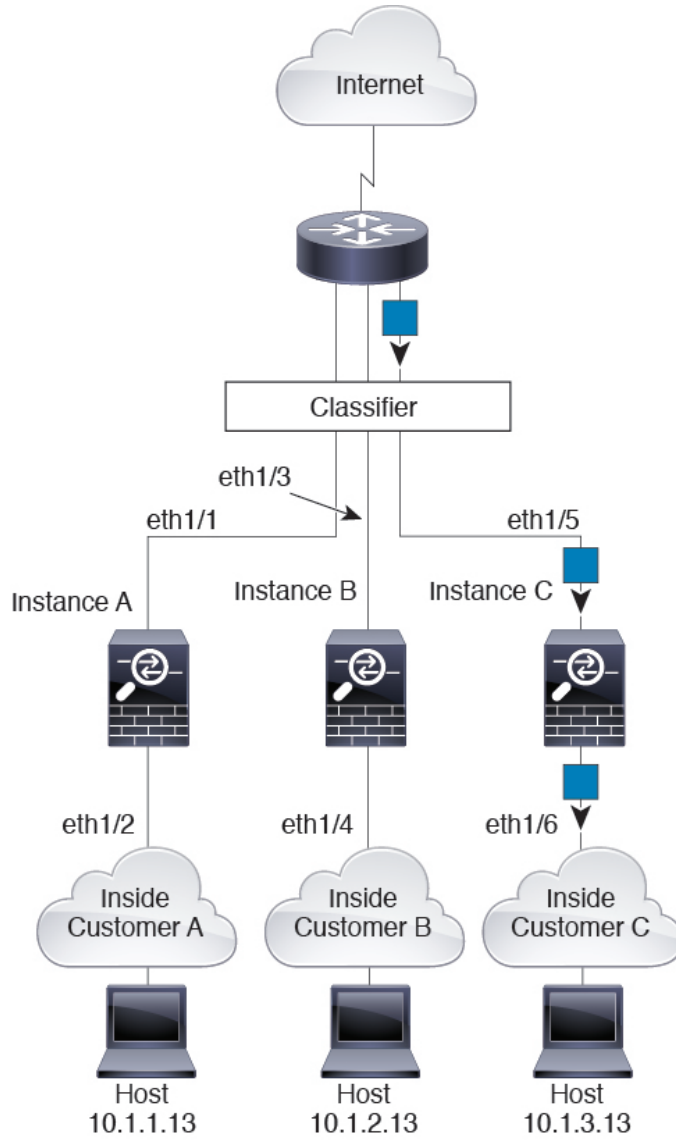
투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 다음 그림에는 인터넷의 네트워크 내 인스턴스 C에 있는 호스트로 전송되는 패킷이 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 인터넷 1/2.3이기 때문입니다.

그림 3: 투명한 방화벽 인스턴스



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 4: 인라인 집합 FTD

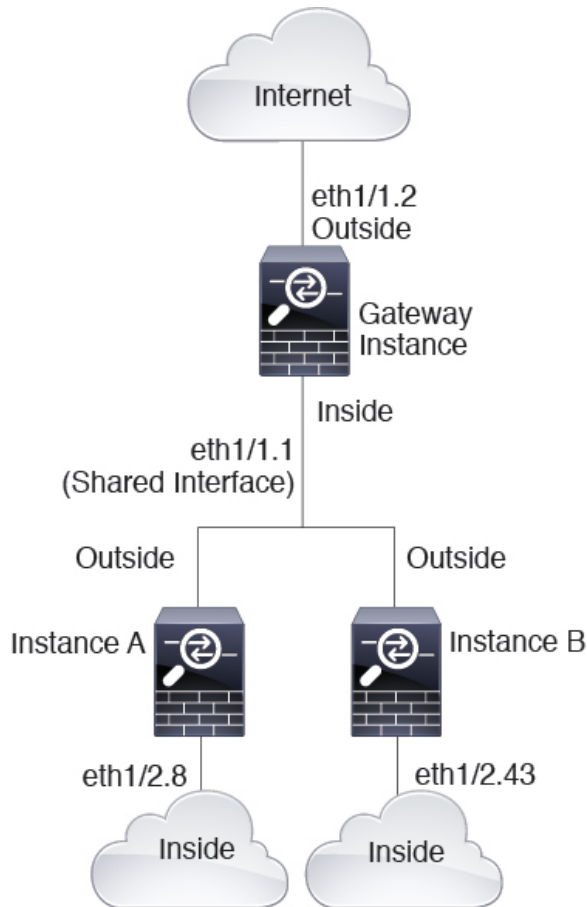


연속 컨테이너 인스턴스

다른 인스턴스 바로 앞에 컨테이너 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.

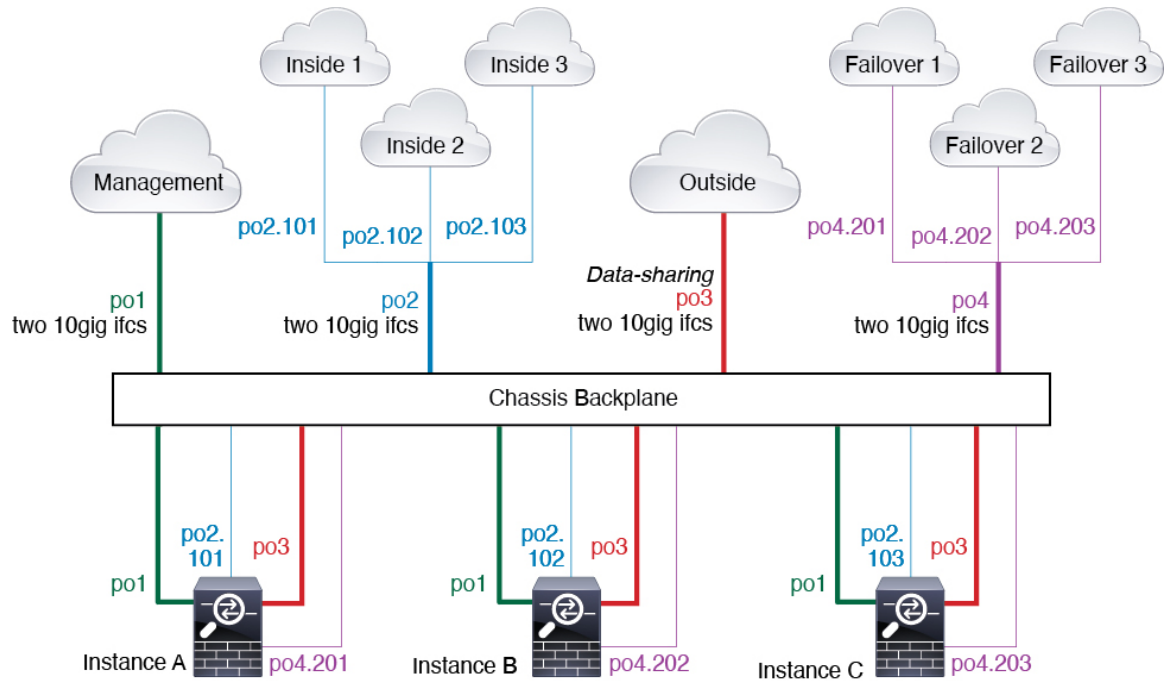
그림 5: 연속 컨테이너 인스턴스



일반적인 다중 인스턴스 구축

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

- **Management(관리)** — 모든 인스턴스가 Port-Channel1 인터페이스(관리 유형)를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 애플리케이션 내에서 인터페이스는 동일한 관리 네트워크의 고유 IP 주소를 사용합니다.
- **Inside(내부)** — 각 인스턴스가 Port-Channel2(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.
- **Outside(외부)** — 모든 인스턴스가 Port-Channel3 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-Channel4(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.



컨테이너 인스턴스 인터페이스용 자동 MAC 주소

FXOS 새시는 컨테이너 인스턴스 인터페이스용 MAC 주소를 자동으로 생성하며 각 인스턴스의 공유 인터페이스가 고유한 MAC 주소를 사용하도록 보장합니다.

애플리케이션 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 애플리케이션 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.

FXOS 새시는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2xx.yyzz.zzzz

여기서 xx.yy는 사용자 정의 접두사 또는 시스템 정의 접두사이고 zz.zzzz는 새시에서 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.f0bf 이면 시스템 접두사는 f0b0입니다.

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

A24D.00zz.zzzz

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2F1.03zz.zzzz

컨테이너 인스턴스 리소스 관리

컨테이너 인스턴스당 리소스 사용량을 지정하려면 FXOS에서 리소스 프로파일을 하나 이상 생성합니다. 논리적 디바이스/애플리케이션 인스턴스를 구축할 때 사용할 리소스 프로파일을 지정합니다. 리소스 프로파일은 CPU 코어 수를 설정합니다. RAM은 코어 수에 따라 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다. 모델당 사용 가능한 리소스를 확인하려면 [컨테이너 인스턴스의 요구 사항 및 사전 요구 사항, 18 페이지](#) 섹션을 참조하십시오. 리소스 프로파일을 추가하려면 [컨테이너 인스턴스에 대한 리소스 프로파일 추가](#) 섹션을 참조하십시오.

다중 인스턴스 기능의 성능 확장 요인

플랫폼의 최대 처리량(연결, VPN 세션 및 TLS 프록시 세션)은 네이티브 인스턴스의 메모리 및 CPU 사용에 대해 계산됩니다. 이 값은 **show resource usage**에 표시됩니다. 다중 인스턴스를 사용하는 경우 처리량은 인스턴스에 할당하는 CPU 코어의 비율을 기준으로 계산해야 합니다. 예를 들어, 코어가 50%인 컨테이너 인스턴스를 사용하는 경우, 처음에는 처리량의 50%를 계산해야 합니다. 또한, 컨테이너 인스턴스에 사용 가능한 처리량은 기본 인스턴스로 줄여야 합니다.

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

컨테이너 인스턴스 및 고가용성

2개의 개별 새시에서 컨테이너 인스턴스를 사용하여 고가용성을 사용할 수 있습니다. 예를 들어 각각 인스턴스가 10개인 새시가 2개 있으면 고가용성 쌍 10개를 생성할 수 있습니다. FXOS에서 고가용성이 구성되지 않았으면 애플리케이션 관리자에서 각 고가용성 쌍을 구성합니다.

자세한 요구 사항은 [고가용성 요구 사항 및 사전 요건, 17 페이지](#) 및 [고가용성 쌍 추가, 38 페이지](#)의 내용을 참조하십시오.

컨테이너 인스턴스 및 클러스터링

보안 모듈/엔진당 하나의 컨테이너 인스턴스를 사용하여 컨테이너 인스턴스 클러스터를 생성할 수 있습니다. 자세한 요구 사항은 [클러스터링의 요구 사항 및 사전 요구 사항, 13 페이지](#)의 내용을 참조하십시오.

논리적 디바이스의 요구 사항 및 사전 요구 사항

요구 사항 및 사전 요구 사항에 대한 내용은 다음 섹션을 참조하십시오.

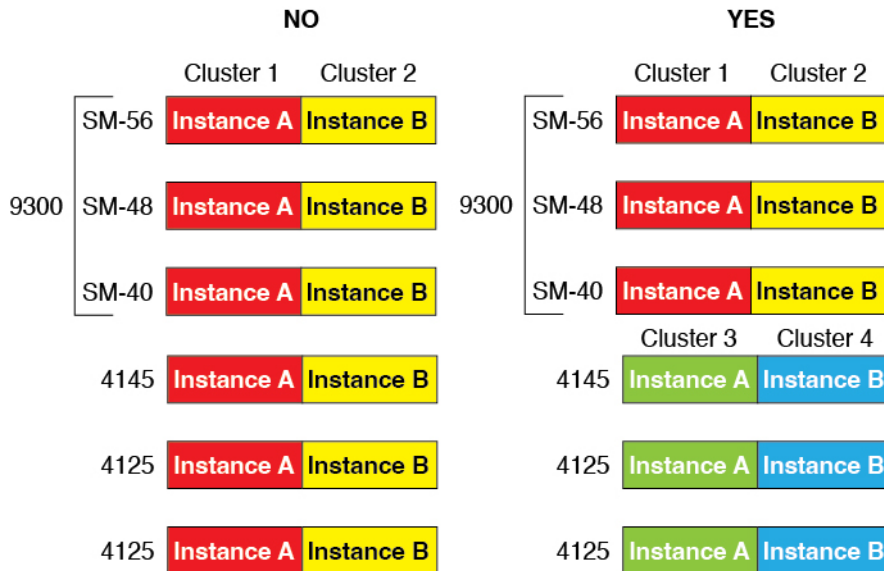
하드웨어 및 소프트웨어 조합에 대한 요구 사항 및 사전 요구 사항

Firepower 4100/9300에서는 여러 모델, 보안 모듈, 애플리케이션 유형, 고가용성 및 확장성 기능을 지원합니다. 허용되는 조합에 대한 다음과 같은 요건을 참조하십시오.

Firepower 9300 요건

Firepower 9300에는 3개의 보안 모듈 슬롯 및 여러 유형의 보안 모듈이 포함되어 있습니다. 다음 요건을 참조하십시오.

- 보안 모듈 유형 - Firepower 9300에 다양한 유형의 모듈을 설치할 수 있습니다. 예를 들어, SM-48을 모듈 1로, SM-40을 모듈 2로, SM-56를 모듈 3으로 설치할 수 있습니다.
- 기본 및 컨테이너 인스턴스 - 보안 모듈에 컨테이너 인스턴스를 설치하는 경우 해당 모듈에서는 다른 컨테이너 인스턴스만 지원할 수 있습니다. 기본 인스턴스에서는 모듈의 모든 리소스를 사용하므로 모듈에는 하나의 기본 인스턴스만 설치할 수 있습니다. 일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다. 예를 들어 모듈 1 및 모듈 2에는 기본 인스턴스를 설치할 수 있지만, 모듈 3에는 컨테이너 인스턴스를 설치할 수 있습니다.
- 네이티브 인스턴스 클러스터링 - 클러스터의 모든 보안 모듈이 인트라 새시(intra-chassis)든, 새시 간(inter-chassis)이든 상관없이 동일한 유형이어야 합니다. 빈 슬롯을 포함하여 새시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 새시에 설치된 보안 모듈의 수는 다를 수 있습니다. 예를 들어, 새시 1에는 2개의 SM-40을 설치하고 새시 2에는 3개의 SM-40을 설치할 수 있습니다. 동일한 새시에 1개의 SM-48 및 2개의 SM-40을 설치하는 경우에는 클러스터링을 사용할 수 없습니다.
- 컨테이너 인스턴스 클러스터링 - 다양한 모델 유형에서 인스턴스를 사용하여 클러스터를 생성할 수 있습니다. 예를 들어 Firepower 9300 SM-56, SM-48, SM-40에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 그러나 동일한 클러스터에서 Firepower 9300과 Firepower 4100을 혼합할 수는 없습니다.



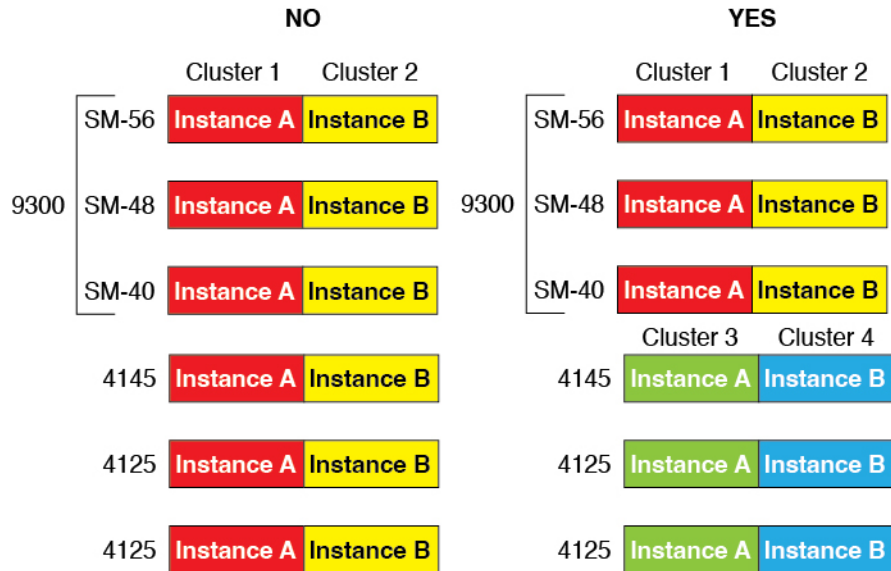
- 고가용성 - 고가용성은 Firepower 9300에서 동일한 유형의 모듈 간에만 지원됩니다. 그러나 두 새시에는 혼합 모듈을 포함할 수 있습니다. 각 새시에 SM-56, SM-48 및 SM-40이 있는 경우를 예로 들 수 있습니다. SM-40 모듈 간, SM-48 모듈 간, SM-56 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

- ASA 및 FTD 애플리케이션 유형 - 새시의 개별 모듈에 서로 다른 애플리케이션 유형을 설치할 수 있습니다. 예를 들어, 모듈 1 및 모듈 2에는 ASA를 설치하고 모듈 3에는 FTD를 설치할 수 있습니다.
- ASA 또는 FTD 버전 - 애플리케이션 인스턴스 유형의 서로 다른 버전을 별도의 모듈에서 실행하거나 동일한 모듈에서 별도의 컨테이너 인스턴스로 실행할 수 있습니다. 예를 들어, 모듈 1에는 FTD 6.3을, 모듈 2에는 FTD 6.4를 설치하고, 모듈 3에는 FTD 6.5를 설치할 수 있습니다.

Firepower 4100 요건

Firepower 4100은 여러 모델로 제공됩니다. 다음 요건을 참조하십시오.

- 기본 및 컨테이너 인스턴스 - Firepower 4100에 컨테이너 인스턴스를 설치하는 경우 해당 디바이스에서는 다른 컨테이너 인스턴스만 지원할 수 있습니다. 기본 인스턴스에서는 디바이스의 모든 리소스를 사용하므로 디바이스에는 하나의 기본 인스턴스만 설치할 수 있습니다.
- 네이티브 인스턴스 클러스터링 - 클러스터의 모든 새시는 동일한 모델이어야 합니다.
- 컨테이너 인스턴스 클러스터링 - 다양한 모델 유형에서 인스턴스를 사용하여 클러스터를 생성할 수 있습니다. 예를 들어 Firepower 4145 및 4125에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 그러나 동일한 클러스터에서 Firepower 9300과 Firepower 4100을 혼합할 수는 없습니다.



- 고가용성 - 고가용성은 동일한 유형의 모듈 간에만 지원됩니다.
- ASA 및 FTD 애플리케이션 유형 - Firepower 4100에서는 하나의 애플리케이션 유형만 실행할 수 있습니다.
- FTD 컨테이너 인스턴스 버전 - 동일한 모듈에서 별도의 컨테이너 인스턴스로 서로 다른 버전의 FTD를 실행할 수 있습니다.

클러스터링의 요구 사항 및 사전 요구 사항

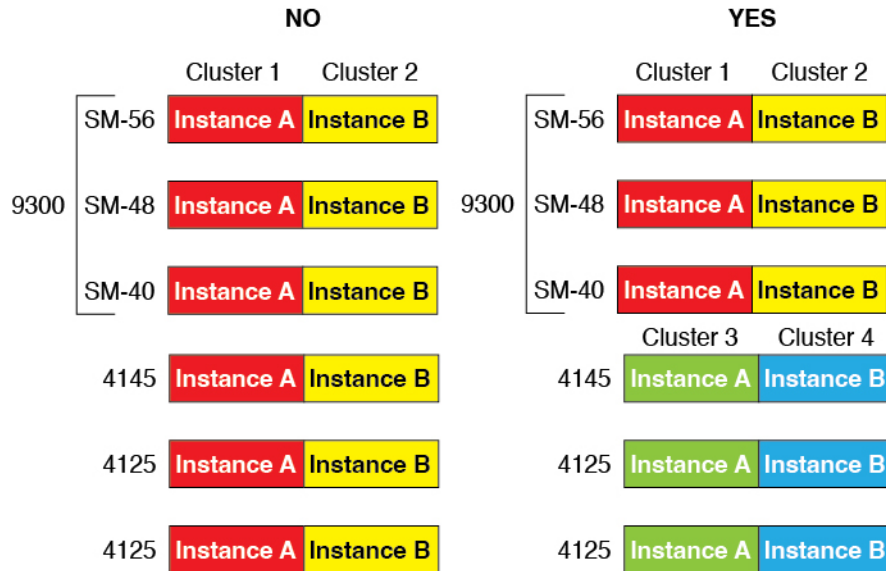
클러스터 모델 지원

- Firepower 9300의 ASA - 최대 16개 모듈 예를 들어 새시 16개에 모듈 1개, 새시 8개에 모듈 2개, 또는 모듈을 16개까지 제공하는 어떤 조합도 사용할 수 있습니다. 새시의 모든 모듈은 클러스터에 속해야 합니다. 새시 내, 새시 간 및 사이트 간 클러스터링에 지원됨.
- ASA의 Firepower 4100 Series - 최대 16개 새시. 새시 간 및 사이트 간 클러스터링에 지원됨.
- FMC를 사용한 Firepower 9300의 FTD- 1 새시에 최대 6개 모듈 예를 들어 새시 3개에 모듈 2개, 새시 2개에 모듈 3개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다. 새시의 모든 모듈은 클러스터에 속해야 합니다. 새시 내 및 새시 간 클러스터링에 지원됨.
- FMC를 사용한 Firepower 4100 Series의 FTD - 최대 6개 새시 새시 간 클러스터링에 지원됨.
- Radware DefensePro- ASA와의 새시 내 클러스터링에 지원됨.
- Radware DefensePro - FTD와의 새시 내 클러스터링에 지원됨. 다중 인스턴스 클러스터링을 지원하지 않습니다.

클러스터링 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 새시:

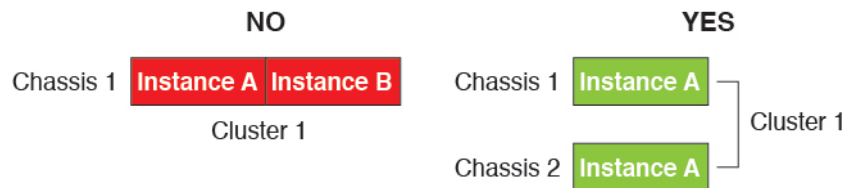
- 네이티브 인스턴스 클러스터링 - Firepower 4100의 경우 모든 새시가 동일한 모델이어야 합니다. Firepower 9300의 경우: 모든 보안 모듈이 동일한 유형이어야 합니다. 예를 들어 클러스터링을 사용하는 경우 Firepower 9300의 모든 모듈은 SM-40이어야 합니다. 빈 슬롯을 포함하여 새시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 새시에 설치된 보안 모듈의 수는 다를 수 있습니다.
- 컨테이너 인스턴스 클러스터링 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 새시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-48, SM-40에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4145 및 4125에서 클러스터를 생성할 수 있습니다.



- 이미지 업그레이드 시 동일한 FXOS 소프트웨어 예외를 실행해야 합니다.
- 클러스터에 할당하는 인터페이스에 대한 것과 동일한 인터페이스 구성을 포함해야 합니다(예: EtherChannel, 활성 인터페이스, 속도 및 이중 등). 동일한 인터페이스 ID에 대해 용량이 일치하고 동일한 Spanned EtherChannel에서 성공적인 인터넷 번들링이 가능한 한 새시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있습니다. 모든 데이터 인터페이스는 새시 간 클러스터링에서 EtherChannel이어야 합니다. 인터페이스 모듈을 추가 또는 제거하거나 EtherChannel을 구성하는 등의 방법을 통해 클러스터링을 활성화한 후 FXOS에서 인터페이스를 변경하는 경우에는 각 새시에서 데이터 노드부터 시작하여 마지막으로 제어 노드까지 같은 변경을 수행합니다.
- 동일한 NTP 서버를 사용해야 합니다. FTD의 경우 FMC는 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정해서는 안 됩니다.
- ASA: 각 FXOS 새시를 License Authority 또는 Satellite Server에 등록해야 합니다. 데이터 노드에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 새시용으로 별도의 라이선스를 구매해야 합니다. FTD의 경우 모든 라이선싱이 FMC에서 처리됩니다.

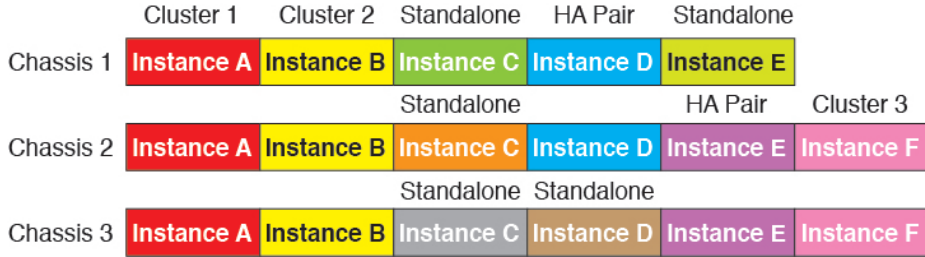
멀티 인스턴스 클러스터링 요구 사항

- 모든 내부 보안 모듈/엔진 클러스터링 안 함 - 지정된 클러스터에 대해 보안 모듈/엔진당 단일 컨테이너 인스턴스만 사용할 수 있습니다. 동일한 모듈에서 실행 중인 경우에는 두 컨테이너 인스턴스를 동일한 클러스터에 추가할 수 없습니다.



- 클러스터 및 독립형 인스턴스를 혼용 - 보안 모듈/엔진의 모든 컨테이너 인스턴스가 하나의 클러스터에 속할 필요가 없습니다. 일부 인스턴스는 독립형이나 고가용성 노드로 사용할 수 있습니다

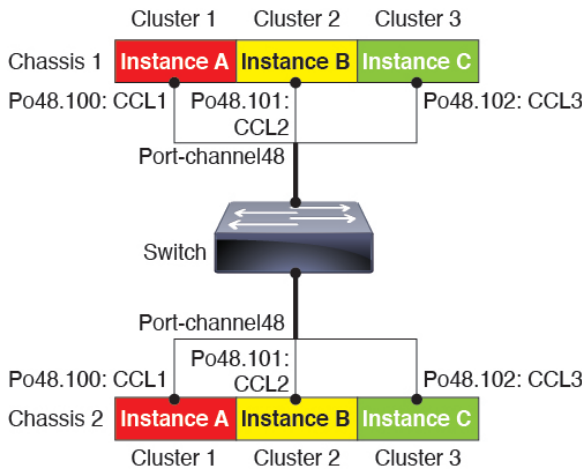
다. 동일한 보안 모듈/엔진에서 별도의 인스턴스를 사용해 여러 클러스터를 생성할 수도 있습니다.



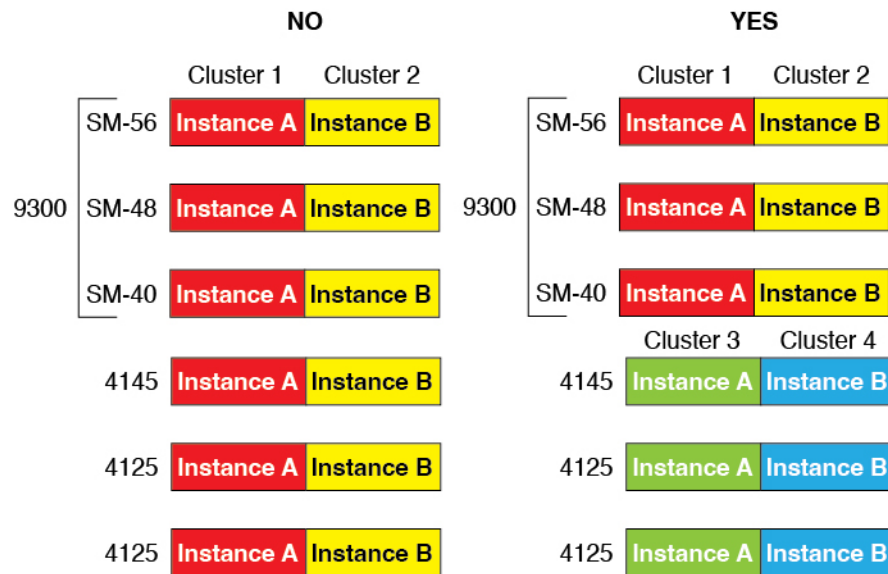
- Firepower 9300의 모든 모듈 세 가지는 해당 클러스터에 속해야 합니다 - Firepower 9300의 경우 클러스터에는 모든 3개의 모듈에서 단일 컨테이너 인스턴스가 필요합니다. 모듈 1 및 2의 인스턴스를 사용하여 클러스터를 생성한 다음 모듈 3 또는 예제에서 네이티브 인스턴스를 사용할 수 없습니다.



- 리소스 프로파일 일치 - 클러스터의 각 노드가 동일한 리소스 프로파일 특성을 사용하는 것이 좋습니다. 그러나 클러스터 노드를 다른 리소스 프로파일로 변경하거나 다른 모델을 사용하는 경우 일치하지 않는 리소스가 허용됩니다.
- 전용 클러스터 제어 링크 - 새시 간 클러스터링의 경우 각 클러스터에 전용 클러스터 제어 링크가 필요합니다. 예를 들어 각 클러스터는 동일한 클러스터 유형 EtherChannel에서 별도의 하위 인터페이스를 사용하거나 별도의 EtherChannel을 사용할 수 있습니다.



- 공유 인터페이스 없음 - 클러스터링에서 공유 유형 인터페이스를 지원하지 않습니다. 그러나 동일한 관리 및 이벤트 인터페이스는 여러 클러스터에서 사용할 수 있습니다.
- 하위 인터페이스 없음 - 다중 인스턴스 클러스터는 FXOS 정의 VLAN 하위 인터페이스를 사용할 수 없습니다. 클러스터 EtherChannel의 하위 인터페이스를 사용할 수 있는 클러스터 제어 링크는 예외입니다.
- 새시 모델 혼합 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 새시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-48, SM-40에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4145 및 4125에서 클러스터를 생성할 수 있습니다.



- 최대 6개 노드 - 하나의 클러스터에서 최대 6개의 컨테이너 인스턴스를 사용할 수 있습니다.

새시 간 클러스터링을 위한 스위치 요구 사항

- Firepower 4100/9300 새시에서 클러스터링을 구성하기 전에 스위치 구성을 완료하고 새시의 모든 EtherChannel을 스위치에 성공적으로 연결하십시오.
- 지원되는 스위치 특성은 [Cisco FXOS 호환성](#)을 참고하십시오.

사이트 간 클러스터링을 위한 **Data Center Interconnect** 크기 조정

클러스터 제어 링크 트래픽을 처리하기 위한 DCI(data center interconnect) 대역폭을 다음 계산과 같이 예약해야 합니다.

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

각 사이트의 멤버 수가 다를 경우, 더 큰 숫자를 계산에 사용합니다. DCI의 최소 대역폭은 한 멤버에 대한 클러스터 제어 링크의 크기보다 작으면 안 됩니다.

예를 들면 다음과 같습니다.

• 2개 사이트에 멤버가 4개인 경우:

- 총 클러스터 멤버 4개
- 각 사이트당 멤버 2개
- 멤버당 5Gbps 클러스터 제어 링크

예약된 DCI 대역폭 = $5\text{Gbps}(2/2 \times 5\text{Gbps})$

• 3개 사이트에 멤버가 6개인 경우 크기가 다음과 같이 증가함:

- 총 클러스터 멤버 6개
- 사이트 1에 멤버 3개, 사이트 2에 멤버 2개, 사이트 3에 멤버 1개
- 멤버당 10Gbps 클러스터 제어 링크

예약된 DCI 대역폭 = $15\text{Gbps}(3/2 \times 10\text{Gbps})$

• 2개 사이트에 멤버가 2개인 경우:

- 총 클러스터 멤버 2개
- 사이트당 멤버 1개
- 멤버당 10Gbps 클러스터 제어 링크

예약된 DCI 대역폭 = $10\text{Gbps}(1/2 \times 10\text{Gbps} = 5\text{Gbps})$. 그러나 최소 대역폭은 클러스터 제어 링크의 크기(10Gbps)보다 작으면 안 됩니다.

고가용성 요구 사항 및 사전 요건

- 고가용성 페일오버 설정에는 2개의 유닛이 필요합니다.
 - 별도의 새시에 있어야 합니다. Firepower 9300용 새시 내 고가용성은 지원되지 않습니다.
 - 같은 모델이어야 합니다.
 - 고가용성 논리 디바이스에는 동일한 인터페이스가 할당되어야 합니다.
 - 인터페이스 개수와 유형이 같아야 합니다. 고가용성을 활성화하기 전에 모든 인터페이스는 FXOS와 동일하게 사전 설정되어야 합니다.
- 고가용성은 Firepower 9300에서 동일한 유형의 모듈 간에만 지원되지만, 두 새시는 혼합된 모듈을 포함할 수 있습니다. 각 새시에 SM-56, SM-48 및 SM-40이 있는 경우를 예로 들 수 있습니다. SM-56 모듈 간, SM-48 모듈 간, SM-40 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

- 컨테이너 인스턴스의 각 유닛은 동일한 리소스 프로파일 속성을 사용해야 합니다.
- 기타 고가용성을 위한 시스템 요구 사항은 고가용성을 위한 애플리케이션 구성 가이드 장의 내용을 참조하십시오.

컨테이너 인스턴스의 요구 사항 및 사전 요구 사항

지원되는 애플리케이션 유형

- FMC를 사용한 FTD

모델당 최대 컨테이너 인스턴스 및 리소스

각 컨테이너 인스턴스에 대해 인스턴스에 할당할 CPU 코어의 수를 지정할 수 있습니다. 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	사용 가능한 RAM	사용 가능한 디스크 공간
Firepower 4110	3	22	53GB	125.6GB
Firepower 4112	3	22	78GB	308GB
Firepower 4115	7	46	162GB	308GB
Firepower 4120	3	46	101GB	125.6GB
Firepower 4125	10	62	162GB	644GB
Firepower 4140	7	70	222GB	311.8GB
Firepower 4145	14	86	344GB	608GB
Firepower 4150	7	86	222GB	311.8GB
Firepower 9300 SM-24 보안 모듈	7	46	226GB	656.4GB
Firepower 9300 SM-36 보안 모듈	11	70	222GB	640.4GB
Firepower 9300 SM-40 보안 모듈	13	78	334GB	1359GB
Firepower 9300 SM-44 보안 모듈	14	86	218GB	628.4GB
Firepower 9300 SM-48 보안 모듈	15	94	334GB	1341GB
Firepower 9300 SM-56 보안 모듈	18	110	334GB	1314GB

FMC 필수조건

Firepower 4100 새시 또는 Firepower 9300 모듈의 모든 인스턴스에서는 라이선싱 구현으로 인해 동일한 FMC를 사용해야 합니다.

논리적 디바이스 관련 지침 및 제한 사항

지침 및 제한 사항은 다음 섹션을 참조하십시오.

일반 지침 및 제한 사항

방화벽 모드

FTD 및 ASA의 부트스트랩 구성에서 방화벽 모드를 라우팅 또는 투명으로 설정할 수 있습니다.

고가용성

- 애플리케이션 구성 내에서 고가용성을 구성합니다.
- 모든 데이터 인터페이스를 페일오버 및 상태 링크로 사용할 수 있습니다. 데이터 공유 인터페이스가 지원되지 않습니다.

다중 인스턴스 및 컨텍스트 모드

- 다중 상황 모드는 ASA에서만 지원됩니다.
- 구축 후에 ASA에서 다중 컨텍스트 모드를 활성화합니다.
- 컨테이너 인스턴스와의 다중 인스턴스 기능은 FMC를 사용하는 FTD에서만 사용 가능합니다.
- FTD 컨테이너 인스턴스의 경우에는 단일 FMC에서 보안 모듈/엔진의 모든 인스턴스를 관리해야 합니다.
- 의 TLS 암호화 가속에서 최대 16 개의 컨테이너 인스턴스를 활성화할 수 있습니다.
- FTD 컨테이너 인스턴스의 경우에는 다음 기능이 지원되지 않습니다.
 - Radware DefensePro 링크 데코레이터
 - FMC UCAPL/CC 모드
 - 하드웨어로의 플로우 오프로드

클러스터링 지침 및 제한 사항

새시 간 클러스터링을 위한 스위치

- 연결된 스위치가 클러스터 데이터 인터페이스 및 클러스터 제어 링크 인터페이스 모두의 MTU와 일치해야 합니다. 클러스터 제어 링크 인터페이스 MTU를 데이터 인터페이스 MTU보다 100바이트 이상 높게 설정해야 하므로 스위치를 연결하는 클러스터 제어 링크를 적절하게 설정해야 합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다.
- Cisco IOS XR 시스템의 경우 기본이 아닌 MTU를 설정하려면 IOS 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 IOS XR IPv4 MTU와 일치해야 합니다. Cisco Catalyst 및 Cisco Nexus 스위치에는 이 조정이 필요하지 않습니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다.
- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 비활성화하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 **keepalive** 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

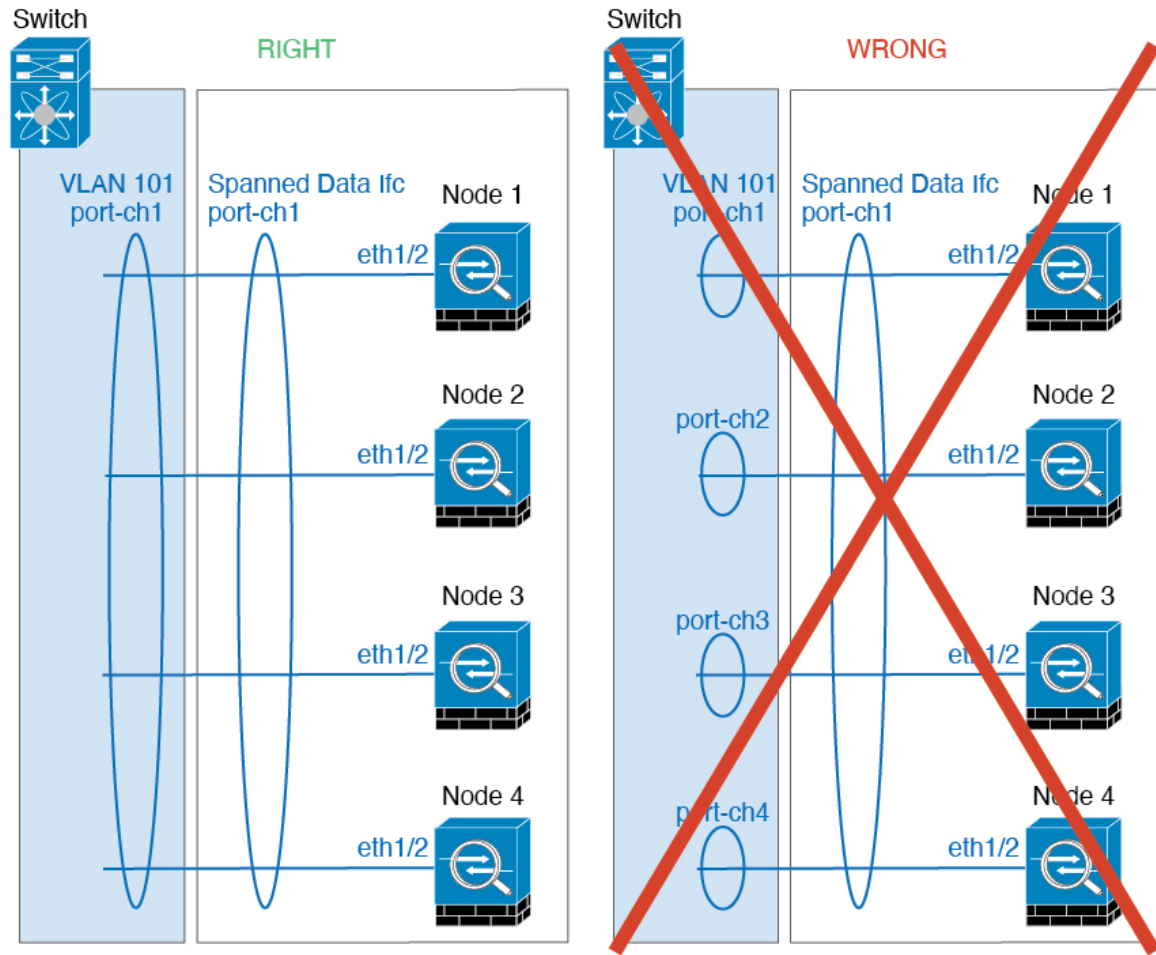
```
router(config) # port-channel id hash-distribution fixed
```

VSS 피어링 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.
- Firepower 4100/9300 클러스터는 LACP 단계적 통합을 지원합니다. 따라서 연결된 Cisco Nexus 스위치에서 LACP 단계적 통합을 활성화된 상태로 둘 수 있습니다.

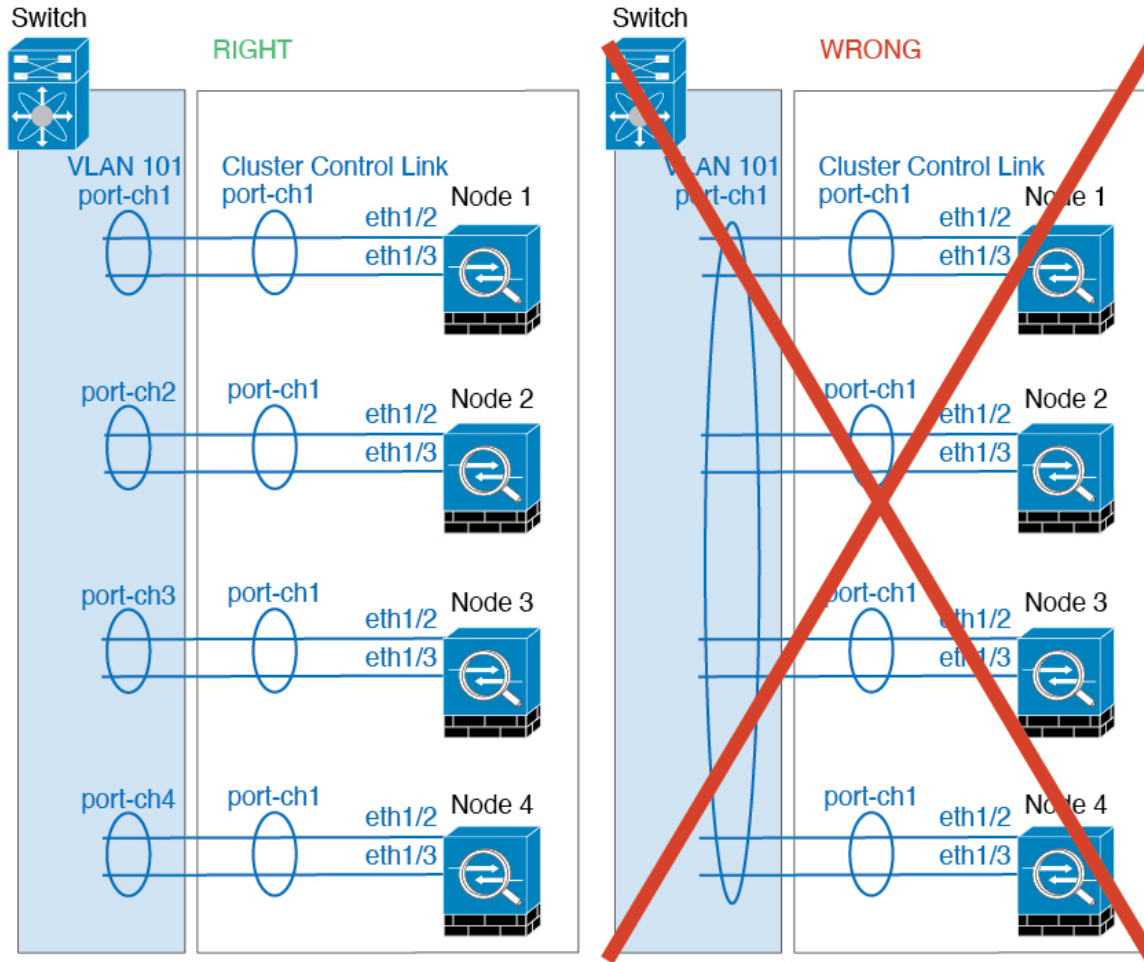
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. FXOS EtherChannel에서는 기본적으로 LACP 속도가 fast(고속)로 설정됩니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.

새시 간 클러스터링을 위한 **EtherChannel**

- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel이 교차 스택에 연결되어 있는 상태에서 제어 유닛 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.
- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
 - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 스펀 EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



- 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



사이트 간 클러스터링

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 클러스터 제어 링크 레이턴시는 RTT(왕복 시간)가 20ms 이하여야 합니다.
- 클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 전용 링크를 사용해야 합니다.
- 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 리밸런싱됩니다.
- DCCI(Data Center Interconnect)에서 사용되는 경우에도 전용 링크이므로 클러스터 제어 링크에서 전달된 데이터 트래픽을 암호화하지 않습니다. OTV(Overlay Transport Virtualization)를 사용하거나 로컬 제어 도메인 외부에서 클러스터 제어 링크를 확장하는 경우 OTV를 통한 802.1AE MacSec과 같은 보더 라우터에서 암호화를 구성할 수 있습니다.
- 클러스터를 구현할 경우 들어오는 연결에 대한 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적

인 동작입니다. 그러나 관리자 지역화를 활성화하는 경우 항상 연결 소유자와 동일한 사이트에서 로컬 관리자 역할이 선택됩니다(사이트 ID에 따라). 원래 소유자가 실패하면 로컬 관리자는 동일한 사이트에서 새 소유자를 선택합니다.(참고: 트래픽이 사이트 간에 비동기 상태이고 원래 소유자가 실패한 후 원격 사이트로부터 계속 트래픽이 발생하면, 원격 사이트의 노드가 재호스팅 기간 내에 데이터 패킷을 수신하는 경우 새로운 소유자가 될 수 있습니다.)

- 관리자 지역화의 경우 NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 지역화를 지원하지 않습니다.
- 투명 모드에서, 클러스터가 내부 및 외부 라우터(north-south 삽입이라고도 함) 쌍 사이에 위치하면 내부 라우터 모두에서 MAC 주소를 공유해야 하며 외부 라우터 모두에서도 MAC 주소를 공유해야 합니다. 사이트 1의 클러스터 멤버가 사이트 2의 멤버에 연결을 전달할 경우, 목적지 MAC 주소가 유지됩니다. MAC 주소가 사이트 1의 라우터와 동일할 경우 패킷은 사이트 2의 라우터에만 도달합니다.
- 투명 모드에서 클러스터가 내부 네트워크(East-West 삽입이라고 함) 사이에서 방화벽을 위해 각 사이트에서 데이터 네트워크 및 게이트웨이 라우터 사이에 위치하면 각 게이트웨이 라우터는 HSRP와 같은 첫 번째 홉 이중화 프로토콜(FHRP)을 사용하여 각 사이트에서 동일한 가상 IP 및 MAC 주소 대상을 제공해야 합니다. 데이터 VLAN은 OTV(오버레이 전송 가상화) 또는 유사한 기능을 사용하는 사이트 전체로 확장됩니다. DCI를 통해 다른 사이트로 전송 중인 로컬 게이트웨이 라우터에 예약된 트래픽을 방지하려면 필터를 생성해야 합니다. 게이트웨이 라우터가 1개의 사이트에 연결할 수 없게 되면, 모든 필터를 제거해야 트래픽이 성공적으로 다른 사이트의 게이트웨이에 연결할 수 있습니다.
- 투명 모드의 경우, 클러스터가 HSRP 라우터에 연결된 경우 라우터 HSRP MAC 주소를 . 인접 라우터가 HSRP를 사용하는 경우, HSRP IP 주소로 향하는 트래픽은 HSRP MAC 주소로 전송되지 만, 반환 트래픽은 HSRP 쌍에 있는 특정 라우터 인터페이스의 MAC 주소에서 제공됩니다. 따라서 MAC 주소 테이블은 일반적으로 HSRP IP 주소에 대한 ARP 테이블 항목이 만료되고 가 ARP 요청을 보내고 응답을 수신하는 경우에만 업데이트됩니다. 의 ARP 테이블 항목은 기본적으로 14,400초 후에 만료되지만 MAC 주소 테이블 항목은 기본적으로 300초 후에 만료되므로 MAC 주소 테이블 만료 트래픽 삭제를 방지하려면 고정 MAC 주소 항목이 필요합니다.
- Spanned EtherChannel을 사용하는 라우팅 모드의 경우 사이트별 MAC 주소를 구성하십시오. OTV 또는 유사한 것을 사용하여 사이트 전체로 데이터 VLAN을 확장하십시오. 전역 MAC 주소로 향하는 트래픽이 DCI를 통해 다른 사이트에 가지 않도록 필터를 생성해야 합니다. 어떤 사이트에서 클러스터가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 노드에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. 사이트 간 클러스터가 확장 세그먼트의 FHR(First Hop Router)로 작동하는 경우에는 동적 라우팅이 지원되지 않습니다.

추가 지침

- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel 인터페이스에 연결된 Windows 2003 서버를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않아 대량의 ICMP 메시지가 클러스터에

다시 전송됩니다. 이러한 메시지로 인해 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.

- 이중화를 위해 EtherChannel을 VSS, vPC, StackWise 또는 StackWise Virtual에 연결하는 것이 좋습니다.
- 새시 내에서 일부 보안 모듈을 클러스터하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.
- 암호 해독된 TLS/SSL 연결의 경우, 암호 해독 상태가 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.

기본값

- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 실패한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도하도록 설정됩니다.
- 실패한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도하도록 설정됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

독립형 논리적 디바이스 추가

단독으로 또는 고가용성 유닛으로 독립형 논리적 디바이스를 사용할 수 있습니다. 고가용성 사용량에 대한 자세한 내용은 [고가용성 쌍 추가, 38 페이지](#) 섹션을 참조하십시오.

독립형 ASA 추가

독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다. 보안 모듈이 여러 개인 Firepower 9300에서는 클러스터 또는 독립형 디바이스를 구축할 수 있습니다. 클러스터는 모든 모듈을 사용해야 하므로 모듈이 2개인 클러스터와 단일 독립형 디바이스를 혼용하는 방식은 사용할 수 없습니다.

Firepower 4100/9300 새시에서 라우팅된 방화벽 모드 또는 투명 방화벽 모드 ASA를 구축할 수 있습니다.

다중 컨텍스트 모드의 경우 먼저 논리적 디바이스를 구축한 다음 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화해야 합니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 새시.



참고 Firepower 9300의 경우 새시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 새시 관리용으로만 사용되는 새시 관리 포트(**Interfaces**(인터페이스) 탭 상단에 **MGMT**(관리)로 표시됨)와는 다릅니다.
- 다음 정보를 수집합니다.
 - 이 디바이스의 인터페이스 ID
 - 관리 인터페이스 IP 주소 및 네트워크 마스크
 - 게이트웨이 IP 주소

프로시저

단계 1 Logical Devices(논리적 디바이스)를 선택합니다.

단계 2 Add(추가) > **Standalone**(독립형)를 클릭하고 다음 파라미터를 설정합니다.

a) **Device Name**(디바이스 이름)을 입력합니다.

이 이름은 새시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

b) **Template**(템플릿)은 **Cisco: Adaptive Security Appliance**를 선택합니다.

c) **Image Version**(이미지 버전)을 선택합니다.

d) **OK**(확인)를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 3 Data Ports(데이터 포트) 영역을 확장하고 디바이스에 할당할 각 포트를 클릭합니다.

이전에 **Interfaces**(인터페이스) 페이지에서 활성화한 데이터 인터페이스만 할당할 수 있습니다. 나중에 IP 주소 설정을 비롯하여 ASA에서 이러한 인터페이스를 활성화하고 구성하게 됩니다.

단계 4 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 5 **General Information**(일반 정보) 페이지에서 다음 작업을 수행합니다.

- (Firepower 9300의 경우) **Security Module Selection**(보안 모듈 선택) 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭합니다.
- Management Interface**(관리 인터페이스)를 선택합니다.
이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 새시 관리 포트와 별개입니다.
- 관리 인터페이스 **Address Type**(주소 유형)을 **IPv4 only**(IPv4 전용), **IPv6 only**(IPv6 전용) 또는 **IPv4 and IPv6**(IPv4 및 IPv6) 중에서 선택합니다.
- Management IP**(관리 IP) 주소를 구성합니다.
이 인터페이스의 고유 IP 주소를 설정합니다.
- Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)를 입력합니다.
- Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.

단계 6 **Settings**(설정) 탭을 클릭합니다.

The screenshot shows the 'Cisco Adaptive Security Appliance - Bootstrap Configuration' window with the 'Settings' tab selected. Under 'Firewall Mode', a dropdown menu is set to 'Transparent'. Below it are 'Password' and 'Confirm Password' fields, both containing masked characters (dots).

단계 7 **Firewall Mode**(방화벽 모드)를 **Routed**(라우팅) 또는 **Transparent**(투명) 중에서 선택합니다.

라우팅 모드에서 ASA는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

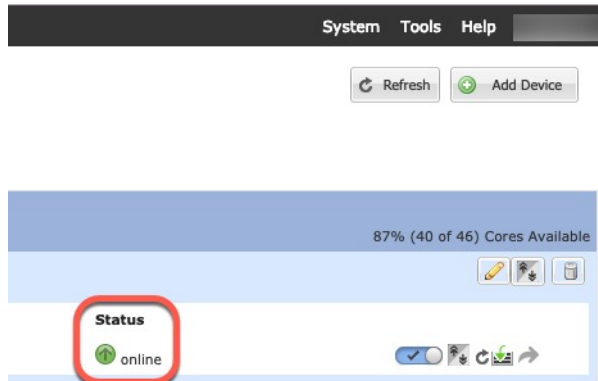
단계 8 관리자 및 비밀번호 활성화에 대해 **Password**(비밀번호)를 입력하고 확인합니다.

비밀번호를 복구할 때는 사전 구성된 ASA 관리 사용자/비밀번호 및 비밀번호 활성화를 사용하면 유용합니다. FXOS 액세스 권한이 있는데 관리 사용자 비밀번호/비밀번호 활성화를 잊어버린 경우 이를 재설정할 수 있습니다.

단계 9 OK(확인)를 클릭하여 구성 대화 상자를 닫습니다.

단계 10 Save(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 **Status**(상태)가 **online**(온라인)으로 표시되면 애플리케이션 내에서 보안 정책 구성을 시작할 수 있습니다.



단계 11 보안 정책 구성을 시작하려면 ASA 구성 가이드를 참조하십시오.

FMC에 대한 독립형 FTD 추가

독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다. 보안 모듈이 여러 개인 Firepower 9300에서는 클러스터 또는 독립형 디바이스를 구축할 수 있습니다. 클러스터는 모든 모듈을 사용해야 하므로 모듈이 2개인 클러스터와 단일 독립형 디바이스를 혼용하는 방식은 사용할 수 없습니다.

일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 새시.



참고 Firepower 9300의 경우 새시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

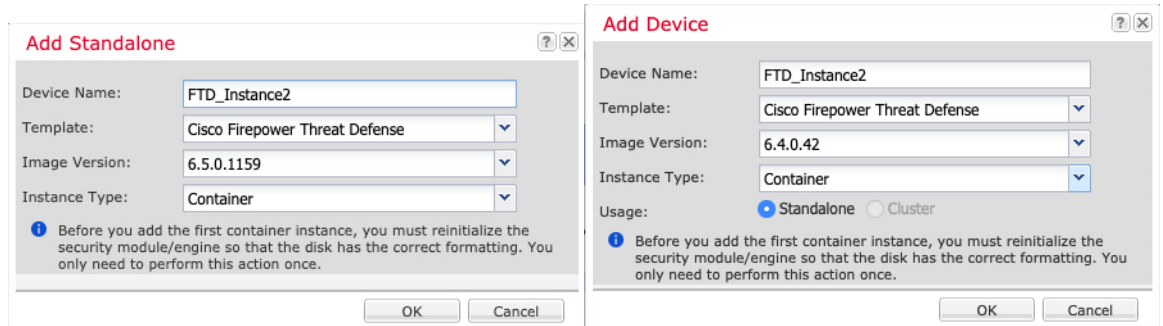
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 새시 관리용으로만 사용되는 새시 관리 포트(**Interfaces**(인터페이스) 탭 상단에 **MGMT**(관리)로 표시됨)와는 다릅니다.

- 나중에 데이터 인터페이스에서 관리를 활성화할 수 있습니다. 데이터 관리를 활성화한 후 이를 사용하지 않으려는 경우에도 관리 인터페이스를 논리적 디바이스에 할당해야 합니다. 자세한 내용은 [FTD 명령 참조](#)의 **configure network management-data-interface** 명령을 참조하십시오.
- 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다. 또는 Firepower 이벤트 처리 인터페이스를 생성하여 모든 이벤트 트래픽을 전달할 수 있습니다(예: 웹 이벤트). 자세한 내용은 [인터페이스 유형](#)을 참조하십시오.
- 컨테이너 인스턴스의 경우 기본 프로필을 사용하지 않으려면 [컨테이너 인스턴스에 대한 리소스 프로파일 추가](#)에 따라 리소스 프로필을 추가합니다.
- 컨테이너 인스턴스의 경우 컨테이너 인스턴스를 처음으로 설치하기 전에 디스크가 올바른 형식을 갖도록 보안 모듈/엔진을 다시 초기화해야 합니다. **Security Modules**(보안 모듈) 또는 **Security Engine**(보안 엔진)을 선택하고 **Reinitialize**(초기화) 아이콘을 클릭합니다. 기존 논리적 디바이스가 삭제된 후에 새 디바이스로 재설치되며 로컬 애플리케이션 구성은 손실됩니다. 기본 인스턴스를 컨테이너 인스턴스로 교체할 때는 어떤 경우든 기본 인스턴스를 삭제해야 합니다. 기본 인스턴스를 컨테이너 인스턴스로 자동 마이그레이션할 수는 없습니다. 자세한 내용은 [보안 모듈/엔진 확인 다시 초기화](#)를 참조하십시오.
- 다음 정보를 수집합니다.
 - 이 디바이스의 인터페이스 ID
 - 관리 인터페이스 IP 주소 및 네트워크 마스크
 - 게이트웨이 IP 주소
 - FMC 선택한 IP 주소 및/또는 NAT ID
 - DNS 서버 IP 주소
 - FTD 호스트 이름 및 도메인 이름

프로시저

단계 1 **Logical Devices**(논리적 디바이스)를 선택합니다.

단계 2 **Add**(추가) > **Standalone**(독립형)를 클릭하고 다음 파라미터를 설정합니다.



a) **Device Name**(디바이스 이름)을 입력합니다.

이 이름은 새시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

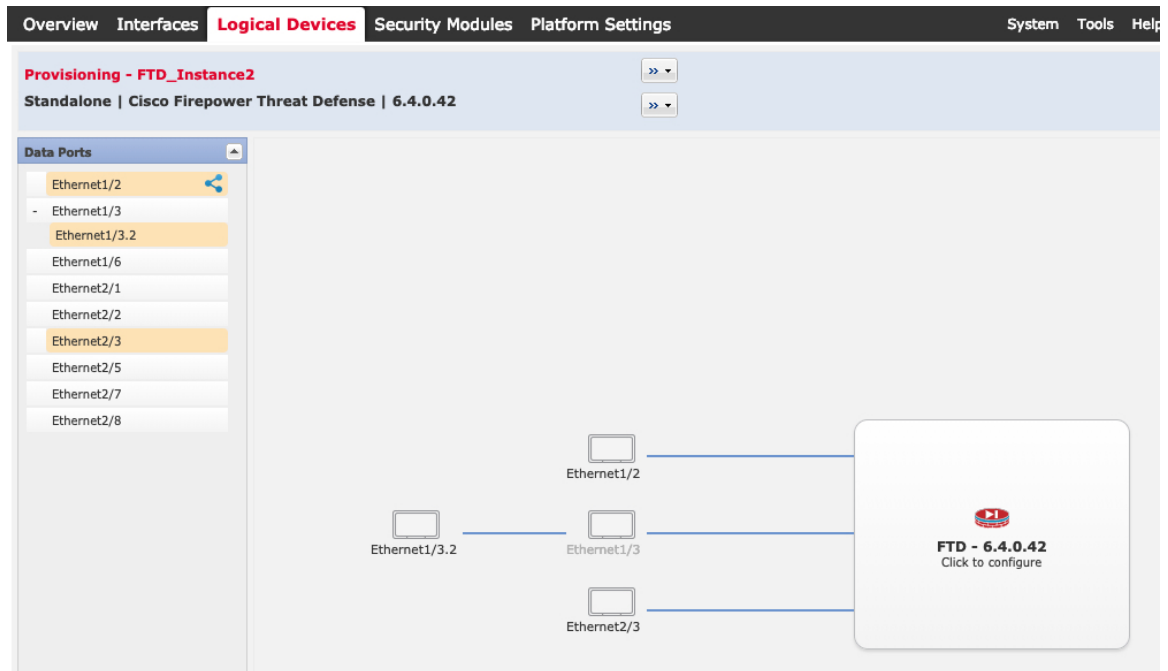
- b) **Template**(템플릿)에서 **Cisco Firepower Threat Defense**를 선택합니다.
- c) **Image Version**(이미지 버전)을 선택합니다.
- d) **Instance Type**(인스턴스 유형)을 **Container**(컨테이너) 또는 **Native**(기본) 중에서 선택합니다.

기본 인스턴스에서는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다. 컨테이너 인스턴스에서는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다.

- e) **OK**(확인)를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 3 Data Ports(데이터 포트) 영역을 확장하고 디바이스에 할당할 각 인터페이스를 클릭합니다.



이전에 **Interfaces**(인터페이스) 페이지에서 활성화한 데이터 및 데이터 공유 인터페이스만 할당할 수 있습니다. 나중에 IP 주소 설정을 비롯하여 FMC에서 이러한 인터페이스를 활성화하고 구성하게 됩니다.

컨테이너 인스턴스에는 데이터 공유 인터페이스를 10개까지만 할당할 수 있습니다. 또한 각 데이터 공유 인터페이스는 최대 14개의 컨테이너 인스턴스에 할당할 수 있습니다. 데이터 공유 인터페이스는 공유 아이콘(🔗)으로 표시됩니다.

하드웨어 바이패스 지원 포트가 아이콘(🔗)과 함께 표시됩니다. 특정 인터페이스 모듈의 경우 인라인 집합 인터페이스에 대해서만 하드웨어 우회 기능을 활성화할 수 있습니다(FMC 구성 가이드 참조). **Hardware Bypass**는 정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있

습니다. 하드웨어 바이패스 쌍에서 두 인터페이스를 할당하지 않는 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다. 하드웨어 바이패스 기능을 사용할 필요가 없으므로 원하는 경우 단일 인터페이스를 할당할 수 있습니다.

단계 4 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 5 **General Information**(일반 정보) 페이지에서 다음 작업을 수행합니다.

- a) (Firepower 9300의 경우) **Security Module Selection**(보안 모듈 선택) 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭합니다.
- b) 컨테이너 인스턴스에 대해 **Resource Profile**(리소스 프로파일)을 지정합니다.

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.

- c) **Management Interface**(관리 인터페이스)를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 새시 관리 포트와 별개입니다.

- d) 관리 인터페이스 **Address Type**(주소 유형)을 **IPv4 only**(IPv4 전용), **IPv6 only**(IPv6 전용) 또는 **IPv4 and IPv6**(IPv4 및 IPv6) 중에서 선택합니다.
- e) **Management IP**(관리 IP) 주소를 구성합니다.
이 인터페이스의 고유 IP 주소를 설정합니다.
- f) **Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)를 입력합니다.
- g) **Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.

단계 6 **Settings(설정)** 탭에서 다음 작업을 수행합니다.

The image shows two screenshots of the Cisco Firepower Threat Defense - Bootstrap Configuration Settings page. The top screenshot shows the 'Management type of application instance' dropdown set to 'FMC'. The bottom screenshot shows the 'Registration Key', 'Confirm Registration Key', and 'Password' fields filled with masked characters.

- a) 네이티브 인스턴스의 경우, **Management type of application instance**(애플리케이션 인스턴스의 관리 유형) 드롭다운 목록에서 **FMC**를 선택합니다.

네이티브 인스턴스에서는 FDM을 관리자로도 지원합니다. 논리적 디바이스를 구축한 후에는 관리자 유형을 변경할 수 없습니다.

- b) FMC 관리에 사용할 **Firepower Management Center IP**를 입력합니다. FMC IP 주소를 알 수 없는 경우, 이 필드를 비워두고 **Firepower Management Center NAT ID** 필드에 암호를 입력합니다.

- c) 컨테이너 인스턴스의 경우, **Permit Export mode from FTD SSH sessions**(FTD SSH 세션에서 전문가 모드 허용)에 대해 **Yes**(예) 또는 **No**(아니요)를 선택합니다. 전문가 모드에서는 고급 트러블슈팅을 위한 FTD 셸 액세스 기능이 제공됩니다.

이 옵션에 대해 **Yes**(예)를 선택하는 경우 SSH 세션에서 컨테이너 인스턴스에 직접 액세스할 수 있는 사용자가 전문가 모드를 시작할 수 있습니다. **No**(아니요)를 선택하는 경우에는 FXOS CLI에서 컨테이너 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리할 수 있도록 **No**(아니요)를 선택하는 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 FTD CLI에서 **expert** 명령을 사용합니다.

- d) **Search Domains**(검색 도메인)를 쉼표로 구분된 목록으로 입력합니다.
e) **Firewall Mode**(방화벽 모드)를 **Transparent**(투명) 또는 **Routed**(라우팅) 중에서 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

- f) **DNS Servers**(DNS 서버)를 쉼표로 구분된 목록으로 입력합니다.

예를 들어, FMC의 호스트 이름을 지정하는 경우, FTD에서는 DNS를 사용합니다.

- g) FTD의 **Fully Qualified Hostname**(정규화된 호스트 이름)을 입력합니다.
h) 등록 시 FMC와 디바이스 간에 공유할 **Registration Key**(등록 키)를 입력합니다.

이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

- i) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password**(비밀번호)를 입력합니다.
j) 이벤트를 전송할 **Eventing Interface**(이벤트 인터페이스)를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

이 인터페이스는 Firepower 이벤트 처리 인터페이스로 정의해야 합니다.

- k) 컨테이너 인스턴스의 경우 **Hardware Crypto**(하드웨어 암호화)를 **Enabled**(활성화됨) 또는 **Disabled**(비활성화됨)로 설정합니다.

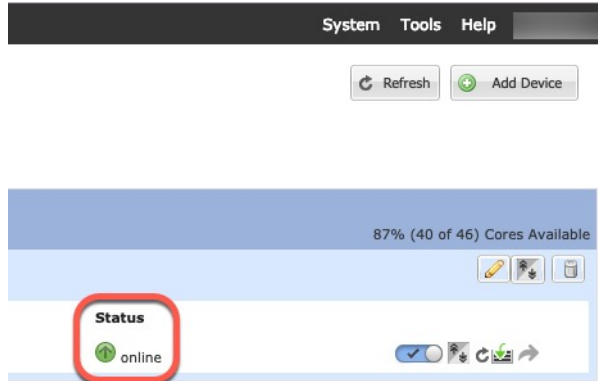
이 설정은 하드웨어에서 TLS 암호화 가속화를 활성화하고 특정 유형의 트래픽에 대한 성능을 개선합니다. 이 기능은 기본적으로 활성화되어 있습니다. 보안 모듈당 최대 16개의 인스턴스에 대해 TLS 암호화 가속화를 활성화할 수 있습니다. 이 기능은 네이티브 인스턴스에서 항상 사용할 수 있습니다. 이 인스턴스에 할당된 하드웨어 암호화 리소스의 백분율을 보려면 **show hw-crypto** 명령을 입력합니다.

단계 7 **Agreement**(계약) 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 8 **OK**(확인)를 클릭하여 구성 대화 상자를 닫습니다.

단계 9 **Save**(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 **Status**(상태)가 **online**(온라인)으로 표시되면 애플리케이션 내에서 보안 정책 구성을 시작할 수 있습니다.



단계 10 FTD를 매니지드 디바이스로 추가하고 보안 정책 구성을 시작하려면 FMC 구성 가이드를 참조합니다.

FDM에 대한 독립형 FTD 추가

네이티브 인스턴스로 FDM을 사용할 수 있습니다. 컨테이너 인스턴스는 지원되지 않습니다. 독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 새시.



참고 Firepower 9300의 경우 새시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 새시 관리용으로만 사용되는 새시 관리 포트(**Interfaces**(인터페이스) 탭 상단에 **MGMT**(관리)로 표시됨)와는 다릅니다.
- 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다.
- 다음 정보를 수집합니다.
 - 이 디바이스의 인터페이스 ID
 - 관리 인터페이스 IP 주소 및 네트워크 마스크

- 게이트웨이 IP 주소
- DNS 서버 IP 주소
- FTD 호스트 이름 및 도메인 이름

프로시저

단계 1 Logical Devices(논리적 디바이스)를 선택합니다.

단계 2 Add(추가) > Standalone(독립형)를 클릭하고 다음 파라미터를 설정합니다.

a) **Device Name**(디바이스 이름)을 입력합니다.

이 이름은 새시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

b) **Template**(템플릿)에서 **Cisco Firepower Threat Defense**를 선택합니다.

c) **Image Version**(이미지 버전)을 선택합니다.

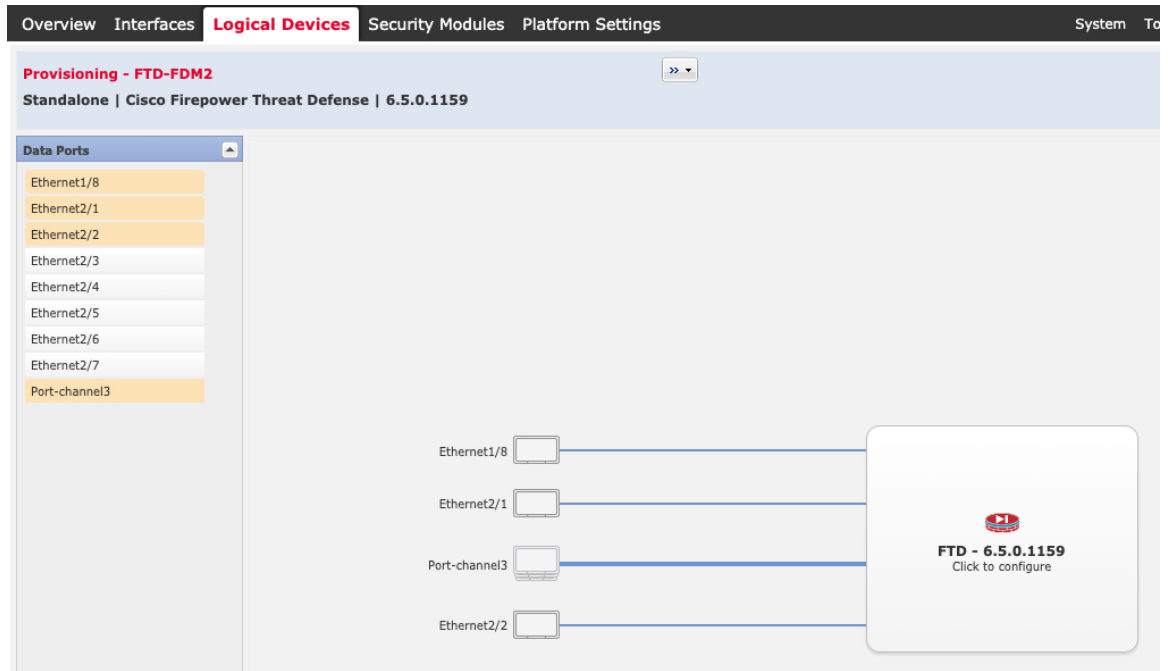
d) **Instance Type**(인스턴스 유형)은 **Native**(네이티브)를 선택합니다.

컨테이너 인스턴스는 FDM에서 지원되지 않습니다.

e) **OK**(확인)를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 3 Data Ports(데이터 포트) 영역을 확장하고 디바이스에 할당할 각 인터페이스를 클릭합니다.

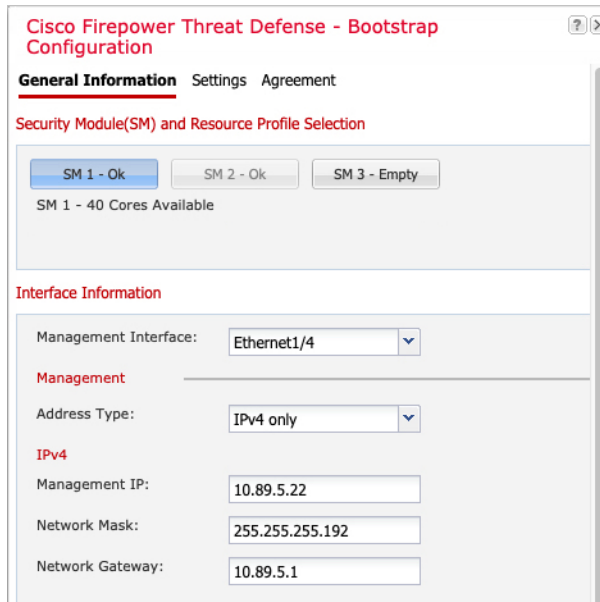


이전에 **Interfaces**(인터페이스) 페이지에서 활성화한 데이터 인터페이스만 할당할 수 있습니다. 나중에 IP 주소 설정을 비롯하여 FDM에서 이러한 인터페이스를 활성화하고 구성하게 됩니다.

단계 4 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 5 **General Information**(일반 정보) 페이지에서 다음 작업을 수행합니다.



- a) (Firepower 9300의 경우) **Security Module Selection**(보안 모듈 선택) 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭합니다.
- b) **Management Interface**(관리 인터페이스)를 선택합니다.
이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 새시 관리 포트와 별개입니다.
- c) 관리 인터페이스 **Address Type**(주소 유형)을 **IPv4 only**(IPv4 전용), **IPv6 only**(IPv6 전용) 또는 **IPv4 and IPv6**(IPv4 및 IPv6) 중에서 선택합니다.
- d) **Management IP**(관리 IP) 주소를 구성합니다.
이 인터페이스의 고유 IP 주소를 설정합니다.
- e) **Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)를 입력합니다.
- f) **Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.

단계 6 **Settings**(설정) 탭에서 다음 작업을 수행합니다.

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The fields are as follows:

- Management type of application instance: **LOCALLY_MANAGED** (dropdown)
- Firepower Management Center IP: (empty text box)
- Search domains: **cisco.com** (text box)
- Firewall Mode: **Routed** (dropdown)
- DNS Servers: **10.8.9.6** (text box)
- Firepower Management Center NAT ID: (empty text box)
- Fully Qualified Hostname: **ftd.example.cisco.com** (text box)
- Registration Key: (empty text box)
- Confirm Registration Key: (empty text box)
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Eventing Interface: (empty dropdown)

Buttons at the bottom: OK, Cancel

- a) **Management type of application instance**(애플리케이션 인스턴스의 관리 유형) 드롭다운 목록에서 **LOCALLY_MANAGED**를 선택합니다.
네이티브 인스턴스에서는 Firepower Management Center을 관리자로도 지원합니다. 논리적 디바이스를 구축한 후 관리자를 변경하면 구성이 지워지고 디바이스가 다시 초기화됩니다.
- b) **Search Domains**(검색 도메인)를 쉼표로 구분된 목록으로 입력합니다.
- c) **Firewall Mode**(방화벽 모드)에서는 **Routed**(라우팅) 모드만 지원합니다.

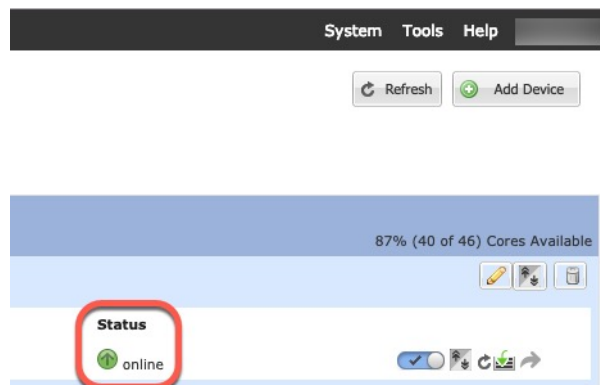
- d) **DNS Servers(DNS 서버)**를 쉼표로 구분된 목록으로 입력합니다.
- e) FTD의 **Fully Qualified Hostname(정규화된 호스트 이름)**을 입력합니다.
- f) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password(비밀번호)**를 입력합니다.

단계 7 **Agreement(계약)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 8 **OK(확인)**를 클릭하여 구성 대화 상자를 닫습니다.

단계 9 **Save(저장)**를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(논리적 디바이스)** 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 **Status(상태)**가 **online(온라인)**으로 표시되면 애플리케이션 내에서 보안 정책 구성을 시작할 수 있습니다.



단계 10 보안 정책 구성을 시작하려면 FDM 구성 가이드를 참조하십시오.

고가용성 쌍 추가

FTD 또는 ASA 고가용성(장애 조치라고도 함)은 FXOS가 아닌 애플리케이션 내에 구성됩니다. 그러나 고가용성을 사용할 수 있도록 새시를 준비하려는 경우 다음 단계를 참조하십시오.

시작하기 전에

[고가용성 요구 사항 및 사전 요건, 17 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 각 논리적 디바이스에 동일한 인터페이스를 할당합니다.

단계 2 페일오버 및 상태 링크용으로 데이터 인터페이스 1~2개를 할당합니다.

이러한 인터페이스는 두 새시 간의 고가용성 트래픽을 교환합니다. 페일오버 및 상태 링크를 함께 사용하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다. 사용 가능한 인터페이스가 있다면 페일오버 및 상태 링크를 각각 별도로 사용할 수 있습니다. 상태 링크에는 최대 대역폭이 필요합니다.

관리 유형 인터페이스는 페일오버 또는 상태 링크용으로 사용할 수 없습니다. 페일오버 인터페이스와 같은 네트워크 세그먼트에 다른 디바이스가 없는 상태로 새시 간에 스위치를 사용하는 것이 좋습니다.

컨테이너 인스턴스의 경우 데이터 공유 인터페이스는 페일오버 링크용으로 지원되지 않습니다. 상위 인터페이스 또는 EtherChannel에서 하위 인터페이스를 생성한 다음 각 인스턴스에 대해 페일오버 링크로 사용할 하위 인터페이스를 할당하는 것이 좋습니다. 동일한 상위 인터페이스에 있는 모든 하위 인터페이스를 페일오버 링크로 사용해야 합니다. 하위 인터페이스 하나를 페일오버 링크로 사용하고 다른 하위 인터페이스(또는 상위 인터페이스)를 일반 데이터 인터페이스로 사용할 수는 없습니다.

단계 3 논리적 디바이스에서 고가용성을 활성화합니다.

단계 4 고가용성을 활성화한 후에 인터페이스를 변경해야 하는 경우에는 먼저 스탠바이 유닛에서 변경을 수행한 다음 액티브 유닛에서 변경을 수행합니다.

참고 ASA의 경우 네트워크 모듈/EtherChannel을 제거하거나 EtherChannel에 인터페이스를 재할당하는 등 FXOS에서 인터페이스를 제거하면 ASA 구성에서 원래 명령이 유지되므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하는 경우에는 구성 전반에 걸쳐 영향을 줄 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.

클러스터 추가

클러스터링을 사용하면 여러 개의 디바이스를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. 여러 모듈을 포함하는 Firepower 9300은 단일 새시의 모든 모듈을 하나의 클러스터로 그룹화하는 인트라 새시 클러스터링(intra-chassis clustering)을 지원합니다. 여러 새시가 그룹화되는 새시 간 클러스터링을 사용할 수도 있습니다. Firepower 4100 Series 같은 단일 모듈 디바이스에는 새시 간 클러스터링이 유일한 옵션입니다.

Firepower 4100/9300 새시 클러스터링 정보

Firepower 4100/9300 새시에서 클러스터를 구축할 때는 다음 작업이 수행됩니다.

- 네이티브 인스턴스 클러스터링의 경우: 유닛 간 통신에 사용되는 클러스터 제어 링크(기본값: port-channel 48)를 생성합니다.

다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

새시 내 클러스터링(Firepower 9300 전용)의 경우, 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다.

새시 간 클러스터링의 경우, 새시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.

- 애플리케이션 내부에 클러스터 부트스트랩 구성을 생성합니다.

클러스터를 구축할 때, 새시 슈퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다. 클러스터링 환경을 사용자 정의하려는 경우, 사용자가 일부 부트스트랩 구성을 애플리케이션 내부에 구성할 수 있습니다.

- 데이터 인터페이스를 *Spanned* 인터페이스로 클러스터에 할당합니다.

새시 내 클러스터링의 경우, 스패 인터페이스는 새시 간 클러스터링과 마찬가지로 EtherChannel에 국한되지 않습니다. Firepower 9300 슈퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 Spanned(스팬) 모드에서 작동합니다. 새시 간 클러스터링의 경우, 모든 데이터 인터페이스에 Spanned EtherChannel을 사용해야 합니다.



참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

기본 유닛 및 보조 유닛 역할

클러스터의 멤버 중 하나는 기본 유닛입니다. 기본 유닛은 자동으로 결정됩니다. 기타 모든 멤버는 보조 유닛입니다.

기본 유닛에서만 모든 구성을 수행해야 하며 이후에 구성은 보조 유닛에 복제됩니다.

클러스터 제어 링크

네이티브 인스턴스 클러스터링의 경우: 클러스터 제어 링크는 Port-channel 48 인터페이스를 사용하여 자동으로 생성됩니다.

다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

새시 내 클러스터링의 경우, 이 인터페이스에는 멤버 인터페이스가 없습니다. 이 클러스터 유형 EtherChannel은 인트라 새시 클러스터링(intra-chassis clustering)을 위한 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 새시 간 클러스터링의 경우에는 EtherChannel에 인터페이스를 하나 이상 추가해야 합니다.

2-멤버 새시 간 클러스터의 경우 클러스터 제어 링크를 한 새시에서 다른 새시로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

새시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 새시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

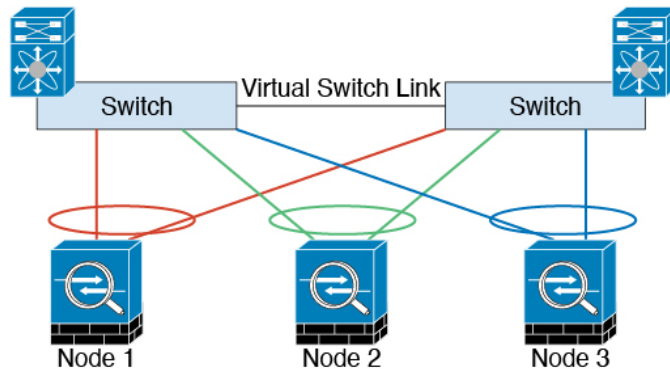
대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.



참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

새시 간 클러스터링을 위한 클러스터 제어 링크 이중화

다음 다이어그램은 EtherChannel을 VSS(Virtual Switching System), vPC(Virtual Port Channel), StackWise 또는 StackWise 가상 환경에서 클러스터 제어 링크로 사용하는 방법을 보여줍니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 중복 시스템의 일부인 경우 동일한 EtherChannel 내의 방화벽 인터페이스를 중복 시스템의 개별 스위치에 연결할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스펠 EtherChannel입니다.



새시 간 클러스터링을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 네트워크

Firepower 4100/9300 새시에서는 새시 ID 및 슬롯 ID `127.2.chassis_id.slot_id`를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 일반적으로 같은 EtherChannel의 다른 VLAN 하위 인터페이스를 사용하는 다중 인스턴스 클러스터의 경우 VLAN 분리로 인해 서로 다른 클러스터에 같은 IP 주소를 사용할 수 있습니다. 클러스터를 구축할 때 이 IP 주소를 맞춤 설정할 수 있습니다. 클러스터 제어 링크 네트워크는 유닛 간에 라우터를 포함할 수 없으며 레이어 2 스위칭만 허용됩니다. 사이트 간 트래픽의 경우에는 OTV(Overlay Transport Virtualization)를 사용하는 것이 좋습니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당해야 합니다. 이 인터페이스는 Spanned 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다.

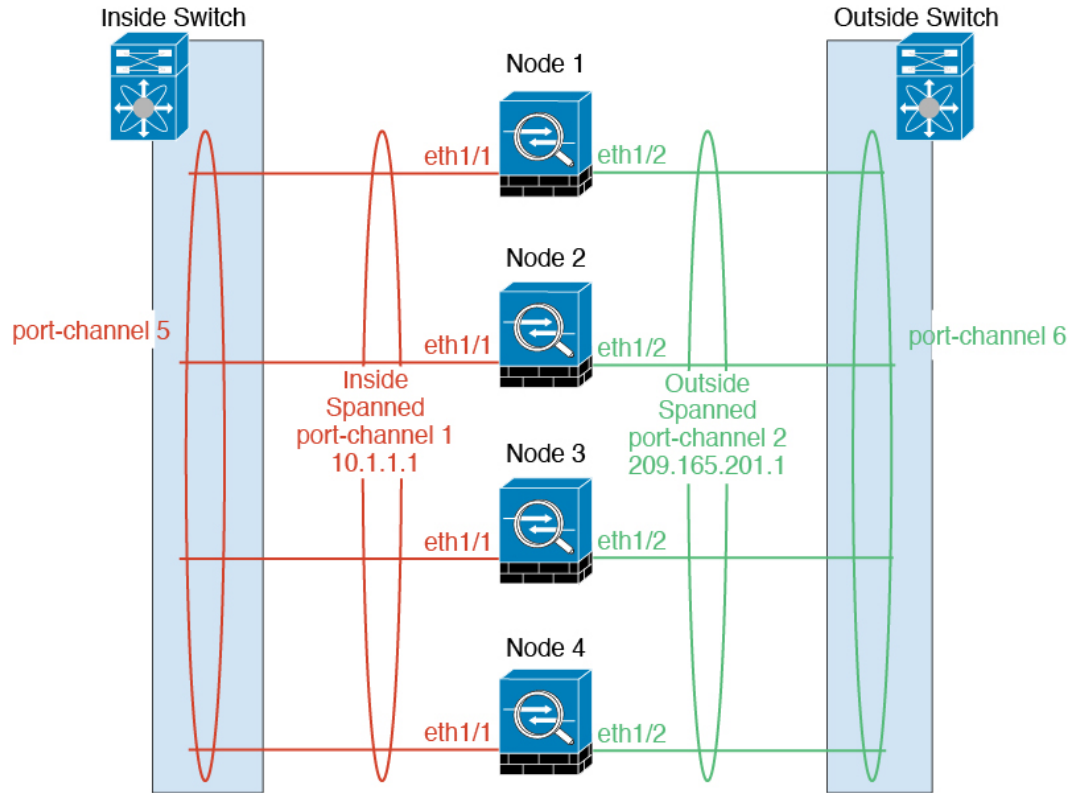
ASA의 경우, 기본 클러스터 IP 주소는 현재 기본 유닛에 항상 속해 있는 클러스터를 위한 고정 주소입니다. 또한 주소의 범위를 구성하여 현재 기본 유닛을 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 해야 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 기본 유닛이 변경될 경우 기본 클러스터 IP 주소는 새 기본 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 로컬 IP 주소는 라우팅에 사용되며 트러블슈팅에도 도움이 됩니다. 예를 들어, 현재 기본 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다. TFTP 또는 syslog 같은 아웃바운드 관리 트래픽의 경우 기본 유닛을 비롯한 각 유닛에서 로컬 IP 주소를 사용하여 서버에 연결합니다.

FTD의 경우, 동일한 네트워크의 각 유닛에 관리 IP 주소를 할당합니다. 각 유닛을 FMC에 추가할 때 이 IP 주소를 사용합니다.

스팬 EtherChannels

새시당 하나 이상의 인터페이스를 클러스터 내의 모든 새시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.

다중 인스턴스 클러스터의 경우 각 클러스터에 전용 데이터 EtherChannel이 필요하며 공유 인터페이스 또는 VLAN 하위 인터페이스를 사용할 수 없습니다.



사이트 간 클러스터링

사이트 간 설치 시 다음 권장 지침을 준수하면 클러스터링을 활용할 수 있습니다.

각 클러스터 새시를 별도의 사이트 ID에 속하도록 구성할 수 있습니다.

사이트 ID는 사이트별 MAC 주소 및 IP 주소와 작동합니다. 클러스터에서 이그레스되는 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면, 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다. 사이트별 MAC 주소 및 IP 주소는 Spanned EtherChannel만을 사용하는 라우팅 모드에서 지원됩니다.

사이트 ID는 LISP 검사를 사용한 플로우 모빌리티 활성화, 데이터 센터의 사이트 간 클러스터링에 대해 왕복 시간 레이턴시를 줄이고 성능을 개선하기 위한 관리자 지역화, 그리고 트래픽 플로우의 백업 소유자가 항상 소유자와 다른 사이트에 있는 연결에 대한 사이트 이중화에도 사용됩니다.

사이트 간 클러스터링에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 데이터 센터 인터커넥트 크기 조정 -클러스터링의 요구 사항 및 사전 요구 사항, 13 페이지
- 사이트 간 지침 -클러스터링 지침 및 제한 사항, 20 페이지
- 사이트 간 예시 -사이트 간 클러스터링 예시, 87 페이지

ASA 클러스터 추가

단일 Firepower 9300 새시를 새시 내 클러스터로 추가하거나 새시 간 클러스터링용으로 여러 새시를 추가할 수 있습니다. 새시 간 클러스터링의 경우, 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 추가한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 구성을 다음 새시에 복사합니다.

ASA 클러스터 생성

이미지 버전의 범위를 설정합니다.

Firepower 4100/9300 새시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다.

새시 간 클러스터링의 경우 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 컨피그레이션을 다음 새시에 복사합니다.

모듈을 설치하지 않은 경우에도 Firepower 9300 새시의 3개 모듈 슬롯 모두 또는 컨테이너 인스턴스, 각 슬롯의 컨테이너 인스턴스에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

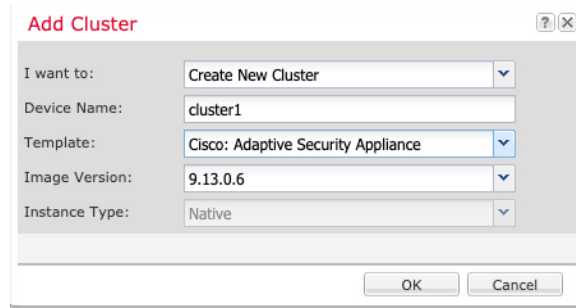
다중 컨텍스트 모드의 경우 먼저 논리적 디바이스를 구축한 다음 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화해야 합니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음, 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다.
- 다음 정보를 수집합니다.
 - 관리 인터페이스 ID, IP 주소, 네트워크 마스크
 - 게이트웨이 IP 주소

프로시저

-
- 단계 1 인터페이스를 구성합니다.
 - 단계 2 **Logical Devices**(논리적 디바이스)를 선택합니다.
 - 단계 3 **Add**(추가) > **Cluster**(클러스터)를 클릭하고 다음 파라미터를 설정합니다.



a) **I want to:**(수행할 작업:) > **Create New Cluster**(새 클러스터 생성)를 선택합니다.

b) **Device Name**(디바이스 이름)을 입력합니다.

이 이름은 내부적으로 새 시퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

c) **Template**(템플릿)은 **Cisco Adaptive Security Appliance**를 선택합니다.

d) **Image Version**(이미지 버전)을 선택합니다.

e) **Instance Type**(인스턴스 유형)의 경우, **Native**(네이티브) 유형만 지원됩니다.

f) **OK**(확인)를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 4 이 클러스터에 할당할 인터페이스를 선택합니다.

유효한 모든 인터페이스가 기본적으로 할당되어 있습니다. 여러 클러스터 유형의 인터페이스를 지정했다면 하나를 제외하고 모두 선택 해제합니다.

단계 5 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 6 **Cluster Information**(클러스터 정보) 페이지에서 다음 작업을 수행합니다.

Cisco: Adaptive Security Appliance - Bootstrap Configuration [?] [X]

Cluster Information Settings

Security Module

Security Module-1, Security Module-2, Security Module-3

Interface Information

Chassis ID:

Site ID:

Cluster Key:

Confirm Cluster Key:

Cluster Group Name:

Management Interface:

CCL Subnet IP:

DEFAULT

Address Type:

IPv4

Management IP Pool: -

Virtual IPv4 Address:

Network Mask:

Network Gateway:

OK Cancel

- a) 새시 간 클러스터링의 경우, **Chassis ID**(새시 ID) 필드에 새시 ID를 입력합니다. 클러스터의 각 새시는 고유 ID를 사용해야 합니다.

이 필드는 클러스터 제어 링크 Port-Channel 48에 멤버 인터페이스를 추가한 경우에만 나타납니다.

- b) 사이트 간 클러스터링의 경우 이 새시에 대해 **Site ID**(사이트 ID) 필드에 1~8의 사이트 ID를 입력합니다.
- c) **Cluster Key**(클러스터 키) 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.

공유 비밀은 1자~63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

d) **Cluster Group Name**(클러스터 그룹 이름)(논리적 디바이스 구성의 클러스터 그룹 이름)을 설정합니다.

이름은 1자~38자로 된 ASCII 문자열이어야 합니다.

e) **Management Interface**(관리 인터페이스)를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 새시 관리 포트와 별개입니다.

f) (선택 사항) **CCL Subnet IP**(CCL 서브넷 IP)를 *a.b.0.0*으로 설정합니다.

기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 이 경우 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 및 내부 (169.254.0.0/16) 주소를 제외한 모든 /16 네트워크 주소를 클러스터용 고유 네트워크에 지정합니다. 값을 0.0.0.0으로 설정하는 경우 기본 네트워크가 사용됩니다.

새시에서는 새시 ID 및 슬롯 ID *a.b.chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.

g) 관리 인터페이스의 **Address Type**(주소 유형)을 선택합니다.

이 정보는 ASA 구성에서 관리 인터페이스를 구성하는 데 사용됩니다. 다음 정보를 설정합니다.

- **Management IP Pool**(관리 IP 풀) - 시작 및 종료 주소를 하이픈으로 구분하여 입력해 로컬 IP 주소의 풀을 구성합니다. 이 중 하나는 인터페이스의 각 클러스터 유닛에 할당됩니다.

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. Firepower 9300에서는 모든 모듈 슬롯을 채우지 않은 경우에도 새시당 3개 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 제어 유닛에 속하는 가상 IP 주소(기본 클러스터 IP 주소)는 이러한 풀에 속하지 않습니다. 따라서 동일한 네트워크에서 기본 클러스터 IP 주소에 대한 IP 주소를 예약해 두어야 합니다. IPv4 및/또는 IPv6 주소를 사용할 수 있습니다.

- **Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)

- 네트워크 게이트웨이

- **Virtual IP address**(가상 IP 주소) — 현재 제어 유닛의 관리 IP 주소를 설정합니다. 이 IP 주소는 같은 네트워크의 클러스터 풀 주소로 있어야 하지만 풀의 일부는 아닙니다.

단계 7 **Settings**(설정) 페이지에서 다음 작업을 완료합니다.

Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information **Settings**

Firewall Mode:

Password:

Confirm Password:

- a) **Firewall Mode**(방화벽 모드) 드롭다운 목록에서 **Transparent**(투명) 또는 **Routed**(라우팅됨)를 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

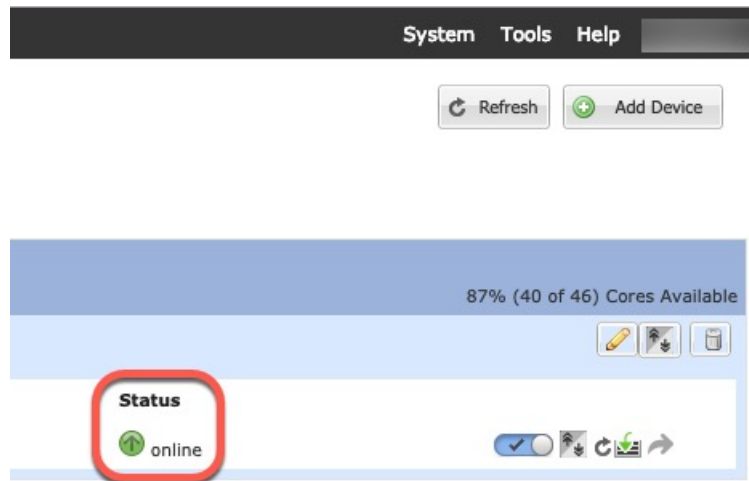
- b) 관리자 및 비밀번호 활성화에 대해 **Password**(비밀번호)를 입력하고 확인합니다.

비밀번호를 복구할 때는 사전 구성된 ASA 관리자가 있으면 유용합니다. FXOS 액세스 권한이 있다면 관리자 비밀번호를 잊어버린 경우 재설정할 수 있습니다.

단계 8 **OK**(확인)를 클릭하여 구성 대화 상자를 닫습니다.

단계 9 **Save**(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 상태가 **online**(온라인)으로 표시되면 나머지 클러스터 새시를 추가할 수도 있고, 새시 내 클러스터링의 경우 애플리케이션 내에서 클러스터 구성을 시작할 수도 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 10 새시 간 클러스터링의 경우, 다음 새시를 클러스터에 추가합니다.

- Firepower Chassis Manager의 첫 번째 새시에서 오른쪽 상단에 있는 **Show Configuration**(구성 표시) 아이콘을 클릭하여 표시된 클러스터 구성을 복사합니다.
- 다음 새시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.
- I want to:**(수행할 작업:) > **Join an Existing Cluster**(기존 클러스터에 조인)를 선택합니다.
- OK**(확인)를 클릭합니다.

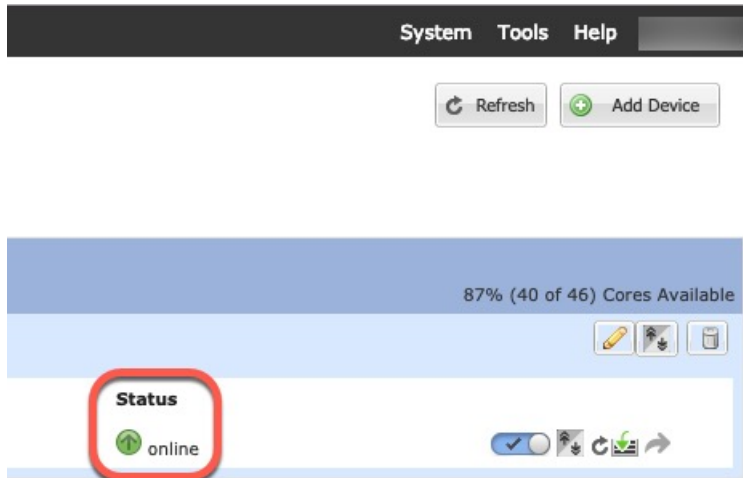
- e) **Copy Cluster Details**(클러스터 세부사항 복사) 상자에서 첫 번째 새시의 클러스터 구성에 붙여 넣고 **OK**(확인)를 클릭합니다.
- f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID**(새시 ID) - 고유한 새시 ID를 입력합니다.
- **Site ID**(사이트 ID) - 올바른 사이트 ID를 입력합니다.
- **Cluster Key**(클러스터 키) - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.

OK(확인)를 클릭합니다.

- g) **Save**(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status**(상태)가 **online**(온라인)으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 11 제어 유닛 ASA에 연결하여 클러스터링 컨피그레이션을 맞춤화합니다.

클러스터 멤버 더 추가

ASA 클러스터 멤버를 추가하거나 교체합니다.




참고 이 절차는 새시 추가 또는 교체 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 모듈을 추가하거나 교체하는 경우에는 모듈이 자동으로 추가됩니다.

시작하기 전에

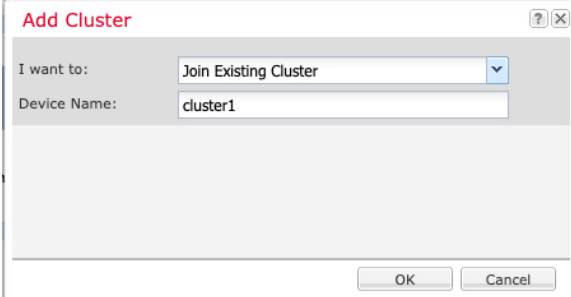
- 기존 클러스터에서 이 새 멤버의 관리 IP 주소 풀에 충분한 IP 주소가 있는지 확인하십시오. IP 주소가 충분하지 않은 경우, 이 새 멤버를 추가하기 전에 각 새시에서 기존 클러스터 부트스트랩 구성을 수정해야 합니다. 이러한 변경으로 인해 논리적 디바이스가 재시작됩니다.
- 인터페이스 구성은 새 새시에서 동일해야 합니다. FXOS 새시 구성 내보내기과 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.
- 다중 컨텍스트 모드인 경우 첫 번째 클러스터 멤버의 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화합니다. 그러면 추가 클러스터 멤버가 다중 컨텍스트 모드 구성을 자동으로 상속합니다.

프로시저

단계 1 기존 클러스터 Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다.

단계 2 오른쪽 상단의 구성 표시 아이콘()를 클릭하여 표시되는 클러스터 구성을 복사합니다.

단계 3 새 새시에서 Firepower Chassis Manager에 연결한 다음 **Add**(추가) > **Cluster**(클러스터)를 클릭합니다.



The image shows a 'Add Cluster' dialog box with the following fields and options:

- I want to:** A dropdown menu with 'Join Existing Cluster' selected.
- Device Name:** A text input field containing 'cluster1'.
- Buttons: 'OK' and 'Cancel' at the bottom.

단계 4 **I want to:**(수행할 작업:) > **Join an Existing Cluster**(기존 클러스터에 조인)를 선택합니다.

단계 5 **Device Name**(디바이스 이름)에 논리적 디바이스의 이름을 입력합니다.

단계 6 **OK**(확인)를 클릭합니다.

단계 7 **Copy Cluster Details**(클러스터 세부사항 복사) 상자에서 첫 번째 새시의 클러스터 구성에 붙여 넣고 **OK**(확인)를 클릭합니다.

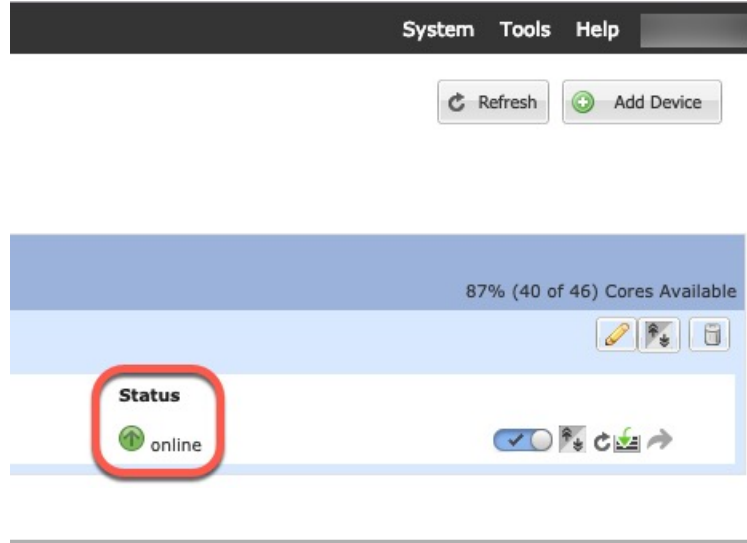
단계 8 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID**(새시 ID) - 고유한 새시 ID를 입력합니다.
- **Site ID**(사이트 ID) - 올바른 사이트 ID를 입력합니다.
- **Cluster Key**(클러스터 키) - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.

OK(확인)를 클릭합니다.

단계 9 **Save**(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status**(상태)가 **online**(온라인)으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



FTD 클러스터 추가

네이티브 모드에서 단일 Firepower 9300 새시를 새시 내 클러스터로 추가하거나 새시 간 클러스터링 용으로 여러 새시를 추가할 수 있습니다.

다중 인스턴스 모드에서 단일 Firepower 9300 새시에 하나 이상의 클러스터를 새시 내 클러스터로 추가하거나(각 모듈에 인스턴스를 포함해야 함) 새시 간 클러스터링 용으로 여러 새시에 하나 이상의 클러스터를 추가할 수 있습니다.

새시 간 클러스터링의 경우 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 추가한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 구성을 다음 새시에 복사합니다.

FTD 클러스터 생성

Firepower 4100/9300 새시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다.

새시 간 클러스터링의 경우 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 컨피그레이션을 다음 새시에 복사합니다.

모듈을 설치하지 않은 경우에도 Firepower 9300 새시의 3개 모듈 슬롯 모두 또는 컨테이너 인스턴스, 각 슬롯의 컨테이너 인스턴스에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음, 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다.
- 컨테이너 인스턴스의 경우 기본 프로필을 사용하지 않으려면 [컨테이너 인스턴스에 대한 리소스 프로파일 추가](#)에 따라 리소스 프로필을 추가합니다.
- 컨테이너 인스턴스의 경우 컨테이너 인스턴스를 처음으로 설치하기 전에 디스크가 올바른 형식을 갖도록 보안 모듈/엔진을 다시 초기화해야 합니다. **Security Modules**(보안 모듈) 또는 **Security Engine**(보안 엔진)을 선택하고 다시 초기화 아이콘(🔄)을 클릭합니다. 기존 논리적 디바이스가 삭제된 후에 새 디바이스로 재설치되며 로컬 애플리케이션 구성은 손실됩니다. 기본 인스턴스를 컨테이너 인스턴스로 교체할 때는 어떤 경우든 기본 인스턴스를 삭제해야 합니다. 기본 인스턴스를 컨테이너 인스턴스로 자동 마이그레이션할 수는 없습니다. 자세한 내용은 [보안 모듈/엔진 확인 다시 초기화](#)를 참조하십시오.
- 다음 정보를 수집합니다.
 - 관리 인터페이스 ID, IP 주소, 네트워크 마스크
 - 게이트웨이 IP 주소
 - FMC 선택한 IP 주소 및/또는 NAT ID
 - DNS 서버 IP 주소
 - FTD 호스트 이름 및 도메인 이름

프로시저

단계 1 인터페이스를 구성합니다.

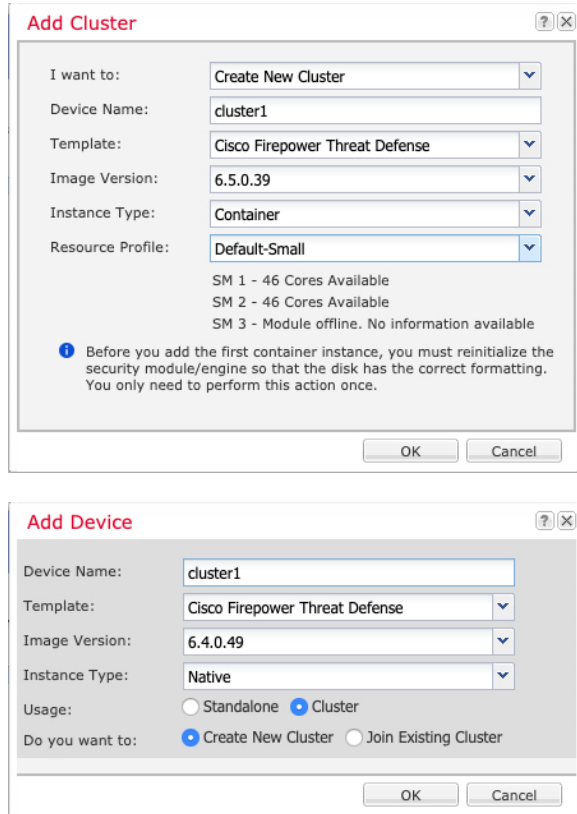
단계 2 **Logical Devices**(논리적 디바이스)를 선택합니다.

단계 3 **Add**(추가) > **Cluster**(클러스터)를 클릭하고 다음 파라미터를 설정합니다.

그림 6: 네이티브 클러스터

Field	Value
I want to:	Create New Cluster
Device Name:	cluster1
Template:	Cisco Firepower Threat Defense
Image Version:	6.5.0.1159
Instance Type:	Native

그림 7: 다중 인스턴스 클러스터



- a) **I want to:**(수행할 작업:)> **Create New Cluster**(새 클러스터 생성)를 선택합니다.
- b) **Device Name**(디바이스 이름)을 입력합니다.

이 이름은 내부적으로 새시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

- c) **Template**(템플릿)에서 **Cisco Firepower Threat Defense**를 선택합니다.
- d) **Image Version**(이미지 버전)을 선택합니다.
- e) **Instance Type**(인스턴스 유형)의 경우 **Native**(네이티브) 또는 **Container**(컨테이너)를 선택합니다.

네이티브 인스턴스는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다. 컨테이너 인스턴스는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다.

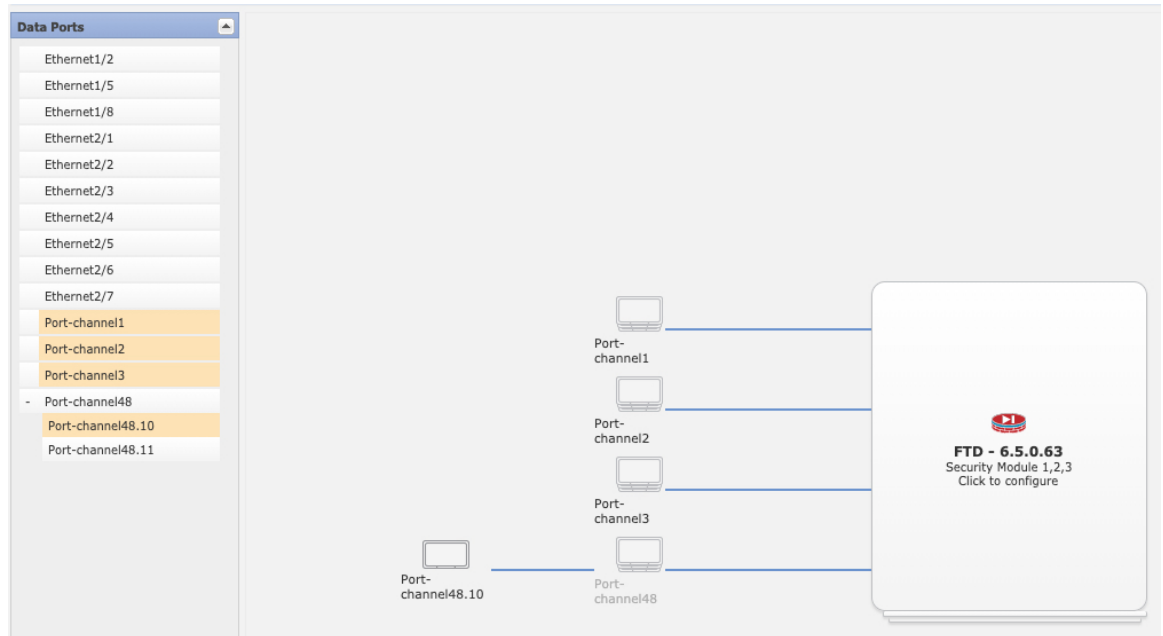
- f) (컨테이너 인스턴스만 해당) **Resource Type**(리소스 유형)의 드롭다운 목록에서 리소스 프로파일 중 하나를 선택합니다.

Firepower 9300의 경우 이 프로파일은 보안 모듈의 각 인스턴스에 적용됩니다. 이 절차에서 나중에 보안 모듈별로 서로 다른 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다. 클러스터를 생성하기 전에 올바른 프로파일을 선택하는 것이 좋습니다. 새 프로파일을 생성해야 하는 경우 클러스터 생성을 취소하고 **컨테이너 인스턴스에 대한 리소스 프로파일 추가**를 사용해 하나를 추가합니다.

g) **OK(확인)**를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 4 이 클러스터에 할당할 인터페이스를 선택합니다.



네이티브 모드 클러스터링의 경우: 유효한 모든 인터페이스가 기본적으로 할당되어 있습니다. 여러 클러스터 유형의 인터페이스를 지정했다면 하나를 제외하고 모두 선택 해제합니다.

다중 인스턴스 클러스터링의 경우: 클러스터에 할당할 각 데이터 인터페이스를 선택하고 클러스터 유형 포트 채널 또는 포트 채널 하위 인터페이스도 선택합니다.

단계 5 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 6 Cluster Information(클러스터 정보) 페이지에서 다음 작업을 수행합니다.

그림 8: 네이티브 클러스터

The image shows a configuration window titled "Cisco Firepower Threat Defense - Bootstrap Configuration". It has a tabbed interface with "Cluster Information", "Settings", "Interface Information", and "Agreement". The "Cluster Information" tab is active and contains the following fields:

- Security Module:** Security Module-1, Security Module-2, Security Module-3
- Interface Information:**
 - Chassis ID: 1
 - Site ID: 1
 - Cluster Key: ••••
 - Confirm Cluster Key: ••••
 - Cluster Group Name: cluster1
 - Management Interface: Ethernet1/4 (dropdown menu)
 - CCL Subnet IP: Eg:x.x.0.0

At the bottom of the window are "OK" and "Cancel" buttons.

그림 9: 다중 인스턴스 클러스터

- (Firepower 9300 컨테이너 인스턴스만 해당) 보안 모듈(SM) 및 리소스 프로파일 선택 영역에서 별도로 다른 리소스 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다.
- 새시 간 클러스터링의 경우, **Chassis ID**(새시 ID) 필드에 새시 ID를 입력합니다. 클러스터의 각 새시는 고유 ID를 사용해야 합니다.

이 필드는 클러스터 제어 링크 Port-Channel 48에 멤버 인터페이스를 추가한 경우에만 나타납니다.

- 사이트 간 클러스터링의 경우 이 새시에 대해 **Site ID**(사이트 ID) 필드에 1~8의 사이트 ID를 입력합니다. FlexConfig 기능, 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FMC FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.
- Cluster Key**(클러스터 키) 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.

공유 비밀은 1자~63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

- Cluster Group Name**(클러스터 그룹 이름)(논리적 디바이스 구성의 클러스터 그룹 이름)을 설정합니다.

이름은 1자 ~ 38자로 된 ASCII 문자열이어야 합니다.

- f) **Management Interface**(관리 인터페이스)를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 새시 관리 포트와 별개입니다.

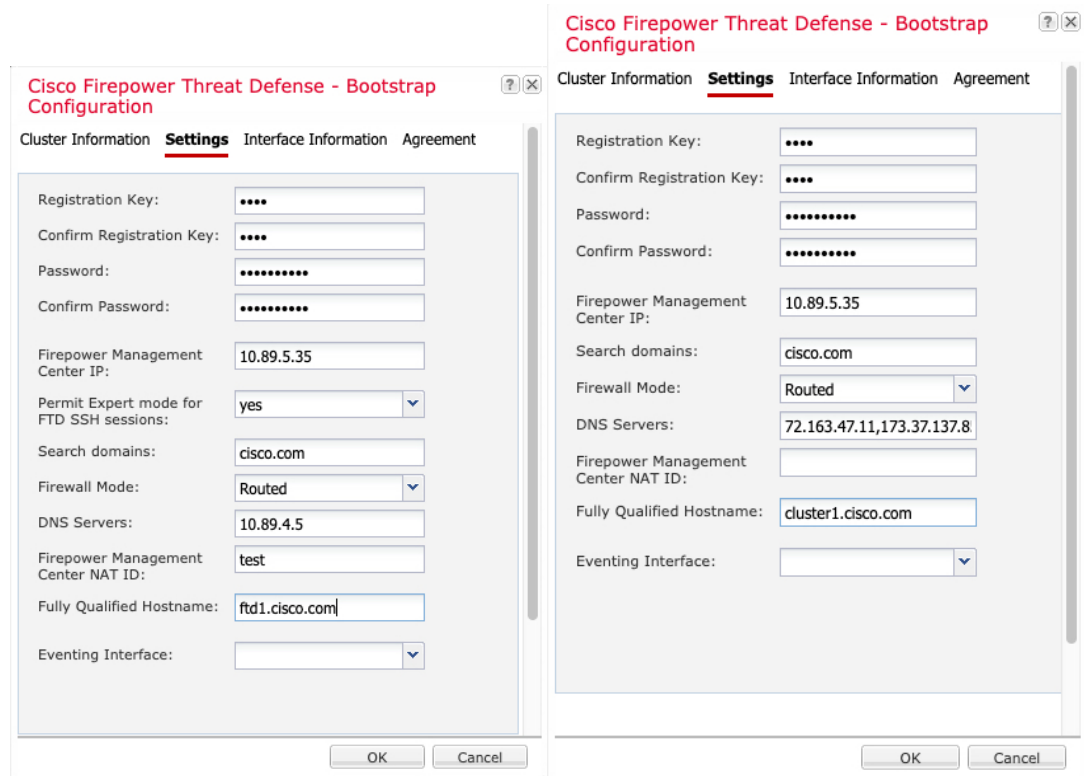
하드웨어 바이패스 지원 인터페이스를 Management(관리) 인터페이스로 할당할 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다.

- g) (선택 사항) **CCL Subnet IP**(CCL 서브넷 IP)를 *a.b.0.0*으로 설정합니다.

기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 이 경우 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 및 내부 (169.254.0.0/16) 주소를 제외한 모든 /16 네트워크 주소를 클러스터용 고유 네트워크에 지정합니다. 값을 0.0.0.0으로 설정하는 경우 기본 네트워크가 사용됩니다.

새시에서는 새시 ID 및 슬롯 ID *a.b.chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.

단계 7 **Settings**(설정) 페이지에서 다음 작업을 완료합니다.



- a) **Registration Key**(등록 키) 필드에 등록하는 동안 FMC와 클러스터 멤버 간에 공유할 키를 입력합니다.

이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

- b) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password(비밀번호)**를 입력합니다.
- c) **Firepower Management Center IP** 필드에 FMC를 관리하기 위한 IP 주소를 입력합니다. FMC IP 주소를 알 수 없는 경우, 이 필드를 비워두고 **Firepower Management Center NAT ID** 필드에 암호를 입력합니다.
- d) (선택 사항) 컨테이너 인스턴스의 경우, **Permit Export mode from FTD SSH sessions(FTD SSH 세션에서 전문가 모드 허용)**에 대해 **Yes(예)** 또는 **No(아니요)**를 선택합니다. 전문가 모드에서는 고급 트러블슈팅을 위한 FTD 셸 액세스 기능이 제공됩니다.

이 옵션에 대해 **Yes(예)**를 선택하는 경우 SSH 세션에서 컨테이너 인스턴스에 직접 액세스할 수 있는 사용자가 전문가 모드를 시작할 수 있습니다. **No(아니요)**를 선택하는 경우에는 FXOS CLI에서 컨테이너 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리할 수 있도록 **No(아니요)**를 선택하는 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 FTD CLI에서 **expert** 명령을 사용합니다.

- e) (선택 사항) **Search Domains(검색 도메인)** 필드에 관리 네트워크의 쉼표로 구분된 검색 도메인 목록을 입력합니다.
- f) (선택 사항) **Firewall Mode(방화벽 모드)** 드롭다운 목록에서 **Transparent(투명)** 또는 **Routed(라우팅됨)**를 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

- g) (선택 사항) **DNS Servers(DNS 서버)** 필드에 쉼표로 구분된 DNS 서버 목록을 입력합니다.
예를 들어, FMC의 호스트 이름을 지정하는 경우, FTD에서는 DNS를 사용합니다.
- h) (선택 사항) 새 디바이스로 클러스터를 추가할 때 FMC에도 입력할 암호를 **Firepower Management Center NAT ID** 필드에 입력합니다.

일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. 1~37자의 임의의 텍스트 문자열을 NAT ID로 지정할 수 있습니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

- i) (선택 사항) **Fully Qualified Hostname(정규화된 호스트 이름)** 필드에 FTD 디바이스의 정규화된 이름을 입력합니다.

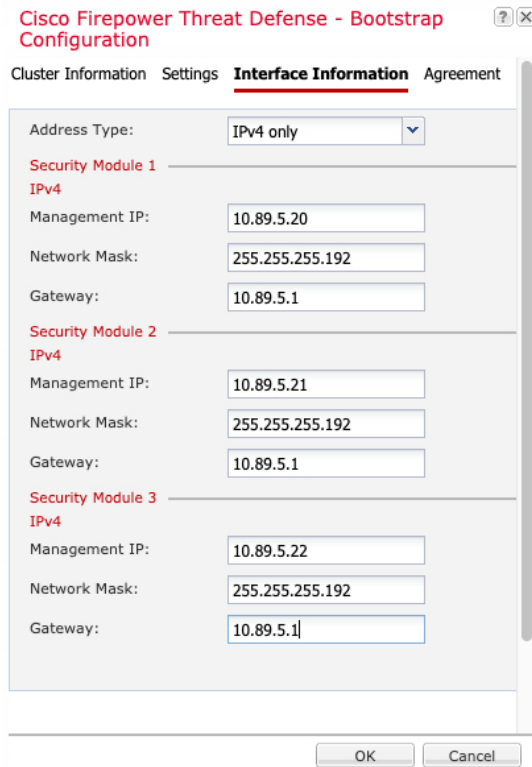
유효한 문자는 a부터 z까지의 문자, 0과 9 사이의 숫자, 점(.) 및 하이픈(-)입니다. 최대 문자 수는 253자입니다.

- j) (선택 사항) **Eventing Interface(Eventing 인터페이스)** 드롭다운 목록에서 이벤트가 전송되어야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

이벤트에 사용할 별도의 인터페이스를 지정하려면 인터페이스를 **Firepower** 이벤트 처리 인터페이스로 구성해야 합니다. 하드웨어 바이패스 지원 인터페이스를 **Eventing(이벤트) 인터페이스**로 할당하는 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다.

단계 8 Interface Information(인터페이스 정보) 페이지에서 클러스터의 각 보안 모듈의 관리 IP 주소를 구성합니다. **Address Type(주소 유형)** 드롭다운 목록에서 주소 유형을 선택한 다음 각 보안 모듈에 대해 다음 작업을 수행합니다.

참고 모듈을 설치하지 않은 경우에도 새시의 3개 모듈 슬롯 모두에 대해 IP 주소를 설정해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.



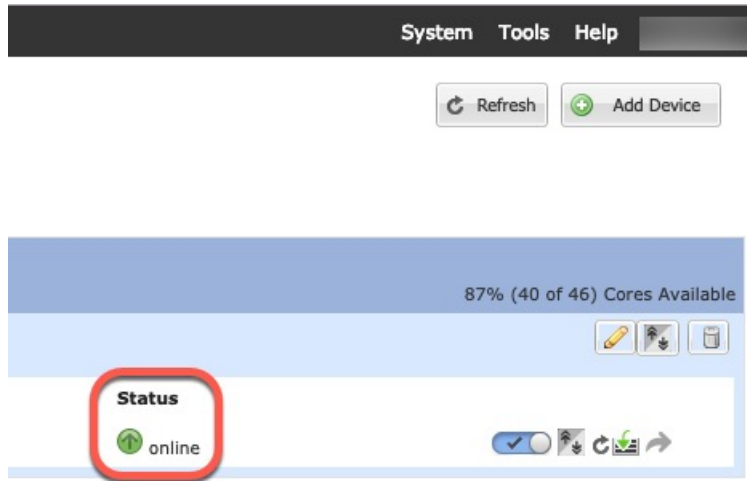
- a) **Management IP(관리 IP)** 필드에서 IP 주소를 구성합니다.
각 모듈에 대해 동일한 네트워크에서 고유한 IP 주소를 지정합니다.
- b) **Network Mask(네트워크 마스크)** 또는 **Prefix Length(접두사 길이)**를 입력합니다.
- c) **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.

단계 9 Agreement(계약) 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 10 OK(확인)를 클릭하여 구성 대화 상자를 닫습니다.

단계 11 Save(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 상태가 **online**(온라인)으로 표시되면 나머지 클러스터 새시를 추가할 수도 있고, 새시 내 클러스터링의 경우 애플리케이션 내에서 클러스터 구성을 시작할 수도 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 12 새시 간 클러스터링의 경우, 다음 새시를 클러스터에 추가합니다.

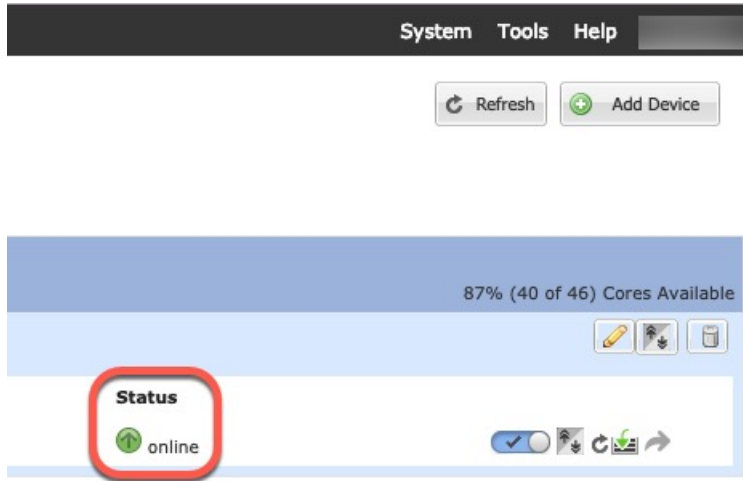
- Firepower Chassis Manager의 첫 번째 새시에서 오른쪽 상단에 있는 **Show Configuration**(구성 표시) 아이콘을 클릭하여 표시된 클러스터 구성을 복사합니다.
- 다음 새시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.
- I want to:(수행할 작업:)** > **Join an Existing Cluster**(기존 클러스터에 조인)를 선택합니다.
- OK**(확인)를 클릭합니다.
- Copy Cluster Details**(클러스터 세부사항 복사) 상자에서 첫 번째 새시의 클러스터 구성에 붙여 넣고 **OK**(확인)를 클릭합니다.
- 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID**(새시 ID) - 고유한 새시 ID를 입력합니다.
- **Site ID**(사이트 ID) - 사이트 간 클러스터링의 경우 이 새시에 대해 1~8 사이의 사이트 ID를 입력합니다. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 FMC FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.
- **Cluster Key**(클러스터 키) - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP**(관리 IP) - 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인)를 클릭합니다.

g) **Save(저장)**를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(상태)**가 **online(온라인)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 13 관리 IP 주소를 사용하여 제어 유닛을 FMC에 추가합니다.

FMC에 추가하기 전에 모든 클러스터 유닛이 FXOS에서 성공적으로 형성된 클러스터에 있어야 합니다.

그러면 FMC에서 데이터 유닛을 자동으로 탐지합니다.

클러스터 노드 추가

기존 클러스터에서 FTD 클러스터 노드를 추가하거나 교체합니다. FXOS에서 새 클러스터 노드를 추가할 때 FMC에서는 노드를 자동으로 추가합니다.



참고 이 절차의 FXOS 단계는 새 새시 추가 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 새 모듈을 추가하는 경우에는 모듈이 자동으로 추가됩니다.

시작하기 전에

- 교체 시 기존 클러스터 노드를 FMC에서 삭제해야 합니다. 새 노드로 교체할 경우, 해당 유닛은 FMC에서 새 디바이스로 간주됩니다.


- 인터페이스 구성은 새 새시에서 동일해야 합니다. FXOS 새시 구성 내보내기과 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.

프로시저

단계 1 이전에 FMC를 사용하여 FTD 이미지를 업그레이드한 경우 클러스터의 각 새시에서 다음 단계를 수행합니다.

FMC에서 업그레이드할 때 FXOS 구성의 시작 버전이 업데이트되지 않았으며 독립형 패키지가 새시에 설치되지 않았습니다. 새 노드가 올바른 이미지 버전을 사용하여 클러스터에 참여할 수 있도록 이러한 항목을 모두 수동으로 설정해야 합니다.

참고 패치 릴리스만 적용한 경우 이 단계를 건너뛸 수 있습니다. Cisco는 패치용 독립형 패키지를 제공하지 않습니다.

- System(시스템) > Updates(업데이트)** 페이지를 사용하여 새시에 실행 중인 FTD 이미지를 설치합니다.
- Logical Devices(논리적 디바이스)**를 클릭하고 버전 설정 아이콘()를 클릭합니다. 여러 모듈이 있는 Firepower 9300의 경우 각 모듈의 버전을 설정합니다.

Startup Version(시작 버전)에는 구축에 사용한 원래 패키지가 표시됩니다. **Current Version(현재 버전)**에는 업그레이드한 버전이 표시됩니다.

- New Version(새 버전)** 드롭다운 메뉴에서 업로드한 버전을 선택합니다. 이 버전은 표시된 현재 버전과 일치해야 하며, 새 버전과 일치하도록 시작 버전을 설정합니다.
- 새 새시에 새 이미지 패키지가 설치되어 있는지 확인합니다.

단계 2 기존 클러스터 새시 Firepower Chassis Manager에서 **Logical Devices(논리적 디바이스)**를 클릭합니다.

단계 3 오른쪽 상단에 있는 설정 표시 아이콘을 클릭하여 표시된 클러스터 설정을 복사합니다.

단계 4 새 새시에서 Firepower Chassis Manager에 연결한 다음 **Add(추가) > Cluster(클러스터)**를 클릭합니다.

단계 5 **Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 입력합니다.

단계 6 **OK(확인)**를 클릭합니다.

단계 7 **Copy Cluster Details(클러스터 세부사항 복사)** 상자에서 첫 번째 새시의 클러스터 구성에 붙여 넣고 **OK(확인)**를 클릭합니다.

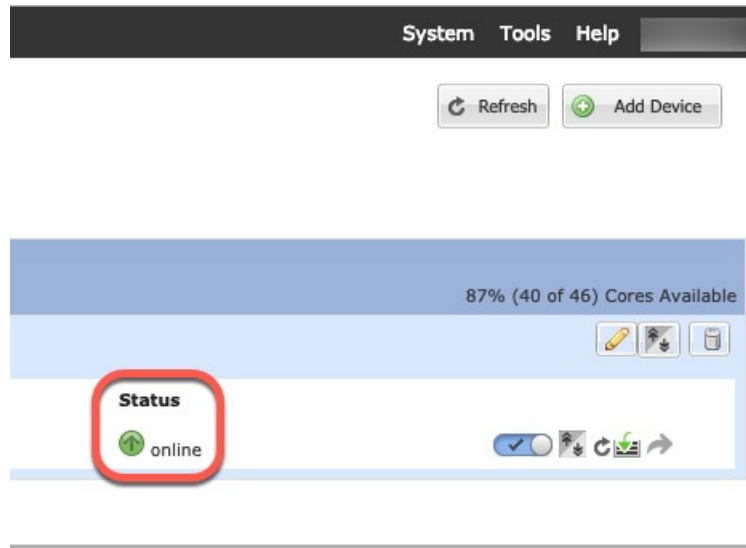
단계 8 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID(새시 ID)** - 고유한 새시 ID를 입력합니다.
- **Site ID(사이트 ID)** - 사이트 간 클러스터링의 경우 이 새시에 대해 1~8 사이의 사이트 ID를 입력합니다. FMC FlexConfig 기능을 통해서만 이 기능을 구성할 수 있습니다.
- **Cluster Key(클러스터 키)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(관리 IP)** - 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인)를 클릭합니다.

단계 9 Save(저장)를 클릭합니다.

새시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices**(논리적 디바이스) 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status**(상태)가 **online**(온라인)으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



Radware DefensePro 구성

Cisco Firepower 4100/9300 새시에서는 단일 블레이드에 있는 여러 서비스(예: 방화벽 및 서드파티 DDoS 애플리케이션)를 지원할 수 있습니다. 이 애플리케이션 및 서비스는 서비스 체인을 구성하기 위해 함께 연결될 수 있습니다.

Radware DefensePro 정보

현재 지원되는 서비스 체이닝 구성에서 서드파티 Radware DefensePro 가상 플랫폼을 설치하여 ASA 방화벽 또는 FTD 앞에서 실행할 수 있습니다. Radware DefensePro는 Firepower 4100/9300 새시에서 DDoS(Distributed Denial-of-Service) 탐지 및 완화 기능을 제공하는 KVM 기반 가상 플랫폼입니다. 서비스 체이닝이 Firepower 4100/9300 새시에서 활성화된 경우, 네트워크의 트래픽은 기본 ASA 또는 FTD 방화벽에 도달하기 전에 먼저 DefensePro 가상 플랫폼을 통과해야 합니다.



참고

- Radware DefensePro 가상 플랫폼은 *Radware vDP*(가상 DefensePro) 또는 간단하게 *vDP*라고도 합니다.
- Radware DefensePro 가상 플랫폼은 경우에 따라 링크 데코레이터라고도 합니다.

Radware DefensePro에 대한 사전 요구 사항

Firepower 4100/9300 새시에 Radware DefensePro를 구축하기 전에 **etc/UTC** 표준 시간대로 NTP 서버를 사용하도록 Firepower 4100/9300 새시를 구성해야 합니다. Firepower 4100/9300 새시에서 날짜 및 시간을 설정하는 방법에 대한 자세한 내용은 [날짜 및 시간 설정](#)을 참조하십시오.

서비스 체이닝 관련 지침

모델

- ASA - Radware DefensePro(vDP) 플랫폼은 다음 모델에서 ASA와 함께 지원됩니다.
 - Firepower 9300
 - Firepower 4110
 - Firepower 4115
 - Firepower 4120
 - Firepower 4125
 - Firepower 4140
 - Firepower 4145
 - Firepower 4150
- FTD- Radware DefensePro 플랫폼은 다음 모델에서 FTD와 함께 지원됩니다.
 - Firepower 9300
 - Firepower 4110 - 논리적 디바이스와 동시에 데코레이터를 구축해야 합니다. 논리적 디바이스가 이미 디바이스에 구성된 이후에는 데코레이터를 설치할 수 없습니다.
 - Firepower 4112
 - Firepower 4115
 - Firepower 4120 - 논리적 디바이스와 동시에 데코레이터를 구축해야 합니다. 논리적 디바이스가 이미 디바이스에 구성된 이후에는 데코레이터를 설치할 수 없습니다.
 - Firepower 4125

- Firepower 4140
- Firepower 4145
- Firepower 4150

추가 지침

- 서비스 체이닝은 새시 간 클러스터 구성에서 지원되지 않습니다. 그러나 새시 간 클러스터 시나리오의 독립형 구성에서는 Radware DefensePro(vDP) 애플리케이션을 구축할 수 있습니다.

독립형 논리적 디바이스에 Radware DefensePro 구성

다음 절차는 독립형 ASA 또는 FTD 논리적 디바이스의 앞에 있는 단일 서비스 체인에 Radware DefensePro를 설치하는 방법을 보여줍니다.



참고 이 절차가 끝날 때 vDP 애플리케이션을 설정하고 변경 사항을 커밋하면 논리적 디바이스(ASA 또는 FTD)가 재부팅됩니다.

Firepower 4120 또는 4140 보안 어플라이언스에서 ASA 앞에 Radware vDP를 설치하는 경우 FXOS CLI를 사용하여 데코레이터를 구축해야 합니다. Firepower 4100 디바이스에서 ASA 앞의 서비스 체인에 Radware DefensePro를 설치하고 구성하는 방법에 대한 전체 CLI 지침은 FXOS CLI 환경 설정 가이드를 참조하십시오.

시작하기 전에

- Cisco.com에서 vDP 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#) 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Security Appliance에 이미지 업로드](#) 참조).
- 새시 내 클러스터에서 독립형 구성으로 Radware DefensePro 애플리케이션을 구축할 수 있습니다. 새시 내 클러스터링에 대해서는 [인트라 새시\(Intra-Chassis\) 클러스터에 Radware DefensePro 구성, 66 페이지](#) 섹션을 참조하십시오.

프로시저

단계 1 vDP용으로 별도의 관리 인터페이스를 사용하려는 경우 인터페이스를 활성화한 다음 [실제 인터페이스 구성](#)에 따라 mgmt 유형으로 설정합니다. 그렇지 않은 경우에는 애플리케이션 관리 인터페이스를 공유할 수 있습니다.

단계 2 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다.

Logical Devices(논리적 디바이스) 페이지는 새시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 이를 알리는 메시지가 표시됩니다.

- 단계 3 독립형 ASA 또는 FTD 논리적 디바이스를 생성합니다(독립형 ASA 추가, 25 페이지 또는 FMC에 대한 독립형 FTD 추가, 28 페이지 참조).
- 단계 4 **Decorators**(데코레이터) 영역에서 vDP를 선택합니다. Radware: Virtual DefensePro - Configuration(Radware: Virtual DefensePro - 구성) 창이 나타납니다. **General Information**(일반 정보) 탭에서 다음 필드를 구성합니다.
- 단계 5 둘 이상의 vDP 버전을 Firepower 4100/9300 새시에 업로드한 경우, 사용할 버전을 **Version**(버전) 드롭다운에서 선택합니다.
- 단계 6 리소스를 구성할 수 있는 Radware DefensePro 애플리케이션이 있는 경우 **Resource Profile**(리소스 프로필) 드롭다운 아래에 지원되는 리소스 프로필 목록이 나타납니다. 디바이스에 할당할 리소스 프로필을 선택합니다. 리소스 프로필을 선택하지 않으면 기본 설정이 사용됩니다.
- 단계 7 **Management Interface**(관리 인터페이스) 드롭다운에서 이 절차의 1단계에서 생성한 관리 인터페이스를 선택합니다.
- 단계 8 **Address Type**(주소 유형)을 IPv4 전용, IPv6 전용 또는 IPv4 및 IPv6 중에서 선택합니다.
- 단계 9 이전 단계의 **Address Type**(주소 유형) 선택을 기준으로 다음 필드를 구성합니다.
- Management IP**(관리 IP) 필드에서 로컬 IP 주소를 구성합니다.
 - IPv4 전용: **Network Mask**(네트워크 마스크)를 입력합니다.
IPv6 전용: **Prefix Length**(접두사 길이)를 입력합니다.
 - Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.
- 단계 10 디바이스에 할당할 각 데이터 포트 옆에 있는 체크 박스를 클릭합니다.
- 단계 11 **OK**(확인)를 클릭합니다.
- 단계 12 **Save**(저장)를 클릭합니다.

FXOS에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 지정된 보안 모듈에 입력하여 논리적 디바이스를 구축합니다.

다음에 수행할 작업

DefensePro 애플리케이션의 비밀번호를 설정합니다. 비밀번호를 설정할 때까지 애플리케이션은 온라인 상태가 되지 않습니다. 자세한 내용은 cisco.com에서 Radware DefensePro DDoS 완화 사용 설명서를 참조하십시오.

인트라 새시(Intra-Chassis) 클러스터에 Radware DefensePro 구성

다음 절차는 Radware DefensePro 이미지를 설치하고 이 이미지를 ASA 또는 FTD 내장 새시 클러스터 앞에 있는 서비스 체인에 구성하는 방법을 보여줍니다.



참고 서비스 체이닝은 새시 간 클러스터 구성에서 지원되지 않습니다. 그러나 새시 간 클러스터 시나리오의 독립형 구성에서는 Radware DefensePro 애플리케이션을 구축할 수 있습니다.

시작하기 전에

- Cisco.com에서 vDP 이미지를 다운로드(Cisco.com에서 이미지 다운로드 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다(Security Appliance에 이미지 업로드 참조).

프로시저

- 단계 1 vDP용으로 별도의 관리 인터페이스를 사용하려는 경우 인터페이스를 활성화한 다음 **실제 인터페이스 구성**에 따라 mgmt 유형으로 설정합니다. 그렇지 않은 경우에는 애플리케이션 관리 인터페이스를 공유할 수 있습니다.
- 단계 2 ASA 또는 FTD 내장 새시 클러스터를 구성합니다(ASA 클러스터 생성, 44 페이지 또는 FTD 클러스터 생성, 51 페이지 참조).
- 인트라 새시 클러스터를 구성하는 마지막 절차에서 **Save(저장)**를 클릭하기 전에 먼저 다음 단계를 수행하여 vDP 데코레이터를 클러스터에 추가해야 합니다.
- 단계 3 **Decorators(데코레이터)** 영역에서 vDP를 선택합니다. **Radware: Virtual DefensePro - Configuration(Radware: Virtual DefensePro - 구성)** 대화 상자가 나타납니다. **General Information(일반 정보)** 탭에서 다음 필드를 구성합니다.
- 단계 4 둘 이상의 vDP 버전을 Firepower 4100/9300 새시에 업로드한 경우, 사용할 vDP 버전을 **Version(버전)** 드롭다운에서 선택합니다.
- 단계 5 리소스를 구성할 수 있는 Radware DefensePro 애플리케이션이 있는 경우 **Resource Profile(리소스 프로파일)** 드롭다운 아래에 지원되는 리소스 프로파일 목록이 나타납니다. 디바이스에 할당할 리소스 프로필을 선택합니다. 리소스 프로필을 선택하지 않으면 기본 설정이 사용됩니다.
- 단계 6 **Management Interface(관리 인터페이스)** 드롭다운에서 관리 인터페이스를 선택합니다.
- 단계 7 vDP 데코레이터에 할당할 각 데이터 포트 옆에 있는 확인란을 클릭합니다.
- 단계 8 **Interface Information(인터페이스 정보)** 탭을 클릭합니다.
- 단계 9 사용할 **Address Type(주소 유형)**을 IPv4 전용, IPv6 전용 또는 IPv4 및 IPv6 중에서 선택합니다.
- 단계 10 각 보안 모듈에 대해 다음 필드를 구성합니다. 표시되는 필드는 이전 단계의 **Address Type(주소 유형)** 선택에 따라 결정됩니다.
- a) **Management IP(관리 IP)** 필드에서 로컬 IP 주소를 구성합니다.
 - b) IPv4 전용: **Network Mask(네트워크 마스크)**를 입력합니다.
IPv6 전용: **Prefix Length(접두사 길이)**를 입력합니다.
 - c) **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.
- 단계 11 **OK(확인)**를 클릭합니다.
- 단계 12 **Save(저장)**를 클릭합니다.
- FXOS에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 지정된 보안 모듈에 입력하여 논리적 디바이스를 구축합니다.
- 단계 13 **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.

단계 14 구성된 논리적 디바이스 목록에서 vDP 항목으로 스크롤합니다. **Management IP(관리 IP)** 열에 나열된 해당 속성을 확인합니다.

- **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 *unknown*(알 수 없음)으로 표시되는 경우, DefensePro 애플리케이션을 시작하고 제어 유닛 IP 주소를 구성하여 vDP 클러스터 생성을 완료합니다.
- **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 *primary* 또는 *secondary* 로 표시되는 경우, 애플리케이션이 온라인 상태로 클러스터에서 형성됩니다.

다음에 수행할 작업

DefensePro 애플리케이션의 비밀번호를 설정합니다. 비밀번호를 설정할 때까지 애플리케이션은 온라인 상태가 되지 않습니다. 자세한 내용은 cisco.com에서 Radware DefensePro DDoS 완화 사용 설명서를 참조하십시오.

UDP/TCP 포트 열기 및 vDP 웹 서비스 활성화

Radware APSolute Vision Manager 인터페이스는 다양한 UDP/TCP 포트를 사용하여 Radware vDP 애플리케이션과 통신합니다. vDP 애플리케이션이 APSolute Vision Manager와 통신하려면 이러한 포트에 액세스 가능하며 방화벽으로 인해 차단되지 않는지 확인해야 합니다. 열리는 특정 포트에 대한 자세한 내용은 APSolute Vision 사용 설명서의 다음 표를 참조하십시오.

- **APSolute Vision Server-WBM** 통신 및 운영 체제에 대한 포트
- **Radware** 디바이스를 사용하는 **APSolute Vision Server**의 통신 포트

Radware APSolute Vision에서 FXOS 새시에 구축된 가상 DefensePro 애플리케이션을 관리하려면 FXOS CLI를 사용하여 vDP 웹 서비스를 활성화해야 합니다.

프로시저

단계 1 FXOS CLI에서 vDP 애플리케이션 인스턴스에 연결합니다.

```
connect module 슬롯 console
```

```
connect vdp
```

단계 2 vDP 웹 서비스를 활성화합니다.

```
manage secure-web status set enable
```

단계 3 vDP 애플리케이션 콘솔을 종료하고 FXOS 모듈 CLI로 돌아갑니다.

```
Ctrl ]
```

TLS 암호화 가속화 구성

다음 주제에서는 TLS 암호화 가속을 설명하고, 활성화하는 방법 및 FMC를 사용하여 상태를 확인하는 방법에 대해 설명합니다.

다음 표에서는 FTD 및 FXOS 버전을 필수 TSL 암호화와 매핑합니다.



참고 FXOS 2.6.1이 FXOS 2.7.x 이상으로 업그레이드된 경우, FTD 6.4는 TLS 암호화와 호환되지 않으므로 6.4는 암호화를 자동으로 활성화하지 않습니다.

FTD	FXOS	Crypto
6.4	2.6	하나의 컨테이너 인스턴스만 지원(1단계)
6.4	2.7 이상	해당 없음
6.5 이상	2.7 이상	16 컨테이너 인스턴스 지원 (2단계)

정보 TLS 암호화 가속

Firepower 4100/9300은 전송 레이어 보안(TLS) 암호화 가속을 지원합니다. 이는 하드웨어에서 전송 레이어 보안(TLS)/보안 소켓 레이어(SSL)(TLS/SSL) 암호화 및 복호화를 수행하여 다음을 수행하는 속도를 크게 향상시킵니다.

- TLS/SSL 암호화 및 복호화
- TLS/SSL 및 IPsec을 포함한 VPN

네이티브 인스턴스에서는 TLS 암호화 가속화를 비활성화할 수 없습니다. 보안 엔진/모듈당 ~16 FTD 컨테이너 인스턴스개의 TLS 암호화 가속을 활성화할 수도 있습니다.

TLS 암호화 가속화 가이드라인 및 제한사항

FTD이 TLS 암호화 가속을 활성화한 경우 다음 사항에 유의하십시오.

검사 엔진 오류

검사 엔진이 연결을 유지하도록 구성되고 검사 엔진이 예기치 않게 실패하는 경우 엔진이 재시작될 때까지 TLS/SSL트래픽이 중단됩니다.

이 동작은 FTD 명령 `configure snort preserve-connection {enable | disable}` 명령이 제어합니다.

HTTP 전용 성능

트래픽을 암호 해독하지 않는 FTD 컨테이너 인스턴스에서 TLS 암호화 가속을 사용하면 성능에 영향을 줄 수 있습니다. TLS/SSL 트래픽을 암호 해독하는 FTD 컨테이너 인스턴스에 한해 TLS 암호화 가속을 활성화하는 것을 권장합니다.

FIPS(Federal Information Processing Standards)

TLS 암호화 가속 및 FIPS(Federal Information Processing Standard)가 모두 활성화되는 경우, 다음 옵션과의 연결은 실패합니다.

- 크기가 2,048 바이트보다 작은 RSA 키
- RC4(Rivest Cipher 4)
- 단일 데이터 암호화 표준(단일 DES)
- MD5(Merkle-Damgard 5)
- SSL v3

보안 인증 컴플라이언스 모드에서 작동하도록 FMC 및 FTD를 구성하는 경우 FIPS가 활성화됩니다. 해당 모드에서 작동 중 연결을 허용하려면, FTD 컨테이너 인스턴스에서 TLS 암호화 가속을 비활성화하거나 웹 브라우저가 더 안전한 옵션을 허용하도록 구성합니다.

자세한 내용:

- [공통 평가 기준](#)

HA(High Availability, 고가용성) 및 클러스터링

HA(High Availability, 고가용성) 또는 클러스터링된 FTD가 있을 경우, 각 FTD에서 개별적으로 TLS 암호화 가속을 활성화해야 합니다. HA 쌍 cluster에서 한 디바이스의 TLS 암호화 가속 구성은 다른 디바이스와 공유되지 않습니다.

TLS 하트비트

일부 애플리케이션은 TLS 하트비트를 TLS(Transport Layer Security) 및 DTLS(Datagram Transport Layer Security) 프로토콜로 확장합니다. 이 프로토콜은 [RFC6520](#)에서 정의합니다. TLS 하트비트는 연결 상태를 확인하는 방법을 제공합니다. 즉 클라이언트 또는 서버가 특정 바이트의 데이터를 전송하고 상대방의 에코 응답을 요청합니다. 성공한 경우, 암호화된 데이터가 전송됩니다.

TLS 암호화 가속된 FMC에 의해 관리되는 FTD가 TLS 하트비트 확장을 사용하는 패킷을 발견하면, FTD는 SSL 정책의 **Undecryptable Actions**(암호 해독 불가 작업)의 **Decryption Errors**(암호 해독 오류)에 대한 FMC 설정에서 지정된 작업을 수행합니다.

- Block(차단)
- Block with Reset(차단 후 재설정)

애플리케이션에서 TLS 하트비트를 사용하는지 확인하려면, *Firepower Management Center* 구성 가이드에서 TLS/SSL 규칙 트러블슈팅에 대한 장을 참조하십시오.

TLS 암호화 가속이 FTD 컨테이너 인스턴스에서 비활성화되어 있을 경우, FMC의 NAP(Network Analysis Policy)에서 **Max Heartbeat Length**(최대 하트비트 길이)를 구성하여 TLS 하트비트를 처리하는 방법을 결정할 수 있습니다.

TLS 하트비트에 대한 자세한 내용은 *Firepower Management Center* 구성 가이드의 TLS/SSL 규칙 트리블슈팅 장을 참조하십시오.

TLS/SSL 초과 서브스크립션

TLS/SSL oversubscription(오버서브스크립션)은 FTD가 TLS/SSL 래픽으로 오버로드된 상태입니다. 모든 FTD에서 TLS/SSLoversubscription이 발생할 수 있지만 TLS 암호화 가속을 지원하는 FTD만 이를 처리하는 구성 방법을 제공합니다.

TLS 암호화 가속이 활성화된 FMC에 의해 관리되는 FTD가 oversubscription되는 경우, FTD가 수신한 모든 패킷은 SSL 정책 **Undecryptable Actions**(암호 해독 불가 작업)의 **Handshake Errors**(핸드셰이크 오류)설정에 따라 수행됩니다.

- 기본 작업 상속
- Do not decrypt(암호 해독 안 함)
- Block(차단)
- Block with Reset(차단 후 재설정)

SSL 정책 **Undecryptable Actions**(암호 해독 불가 작업)의 **Handshake Errors**(핸드셰이크 오류)에 대한 설정이 **Do Not decrypt**(암호 해독 안 함)이며 관련 액세스 제어 정책이 트래픽을 검사하도록 구성하는 경우, 검사가 이루어지며 암호 해독은 진행되지 않습니다.

초과 서브스크립션이 많이 발생하는 경우, 다음 방법을 사용합니다.

- TLS/SSL 처리 용량이 더 많은 FTD로 업그레이드하십시오.
- SSL 정책을 변경하여 암호 해독 우선 순위가 높지 않은 트래픽의 **Do Not Decrypt**(암호 해독 안 함) 규칙을 추가합니다.

TLS 초과 서브스크립션에 대한 자세한 내용은 *Firepower Management Center* 구성 가이드의 TLS/SSL 규칙 트리블슈팅 장을 참조하십시오.

패시브 및 인라인 탭 세트는 지원되지 않음

TLS 암호화 가속이 활성화되어 있으면 패시브 또는 인라인 탭 모드 세트에서 TLS/SSL 트래픽 암호를 해독할 수 없습니다.

컨테이너 인스턴스에 대해 TLS 암호화 가속화 활성화

FMC에 대한 독립형 FTD 추가, 28 페이지에 설명된 대로 논리적 인스턴스를 구축할 때 TLS 암호화 가속이 자동으로 활성화됩니다.

TLS 암호화 가속은 모든 네이티브 인스턴스에서 활성화되며 비활성화할 수 없습니다.


TLS 암호화 가속 상태 보기

이 주제에서는 TLS 암호화 가속 활성화 여부를 확인하는 방법을 설명합니다.
FMC에서 다음 작업을 수행하십시오.

프로시저

단계 1 FMC에 로그인합니다.

단계 2 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 클릭합니다.

단계 3 수정()을 클릭하여 매니지드 디바이스를 편집합니다.

단계 4 **Device**(디바이스) 페이지를 클릭합니다. TLS 암호화 가속 상태가 **General**(일반) 섹션에 표시됩니다.

FTD 링크 상태 동기화를 활성화합니다.

이제 새시가 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료로 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다.

이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 이 기능은 관리 또는 클러스터와 같은 비 데이터 인터페이스에는 영향을 주지 않습니다.

FTD 링크 상태 동기화를 활성화하면, FXOS에 있는 인터페이스의 **Service State**(서비스 상태)가 FTD에 있는 이 인터페이스의 관리 상태와 동기화됩니다. 예를 들어 FTD에서 인터페이스를 종료하는 경우 **Service State**(서비스 상태)가 **Disabled**(비활성화됨)로 표시됩니다. FTD 애플리케이션을 종료하면 모든 인터페이스가 **Disabled**(비활성화됨)로 표시됩니다. 하드웨어 우회 인터페이스의 경우 FTD에서 인터페이스를 관리적으로 종료하면 **Service State**(서비스 상태)가 **Disabled**(비활성화됨)로 설정됩니다. 하지만 FTD 애플리케이션을 종료하거나 다른 새시 레벨 종료(전원 끄기 포함)를 수행하면 인터페이스 쌍이 **Disabled**(활성화됨) 상태로 유지됩니다.

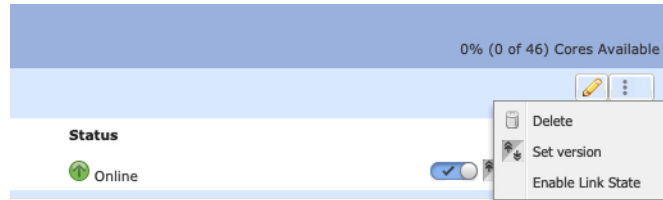
FTD 링크 상태 동기화를 비활성화하면 **Service State**(서비스 상태)는 항상 **Enabled**(활성화됨)로 표시됩니다.



참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 테코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다.

프로시저

- 단계 1 **Logical Devices**(논리적 디바이스)를 선택하고, FTD 논리적 디바이스에 대해 드롭다운 목록에서 **Enable Link State**(링크 상태 활성화)를 선택합니다.



이 기능을 비활성화하려면 **Disable Link State**(링크 상태 비활성화)를 선택합니다.

- 단계 2 현재 인터페이스 상태와 마지막 중단 이유를 봅니다.

show interface expand detail

예제:

```
Firepower # scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface expand detail
Interface:
  Port Name: Ethernet1/2
  User Label:
  Port Type: Data
  Admin State: Enabled
  Oper State: Up
  State Reason:
  flow control policy: default
  Auto negotiation: Yes
  Admin Speed: 1 Gbps
  Oper Speed: 1 Gbps
  Admin Duplex: Full Duplex
  Oper Duplex: Full Duplex
  Ethernet Link Profile name: default
  Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
  Uddl Oper State: Admin Disabled
  Inline Pair Admin State: Enabled
  Inline Pair Peer Port Name:
  Service State: Enabled
  Last Service State Down Reason: None
  Allowed Vlan: All
  Network Control Policy: default
  Current Task:
  <...>
```

논리적 디바이스 관리

논리적 디바이스를 삭제하고, ASA를 투명 모드로 변환하고, 인터페이스 구성을 변경하고, 기존 논리적 디바이스에서 기타 작업을 수행할 수 있습니다.

애플리케이션 콘솔에 연결

다음 절차를 수행하여 애플리케이션의 콘솔에 연결합니다.

프로시저

단계 1 콘솔 연결 또는 텔넷 연결을 사용하여 모듈 CLI에 연결합니다.

connect module slot_number {console | telnet}

여러 보안 모듈을 지원하지 않는 디바이스의 보안 엔진에 연결하려면 항상 **1**을 *slot_number*로 사용합니다.

텔넷 연결 사용 시에는 동시에 여러 세션을 모듈에 연결할 수 있으며 연결 속도가 더 빠르다는 이점이 있습니다.

예제:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

단계 2 애플리케이션 콘솔에 연결합니다. 디바이스에 적절한 명령을 입력합니다.

connect asa name

connect ftd name

connect vdp name

인스턴스 이름을 확인하려면 이름 없이 명령을 입력합니다.

예제:

```
Firepower-module1> connect asa asal
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

예제:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

단계 3 애플리케이션 콘솔을 FXOS 모듈 CLI로 종료합니다.

- ASA - **Ctrl-a, d**를 입력합니다.
- FTD - **exit**를 입력합니다.
- vDP - **Ctrl-], .**를 입력합니다.

단계 4 FXOS CLI의 Supervisor(관리자) 수준으로 돌아갑니다.

콘솔을 종료합니다.

a) ~를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

```
telnet>quit
```

텔넷 세션을 종료합니다.

a) **Ctrl-], .**를 입력합니다.

예시

다음 예시에서는 보안 모듈 1에 있는 ASA에 연결한 다음 FXOS CLI의 슈퍼바이저 레벨로 다시 종료합니다.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asal
asa> ~
telnet> quit
Connection closed.
Firepower#
```

논리적 디바이스 삭제

프로시저

단계 1 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다.

Logical Devices(논리적 디바이스) 페이지는 새시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

단계 2 삭제할 논리적 디바이스에 대해 **Delete(삭제)**를 클릭합니다.

단계 3 **Yes(예)**를 클릭하여 논리적 디바이스를 삭제할 것임을 확인합니다.

단계 4 **Yes(예)**를 클릭하여 애플리케이션 구성을 삭제할 것임을 확인합니다.

클러스터 유닛 제거

다음 섹션에서는 클러스터에서 유닛을 일시적으로 또는 영구적으로 제거하는 방법을 설명합니다.

임시 제거

하드웨어나 네트워크 장애 등의 이유 때문에 클러스터 유닛이 클러스터에서 자동으로 제거됩니다. 이 제거는 조건을 수정할 때까지 임시로 적용되며, 클러스터에 다시 참여할 수 있습니다. 클러스터링을 수동으로 비활성화할 수도 있습니다.

디바이스가 현재 클러스터에 있는지 확인하려면, 애플리케이션에서 **show cluster info** 명령을 사용해 Firepower Chassis Manager **Logical Devices**(논리적 디바이스) 페이지:

Management Port	Status
Ethernet1/4	online

Attributes



- Cluster Operational Status : not-in-cluster
- FIREPOWER-MGMT-IP : 10.89.5.20
- CLUSTER-ROLE : none
- CLUSTER-IP : 127.2.1.1
- MGMT-URL : https://10.89.5.35/
- UUID : 8e459170-451d-11e9-8475-f22f06c32630

FMC을(를) 사용하는 FTD의 경우에는 FMC 디바이스 목록에 디바이스를 남겨 두어야 클러스터링 재 활성화 후 전체 기능을 다시 사용할 수 있습니다.

- 애플리케이션에서 클러스터링 비활성화 - 애플리케이션 CLI를 사용하여 클러스터링을 비활성화할 수 있습니다. **cluster remove unit name** 명령을 입력해 로그인한 유닛 외의 모든 유닛을 제거합니다. 부트스트랩 설정과 제어 유닛에서 동기화한 마지막 설정도 그대로 유지되므로 나중에 설정이 유실되는 일 없이 유닛을 다시 추가할 수 있습니다. 이 명령을 데이터 유닛에 입력해서 제어 유닛을 제거하면 새로운 제어 유닛이 선택됩니다.

디바이스가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우에는 관리 인터페이스가 비활성화됩니다.


클러스터링을 다시 활성화하려면 ASA에 **cluster group name**을 입력하고 **enable**을(를) 입력합니다. 클러스터링을 다시 활성화하려면 FTD에 **cluster enable**을(를) 입력합니다.

- 애플리케이션 인스턴스 비활성화 - **Logical Devices**(논리적 디바이스) 페이지의 Firepower Chassis Manager에서 슬라이더 활성화됨()을(를) 클릭합니다. 나중에 슬라이더 비활성화됨()을(를) 사용하여 다시 활성화할 수 있습니다.
- 보안 모듈/엔진 종료 - **Security Module/Engine**(보안 모듈/엔진) 페이지의 Firepower Chassis Manager에서 전원 끄기 아이콘을 클릭합니다.
- 새시 종료 - **Overview**(개요) 페이지의 Firepower Chassis Manager에서 종료 아이콘을 클릭합니다.

영구 제거

다음 방법을 사용하면 클러스터 멤버를 영구적으로 제거할 수 있습니다.

FMC을(를) 사용하는 FTD의 경우, 새시에서 클러스터링을 비활성화하면 유닛을 FMC 디바이스 목록에서 제거해야 합니다.

- 논리적 디바이스 삭제 - **Logical Devices**(논리적 디바이스) 페이지의 Firepower Chassis Manager에서 삭제()을(를) 클릭합니다. 이제 독립형 논리적 디바이스, 새 클러스터를 구축하거나 동일한 클러스터에 새 논리적 디바이스를 추가할 수 있습니다.
- 서비스에서 새시 또는 보안 모듈 제거- 서비스에서 디바이스를 제거하면, 교체 하드웨어를 클러스터의 새 멤버로 추가할 수 있습니다.

논리적 디바이스와 연결되지 않은 애플리케이션 인스턴스 삭제

논리적 디바이스를 삭제하면 논리적 디바이스의 애플리케이션 구성도 삭제할 것인지 묻는 프롬프트가 표시됩니다. 애플리케이션 구성을 삭제하지 않는 경우, 해당 애플리케이션 인스턴스를 삭제할 때까지 다른 애플리케이션을 사용하여 논리적 디바이스를 생성할 수 없습니다. 논리적 디바이스와 더 이상 연결되지 않은 애플리케이션 인스턴스를 보안 모듈/엔진에서 삭제하려면 다음 절차를 사용할 수 있습니다.

프로시저

단계 1 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다.

Logical Devices(논리적 디바이스) 페이지는 새시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다. 논리적 디바이스 목록 아래에서 논리적 디바이스와 연결되지 않은 애플리케이션 인스턴스 목록을 확인할 수 있습니다.

단계 2 삭제할 애플리케이션 인스턴스에 대해 **Delete**(삭제)를 클릭합니다.

단계 3 **Yes**(예)를 클릭하여 애플리케이션 인스턴스를 삭제할 것임을 확인합니다.

FTD 논리적 디바이스에서 인터페이스 변경

FTD 논리적 디바이스에서 인터페이스를 할당 또는 할당 해제하거나 관리 인터페이스를 교체할 수 있습니다. 그런 다음 FMC 또는 FDM에서 인터페이스 구성을 동기화할 수 있습니다.

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 FTD 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 FTD 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다. 논리적 디바이스에 영향을 주거나 FMC 또는 FDM에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

FMC의 경우: 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다.

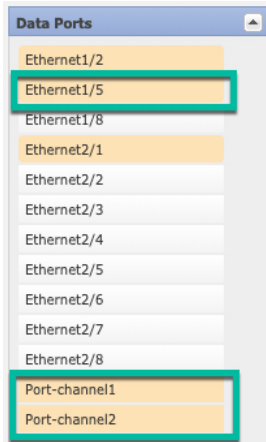
FDM의 경우: 기존 인터페이스를 삭제하기 전에 한 인터페이스에서 다른 인터페이스로 구성을 마이그레이션할 수 있습니다.

시작하기 전에

- 인터페이스를 구성하고 **실제 인터페이스 구성** 및 **EtherChannel(포트 채널)** 추가에 따라 EtherChannel을 추가합니다.
- 모든 인터페이스가 기본적으로 클러스터에 할당된 경우와 같이 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 논리적 디바이스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 디바이스에 EtherChannel을 할당할 수 있습니다.
- 관리 또는 이벤트 인터페이스를 관리 EtherChannel로 교체하려는 경우에는 미할당 데이터 멤버 인터페이스가 하나 이상 포함된 EtherChannel을 생성한 다음 현재 관리 인터페이스를 EtherChannel로 교체해야 합니다. FTD 디바이스가 리부팅되고(관리 인터페이스를 변경하면 리부팅됨) FMC 또는 FDM에서 구성을 동기화한 후에는 이제 할당 해제된 관리 인터페이스를 EtherChannel에 추가할 수도 있습니다.
- 클러스터링 또는 고가용성의 경우에는 FMC 또는 FDM에서 구성을 동기화하기 전에 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 인터페이스는 먼저 데이터/스탠바이 유닛에서 변경한 후에 제어/액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

프로시저

- 단계 1 Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택합니다.
- 단계 2 오른쪽 상단의 **Edit**(수정) 아이콘을 클릭하여 논리적 디바이스를 수정합니다.
- 단계 3 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택하여 새 데이터 인터페이스를 할당합니다.
아직 인터페이스를 삭제하지 마십시오.



단계 4 관리 또는 이벤트 처리 인터페이스를 교체합니다.

이러한 인터페이스 유형의 경우 변경 사항을 저장하고 나면 디바이스가 리부팅됩니다.

- a) 페이지 중앙의 디바이스 아이콘을 클릭합니다.
- b) **General**(일반) 또는 **Cluster Information**(클러스터 정보) 탭의 드롭다운 목록에서 새 **Management Interface**(관리 인터페이스)를 선택합니다.
- c) **Settings**(설정) 탭의 드롭다운 목록에서 새 **Eventing Interface**(이벤트 인터페이스)를 선택합니다.
- d) **OK**(확인)를 클릭합니다.

관리 인터페이스의 IP 주소를 변경하는 경우에는 FMC에서 디바이스의 IP 주소도 변경해야 합니다. 이렇게 하려면 **Device**(디바이스) > **Device Management**(디바이스 관리) > **Device/Cluster**(디바이스/클러스터)로 이동합니다. **Management**(관리) 영역에서 부트스트랩 구성 주소와 일치하도록 IP 주소를 설정합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 FMC에서 인터페이스를 동기화합니다.

- a) FMC에 로그인합니다.
- b) **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 FTD 디바이스에 대한 수정 (🔧)를 클릭합니다. 기본적으로 **Interfaces**(인터페이스) 페이지가 선택됩니다.
- c) **Interfaces**(인터페이스) 페이지 왼쪽 상단의 **Sync Device**(디바이스 동기화) 버튼을 클릭합니다.
- d) 변경 사항이 탐지되면 **Interfaces**(인터페이스) 페이지에 인터페이스 구성이 변경되었음을 나타내는 빨간색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 클릭하여 더 보기 링크를 클릭합니다.
- e) 인터페이스를 삭제하려는 경우, 기존 인터페이스에서 새 인터페이스로 모든 인터페이스 구성을 수동으로 전송합니다.

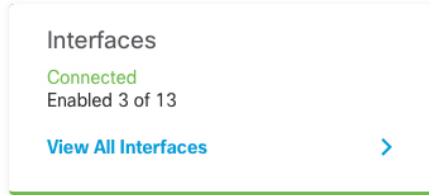
아직 인터페이스를 삭제하지 않았으므로 기존 구성을 참조할 수 있습니다. 이전 인터페이스를 삭제하고 검증 을 다시 실행한 후에 구성을 추가로 수정할 수 있습니다. 검증을 수행하면 이전 인터페이스가 아직 사용되고 있는 모든 위치가 표시됩니다.

- f) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다. 오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

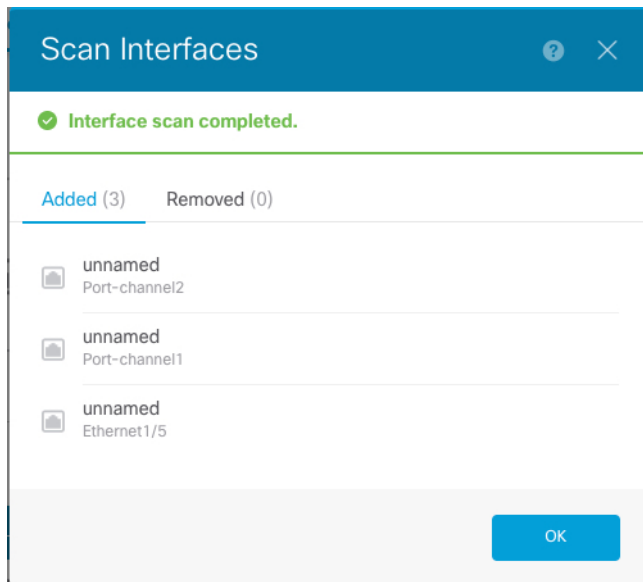
- g) **Save(저장)**를 클릭합니다.
- h) 디바이스를 선택하고 **Deploy(구축)**를 클릭하여 할당된 디바이스에 정책을 구축합니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 7 FDM에서 인터페이스를 동기화하고 마이그레이션합니다.

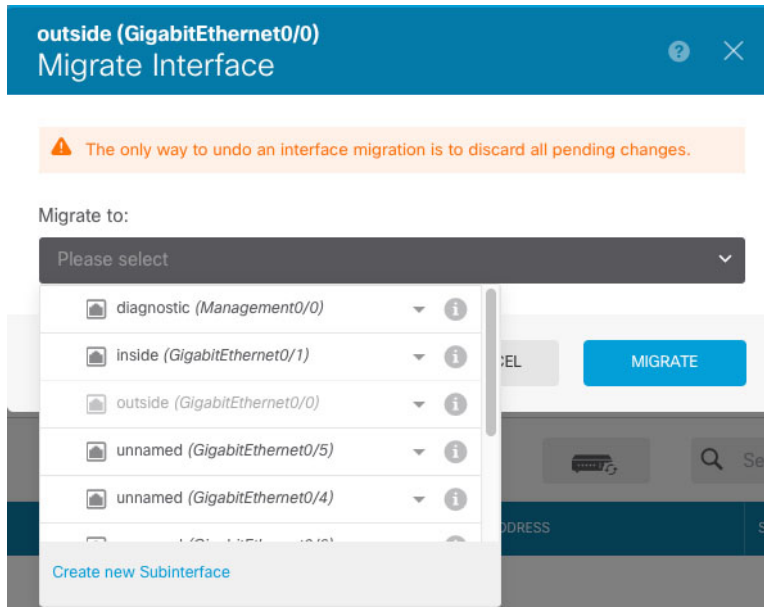
- a) FDM에 로그인합니다.
- b) **Device(디바이스)**를 클릭한 다음, **Interfaces(인터페이스)** 요약에서 **View All Interfaces(모든 인터페이스 보기)** 링크를 클릭합니다.



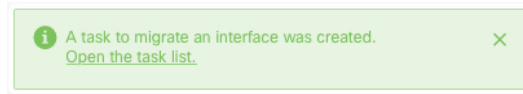
- c) **Scan Interfaces icon(인터페이스 스캔 아이콘)**을 클릭합니다.
- d) 인터페이스가 스캔될 때까지 기다린 다음, **OK(확인)**를 클릭합니다.



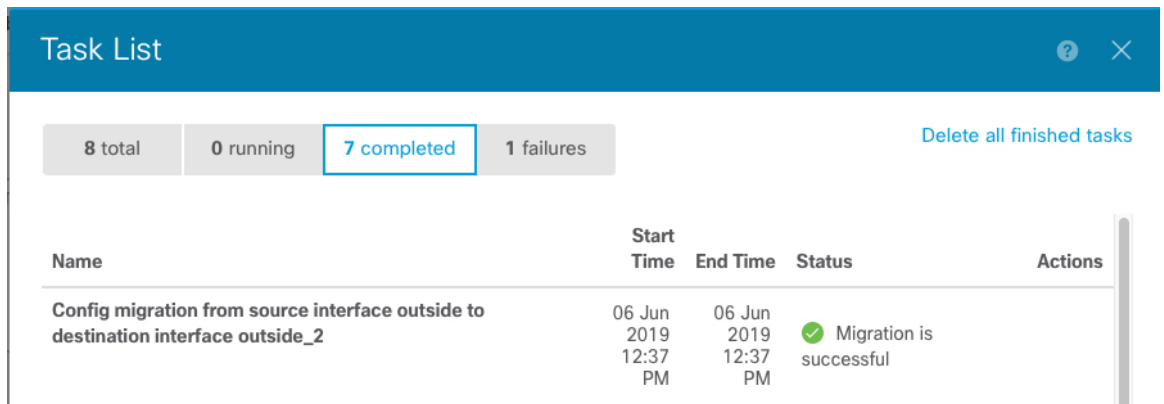
- e) 이름, IP 주소 등을 사용하여 새 인터페이스를 구성합니다.
제거할 인터페이스의 기존 IP 주소 및 이름을 사용하려는 경우에는 새 인터페이스에서 해당 설정을 사용할 수 있도록 기존 인터페이스를 더미 이름 및 IP 주소로 다시 구성해야 합니다.
- f) 기존 인터페이스를 새 인터페이스로 교체하려면 기존 인터페이스의 **Replace(교체)** 아이콘을 클릭합니다.
바꾸기 아이콘
이 프로세스에서는 인터페이스를 참조하는 모든 구성 설정에서 기존 인터페이스가 새 인터페이스로 교체됩니다.
- g) **Replacement Interface(교체 인터페이스)** 드롭다운 목록에서 새 인터페이스를 선택합니다.



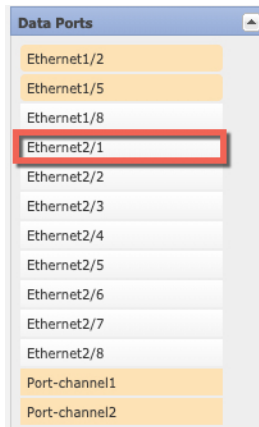
h) **Interfaces**(인터페이스) 페이지에 메시지가 나타납니다. 메시지에서 링크를 클릭합니다.



i) **Task List**(작업 목록)를 확인하여 마이그레이션에 성공했는지 확인합니다.



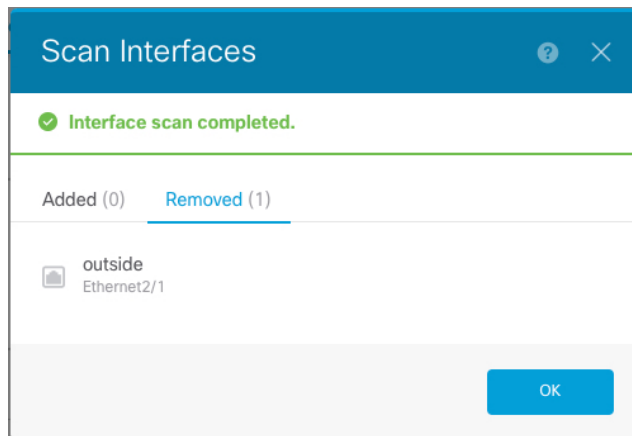
단계 8 Firepower Chassis Manager에서 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택 취소하여 데이터 인터페이스를 할당 해제합니다.



단계 9 **Save**(저장)를 클릭합니다.

단계 10 **FMC** 또는 **FDM**에서 인터페이스를 다시 동기화합니다.

그림 10: **FDM** 스캔 인터페이스



ASA 논리적 디바이스에서 인터페이스 변경

ASA 논리적 디바이스에서 관리 인터페이스를 할당, 할당 해제 또는 교체할 수 있습니다. ASDM은 새 인터페이스를 자동으로 검색합니다.

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 ASA 구성에 미치는 영향은 아주 적습니다. 그러나 FXOS에서 할당된 인터페이스를 제거하고(예: 네트워크 모듈을 제거하거나, EtherChannel을 제거하거나, 할당된 인터페이스를 EtherChannel에 재할당하는 경우), 해당 인터페이스가 보안 정책에서 사용되는 경우, 제거하면 ASA 구성에 영향을 미칩니다. 이 경우 ASA 구성은 원래 명령을 유지하므로 필요한 조정을 수행할 수 있습니다. ASA OS에서 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.



참고 논리적 디바이스에 영향을 주지 않고 할당된 EtherChannel의 멤버십을 수정할 수 있습니다.

시작하기 전에

- 실제 인터페이스 구성 및 EtherChannel(포트 채널) 추가에 따라 인터페이스를 구성하고 EtherChannel을 추가합니다.
- 모든 인터페이스가 기본적으로 클러스터에 할당된 경우와 같이 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 논리적 디바이스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 디바이스에 EtherChannel을 할당할 수 있습니다.
- 관리 인터페이스를 관리 EtherChannel로 교체하려는 경우에는 미할당 데이터 멤버 인터페이스가 하나 이상 포함된 EtherChannel을 생성한 다음 현재 관리 인터페이스를 EtherChannel로 교체해야 합니다. ASA가 다시 로드되고 나면(관리 인터페이스를 변경하면 ASA가 다시 로드됨) 이제 미할당 상태가 된 관리 인터페이스를 EtherChannel에 추가할 수도 있습니다.
- 클러스터링 또는 페일오버의 경우 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 인터페이스는 먼저 데이터/스탠바이 유닛에서 변경한 후에 제어/액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운된 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

프로시저

- 단계 1 Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택합니다.
- 단계 2 오른쪽 상단의 **Edit**(수정) 아이콘을 클릭하여 논리적 디바이스를 수정합니다.
- 단계 3 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택 취소하여 데이터 인터페이스를 할당 해제합니다.
- 단계 4 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택하여 새 데이터 인터페이스를 할당합니다.
- 단계 5 관리 인터페이스를 교체합니다.
이 인터페이스 유형의 경우 변경 사항을 저장하고 나면 디바이스가 다시 로드됩니다.
 - a) 페이지 중앙의 디바이스 아이콘을 클릭합니다.
 - b) **General/Cluster Information**(일반/클러스터 정보) 탭의 드롭다운 목록에서 새 **Management Interface**(관리 인터페이스)를 선택합니다.
 - c) **OK**(확인)를 클릭합니다.
- 단계 6 **Save**(저장)를 클릭합니다.

논리적 디바이스의 부트스트랩 설정 수정 또는 복구

논리적 디바이스의 부트스트랩 설정을 수정할 수 있습니다. 그런 다음 이러한 새 설정을 사용하여 애플리케이션 인스턴스를 즉시 재시작하거나 변경 사항을 저장하고 나중에 새 설정을 사용하여 애플리케이션 인스턴스를 재시작할 수 있습니다.

프로시저

-
- 단계 **1** Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택합니다.
 - 단계 **2** 오른쪽 상단의 **Edit**(수정) 아이콘을 클릭하여 논리적 디바이스를 수정합니다.
 - 단계 **3** 페이지 중앙의 디바이스 아이콘을 클릭합니다.
 - 단계 **4** 필요에 따라 논리적 디바이스 설정을 수정합니다.
 - 단계 **5** **OK**(확인)를 클릭합니다.
 - 단계 **6** 변경 사항을 저장하고 애플리케이션 인스턴스를 즉시 재시작하려면 **Restart Now**(지금 재시작)를 클릭합니다. 애플리케이션 인스턴스를 재시작하지 않고 변경 사항을 저장하려면 **Restart Later**(나중에 재시작)를 클릭합니다.
- 참고 **Restart Later**(나중에 재시작)를 선택한 경우 준비가 되면 **Logical Devices**(논리적 디바이스) 페이지에서 **Restart Instance**(인스턴스 재시작)를 클릭하여 애플리케이션 인스턴스를 재시작할 수 있습니다.
-

논리적 디바이스 페이지

Firepower Chassis Manager의 **Logical Devices**(논리적 디바이스) 페이지를 사용하여 논리적 디바이스를 생성, 수정 및 삭제합니다. **Logical Devices**(논리적 디바이스) 페이지에는 각 Firepower 4100/9300 새시 보안 모듈/엔진에 설치된 논리적 디바이스에 대한 정보 영역이 포함되어 있습니다.

각 논리적 디바이스 영역의 헤더에서는 다음 정보를 제공합니다.

- 논리적 디바이스의 고유한 이름.
- 논리적 디바이스 모드(독립형 또는 클러스터형).
- **Status**(상태) - 논리적 디바이스의 상태를 표시합니다.
 - ok - 논리적 디바이스 구성이 완료되었습니다.
 - incomplete-configuration - 논리적 디바이스 구성이 완료되지 않았습니다.

각 논리적 디바이스 영역에서는 다음 정보를 제공합니다.

- **Application**(애플리케이션) - 보안 모듈에서 실행 중인 애플리케이션을 표시합니다.
- **Version**(버전) - 보안 모듈에서 실행 중인 애플리케이션의 소프트웨어 버전 번호를 표시합니다.



참고 FTD 논리적 디바이스에 대한 업데이트는 FMC를 사용하여 완료되며, Firepower Chassis Manager의 **Logical Devices**(논리적 디바이스) > **Edit**(수정) 및 **System**(시스템) > **Updates**(업데이트) 페이지에 반영되지 않습니다. 이러한 페이지에 표시되는 버전은 FTD 논리적 디바이스를 만드는 데 사용된 소프트웨어 버전(CSP 이미지)을 나타냅니다.

- **Resource Profile**(리소스 프로파일) - 논리적 디바이스/애플리케이션 인스턴스에 할당된 리소스 프로파일을 표시합니다.
- **Management IP**(관리 IP) - 논리적 디바이스 관리 IP로 할당된 로컬 IP 주소를 표시합니다.
- **Gateway**(게이트웨이) - 애플리케이션 인스턴스에 할당된 네트워크 게이트웨이 주소를 표시합니다.
- **Management Port**(관리 포트) - 애플리케이션 인스턴스에 할당된 관리 포트를 표시합니다.
- **Status**(상태) - 애플리케이션 인스턴스의 상태를 표시합니다.
 - **Online**(온라인) - 애플리케이션이 실행되어 작동 중입니다.
 - **Offline**(오프라인) - 애플리케이션이 중지되어 작동하지 않습니다.
 - **Installing**(설치 중) - 애플리케이션 설치가 진행 중입니다.
 - **Not Installed**(설치되지 않음) - 애플리케이션이 설치되지 않았습니다.
 - **Install Failed**(설치 실패) - 애플리케이션 설치가 실패했습니다.
 - **Starting**(시작 중) - 애플리케이션이 시작 중입니다.
 - **Start Failed**(시작 실패) - 애플리케이션 시작에 실패했습니다.
 - **Started**(시작됨) - 애플리케이션이 성공적으로 시작되었고, 앱 에이전트 하트비트를 대기 중입니다.
 - **Stopping**(중지 중) - 애플리케이션이 중지 중입니다.
 - **Stop Failed**(중지 실패) - 애플리케이션을 오프라인으로 전환하지 못했습니다.
 - **Not Responding**(응답 없음) - 애플리케이션이 응답하지 않습니다.
 - **Updating**(업데이트 중) - 애플리케이션 소프트웨어 업데이트가 진행 중입니다.
 - **Update Failed**(업데이트 실패) - 애플리케이션 소프트웨어 업데이트에서 장애가 발생했습니다.
 - **Update Succeeded**(업데이트 성공) - 애플리케이션 소프트웨어 업데이트가 성공했습니다.
 - **Unsupported**(지원되지 않음) - 설치된 애플리케이션이 지원되지 않습니다.

보안 모듈이 없거나 결함이 있는 상태이면 **Status(상태)** 필드에 해당 정보가 표시됩니다. 정보 아이콘에 마우스를 올려 결함에 대한 추가 정보를 확인할 수 있습니다. 보안 모듈 결함에 대한 자세한 내용은 [FXOS 보안 모듈/보안 엔진 정보](#) 섹션을 참조하십시오.

- **Expanded Information Area(확장된 정보 영역)** - 현재 실행 중인 애플리케이션 인스턴스에 대한 추가 속성을 표시합니다.



참고 애플리케이션 인스턴스를 즉시 재시작하지 않고 애플리케이션의 부트스트랩 설정을 수정하는 경우, **Attributes(속성)** 필드는 현재 실행 중인 애플리케이션에 대한 정보를 표시하며 애플리케이션이 재시작될 때까지 수행된 변경 사항을 반영하지 않습니다.

- **Ports(포트)** - 애플리케이션 인스턴스에 할당된 포트를 표시합니다.
- **Cluster Operation Status(클러스터 작동 상태)** - 애플리케이션 인스턴스에 할당된 관리 URL을 표시합니다.
- **Management IP/Firepower Management IP(관리 IP/Firepower 관리 IP)** - 애플리케이션 인스턴스에 할당된 관리 IP 주소를 표시합니다.
- **Cluster Role(클러스터 역할)** - 애플리케이션 인스턴스, 제어 또는 데이터에 대한 클러스터 역할을 표시합니다.
- **Cluster IP(클러스터 IP)** - 애플리케이션 인스턴스에 할당된 네트워크 IP 주소를 표시합니다.
- **HA Role(HA 역할)** - 애플리케이션 인스턴스의 고가용성 역할(액티브 또는 스탠바이)을 표시합니다.
- **Management URL(관리 URL)** - 애플리케이션 인스턴스에 할당된 관리 애플리케이션의 URL을 표시합니다.
- **UUID** - 애플리케이션 인스턴스의 UUID(Universally Unique Identifier)를 표시합니다.

Firepower Chassis Manager의 **Logical Devices(논리적 디바이스)** 페이지에서 논리적 디바이스에 대해 다음 기능을 수행할 수 있습니다.

- **Refresh(새로 고침)** - Logical Devices(논리적 디바이스) 페이지의 정보를 새로 고칩니다.
- **Add Device(디바이스 추가)** - 논리적 디바이스를 생성할 수 있습니다.
- **Edit(수정)** - 기존 논리적 디바이스를 수정할 수 있습니다.
- **Set Version(버전 설정)** - 논리적 디바이스의 소프트웨어를 업그레이드하거나 다운그레이드할 수 있습니다.
- **Delete(삭제)** - 논리적 디바이스를 삭제합니다.
- **Show Configuration(구성 표시)** - 논리적 디바이스나 클러스터에 대한 구성 정보가 JSON 형식으로 표시되는 대화 상자를 엽니다. 구성 정보를 복사하여 클러스터의 일부분인 추가 디바이스를 생성할 때 사용할 수 있습니다.

- **Enable/Disable**(활성화/비활성화) - 애플리케이션 인스턴스를 활성화하거나 비활성화합니다.
- **Upgrade/Downgrade**(업그레이드/다운그레이드) - 애플리케이션 인스턴스를 업그레이드하거나 다운그레이드할 수 있습니다.
- **Restart Instance**(인스턴스 재시작) - 애플리케이션 인스턴스를 재시작할 수 있습니다. 디바이스 부트스트랩 정보를 수정했는데 애플리케이션 인스턴스는 아직 재시작하지 않은 경우 **Restart Instance**(인스턴스 재시작)를 클릭하여 기존 관리 부트스트랩 정보를 지우고 새 부트스트랩 정보를 사용하여 애플리케이션 인스턴스를 재시작할 수 있습니다.
- **Reinstall Instance**(인스턴스 재설치) - 애플리케이션 인스턴스를 재설치할 수 있습니다.
- **Go To Device Manager**(디바이스 매니저로 이동) - 애플리케이션 인스턴스에 대해 정의된 FMC 또는 ASDM으로 이동하는 링크를 제공합니다.
- **Enable/Disable Link State**(링크 상태 활성화/비활성화) - FTD 링크 상태 동기화를 활성화하거나 비활성화합니다. 자세한 내용은 [FTD 링크 상태 동기화를 활성화합니다.](#), 72 페이지를 참고하십시오.

사이트 간 클러스터링 예시

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

사이트별 **MAC** 주소가 있는 **Spanned EtherChannel** 라우팅 모드 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 내부 네트워크 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버를 보여줍니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부 네트워크용 **Spanned EtherChannel** 을 사용하여 로컬 스위치에 연결됩니다. 각 **EtherChannel**은 클러스터의 모든 새시를 포괄합니다.

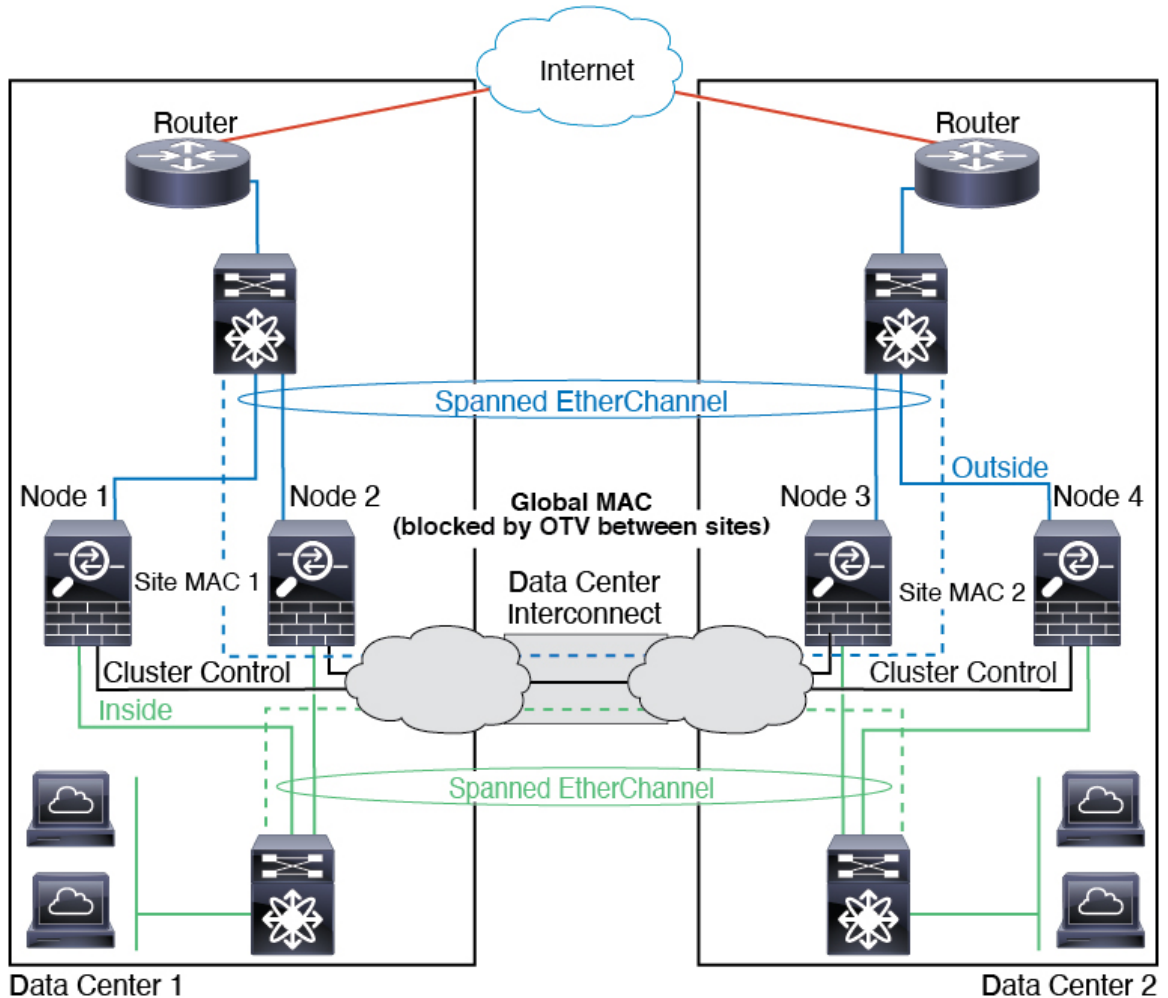
OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 클러스터로 향할 때 DCI를 통과하여 반대쪽 사이트에 가지 않도록 전역 MAC 주소를 차단하는 필터를 추가해야 합니다. 어떤 사이트의 클러스터 노드가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 노드에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. VACL 을 사용하여 전역 MAC 주소를 필터링해야 합니다. ARP 검사를 비활성화해야 합니다.

클러스터는 내부 네트워크의 게이트웨이 역할을 합니다. 모든 클러스터 노드에서 공유되는 전역 가상 MAC은 패킷 수신에만 사용됩니다. 발신 패킷은 각 DC 클러스터의 사이트별 MAC 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다.

이 시나리오에서:

- 클러스터에서 전송한 모든 이그레스(egress) 패킷은 사이트 MAC 주소를 사용하며 데이터 센터에서 지역화됩니다.

- 클러스터에 대한 모든 인그레스 패킷은 전역 MAC 주소를 사용하여 전송되므로, 양 사이트의 어느 노드에서나 수신할 수 있습니다. OTV의 필터는 데이터 센터 내에서 트래픽을 지역화합니다.



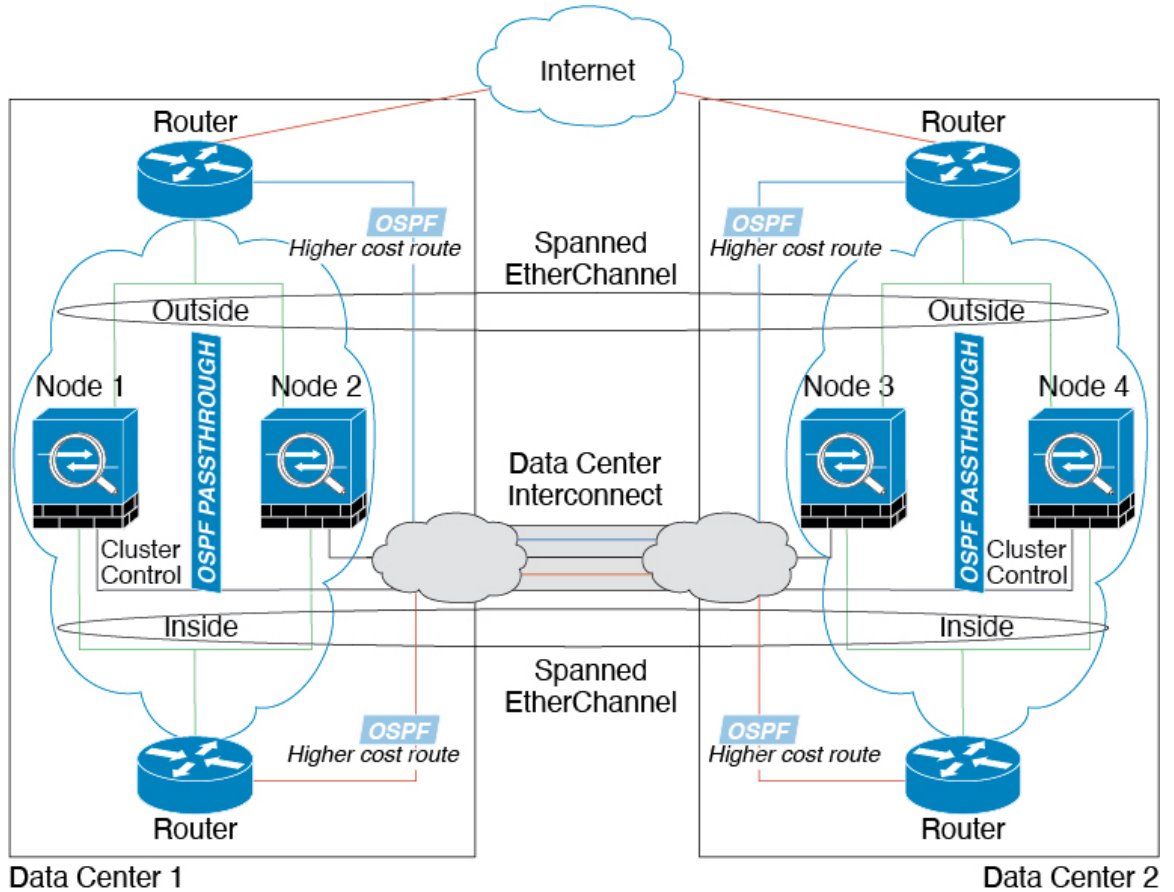
Spanned EtherChannel 투명 모드 노스-사우스 사이트 간의 예

다음 예에서는 내부 라우터와 외부 라우터의 사이에 위치한(노스-사우스 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부용 스패 EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 새시를 포괄합니다.

각 데이터 센터의 내부 및 외부 라우터에서는 투명 ASA를 통과하는 OSPF를 사용합니다. MAC과 달리 라우터 IP는 모든 라우터마다 고유합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 같은 브리지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 클러스터 멤버로 이동합니다.

각 사이트의 스위치 구현 과정에는 다음 사항이 포함될 수 있습니다.

- 사이트 간 VSS, vPC, StackWise 또는 StackWise Virtual - 이 시나리오에서는 데이터 센터 1에 스위치 하나를 설치하고 데이터 센터 2에 다른 스위치를 설치합니다. 한 가지 옵션은 각 데이터 센터의 클러스터 노드가 로컬 스위치에만 연결하는 반면 중복 스위치 트래픽은 DCI를 통과하는 것입니다. 이 경우 연결의 대부분은 각 데이터 센터에 로컬로 저장됩니다. DCI에서 추가 트래픽을 처리할 수 있는 경우, 선택에 따라 각 노드를 DCI 전반의 스위치에 연결할 수 있습니다. 이 경우 트래픽이 데이터 센터 전반에 분산되므로 DCI의 성능이 매우 뛰어나야 합니다.
- 각 사이트의 로컬 VSS, vPC, StackWise 또는 StackWise Virtual - 더 나은 스위치 이중화를 위해 각 사이트에 2개의 개별 이중화 스위치 쌍을 설치할 수 있습니다. 이 경우 여전히 클러스터 노드의 Spanned EtherChannel은 두 로컬 스위치에만 연결된 데이터 센터 1 새시 및 이러한 로컬 스위치에 연결된 데이터 센터 2 새시로 이루어져 있지만, 사실상 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 중복 스위치 시스템은 스패 EtherChannel을 사이트 로컬 EtherChannel로 간주합니다.

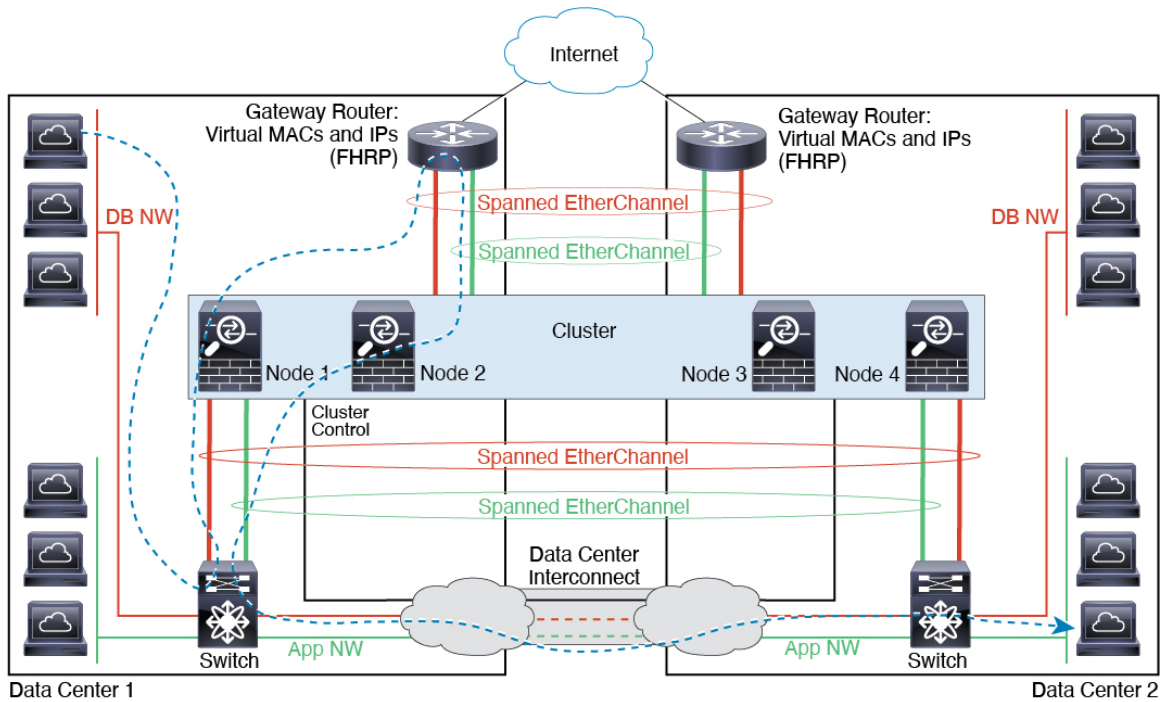


Spanned EtherChannel 투명 모드 이스트-웨스트 사이트 간의 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 두 내부 네트워크, 즉 애플리케이션 네트워크 및 DB 네트워크의 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있

습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부에 있는 애플리케이션 및 DB 네트워크에 대한 스패ن EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 새시를 포괄합니다.

각 사이트의 게이트웨이 라우터는 HSRP와 같은 FHRP를 사용하여 각 사이트에 동일한 목적지 가상 MAC 및 IP 주소를 제공합니다. 의도치 않은 MAC 주소 플래핑(flapping)을 피하는 좋은 방법은. 이러한 항목이 없으면, 사이트 1의 게이트웨이가 사이트 2의 게이트웨이와 통신할 경우 해당 트래픽이 ASA를 통과해 내부 인터페이스에서 사이트 2에 도달하려고 시도하여 문제를 일으킬 수 있습니다. OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 게이트웨이 라우터로 예정된 경우 트래픽에서 다른 사이트에 DCI를 전달하는 것을 방지하려면 필터를 추가해야 합니다. 한 개의 사이트에서 게이트웨이 라우터에 연결할 수 없는 경우, 필터를 제거해야 트래픽이 다른 사이트의 게이트웨이 라우터에 전송될 수 있습니다.



논리적 디바이스의 기록

기능 이름	플랫폼 릴리스	기능 정보
FTD 작동 링크 상태와 물리적 링크 상태 간 동기화	2.9.1	<p>이제 새시가 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다.</p> <p>참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 테코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다.</p> <p>신규/수정된 Firepower Chassis Manager 화면: Logical Devices(논리적 디바이스) > Enable Link State(링크 상태 활성화)</p> <p>신규/수정된 FXOS 명령: set link-state-sync enabled, show interface expand detail</p>
컨테이너 인스턴스에 FMC를 사용하여 FTD 구성 백업 및 복원	2.9.1	<p>이제 FTD 컨테이너 인스턴스에서 FMC 백업/복원 도구를 사용할 수 있습니다.</p> <p>신규/수정된 FMC 화면: System(시스템) > Tools(도구) > Backup/Restore(백업/복원) > Managed Device Backup(매니지드 디바이스 백업)</p> <p>신규/수정된 FTD CLI 명령: restore</p> <p>지원되는 플랫폼: Firepower 4100/9300</p> <p>참고 Firepower 6.7 필요</p>

기능 이름	플랫폼 릴리스	기능 정보
다중 인스턴스 클러스터링	2.8.1	<p>이제 컨테이너 인스턴스로 클러스터를 생성할 수 있습니다. Firepower 9300에서 클러스터의 각 모듈에 하나의 컨테이너 인스턴스를 포함해야 합니다. 보안 엔진/모듈마다 하나 이상의 컨테이너 인스턴스를 추가할 수 없습니다. 각 클러스터 인스턴스에 동일한 보안 모듈 또는 새시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다.</p> <p>신규/수정된 화면:</p> <ul style="list-style-type: none"> • 논리적 디바이스 > 클러스터 추가 • Interfaces(인터페이스) > All Interfaces(모든 인터페이스) > Add New(새로 추가) 드롭다운 메뉴 > Subinterface(하위 인터페이스) > Type(유형) 필드 <p>참고 Firepower 6.6 이상이 필요합니다.</p>
FDM로 FTD을 지원	2.7.1	<p>이제 기본 FTD 인스턴스를 구축하고 FDM 관리를 지정할 수 있습니다. 컨테이너 인스턴스는 지원되지 않습니다.</p> <p>신규/수정된 Firepower Chassis Manager 화면:</p> <p>Logical Devices(논리 디바이스) > Add Device(디바이스 추가) > Settings(설정) > 애플리케이션 인스턴스의 관리 유형</p> <p>참고 FTD 6.5 이상이 필요합니다.</p>
여러 컨테이너 인스턴스에 대한 TLS 암호화 가속	2.7.1	<p>TLS 암호화 가속은 이제 Firepower 4100/9300 새시의 여러 컨테이너 인스턴스(최대 16 개)에서 지원됩니다. 이전에는 모듈/보안 엔진 당 하나의 컨테이너 인스턴스에 대해서만 TLS 암호화 가속을 활성화 할 수 있었습니다.</p> <p>새 인스턴스에는 기본적으로 이 기능이 활성화되어 있습니다. 그러나 업그레이드는 기존 인스턴스에서 가속화를 활성화하지 않습니다. 대신 enter hw-crypto 및 set admin-state enabled FXOS 명령을 사용합니다.</p> <p>신규/수정된 Firepower Chassis Manager 화면:</p> <p>Logical Devices(논리 디바이스) > Add Device(디바이스 추가) > Settings(설정) > Hardware Crypto(하드웨어 암호화) 드롭 다운 메뉴</p> <p>참고 FTD 6.5 이상이 필요합니다.</p>
Firepower 4115, 4125 및 4145 test	2.6.1	<p>Firepower 4115, 4125, 및 4145를 도입했습니다.</p> <p>참고 ASA 9.12(1)이 필요합니다. Firepower 6.4.0에는 FXOS 2.6.1.157이 필요합니다.</p> <p>수정된 화면이 없습니다.</p>

기능 이름	플랫폼 릴리스	기능 정보
Firepower 9300 SM-40, SM-48 및 SM-56 지원	2.6.1	<p>다음 세 가지 보안 모듈을 도입했습니다: SM-40, SM-48, SM-56</p> <p>참고 SM-40 및 SM-48에는 ASA 9.12(1)이 필요합니다. SM-56에는 ASA 9.12(2) 및 FXOS 2.6.1.157이 필요합니다.</p> <p>모든 모듈에는 FTD 6.4 및 FXOS 2.6.1.157이 필요합니다.</p> <p>수정된 화면이 없습니다.</p>
동일한 Firepower 9300의 별도의 모듈에서 ASA 및 FTD에 대한 지원	2.6.1	<p>이제 동일한 Firepower 9300에서 ASA 및 FTD 논리적 디바이스를 구축할 수 있습니다.</p> <p>참고 ASA 9.12(1)이 필요합니다. Firepower 6.4.0에는 FXOS 2.6.1.157이 필요합니다.</p> <p>수정된 화면이 없습니다.</p>
FTD 부트스트랩 구성의 경우, 이제 Firepower Chassis Manager에서 FMC의 NAT ID를 설정할 수 있습니다.	2.6.1	<p>이제 Firepower Chassis Manager에서 FMC NAT ID를 설정할 수 있습니다. 이전에는 FXOS CLI 또는 FTD CLI 내에서만 NAT ID를 설정할 수 있었습니다. 일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.</p> <p>신규/수정된 화면:</p> <p>Logical Devices(논리적 디바이스) > Add Device(디바이스 추가) > Settings(설정) > Firepower Management Center NAT ID 필드</p>
모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에 대한 SSL 하드웨어 가속 지원	2.6.1	<p>이제 모듈/보안 엔진에서 하나의 컨테이너 인스턴스에 대해 SSL 하드웨어 가속을 활성화할 수 있습니다. SSL 하드웨어 가속은 다른 컨테이너 인스턴스에 대해서는 비활성화되어 있지만 기본 인스턴스에 대해서는 활성화되어 있습니다. 자세한 내용은 FMC 구성 가이드를 참조하십시오.</p> <p>신규/수정된 명령: config hwCrypto enable, show hwCrypto</p> <p>수정된 화면이 없습니다.</p>

기능 이름	플랫폼 릴리스	기능 정보
FTD을 위한 다중 인스턴스 기능	2.4.1	<p>이제 단일 보안 엔진/모듈에서 여러 논리적 디바이스를 각각 FTD 컨테이너 인스턴스와 함께 구축할 수 있습니다. 이전에는 단일 기본 애플리케이션 인스턴스만 구축할 수 있었습니다. 기본 인스턴스도 여전히 지원됩니다. Firepower 9300의 경우 일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다.</p> <p>물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 컨테이너 인스턴스를 구축할 때 할당된 CPU 코어 수를 지정해야 합니다. RAM이 코어 수에 따라 동적으로 할당되며, 디스크 공간이 인스턴스당 40GB로 설정됩니다. 이 리소스 관리를 사용하면 각 인스턴스에 대한 성능 기능을 맞춤화할 수 있습니다.</p> <p>개별 채시 2개의 컨테이너 인스턴스를 사용하여 고가용성을 사용할 수 있습니다. 예를 들어 각각 인스턴스가 10개인 채시가 2개 있으면 고가용성 쌍 10개를 생성할 수 있습니다. 클러스터링은 지원되지 않습니다.</p> <p>참고 다중 인스턴스 기능은 ASA 다중 컨텍스트 모드와 비슷하지만 구현은 서로 다릅니다. 다중 컨텍스트 모드에서는 단일 애플리케이션 인스턴스를 분할하는 반면 다중 인스턴스 기능 사용 시에는 독립적인 컨테이너 인스턴스를 사용할 수 있습니다. 컨테이너 인스턴스에서는 하드 리소스 분리, 별도의 구성 관리/다시 로드/소프트웨어 업데이트가 허용되며 전체 FTD 기능이 지원됩니다. 다중 컨텍스트 모드에서는 리소스가 공유되므로 지정된 플랫폼에서 더 많은 컨텍스트가 지원됩니다. FTD에서는 다중 상황 모드를 사용할 수 없습니다.</p> <p>참고 FTD 버전 6.3 이상이 필요합니다.</p> <p>신규/수정된 Firepower Chassis Manager 화면:</p> <p>Overview(개요) > Devices(디바이스)</p> <p>Interfaces(인터페이스) > All Interfaces(모든 인터페이스) > Add New(새로 추가) 드롭다운 메뉴 > Subinterface(하위 인터페이스)</p> <p>Interfaces(인터페이스) > All Interfaces(모든 인터페이스) > Type(유형)</p> <p>Logical Devices(논리적 디바이스) > Add Device(디바이스 추가)</p> <p>Platform Settings(플랫폼 설정) > MAC Pool(MAC 풀)</p> <p>Platform Settings(플랫폼 설정) > Resource Profiles(리소스 프로파일)</p> <p>신규/수정된 FMC 화면:</p> <p>Devices(디바이스) > Device Management(디바이스 관리) > Edit(수정) 아이콘 > Interfaces(인터페이스) 탭</p>

기능 이름	플랫폼 릴리스	기능 정보
ASA 논리적 디바이스에 대한 투명 모드 구축 지원	2.4.1	<p>이제 ASA를 구축할 때 투명 또는 라우팅된 모드를 지정할 수 있습니다.</p> <p>신규/수정된 Firepower Chassis Manager 화면: Logical Devices(논리적 디바이스) > Add Device(디바이스 추가) > Settings(설정) 신규/수정된 옵션: Firewall Mode(방화벽 모드) 드롭다운 목록</p>
클러스터 제어 링크사용자 정의 가능한 IP 주소	2.4.1	<p>기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 새시에서는 새시 ID 및 슬롯 ID 127.2.chassis_id.slot_id를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다.</p> <p>신규/수정된 화면: Logical Devices(논리적 디바이스) > Add Device(디바이스 추가) > Cluster Information(클러스터 정보) > CCL Subnet IP(CCL 서브넷 IP) 필드</p>
FTD 부트스트랩 구성의 경우 이제 FXOS CLI에서 FMC의 NAT ID를 설정할 수 있습니다.	2.4.1	<p>이제 FXOS CLI에서 FMC NAT ID를 설정할 수 있습니다. 이전에는 FTD CLI 내에서만 NAT ID를 설정할 수 있었습니다. 일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.</p> <p>신규/수정된 명령: enter bootstrap-key NAT_ID</p>
ASA에 대한 사이트 간 클러스터링 개선	2.1.1	<p>이제 ASA 클러스터를 구축할 때 각 Firepower 4100/9300 새시에 대한 사이트 ID를 구성할 수 있습니다. 전에는 ASA 애플리케이션 내에서 사이트 ID를 구성해야 했습니다. 이 기능 덕분에 초기 구축이 수월해졌습니다. 더 이상 ASA 구성 내에서 사이트 ID를 설정할 수 없습니다. 또한 사이트 간 클러스터링과의 호환성을 최대한 활용하려면 안정성과 성능이 개선된 ASA 9.7(1) 및 FXOS 2.1.1로 업그레이드하는 것이 좋습니다.</p> <p>수정된 화면: Logical Devices(논리적 디바이스) > Configuration(구성)</p>
Firepower 9300의 6개 FTD 모듈에 대한 새시 간 클러스터링	2.1.1	<p>이제 Firepower 9300에서 FTD을 위해 새시 간 클러스터링을 활성화할 수 있습니다. 최대 6개의 모듈을 포함할 수 있습니다. 예를 들어 새시 6개에 모듈 1개, 새시 3개에 모듈 2개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다.</p> <p>수정된 화면: Logical Devices(논리적 디바이스) > Configuration(구성)</p>

기능 이름	플랫폼 릴리스	기능 정보
Firepower 4100에서 FTD 클러스터링 지원	2.1.1	FTD 클러스터에서 최대 6개의 새시를 클러스터링할 수 있습니다.
ASA 클러스터에서 16 Firepower 4100 새시에 대한 지원	2.0.1	ASA 클러스터에서 최대 16개의 새시를 클러스터링할 수 있습니다.
Firepower 4100에서 ASA 클러스터링에 대한 지원	1.1.4	ASA 클러스터에서 최대 6개의 새시를 클러스터링할 수 있습니다.
Firepower 9300의 FTD에서 인트라 새시 클러스터링(intra-chassis clustering) 지원	1.1.4	Firepower 9300은 FTD 애플리케이션이 있는 인트라 새시 클러스터링(intra-chassis clustering)을 지원합니다. 수정된 화면: Logical Devices (논리적 디바이스) > Configuration (구성)
Firepower 9300에서 ASA 모듈 16개를 위한 인트라 새시 클러스터링(intra-chassis clustering)	1.1.3	현재 ASA를 위한 새시 간 클러스터링을 활성화할 수 있습니다. 최대 16개의 모듈을 포함할 수 있습니다. 예를 들어 새시 16개에 모듈 1개, 새시 8개에 모듈 2개, 또는 모듈을 16개까지 제공하는 어떤 조합도 사용할 수 있습니다. 수정된 화면: Logical Devices (논리적 디바이스) > Configuration (구성)
Firepower 9300에서 ASA를 위한 인트라 새시 클러스터링(intra-chassis clustering)	1.1.1	Firepower 9300 새시 내부에서 모든 ASA 보안 모듈을 클러스터링할 수 있습니다. 추가된 화면: Logical Devices (논리적 디바이스) > Configuration (구성)

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.