



Firepower 4100/9300의 논리적 디바이스

Firepower 4100/9300은 하나 이상의 논리적 디바이스를 설치할 수 있는 유연한 보안 플랫폼입니다.

새시 인터페이스를 구성하고, 논리적 디바이스를 추가하고, Secure Firewall 새시 관리자 또는 FXOS CLI를 사용하는 Firepower 4100/9300 새시의 디바이스에 인터페이스를 할당해야 합니다. device manager에서는 이러한 작업을 수행할 수 없습니다.

이 장에서는 기본 인터페이스 구성 및 새시 관리자를 사용하여 독립형 디바이스 또는 고가용성 논리적 디바이스를 추가하는 방법을 설명합니다. FXOS CLI를 사용하려면 FXOS CLI 구성 가이드를 참조하십시오. 고급 FXOS 절차 및 트러블슈팅에 대한 자세한 내용은 FXOS 구성 가이드를 참조하십시오.

- [인터페이스 정보, 1 페이지](#)
- [Firepower 9300 하드웨어 및 소프트웨어 조합에 대한 요구 사항 및 사전 요구 사항, 3 페이지](#)
- [논리적 디바이스 관련 지침 및 제한 사항, 4 페이지](#)
- [인터페이스 구성, 5 페이지](#)
- [논리적 디바이스 구성, 7 페이지](#)
- [Firepower 4100/9300 논리적 디바이스의 기록, 12 페이지](#)

인터페이스 정보

Firepower 4100/9300 새시에서는 물리적 인터페이스 및 EtherChannel(포트-채널) 인터페이스를 지원합니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

새시 관리 인터페이스

새시 관리 인터페이스는 SSH 또는 새시 관리자를 통한 FXOS 새시 관리에 사용됩니다. 이 인터페이스는 애플리케이션 관리용 논리적 디바이스에 할당하는 관리 유형 인터페이스와는 별개입니다.

이 인터페이스의 파라미터는 CLI에서 구성해야 합니다. FXOS CLI에서 이 인터페이스에 대한 정보를 확인하려면 로컬 관리에 연결한 다음 관리 포트를 표시합니다.

```
Firepower # connect local-mgmt
```

```
Firepower(local-mgmt) # show mgmt-port
```

실제 케이블이나 SFP 모듈 연결을 해제하거나 **mgmt-port shut** 명령을 수행하더라도 새시 관리 인터페이스는 계속 작동합니다.



참고 새시 관리 인터페이스는 점보 프레임을 지원하지 않습니다.

인터페이스 유형

물리적 인터페이스 EtherChannel(포트-채널) 인터페이스는 다음 유형 중 하나가 될 수 있습니다.

- **Data(데이터)** - 일반 데이터에 사용됩니다. 데이터 인터페이스는 논리적 디바이스 간에 공유할 수 없으며 논리적 디바이스는 백플레인을 통해 다른 논리적 디바이스와 통신할 수 없습니다. 데이터 인터페이스의 트래픽의 경우, 모든 트래픽은 하나의 인터페이스에서 새시를 종료하고 다른 인터페이스로 돌아가서 다른 논리적 디바이스에 연결해야 합니다.
- **Data-sharing(데이터 공유)** - 일반 데이터에 사용됩니다. 컨테이너 인스턴스에서만 지원되는 이러한 데이터 인터페이스는 하나 이상의 논리적 디바이스/컨테이너 인스턴스(위협 방어-사용-management center 전용)에서 공유할 수 있습니다.
- **Mgmt(관리)** - 애플리케이션 인스턴스를 관리하는 데 사용됩니다. 이러한 인터페이스는 외부 호스트에 액세스하기 위해 하나 이상의 논리적 디바이스에서 공유할 수 있습니다. 단, 논리적 디바이스에서는 인터페이스를 공유하는 다른 논리적 디바이스와 이 인터페이스를 통해 통신할 수 없습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다. 애플리케이션 및 관리자에 따라 나중에 데이터 인터페이스에서 관리를 활성화할 수 있습니다. 데이터 관리를 활성화한 후 이를 사용하지 않으려는 경우에도 관리 인터페이스를 논리적 디바이스에 할당해야 합니다. 개별 새시 관리 인터페이스에 대한 내용은 [새시 관리 인터페이스, 1 페이지](#) 항목을 참조하십시오.



참고 관리 인터페이스를 변경하면 논리적 디바이스가 재부팅됩니다. 예를 들어 e1/1에서 e1/2로 변경하면 논리적 디바이스가 재부팅되어 새 관리가 적용됩니다.

- 이벤트 처리-위협 방어-사용-management center 디바이스의 보조 관리 인터페이스로 사용됩니다.



참고 각 애플리케이션 인스턴스가 설치될 때 가상 이더넷 인터페이스가 할당됩니다. 애플리케이션에서 이벤트 인터페이스를 사용하지 않는 경우 가상 인터페이스는 관리자 중단 상태가 됩니다.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster(클러스터) - 클러스터형 논리적 디바이스용 클러스터 제어 링크로 사용됩니다. 기본적으로, 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다. 이 클러스터 유형은 EtherChannel 인터페이스에서만 지원됩니다. device manager 및 CDO는 클러스터링을 지원하지 않습니다.

FXOS 인터페이스와 애플리케이션 인터페이스 비교

Firepower 4100/9300에서는 물리적 인터페이스 및 EtherChannel(포트-채널) 인터페이스의 기본 이더넷 설정을 관리합니다. 애플리케이션 내에서는 상위 레벨 설정을 구성합니다. 예를 들어 FXOS에서는 Etherchannel만 생성할 수 있습니다. 그러나 애플리케이션 내의 EtherChannel에 IP 주소를 할당할 수 있습니다.

다음 섹션에서는 FXOS와 인터페이스에 대한 애플리케이션 간의 상호 작용에 대해 설명합니다.

VLAN 하위 인터페이스

논리적 디바이스의 경우에는 애플리케이션 내에서 VLAN 하위 인터페이스를 생성할 수 있습니다.

새시와 애플리케이션의 독립 인터페이스 상태

관리를 위해 새시와 애플리케이션에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 새시와 애플리케이션에서 상태가 일치하지 않을 수도 있습니다.

Firepower 9300 하드웨어 및 소프트웨어 조합에 대한 요구 사항 및 사전 요구 사항

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

논리적 디바이스 관련 지침 및 제한 사항

지침 및 제한 사항은 다음 섹션을 참조하십시오.

인터페이스에 대한 지침 및 제한 사항

기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.

일반 지침 및 제한 사항

고가용성

- 애플리케이션 구성 내에서 고가용성을 구성합니다.
- 모든 데이터 인터페이스를 페일오버 및 상태 링크로 사용할 수 있습니다.
- 고가용성 페일오버 설정에는 2개의 유닛이 필요합니다.
 - 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.
- 자세한 내용은 [고가용성을 위한 시스템 요구 사항](#)를 참고하십시오.

인터페이스 구성

기본적으로 물리적 인터페이스는 비활성화되어 있습니다. 인터페이스 활성화, EtherChannels 추가, 인터페이스 속성 수정 구성 작업을 수행할 수 있습니다.



인터페이스 활성화 또는 비활성화

각 인터페이스의 **Admin State**(관리 상태)를 활성화 또는 비활성화로 변경할 수 있습니다. 기본적으로 물리적 인터페이스는 비활성화되어 있습니다.



프로시저

단계 1 Interfaces(인터페이스)를 선택하여 **Interfaces**(인터페이스) 페이지를 엽니다.

Interfaces(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.

단계 2 인터페이스를 활성화하려면 비활성화된 슬라이더 비활성화됨()를 클릭하여 활성화된 슬라이더 활성화됨()로 변경합니다.

Yes(예)를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 회색에서 녹색으로 변경됩니다.

단계 3 인터페이스를 비활성화하려면 활성화된 슬라이더 활성화됨()를 클릭하여 비활성화된 슬라이더 비활성화됨()로 변경합니다.

Yes(예)를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 녹색에서 회색으로 변경됩니다.

실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스를 설정할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 애플리케이션에서 논리적으로 활성화해야 합니다.



참고 QSFPH40G-CUxM의 경우, 자동 협상은 기본값으로 항상 활성화되어 있으며 비활성화할 수 없습니다.

시작하기 전에

- 이미 EtherChannel의 멤버인 인터페이스는 개별적으로 편집할 수 없습니다. EtherChannel에 인터페이스를 추가하기 전에 설정을 구성하십시오.

EtherChannel(포트 채널) 추가

EtherChannel(포트 채널로 알려짐)은 동일한 미디어 유형 및 용량의 멤버 인터페이스를 최대 16개까지 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 있습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 데이터 인터페이스를 다음과 같이 구성할 수 있습니다.

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



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

Firepower 4100/9300 새시는 각 멤버 인터페이스가 LACP 업데이트를 송수신할 수 있도록 액티브 LACP 모드에서만 EtherChannel을 지원합니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스텐바이 인터페이스를 사용할 수 없으며, 연결 및 구성이 확인되지 않습니다.

Firepower 4100/9300 새시에서 EtherChannel을 생성하면 물리적 링크가 가동 중이더라도 EtherChannel은 논리적 디바이스에 할당될 때까지 Active LACP(액티브 LACP) 모드인 경우 **Suspended**(일시 중단) 상태로, On LACP(LACP 켜짐) 모드인 경우 **Down**(중단) 상태로 유지됩니다. 다음의 상황에서는 EtherChannel의 **Suspended**(일시 중단) 상태가 해제됩니다.

- EtherChannel이 독립형 논리적 디바이스에 대한 데이터 인터페이스 또는 관리 인터페이스로 추가됩니다.
- EtherChannel이 클러스터의 일부인 논리적 디바이스에 대한 관리 인터페이스 또는 클러스터 제어 링크로 추가됩니다.

- EtherChannel이 클러스터의 일부이며 유닛 하나 이상이 클러스터에 조인된 논리적 디바이스에 대한 데이터 인터페이스로 추가됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. EtherChannel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended**(일시 중단) 또는 **Down**(중단) 상태로 전환됩니다.

논리적 디바이스 구성

Firepower 4100/9300 새시에서 독립형 논리적 디바이스 또는 고가용성 쌍을 추가합니다.

Device Manager에 대한 독립형 Threat Defense 추가

네이티브 인스턴스로 device manager를 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.
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 새시 관리용으로만 사용되는 새시 관리 포트와는 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
 - Threat Defense 호스트 이름 및 도메인 이름

프로시저

보안 정책 구성을 시작하려면 device manager 구성 가이드를 참조하십시오.

고가용성 쌍 추가

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

시작하기 전에

[고가용성을 위한 시스템 요구 사항](#)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.

단계 3 논리적 디바이스에서 고가용성을 활성화합니다. [고가용성\(페일오버\)](#) 섹션을 참조하십시오.

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

Threat Defense 논리적 디바이스에서 인터페이스 변경

위협 방어 논리적 디바이스에서 인터페이스를 할당 또는 할당 해제할 수 있습니다. 그런 다음 device manager에서 인터페이스 구성을 동기화할 수 있습니다.

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

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

시작하기 전에

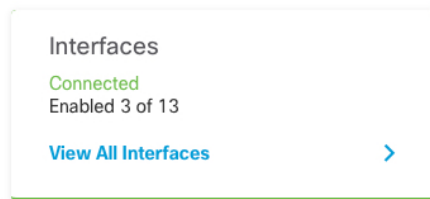
- 인터페이스를 구성하고 [실제 인터페이스 구성, 5 페이지](#) 및 [EtherChannel\(포트 채널\) 추가, 6 페이지](#)에 따라 EtherChannel을 추가합니다.

- 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.
- 고가용성의 경우에는 device manager에서 구성을 동기화하기 전에 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 인터페이스는 먼저 스탠바이 유닛에서 변경한 후에 액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운된 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

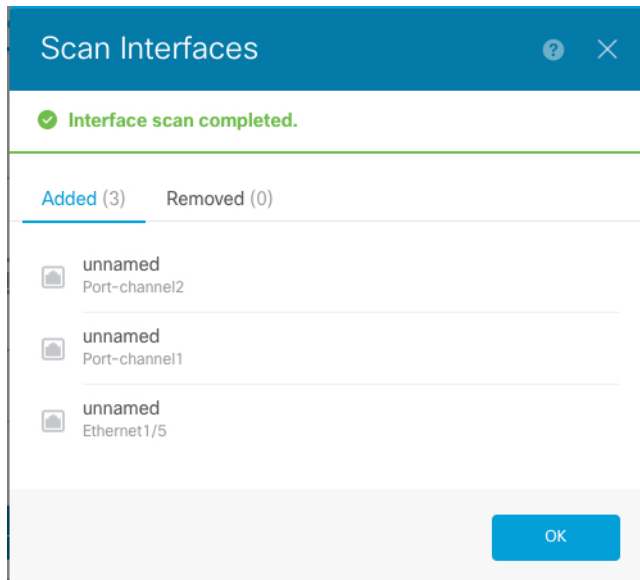
프로시저

단계 1 device manager에서 인터페이스를 동기화하고 마이그레이션합니다.

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



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



- 이름, IP 주소 등을 사용하여 새 인터페이스를 구성합니다.

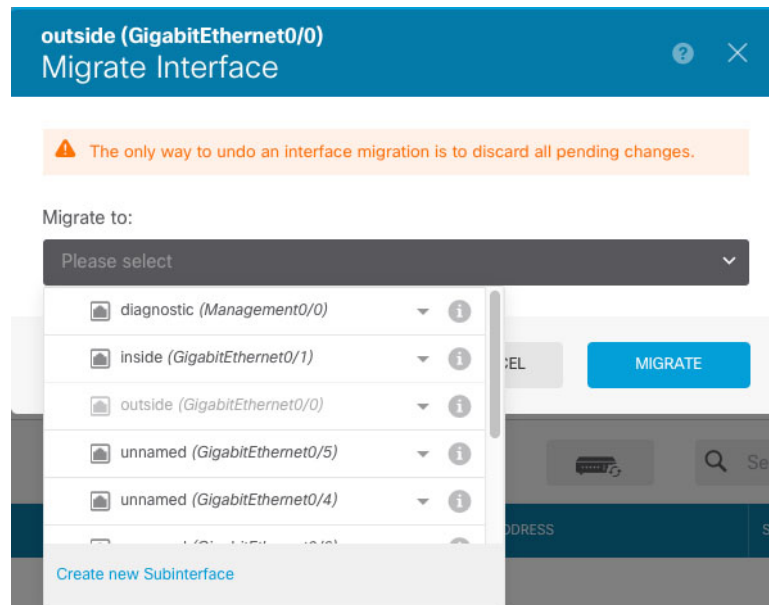
제거할 인터페이스의 기존 IP 주소 및 이름을 사용하려는 경우에는 새 인터페이스에서 해당 설정을 사용할 수 있도록 기존 인터페이스를 더미 이름 및 IP 주소로 다시 구성해야 합니다.

- 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.

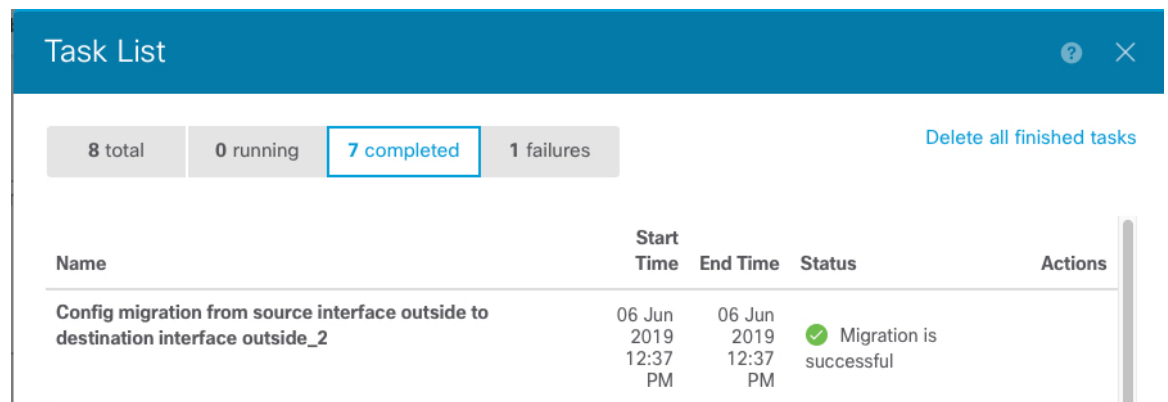
- g) **Replacement Interface(교체 인터페이스)** 드롭다운 목록에서 새 인터페이스를 선택합니다.



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

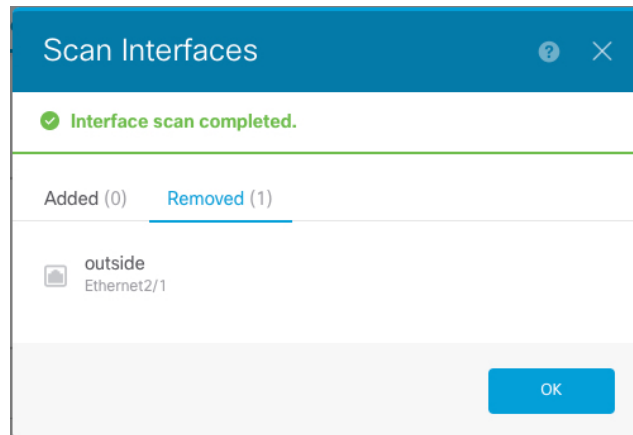


- i) **Task List(작업 목록)**를 확인하여 마이그레이션에 성공했는지 확인합니다.



단계 2 device manager에서 인터페이스를 다시 동기화합니다.

그림 1: Device Manager 스캔 인터페이스



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 1을 slot_number로 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.

connect ftd name

인스턴스 이름을 확인하려면 이름 없이 명령을 입력합니다.

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.

- Threat Defense - **exit**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-J, .**를 입력합니다.

Firepower 4100/9300 논리적 디바이스의 기록

기능	버전	세부 사항
Firepower 4100/9300의 device manager 지원	6.5.0	이제 Firepower 4100/9300에서 위협 방어 논리적 디바이스와 함께 device manager를 사용할 수 있습니다. device manager에서는 다중 인스턴스 기능을 지원하지 않습니다. 네이티브 인스턴스만 지원됩니다. 참고 FXOS 2.7.1이 필요합니다.

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.