디바이스 관리

이 가이드는 온프레미스 Secure Firewall Management Center에 기본 관리자 또는 분석 전용 관리자로 적용됩니다. Cisco Defense Orchestrator(CDO) 클라우드 사용 Firewall Management Center을 기본 관리자로 사용하는 경우, 분석을 위해 온프레미스 management center를 사용할 수 있습니다. 이 가이드를 CDO 관리에 사용하지 마십시오. Cisco Defense Orchestrator에서 클라우드 제공 방화벽 관리 센터를 사용하여 방화벽 위협 방어 관리의 내용을 참조하십시오.

이 장에서는 Secure Firewall Management Center에서 디바이스를 추가하고 관리하는 방법을 설명합니다.

디바이스 관리 관련 정보

management center를 사용하여 디바이스를 관리합니다.

Management Center 및 디바이스 관리 관련 정보

management center는 디바이스를 관리할 때 자체와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. management center는 이 채널을 사용하여 네트워크 트래픽을 분석하고 관리하고자 하는 방

법에 대한 정보를 디바이스로 전송합니다. 디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 management center로 전송합니다.

management center를 사용하여 디바이스를 관리하면 다음을 수행할 수 있습니다.

- 단일 위치에서 모든 디바이스에 대한 정책을 구성하므로 설정을 좀 더 쉽게 변경할 수 있습니다.
- 디바이스에 각종 소프트웨어 업데이트를 설치할 수 있습니다.
- 관리되는 디바이스에 상태 정책을 푸시하고 management center에서 상태를 모니터링할 수 있습니다.

참고 CDO 매니지드 디바이스가 있고 분석용으로만 온프레미스 management center를 사용하는 경우 온프레미스 management center는 정책 구성 또는 업그레이드를 지원하지 않습니다. 장치 구성 및 기타 지원되지 않는 기능과 관련된 이 안내서의 장 및 절차는 기본 관리자가 CDO인 디바이스에는 적용되지 않습니다.

management center는 침입 이벤트, 네트워크 검색 정보 및 디바이스 성능 데이터를 집계하고 상호 연결하므로 사용자는 디바이스가 상호 관계에 대해 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가할 수 있습니다.

management center를 사용하면 디바이스 동작의 거의 모든 부분을 관리할 수 있습니다.

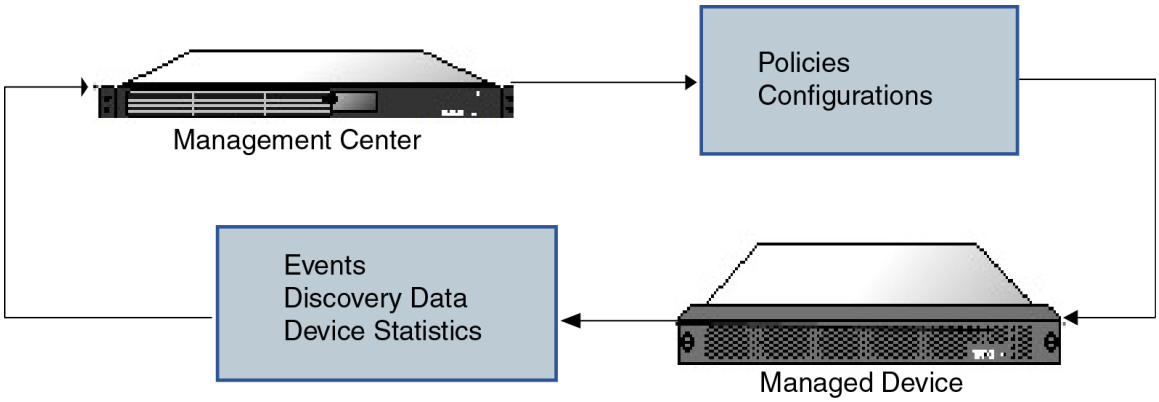
참고 하지만 management center은 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html에서 사용 가능한 호환성 매트릭스에서 지정된 일부 이전 릴리스가 실행되는 디바이스를 관리할 수 있으며 이런 이전 릴리스를 사용하는 threat defense 소프트웨어의 최신 버전이 필요한 디바이스에서는 새로운 기능을 사용할 수 없습니다. 일부 management center 기능은 이전 버전에서 사용할 수 있습니다.

Secure Firewall Management Center로 관리할 수 있는 내용

Secure Firewall Management Center를 중앙 관리 지점으로 사용하여 threat defense 디바이스를 관리할 수 있습니다.

디바이스를 관리할 때에는 management center와 디바이스 간에 안전한 SSL 암호화 TCP 터널을 통해 정보가 전송됩니다.

다음 그림에서는 management center 및 해당 매니지드 디바이스 간에 무엇이 전송되는지를 보여줍니다. 어플라이언스 간에 전송되는 이벤트와 정책의 유형은 디바이스 유형을 기반으로 합니다.



관리 연결 정보

management center 정보를 사용하여 디바이스를 구성하고 management center에 디바이스를 추가한 후에는 디바이스 또는 management center에서 관리 연결을 설정할 수 있습니다. 초기 설정에 따라:

- 디바이스 또는 management center를 시작할 수 있습니다.
- 디바이스만 시작할 수 있습니다.
- management center만 시작할 수 있습니다.

시작은 항상 management center의 eth0 또는 디바이스에서 번호가 가장 낮은 관리 인터페이스에서 시작됩니다. 연결이 설정되지 않은 경우 추가 관리 인터페이스가 시도됩니다. management center의 여러 관리 인터페이스를 사용하면 개별 네트워크에 연결하거나 관리 및 이벤트 트래픽을 분리할 수 있습니다. 그러나 이니시에이터는 라우팅 테이블을 기반으로 최상의 인터페이스를 선택하지 않습니다.

참고 관리 연결은 디바이스와 디바이스 사이의 보안 SSL 암호화 통신 채널입니다. 보안을 위해 사이트 간 VPN과 같은 추가 암호화 터널을 통해 이 트래픽을 실행할 필요가 없습니다. 예를 들어 VPN이 다운되면 관리 연결이 끊어지므로 간단한 관리 경로를 사용하는 것이 좋습니다.

정책 및 이벤트 이상

디바이스에 정책을 구축하고 디바이스에서 이벤트를 수신하는 것 외에도 management center에서는 다른 디바이스 관련 작업을 수행할 수 있습니다.

디바이스 백업

FTD CLI에서는 물리적 매니지드 디바이스를 백업할 수 없습니다. 설정 데이터 및 선택적으로 통합된 파일을 백업하려면 디바이스를 관리하는 management center를 사용하여 디바이스의 백업을 수행할 수 있습니다.

이벤트 데이터를 백업하기 위해서는 디바이스를 관리하는 management center의 백업을 수행합니다.

디바이스 업데이트

Cisco는 다음과 같은 Firepower System의 업데이트를 수시로 배포합니다.

- 새로운 침입 규칙과 업데이트된 침입 규칙이 포함되는 침입 규칙 업데이트
- 취약성 데이터베이스(VDB) 업데이트
- 지리위치 업데이트
- 소프트웨어 패치 및 업데이트

관리하는 디바이스에 업데이트를 설치하려면 management center를 사용할 수 있습니다.

디바이스 관리 인터페이스

각 디바이스는 management center와 통신하기 위한 단일 전용 관리 인터페이스를 포함합니다. 선택적으로 전용 관리 인터페이스 대신 관리용 데이터 인터페이스를 사용하도록 디바이스를 구성할 수 있습니다.

관리 인터페이스 또는 콘솔 포트에서 초기 설정을 수행할 수 있습니다.

관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

Threat Defense에서 관리 및 이벤트 인터페이스

디바이스를 설정할 때 연결할(알고 있는 경우) management center IP 주소 또는 호스트 이름을 지정합니다. 이 경우 디바이스가 연결을 시작하고 관리 및 이벤트 트래픽은 처음 등록할 때 이 주소로 전송됩니다. management center를 알 수 없는 경우 management center는 초기 연결을 설정합니다. 이 경우 처음에는 threat defense에 지정된 것과 다른 management center 관리 인터페이스에서 연결될 수 있습니다. 후속 연결에서는 지정된 IP 주소의 management center 관리 인터페이스를 사용해야 합니다.

management center에 별도의 이벤트 전용 인터페이스가 있는 경우, 네트워크가 허용하는 경우 매니지드 디바이스에서 후속 이벤트 트래픽을 management center 이벤트 전용 인터페이스로 보냅니다. 또한 일부 매니지드 디바이스 모델에는 이벤트 전용 트래픽에 대해 구성할 수 있는 추가 관리 인터페이스가 포함되어 있습니다. 관리를 위해 데이터 인터페이스를 구성하는 경우 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다. 이벤트 네트워크가 다운되면 이벤트 트래픽은 management center 및/또는 매니지드 디바이스의 일반 관리 인터페이스로 되돌아갑니다.

관리를 위한 **Threat Defense** 데이터 인터페이스 사용

management center와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 원격으로 threat defense를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 관리자 액세스가 유용합니다. 또한 데이터 인터페이스를 사용하면 기본 인터페이스가 중단될 경우 관리 기능을 수행하도록 이중화 보조 인터페이스를 구성할 수 있습니다.

관리자 액세스 요구 사항

데이터 인터페이스의 관리자 액세스에는 다음과 같은 요구 사항이 있습니다.

- 물리적 데이터 인터페이스에서만 관리자 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.또한 management center를 사용하여 리던던시(redundancy)를 위해 단일 보조 인터페이스에서 관리자 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 threat defense와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 management center를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다. Amazon Web Services의 threat defense virtual에서는 콘솔 포트를 사용할 수 없으므로 구성을 계속하기 전에 관리 인터페이스에 대한 SSH 액세스를 유지해야 합니다. 또는 관리자 액세스를 위해 데이터 인터페이스를 설정하고 연결을 끊기 전에 모든 CLI 구성(**configure manager add** 명령 포함)을 완료해야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- 클러스터링은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.

디바이스 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

참고 Firepower 4100/9300의 경우 MGMT 인터페이스는 섀시 관리를 위한 것이며 threat defense 논리적 디바이스 관리를 위한 것이 아닙니다. 별도의 인터페이스를 mgmt(및/ 또는 firepower-eventing) 유형으로 구성한 다음 threat defense 논리적 디바이스에 할당해야 합니다.

참고 모든 섀시에 대한 threat defense의 경우 물리적 관리 인터페이스는 SNMP 또는 시스템 로그에 유용한 논리적 진단 인터페이스 인터페이스 간에 공유되며 management center의 데이터 인터페이스 및 management center 통신의 논리적 관리 인터페이스와 함께 구성됩니다. 자세한 내용은 관리/진단 인터페이스를 참조하십시오.

각 매니지드 디바이스 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 *1:* 매니지드 디바이스의 관리 인터페이스 지원

모델	관리 인터페이스	선택적 이벤트 인터페이스
Firepower 1000	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower 2100	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Secure Firewall 3100	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower 4100 및 9300	management0 참고 management0은 물리적 인터페이스 ID와 상관없이 이 인터페이스의 내부 이름입니다.	management1 참고 management1은 물리적 인터페이스 ID와 상관없이 이 인터페이스의 내부 이름입니다.
ISA 3000	br1 참고 br1은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Secure Firewall Threat Defense Virtual	eth0	지원 안 함

디바이스 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. 매니지드 디바이스를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.

참고 관리 인터페이스의 라우팅은 데이터 인터페이스에 대해 구성한 라우팅과는 완전히 분리됩니다. 전용 관리 인터페이스를 사용하는 대신 관리용 데이터 인터페이스를 설정하는 경우 데이터 라우팅 테이블을 사용하도록 트래픽이 백플레인을 통해 라우팅됩니다. 이 섹션의 정보는 적용되지 않습니다.

일부 플랫폼에서는 여러 관리 인터페이스를 설정할 수 있습니다(관리 인터페이스 및 이벤트 전용 인터페이스). 기본 경로는 인그레스 인터페이스를 포함하지 않으므로 선택한 인터페이스는 지정한 게이트웨이 주소와 게이트웨이가 속한 인터페이스의 네트워크에 따라 다릅니다. 기본 네트워크의 여러 인터페이스의 경우 디바이스는 더 낮은 번호의 인터페이스를 인그레스 인터페이스로 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 threat defense로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다.

참고 관리 연결에 사용되는 인터페이스는 라우팅 테이블에 의해 결정되지 않습니다. 연결은 항상 가장 낮은 번호의 인터페이스부터 시도됩니다.

NAT 환경

NAT(Network Address Translation)는 소스 또는 대상 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT는 일반적으로 프라이빗 네트워크와 인터넷이 통신하는 데 사용됩니다. 정적 NAT는 1:1 변환을 수행하여 디바이스와 management center의 통신에 문제를 일으키지 않지만 포트 주소 변환(PAT)이 더욱 일반적입니다. PAT를 사용하면 단일 공용 IP 주소에 고유한 포트를 사용해 공용 네트워크에 접속할 수 있습니다. 이러한 포트는 필요에 따라 동적으로 할당되므로 PAT 라우터 뒤에 있는 디바이스에 연결을 시작할 수 없습니다.

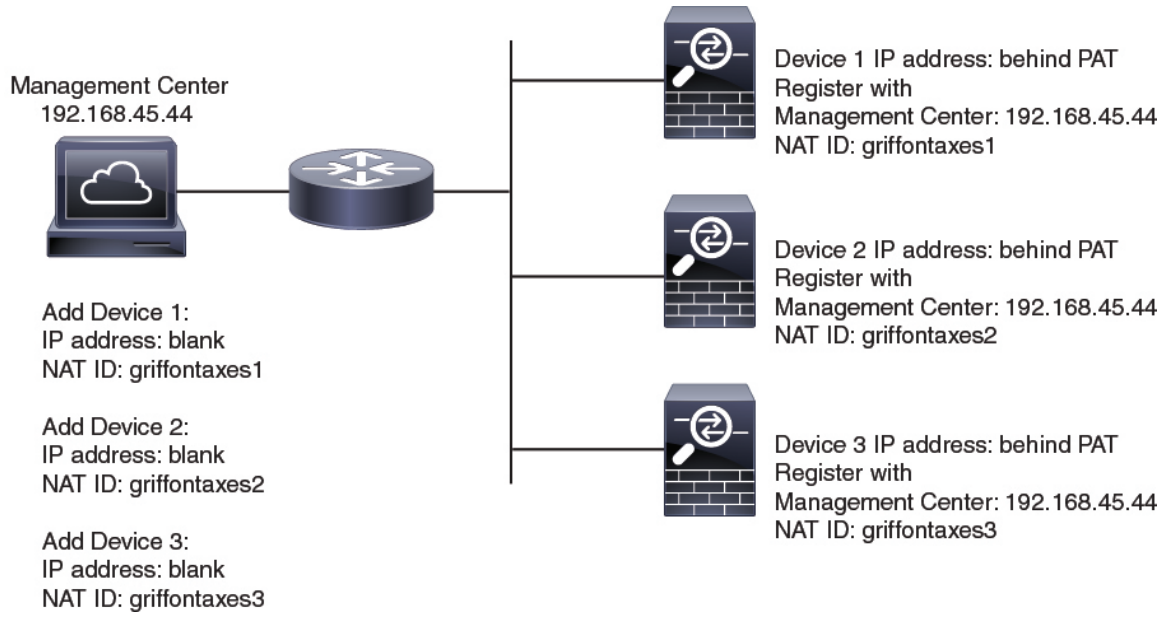
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. management center는 디바이스 IP 주소를 지정하고 디바이스는 management center IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. management center 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

예를 들어 management center에 디바이스를 추가하지만 디바이스 IP 주소를 모르는 경우(디바이스가 PAT 라우터 뒤에 있는 경우) management center에 NAT ID와 등록 키만 지정하고 IP 주소는 공백으로 둡니다. 디바이스에 management center IP 주소, 동일한 NAT ID와 동일한 등록 키를 지정합니다. management center의 IP 주소에 디바이스를 등록합니다. 이때 management center은 IP 주소 대신 NAT ID를 사용해 디바이스를 인증합니다.

NAT 환경에서 NAT ID 사용은 일반적이지만 management center에 많은 디바이스를 추가하려고 할 때에도 NAT ID를 선택할 수 있습니다. management center에는 추가하려는 각 디바이스에 고유한 NAT ID를 지정하고 IP 주소를 공백으로 두고, 각 디바이스에서 management center IP 주소 및 NAT ID를 지정하십시오. 주의: NAT ID는 디바이스별로 고유해야 합니다.

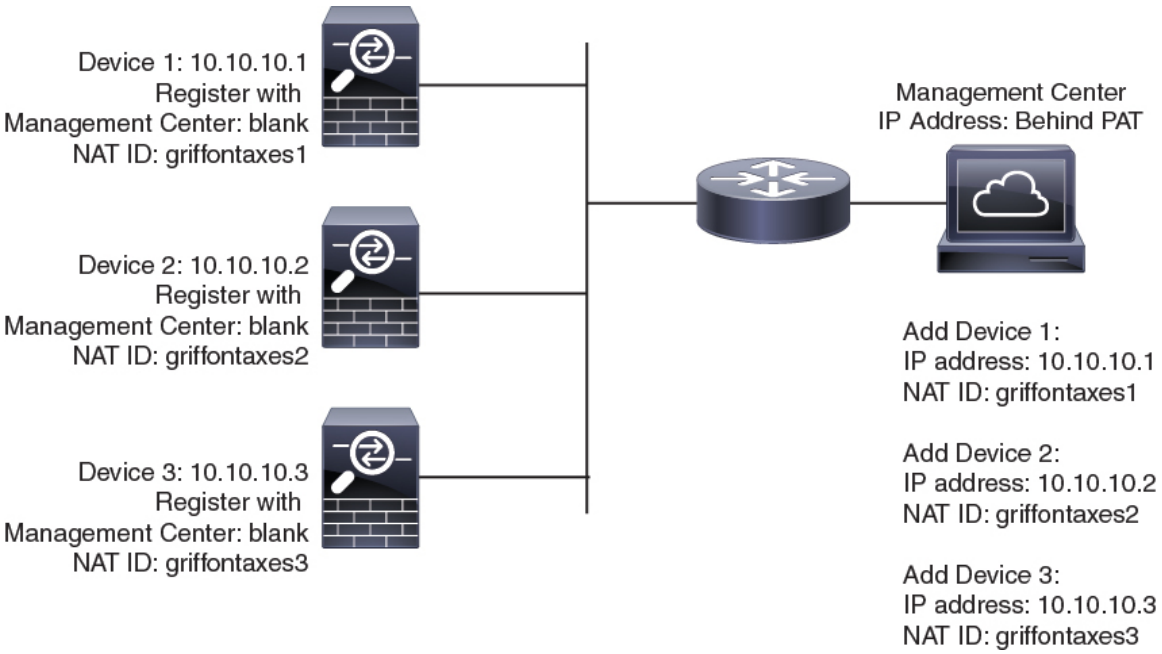
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 management center 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 management center IP 주소를 지정하십시오.

그림 ***1: PAT*** 뒤의 관리되는 디바이스의 ***NAT ID***



다음 예는 PAT ID 주소 뒤의 management center을 보여줍니다. 이 경우 management center 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 management center에 디바이스 IP 주소를 지정하십시오.

그림 ***2: PAT*** 뒤의 ***FMC***에 대한 ***NAT ID***

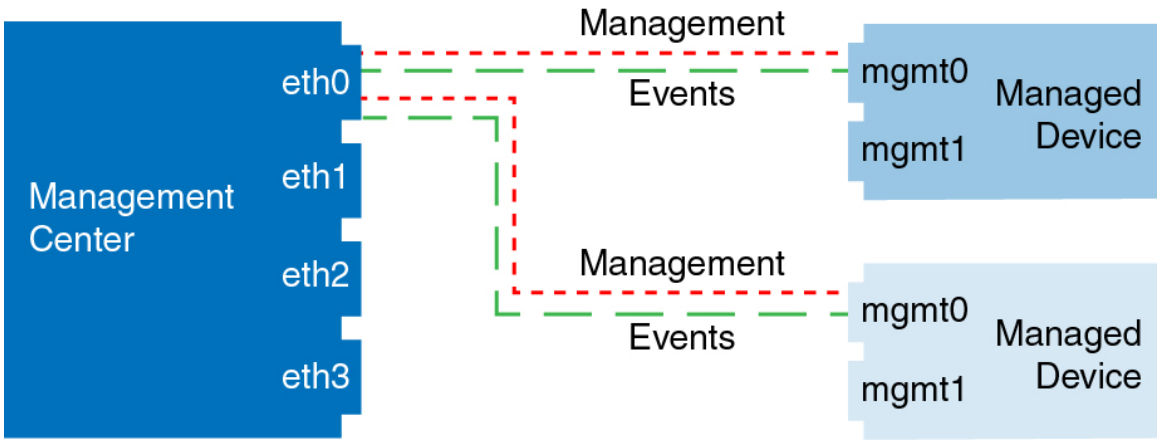


관리 및 이벤트 트래픽 채널 예시

참고 threat defense에서 관리를 위해 데이터 인터페이스를 사용하는 경우 해당 디바이스에 대해 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

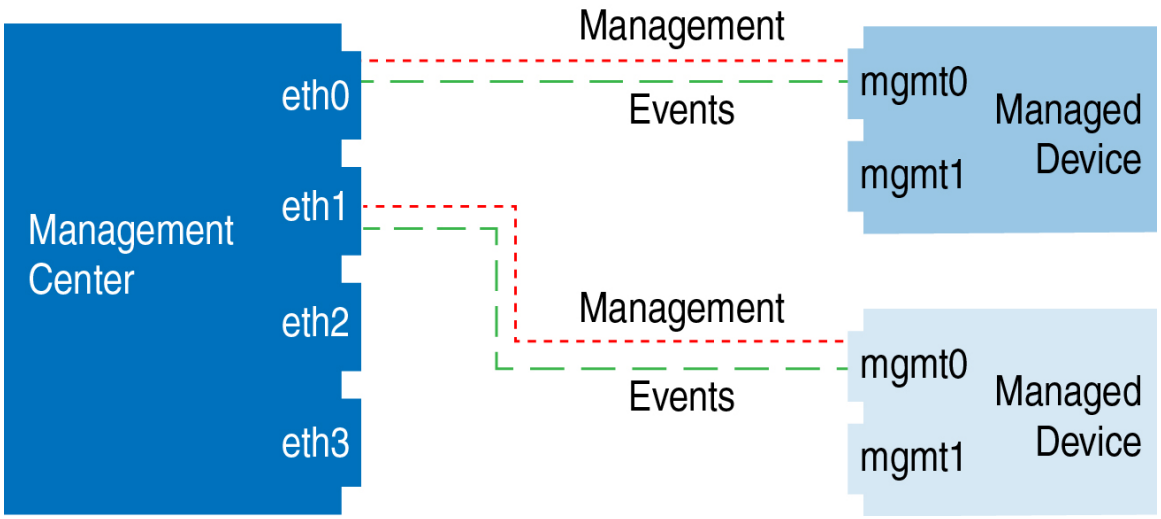
다음 예에서는 기본 관리 인터페이스만 사용하는 management center 및 매니지드 디바이스를 보여 줍니다.

그림 *3:* 단일 관리 인터페이스*: Secure Firewall Management Center*



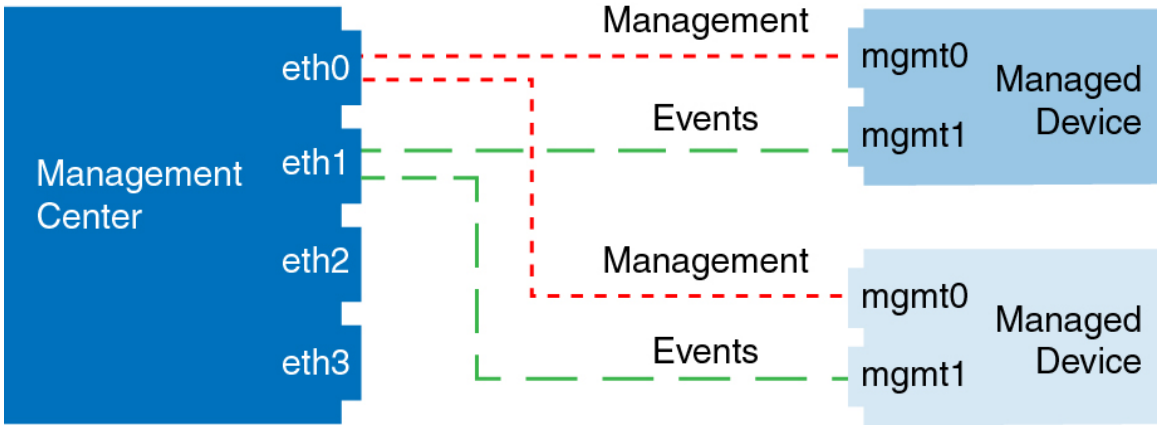
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 management center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

그림 *4:* 다중 관리 인터페이스*: Secure Firewall Management Center*



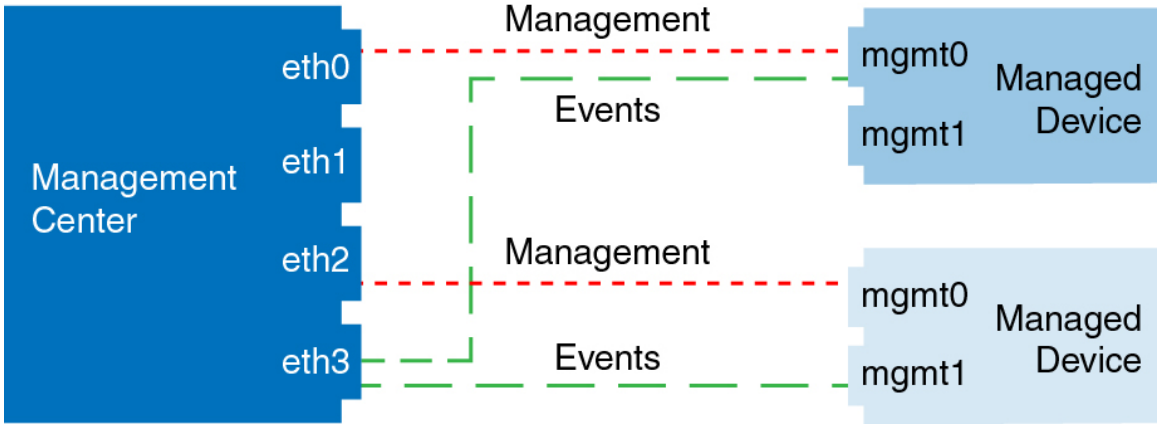
다음 예에서는 별도의 이벤트 인터페이스를 사용하는 management center 및 매니지드 디바이스를 보여 줍니다.

그림 *5: Secure Firewall Management Center* 및 매니지드 디바이스에 대한 별도의 이벤트 인터페이스



다음 예는 별도의 이벤트 인터페이스를 사용하거나 단일 관리 인터페이스를 사용하는 management center 및 여러 매니지드 디바이스에 대한 다중 관리 인터페이스 및 별도의 이벤트 인터페이스를 보여 줍니다.

그림 *6:* 혼합 관리 및 이벤트 인터페이스 사용



디바이스 관리 요구 사항 및 사전 요건

모델 지원

모든 관리되는 디바이스(절차에 명시되지 않는 한)

지원되는 도메인

디바이스가 상주하는 도메인입니다.

사용자 역할

- 관리자

- 네트워크 관리자

Threat Defense 디바이스의 명령줄 인터페이스에 로그인

threat defense 디바이스에서 명령줄 인터페이스에 직접 로그인 할 수 있습니다.

참고 사용자가 3회 연속 SSH를 통한 CLI 로그인에 실패한 경우, 시스템이 SSH 연결을 종료합니다.

시작하기 전에

기본 관리자 사용자를 사용하여 초기 로그인에 대한 초기 설정 프로세스를 완료합니다. **configure user add** 명령을 사용하여 CLI에 로그인할 수 있는 사용자 어카운트를 추가로 생성할 수 있습니다.

프로시저

단계 **1** 콘솔 포트 또는 SSH를 사용하여 threat defense CLI에 연결합니다.

관리 인터페이스에 SSH를 수는 threat defense 디바이스의 관리 인터페이스에 SSH할 수 있습니다. SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스에 있는 주소에 연결할 수도 있습니다. 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 사용 해제 상태입니다. Secure Shell를 참조하여 특정 데이터 인터페이스에 SSH를 연결합니다.

물리적 디바이스의 경우 디바이스에서 콘솔 포트에 직접 연결할 수 있습니다. 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오. 다음 시리얼 설정을 사용하십시오.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

사용자가 콘솔 포트에서 액세스하는 초기 CLI는 디바이스 유형에 따라 다릅니다.

- ISA 3000 - 콘솔 포트의 CLI는 일반 threat defense CLI입니다.
- 기타 모듈—콘솔 포트의 CLI는 FXOS입니다. **connect ftd** 명령을 사용하여 threat defense CLI로 이동할 수 있습니다. FXOS CLI를 섀시 레벨 컨피그레이션 및 문제 해결용으로만 사용합니다. 기본 컨피그레이션, 모니터링 및 일반 시스템 트러블슈팅 시에는 threat defense CLI를 사용합니다. FXOS 명령에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

단계 **2** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **3** CLI 프롬프트(>)에서 명령줄 액세스 수준에서 허용되는 명령 중 하나를 사용합니다.

단계 **4** (선택 사항) 진단 CLI에 액세스합니다.

system support diagnostic-cli

고급 문제 해결용으로 이 CLI를 사용합니다. 이 CLI에는 추가 **show** 및 기타 명령이 포함되어 있습니다.

이 CLI는 사용자 EXEC 모드 및 권한 EXEC 모드라는 두 개의 하위 모드가 있습니다. 권한 EXEC 모드에서 더 많은 명령을 사용할 수 있습니다. 권한 EXEC 모드로 들어가려면 **enable** 명령을 입력합니다. 메시지가 표시되면 비밀번호를 입력하지 않고 enter 키를 누릅니다.

예제:

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

일반 CLI로 돌아가려면 **Ctrl-a**, **d**를 입력합니다.

Threat Defense 초기 구성 완료

Firepower 4100/9300를 제외한 모든 모델에 대해 CLI 또는 device manager를 사용하여 threat defense 초기 구성을 완료할 수 있습니다. Firepower 4100/9300의 경우, 논리적 디바이스를 구축할 때 초기 구성을 완료합니다. Firepower 4100/9300의 논리적 디바이스 섹션을 참조하십시오.

Device Manager 사용으로 Threat Defense 초기 구성 완료

threat defense의 초기 설정을 수행하려면 device manager에 연결합니다. device manager를 사용하여 초기 설정을 수행할 때 관리를 위해 management center로 전환하면 device manager에서 완료된 관리 및 액세스 설정과 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 기본 구성 설정은 유지되지 않습니다. FTD CLI를 사용하는 경우 관리 및 FMC 액세스 설정만 유지됩니다(예: 기본 내부 인터페이스 구성은 유지되지 않음).

- 이 절차는 분석용으로만 온프레미스 *management center*를 사용하려는 CDO 매니지드 디바이스에는 적용되지 않습니다. 이 device manager 구성은 기본 관리자를 구성하기 위한 것입니다. 분석을 위해 디바이스를 구성하는 방법에 대한 자세한 내용은 CLI로 Threat Defense 초기 구성 완료, 18 페이지의 내용을 참조하십시오.
- 이 절차는 Firepower 4100/9300 및 ISA 3000을 제외한 다른 모든 디바이스에 적용됩니다. device manager를 사용하여 이러한 디바이스를 management center에 온보딩할 수 있지만, 이러한 디바이스는 다른 플랫폼과 기본 구성이 다르기 때문에 이 절차의 세부 정보가 이러한 플랫폼에 적용되지 않을 수 있습니다.

프로시저

단계 **1** device manager에 로그인합니다.

a) 브라우저에 다음 URL을 입력합니다.

- 내부—**https://192.168.95.1**.
- 관리—**https://***management_ip*. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다. 이 절차의 일부로 관리 IP 주소를 고정 주소로 설정해야 할 수 있습니다. 따라서 연결이 끊어지지 않도록 내부 인터페이스를 사용하는 것이 좋습니다.

b) 사용자 이름 **admin** 및 기본 비밀번호 **Admin123**으로 로그인합니다.

c) 최종 사용자 라이선스 계약(EULA)에 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.

단계 **2** 초기 설정을 완료하기 전에 처음으로 device manager에 로그인할 때 설정 마법사를 사용합니다. 선택적으로 페이지 하단의 **Skip device setup(**디바이스 설정 건너뛰기**)**을 클릭하여 설정 마법사를 건너뛸 수 있습니다.

설정 마법사를 완료하면 내부 인터페이스에 대한 기본 구성 외에 management center 관리로 전환할 때 유지되는 외부(Ethernet1/1) 인터페이스에 대한 구성이 생성됩니다.

a) 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

1. 외부 인터페이스 주소 — 이 인터페이스는 일반적으로 인터넷 게이트웨이이며 관리자 액세스 인터페이스로 사용될 수 있습니다. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다.

관리자 액세스를 위해 외부(또는 내부)에서 다른 인터페이스를 사용하려는 경우 설정 마법사를 완료한 후 수동으로 구성해야 합니다.

IPv4 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다. 설정 마법사를 사용하여 PPPoE를 구성할 수 없습니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 마법사를 완료한 후 PPPoE를 구성할 수 있습니다.

IPv6 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

2. 관리 인터페이스

CLI에서 초기 설정을 수행한 경우 관리 인터페이스 설정이 표시되지 않습니다.

데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 설정은 계속 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

DNS 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.

방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

b) 시간 설정**(NTP)**을 구성하고 **Next(**다음**)**를 클릭합니다.

1. 표준 시간대 - 시스템의 표준 시간대를 선택합니다.
2. **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

c) **Start 90 day evaluation period without registration(**등록 없이 **90**일 평가 기간 시작**)**을 선택합니다.

threat defense을 Smart Software Manager에 등록하지 마십시오. 모든 라이선싱은 management center에서 수행됩니다.

d) 마침을 클릭합니다.

e) **Cloud Management(**클라우드 관리**)** 또는 **Standalone(**독립형**)**을 선택하라는 메시지가 표시됩니다. management center 관리의 경우 **Standalone(**독립형**)**을 선택한 다음 **Got It(**확인**)**을 선택합니다.

단계 **3** (필요할 수 있음) 관리 인터페이스를 구성합니다.

관리자 액세스에 데이터 인터페이스를 사용하려는 경우에도 관리 인터페이스 구성을 변경해야 할 수 있습니다. device manager 연결을 위해 관리 인터페이스를 사용하는 경우 device manager에 다시 연결해야 합니다.

- 관리자 액세스용 데이터 인터페이스 - 관리 인터페이스에 데이터 인터페이스로 설정된 게이트웨이가 있어야 합니다. 기본적으로 관리 인터페이스는 DHCP에서 IP 주소 및 게이트웨이를 수신합니다. DHCP에서 게이트웨이를 수신하지 못한 경우(예: 이 인터페이스를 네트워크에 연결하지 않은 경우) 게이트웨이는 기본적으로 데이터 인터페이스로 설정되며, 아무것도 구성할 필요가 없습니다. DHCP에서 게이트웨이를 수신한 경우 대신 고정 IP 주소로 이 인터페이스를 구성하고 게이트웨이를 데이터 인터페이스로 설정해야 합니다.
- 관리자 액세스용 관리 인터페이스 - 고정 IP 주소를 구성하려면 기본 게이트웨이도 데이터 인터페이스 대신 고유한 게이트웨이로 설정해야 합니다. DHCP를 사용하는 경우 DHCP에서 게이트웨이를 성공적으로 가져오면 어떤 것도 구성할 필요가 없습니다.

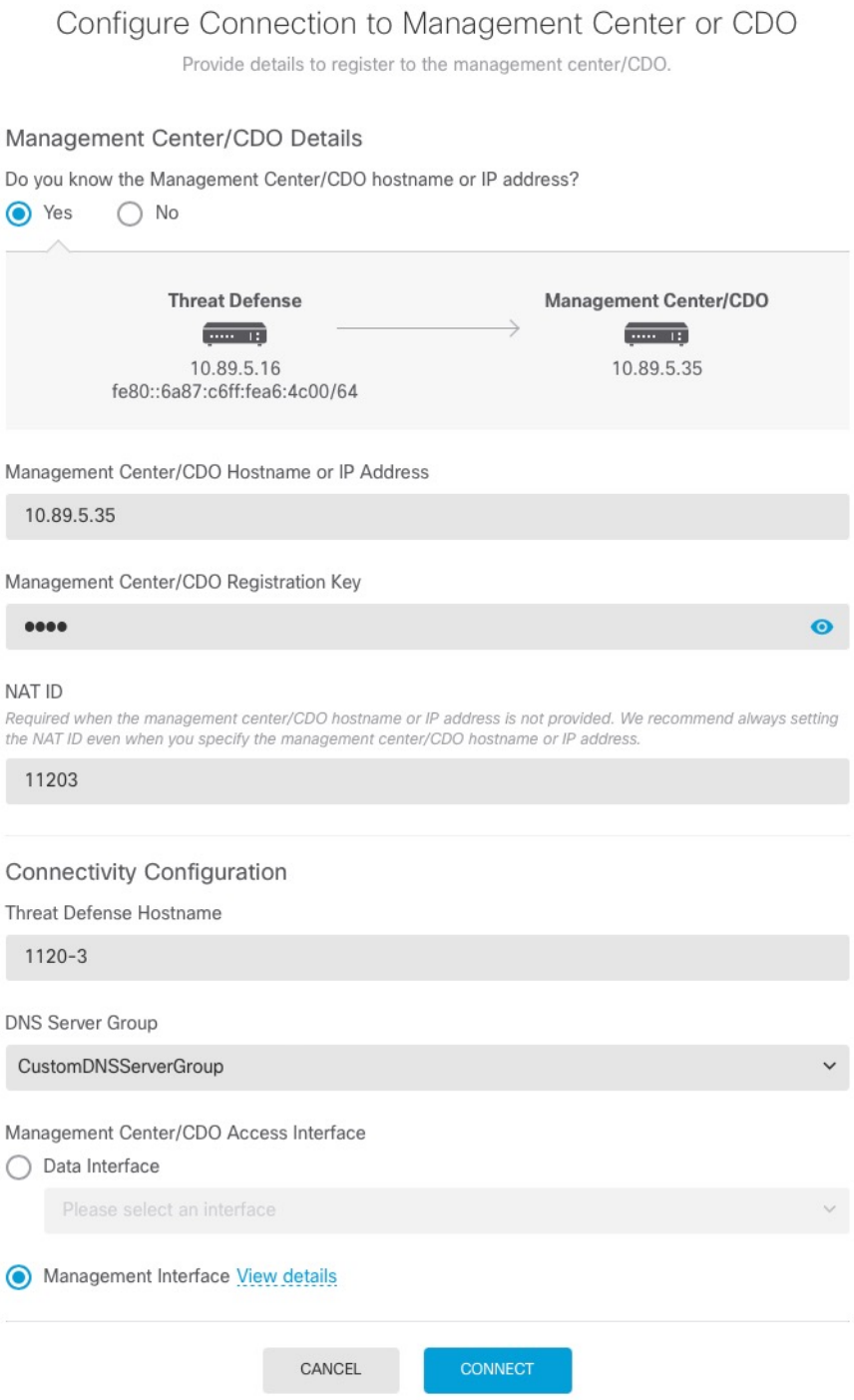
단계 **4** 관리자 액세스에 사용할 외부 또는 내부 이외의 인터페이스를 포함하여 추가 인터페이스를 구성하려면 **Device(**디바이스**)**를 선택하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

디바이스를 management center에 등록할 때 다른 device manager 설정은 유지되지 않습니다.

단계 **5** **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Central Management(**중앙 관리**)**를 선택하고 **Proceed(**계속**)**을 눌러 management center 관리를 설정합니다.

단계 **6** **Management Center/CDO Details(**관리 센터**/CDO** 세부 정보**)**를 구성합니다.

그림 *7: Management Center/CDO* 세부 정보



a) **Do you know the Management Center/CDO hostname or IP address(**관리 센터/**CDO** 호스트 이름 또는 **IP** 주소를 알고 있습니까**)**에 대해 IP 주소 또는 호스트 이름을 사용하여 management center에 도달할 수 있으면 **Yes(**예**)**를, management center에 퍼블릭 IP 주소 또는 호스트 이름이 없거나 NAT 뒤에 있는 경우 **No(**아니요**)**를 클릭합니다.

하나 이상의 디바이스(management center 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다.

b) **Yes(**예**)**를 선택한 경우 **Management Center/CDO Hostname/IP Address(**관리 센터**/CDO** 호스트 이름**/IP** 주소**)**를 입력합니다.

c) **Management Center/CDO Registration Key(**관리 센터**/CDO** 등록 키**)**를 지정합니다.

threat defense 디바이스 등록 시에 management center에서 지정할 일회용 등록 키입니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 여러 디바이스에 사용할 수 있습니다.

d) **NAT ID**를 지정합니다.

이 ID는 management center에서 지정할 고유한 일회성 문자열을 지정합니다. 이 필드는 디바이스 중 하나의 IP 주소만 지정하는 경우 입력해야 합니다. 두 디바이스의 IP 주소를 모두 알고 있는 경우에도 NAT ID를 지정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다. NAT ID는 연결이 올바른 디바이스에서 오는지 확인하기 위해 IP 주소와 함께 사용됩니다. IP 주소/NAT ID 인증 후에만 등록 키가 확인됩니다.

단계 **7** 연결성 설정을 구성합니다.

a) **FTD** 호스트 이름을 지정합니다.

Management Center/CDO Access Interface 액세스를 위해 데이터 인터페이스를 사용하는 경우 이 FQDN이 이 인터페이스에 사용됩니다.

b) **DNS** 서버 그룹을 지정합니다.

기존 그룹을 선택하거나 새로 생성합니다. 기본 DNS 그룹은 **CiscoUmbrellaDNSServerGroup**이며, 여기에는 OpenDNS 서버가 포함됩니다.

관리 센터**/CDO** 액세스 인터페이스에 대한 데이터 인터페이스를 선택하려는 경우 이 설정은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 마법사를 사용하여 설정하는 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다. 관리 및 데이터 트래픽이 모두 외부 인터페이스를 통해 DNS 서버에 연결되므로 관리에 사용한 것과 동일한 DNS 서버 그룹을 선택할 수 있습니다.

management center에서 이 threat defense 디바이스에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center에 threat defense 디바이스를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense 디바이스에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center와 threat defense 디바이스를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center에 의해 유지됩니다.

FMC 액세스 인터페이스용관리 인터페이스를 선택하려는 경우 이 설정은 관리 DNS 서버를 구성합니다.

c) **Management Center/CDO Access Interface(**관리 센터/**CDO** 액세스 인터페이스**)**의 경우 구성된 인터페이스를 선택합니다.

threat defense 디바이스를 management center에 등록한 후 관리자 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.

단계 **8** (선택 사항) 데이터 인터페이스를 선택했는데 외부 인터페이스가 아닌 경우 기본 경로를 추가합니다.

인터페이스를 통과하는 기본 경로가 있는지 확인하라는 메시지가 표시됩니다. 외부를 선택한 경우 설정 마법사의 일부로 이 경로를 이미 구성한 것입니다. 다른 인터페이스를 선택한 경우 management center에 연결하기 전에 기본 경로를 수동으로 구성해야 합니다.

관리 인터페이스를 선택한 경우 이 화면에서 계속 진행하기 전에 게이트웨이를 고유한 게이트웨이로 구성해야 합니다.

단계 **9** (선택 사항) 데이터 인터페이스를 선택한 경우 **Add a Dynamic DNS (DDNS) method(**동적 **DNS(DDNS)** 메서드 추가**)**를 클릭합니다.

DDNS는 management center 의 IP 주소가 변경될 경우 threat defense 디바이스가 FQDN(Fully-Qualified Domain Name)에서 에 연결할 수 있도록 합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)**를 참조하여 DDNS를 구성합니다.

management center에 threat defense 디바이스를 추가하기 전에 DDNS를 구성할 경우 threat defense 디바이스가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 threat defense 디바이스가 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. Threat Defense는 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.

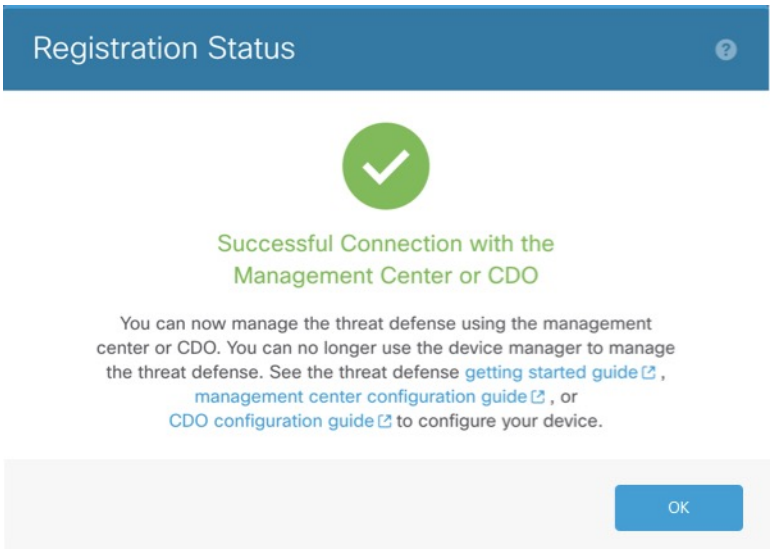
관리자 액세스용 관리 인터페이스를 사용할 때는 DDNS가 지원되지 않습니다.

단계 **10** **Connect(**연결**)**를 클릭합니다. 등록 상태**(Registration Status)** 대화 상자는 management center 전환에 대한 현재 상태를 보여줍니다. **Saving Management Center/CDO Registration Settings(**관리 센터/**CDO** 등록 설정 저장**)** 단계에서 management center로 이동하여 방화벽을 추가합니다.

management center에 대한 전환을 취소하려면 **Cancel Registration(**등록 취소**)**을 클릭합니다. 아니면 **Saving Management Center/CDO Registration Settings(**관리 센터/**CDO** 등록 설정 저장**)** 단계까지 device manager 브라우저를 닫지 마십시오. 이렇게 하면 프로세스가 일시 중지되며, device manager에 다시 연결할 때만 재개됩니다.

Save Management Center/CDO Registration Settings(관리 센터/**CDO** 등록 설정 저장**)** 단계를 수행한 후 device manager에 연결된 상태로 유지되는 경우, 마지막으로 **Successful Connection with Management Center or CDO(**관리 센터 또는 **CDO**와의 연결 성공**)** 대화 상자가 표시된 뒤 device manager으로부터 연결이 해제됩니다.

그림 *8:* 연결 성공



CLI로 Threat Defense 초기 구성 완료

threat defense CLI에 연결하여 설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 포함한 초기 설정을 수행합니다. 전용 관리 인터페이스는 자체 네트워크 설정이 있는 특수 인터페이스입니다. 관리자 액세스에 관리 인터페이스를 사용하지 않으려는 경우, 대신 CLI를 사용하여 데이터 인터페이스를 구성할 수 있습니다. management center 통신 설정도 구성합니다. device manager를 사용하여 초기 설정을 수행할 때 관리를 위해 management center로 전환하면 device manager에서 완료된 관리 인터페이스 및 액세스 인터페이스 설정과 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책과 같은 기타 기본 구성 설정은 유지되지 않습니다.

Before you begin

이 절차는 Firepower 4100/9300을(를) 제외한 모든 모델에 적용됩니다. 논리적 디바이스를 구축하고 Firepower 4100/9300에서 초기 구성을 완료하려면 Firepower 4100/9300의 논리적 디바이스의 내용을 참조하십시오.

Procedure

단계 **1** 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 threat defense CLI에 연결합니다.이 인터페이스는 기본적으로 DHCP 서버에서 IP 주소를 가져옵니다. 네트워크 설정을 변경하려는 경우 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

(Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트는 FXOS CLI에 연결됩니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

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

(Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

Note 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야합니다. Firepower 및 Secure Firewall 하드웨어 모델의 경우: 이미지 재설치 절차에 대한 FXOS 문제 해결 가이드를 참고하십시오. ISA 3000의 경우: 지침은 이미지 재설치 가이드를 참조하십시오.

Example:

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

[...]

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

[...]

firepower#
```

단계 **3** (Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS에 연결한 경우 threat defense CLI에 연결합니다.

connect ftd

Example:

```
firepower# connect ftd
>
```

단계 **4** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

Note 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. threat defense 명령 참조를 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

Note 데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 설정은 계속 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

다음 지침을 참조하십시오.

- **Do you want to configure IPv4?(IPv4**를 구성하시겠습니까**?)** 및/또는 **Do you want to configure IPv6?(IPv6**를 구성하시겠습니까**?)** - 이러한 주소 유형 중 하나 이상에 **y**를 입력합니다.
- **Enter the IPv4 default gateway for the management interface(**관리 인터페이스에 대한 **IPv4** 기본 게이트웨이 입력**)** 및/또는 **Enter the IPv6 gateway for the management interface(**관리 인터페이스에 대한 **IPv6** 게이트웨이 입력**)** - 관리 인터페이스 대신 관리자 액세스에 데이터 인터페이스를 사용하려면 **manual(**수동**)**을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스**(**데이터 인터페이스**)**여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.
- **Enter the IPv4 default gateway for the management interface(**관리 인터페이스에 대한 **IPv4** 기본 게이트웨이 입력**)**및/또는 **Configure IPv6 via DHCP, router, or manually?(DHCP,** 라우터를 통해 또는 수동으로 **IPv6**를 구성하시겠습니까**?)** - 관리 인터페이스 대신 관리자 액세스에 데이터 인터페이스를 사용하려면 게이트웨이를 **data-interfaces(**데이터 인터페이스**)**로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 관리자 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다. 관리자 액세스에 관리 인터페이스를 사용하려면 관리 1/1 네트워크에서 게이트웨이 IP 주소를 설정해야합니다.
- **If your networking information has changed, you will need to reconnect(**네트워킹 정보가 변경된 경우 다시 연결해야 합니다**)** — SSH를 통해 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(**디바이스를 로컬로 관리하시겠습니까**?)**—management center을(를) 사용하려면 **no**를 입력합니다. 예를 입력하면 Firepower Device Manager를 대신 사용하게 됩니다.
- **Configure firewall mode?(**방화벽 모드를 설정하시겠습니까**?)**—초기 설정에서 방화벽 모드를 설정하는 것이 좋습니다. 초기 설정 후에 방화벽 모드를 변경하면 실행 중인 구성이 지워집니다. 데이터 인터페이스 관리자 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:


System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.89.5.1
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
```

```
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

단계 **5** 이 threat defense를 관리할 management center을(를) 식별합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*] [*display_name*]

Note 관리를 위해 CDO를 사용하는 경우 이 단계에서 CDO 생성 **configure manager add** 명령을 사용합니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—management center의 FQDN 또는 IP 주소를 지정합니다. management center의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용하고 *nat_id*도 지정합니다. 하나 이상의 디바이스(management center 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 **DONTRESOLVE**를 지정하는 경우 FTD에 연결할 수 있는 IP 주소 또는 호스트 이름이 있어야 합니다.

- *reg_key* — threat defense 등록시 management center에 지정할 일회용 등록 키를 지정합니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.
- *nat_id* — 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 threat defense를 등록할 때 management center에 지정할 고유한 일회용 문자열을 지정합니다. 예를 들어, management center를 **DONTRESOLVE**로 설정하는 경우 반드시 필요합니다. IP 주소를 지정하는 경우에도 관리를 위해 데이터 인터페이스를 사용한다면 이 주소가 필요합니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다.

  Note 관리에 데이터 인터페이스를 사용하는 경우 두 IP 주소를 모두 지정하더라도 threat defense와 management center에서 모두 NAT ID를 지정해야 합니다.

- *display_name* — **show managers** 명령과 함께 이 관리자를 표시하기 위한 표시 이름을 제공합니다. 이 옵션은 CDO를 기본 관리자 및 분석 전용 management center 온프레미스로 식별하는 경우 유용합니다. 이 인수를 지정하지 않으면 방화벽은 다음 방법 중 하나를 사용하여 표시 이름을 자동으로 생성합니다.
  - *hostname* | *IP_address*(**DONTRESOLVE** 키워드를 사용하지 않는 경우)
  - **manager-***timestamp*

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

management center이(가) NAT 디바이스 뒤에 있는 경우 등록 키와 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정합니다. 예를 들면 다음과 같습니다.

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

threat defense가 NAT 디바이스 뒤에 있는 경우 management center IP 주소 또는 호스트 이름과 함께 고유한 NAT ID를 입력합니다. 예를 들면 다음과 같습니다.

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

단계 **6** CDO를 기본 관리자로 사용하고 분석용으로만 온프레미스 management center를 사용하려는 경우 온프레미스 management center를 식별합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

Example:

다음 예에서는 "CDO"라는 표시 이름이 추가된 CDO에 대해 생성된 명령을 사용한 다음, 분석 전용 온프레미스 management center를 지정합니다.

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

단계 **7** (Optional) 관리자 액세스용 데이터 인터페이스의 이름을 구성합니다

configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

Note 이 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 관리 인터페이스에 SSH를 사용하는 경우 연결이 끊기고 콘솔 포트에 다시 연결해야 할 수 있습니다. SSH 사용량에 대한 자세한 내용은 아래를 참조하십시오.

이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오. 관리를 위한 Threat Defense 데이터 인터페이스 사용, on page 4도 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 원래 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- management center에 threat defense를 추가하면 management center는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. management center에서 나중에 관리자 액세스 인터페이스 구성을 변경할 수 있지만, threat defense 또는 management center가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 threat defense에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 threat defense가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 threat defense가 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. threat defense는 DynDNS 원격 API 사양 (https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.

  management center에서 이 threat defense에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center에 threat defense를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center와 threat defense를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

  또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 FTD

구성과 일치하도록 DNS 서버를 포함하여 management center에서 이러한 모든 설정을 수동으로 구성해야 합니다.

- threat defense를 management center에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **8** (Optional) 특정 네트워크에서 관리자에 대한 데이터 인터페이스 액세스를 제한합니다.

configure network management-data-interface client *ip_address netmask*

기본적으로 모든 네트워크가 허용됩니다.

What to do next

장치를 management center에 등록합니다.

이벤트 인터페이스 구성

항상 관리 트래픽용 데이터 관리 인터페이스가 필요합니다. 디바이스에 두 번째 관리 인터페이스가 있는 경우(예: Firepower 4100/9300) 이벤트 전용 트래픽에 대해 이를 활성화할 수 있습니다.

시작하기 전에

별도의 이벤트 인터페이스를 사용하려면 management center에서 이벤트 인터페이스를 활성화해야 합니다. Cisco Secure Firewall Management Center 관리 가이드를 참조하십시오.

프로시저

단계 **1** 두 번째 관리 인터페이스를 이벤트 전용 인터페이스로 활성화합니다.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

configure network management-interface disable-events-channel 명령을 사용하여 주 관리 인터페이스의 이벤트를 선택적으로 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.

예제**:**

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

단계 **2** 이벤트 인터페이스에서 IP 주소를 구성합니다.

이벤트 인터페이스는 관리 인터페이스와 별도의 네트워크에 있거나 동일한 네트워크에 있을 수 있습니다.

a) IPv4 주소 구성:

configure network ipv4 manual *ip_address netmask gateway_ip* **management1**

이 명령의 *gateway_ip*는 디바이스의 기본 경로를 만드는 데 사용되므로 management0 인터페이스에 이미 설정한 값을 입력해야 합니다. 이벤트 인터페이스에 대한 별도의 고정 경로는 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

예:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

b) IPv6 주소 구성:

- 상태 비저장 자동 구성:

  configure network ipv6 router management1

  예:

  ```
  > configure network ipv6 router management1
  Setting IPv6 network configuration.
  Network settings changed.

  >
  ```

- 수동 구성:

  configure network ipv6 manual *ip6_address ip6_prefix_length* **management1**

  예:

  ```
  > configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
  Setting IPv6 network configuration.
  Network settings changed.

  >
  ```

단계 **3** management center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다.

configure network static-routes {**ipv4** | **ipv6**} **add management1** *destination_ip netmask_or_prefix gateway_ip*

기본 경로의 경우 이 명령을 사용하지 마십시오. **configure network ipv4** 또는 **ipv6** 명령을 사용할 때만 기본 경로 게이트웨이 IP 주소를 변경할 수 있습니다(4단계 참조).단계 2, 25 페이지

예제:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
```

```
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

정적 경로를 표시하려면 **show network-static-routes**를 입력합니다(기본 경로는 표시되지 않음).

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

Management Center에 디바이스 추가

단일 디바이스를 management center에 추가하려면 이 절차를 사용합니다. 고가용성을 위해 디바이스를 연결하려는 경우에도 이 절차를 사용해야 합니다. 고가용성 쌍 추가의 내용을 참조하십시오. 클러스터링에 대해서는 해당 모델의 클러스터링 장을 참조하십시오.

또한 이 절차를 사용하여 CDO에서 제공하는 클라우드 제공 management center에서 관리하는 디바이스를 추가할 수 있으며, 이벤트 로깅 및 분석 목적으로만 온프레미스 management center를 사용하려는 경우에도 이 절차를 사용할 수 있습니다.

참고 management center 고가용성을 설정했거나 설정하려는 경우 액티브(또는 액티브 예정) management center에 한정된 디바이스만 추가합니다. 고가용성 쌍을 설정하면, 액티브 management center에 등록된 디바이스는 자동으로 스탠바이에 등록됩니다.

시작하기 전에

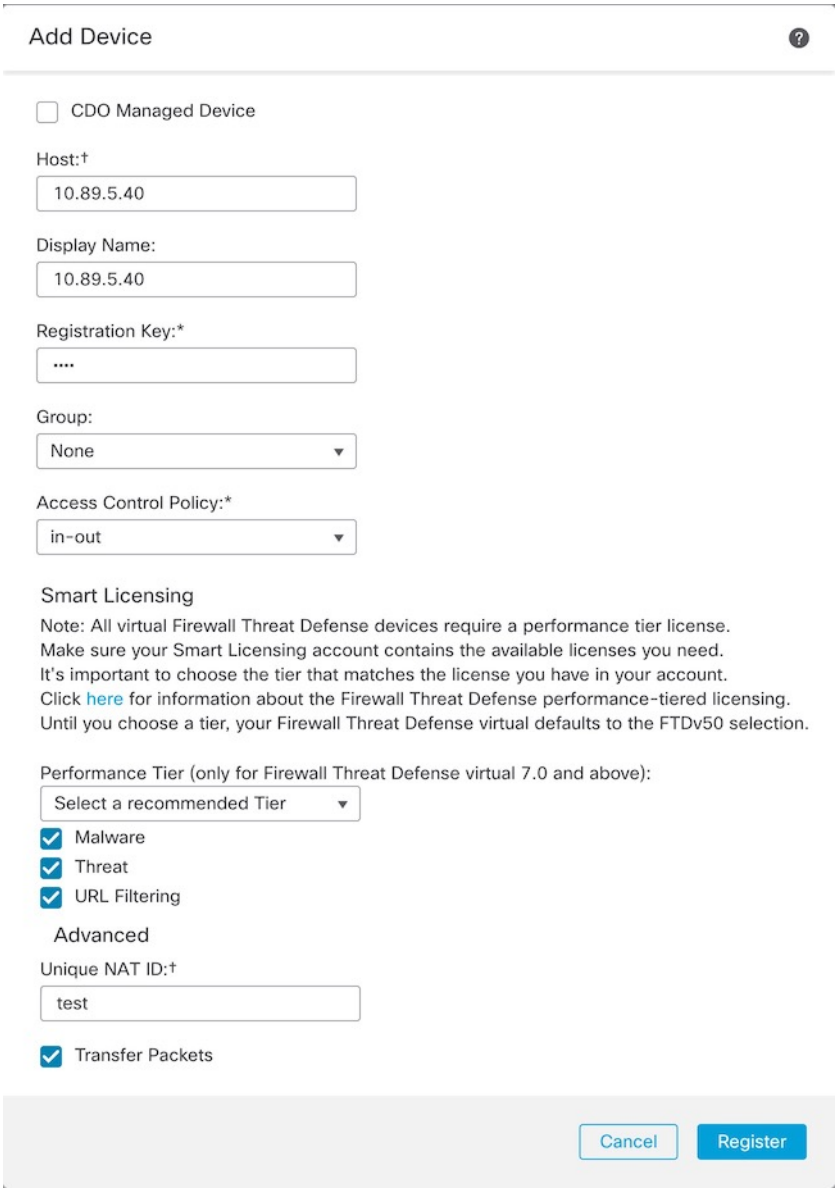
- management center에서 관리할 수 있도록 디바이스를 설정합니다. 참조:
  - Threat Defense 초기 구성 완료, 12 페이지
  - 사용자 모델의 시작 가이드
- management center를 Smart Software Manager에 등록해야 합니다. 유효한 평가 라이선스는 충분하지만, 만료되면 등록에 성공할 때까지 새 디바이스를 추가할 수 없습니다.
- IPv4를 사용하는 디바이스를 등록했으며 IPv6으로 전환하려는 경우, 해당 디바이스를 삭제하고 다시 등록해야 합니다.

프로시저

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

단계 2 **Add(**추가**)** 드롭다운 메뉴에서 **Device(**디바이스**)**를 선택합니다.

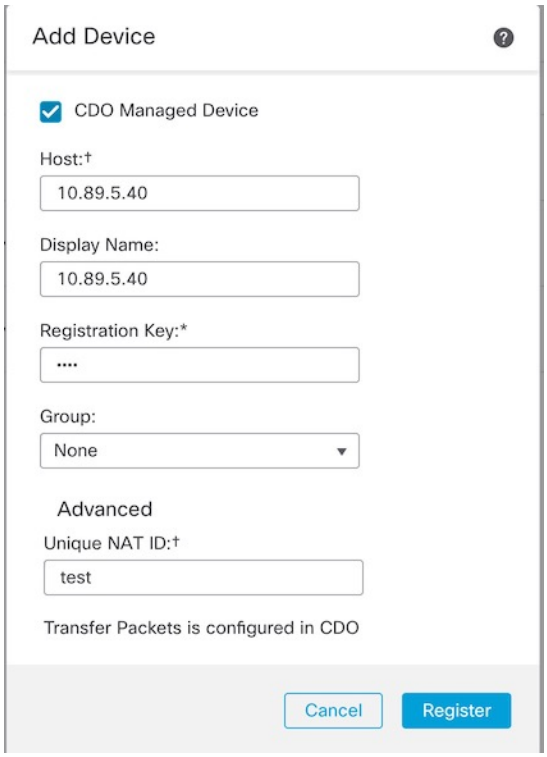
그림 *9:* 디바이스 추가



단계 3 분석 전용으로 온프레미스 management center에 CDO 매니지드 디바이스를 추가하려면 **CDO** 매니지드 디바이스를 클릭합니다.

라이선싱 및 패킷 전송 설정은 CDO에서 관리하므로 숨깁니다. 이 단계를 건너뛸 수 있습니다.

그림 ***10: CDO***용 디바이스 추가



단계 **4** 추가할 디바이스의 IP 주소 또는 호스트 이름을 호스트 필드에 입력합니다.

디바이스의 호스트 이름은 FQDN(Fully Qualified Domain Name) 또는 유효한 IP 주소에 로컬 DNS를 통해 확인하는 이름입니다. 사용자 네트워크가 IP 주소를 할당하기 위해 DHCP를 사용하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

NAT 환경에서는, management center로 관리되는 디바이스를 구성할 때 management center의 IP 주소 또는 호스트 이름을 이미 지정한 경우 디바이스의 IP 주소 또는 호스트 이름을 지정하지 않아도 될 수 있습니다. 자세한 내용은 NAT 환경, 7 페이지의 내용을 참고하십시오.

참고 management center 고가용성 환경에서 두 management center가 모두 NAT 뒤에 있는 경우 보조 management center에 threat defense를 등록하려면 **Host(**호스트**)** 필드에 값을 지정해야 합니다.

단계 **5** management center에 표시할 디바이스의 이름을 표시 이름 필드에 입력합니다.

단계 **6** management center로 관리할 디바이스를 구성할 때 사용한 것과 동일한 등록 키를 등록 키 필드에 입력합니다. 등록 키는 일회용 공유 암호입니다. 키는 영숫자 및 하이픈(-)을 포함할 수 있습니다.

단계 **7** 다중 도메인 구축에서는 현재 도메인과 상관없이 디바이스를 리프 도메인으로 할당합니다.

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

단계 **8** (선택 사항) 디바이스 그룹에 디바이스를 추가합니다.

단계 **9** 등록 시 디바이스를 구축하기 위해 초기 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.

디바이스가 선택한 정책과 호환되지 않는 경우 구축이 실패합니다. 이러한 문제는 라이선싱 불일치, 모델 제약 조건, 수동 대 인라인 문제, 기타 잘못된 구성을 비롯한 여러 가지 이유로 인해 발생할 수 있습니다. 오류 원인을 해결한 뒤 디바이스에 수동으로 설정을 구축합니다.

단계 **10** 디바이스에 적용할 라이선스를 선택합니다.

또한 디바이스를 추가한 후 **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지에서 라이선스를 적용할 수 있습니다.

threat defense virtual의 경우에만 **Performance Tier(**성능 계층**)**도 선택해야 합니다. 어카운트에 있는 라이선스와 일치하는 계층을 선택하는 것이 중요합니다. 계층을 선택할 때까지 디바이스에 FTDv50 선택이 기본값으로 설정됩니다. threat defense virtual에서 사용 가능한 성능 계층 라이선스 자격에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 *FTDv* 라이선스를 참조하십시오.

참고 threat defense virtual를 7.0 이상 버전으로 업그레이드하는 경우 **FTDv - Variable(FTDv - 변수)**를 선택하여 현재 라이선스 컴플라이언스를 유지할 수 있습니다.

단계 **11** 디바이스 설정 중 NAT ID를 사용하는 경우 **Advanced(**고급**)** 섹션에서 **Unique NAT ID(**고유 **NAT ID)** 필드에 동일한 NAT ID를 입력합니다.

고유 **NAT ID**는 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 초기 설정 중에 threat defense에도 지정할 고유한 일회용 문자열을 지정합니다. 예를 들어 **Host(**호스트**)** 필드를 비워둔 경우 이는 필수입니다. IP 주소를 지정하는 경우에도 관리를 위해 threat defense 데이터 인터페이스를 사용하는 경우에도 이 주소가 필요합니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다.

참고 threat defense에서 관리에 데이터 인터페이스를 사용하는 경우 두 IP 주소를 모두 지정하더라도 threat defense와 management center에서 모두 NAT ID를 지정해야 합니다.

단계 **12** 패킷 전송 체크 박스를 선택하여 디바이스가 management center에 패킷을 전송하도록 합니다.

이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 management center에 전송합니다. 이벤트를 비활성화하면 이벤트 정보는 management center에 전송되지만 패킷 데이터는 전송되지 않습니다.

단계 **13** **Register(**등록**)**를 클릭합니다.

management center이 디바이스의 하트비트를 확인하고 통신을 설정하는 데 최대 2분이 소요될 수 있습니다. 등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. 디바이스가 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 디바이스 CLI에 액세스하고 management center IP 주소에 Ping을 보냅니다.

  ping system *ip_address*

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. 디바이스 IP 주소를 변경해야 하는 경우 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용합니다.

- 등록 키, NAT ID 및 management center IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 디바이스에서 등록 키 및 NAT ID를 설정할 수 있습니다.

자세한 문제 해결 정보는 https://cisco.com/go/fmc-reg-error를 참조하십시오.

Management Center에서 디바이스 삭제(등록 해제)

디바이스를 더 이상 관리하지 않으려면 management center에서 등록 취소할 수 있습니다.

클러스터, 클러스터 노드 또는 고가용성 쌍의 등록을 해제하려면 해당 구축에 대한 장을 참고하십시오.

디바이스 등록 취소:

- 모든 서버는 management center과 디바이스 간 통신합니다.
- **Device Management(**디바이스 관리**)** 페이지에서 디바이스를 제거합니다.
- 디바이스가 NTP를 사용하여 management center에서 시간을 수신하도록 디바이스의 플랫폼 설정 정책이 구성된 경우 해당 디바이스를 로컬 시간 관리로 되돌립니다.
- 구성을 그대로 유지하므로 디바이스가 트래픽을 계속 처리합니다.

  NAT 및 VPN, ACL 및 인터페이스 구성과 같은 정책은 그대로 유지됩니다.

디바이스를 동일하거나 다른 management center에 다시 등록하면 구성이 제거되므로, 해당 시점에서 디바이스의 트래픽 처리가 중지됩니다. 등록 시 액세스 제어 정책을 선택할 수 있지만, 등록 후에 다른 정책을 다시 적용하고 구성을 구축해야만 트래픽을 다시 처리할 수 있습니다.

프로시저

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

단계 **2** 등록을 해제하려는 디바이스 옆의 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **3** 디바이스 등록을 해제할지 확인합니다.

디바이스 그룹 추가

management center에서는 디바이스를 그룹화하여 편리하게 정책을 구축하고 여러 디바이스에 업데이트를 설치할 수 있습니다. 그룹에 있는 디바이스의 목록을 확장 및 축소할 수 있습니다.

다중 도메인 구축의 경우 리프 도메인 내에서만 디바이스 그룹을 생성할 수 있습니다. 멀티테넌시에 Secure Firewall Management Center을 구성하는 경우 기존 디바이스 그룹이 제거되지만 리프 도메인 레벨에서 다시 추가할 수 있습니다.

고가용성 쌍의 기본 디바이스를 그룹에 추가하면 두 디바이스 모두 그룹에 추가됩니다. 고가용성 쌍을 중단하는 경우에도 두 디바이스는 해당 그룹에 남아 있습니다.

프로시저

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

단계 **2** 드롭다운 메뉴의 **Add(**추가**)**에서 **Add Group(**그룹 추가**)**를 선택합니다.

기존 그룹을 수정하려면 수정하려는 그룹에 대한 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** **Available Devices(**사용 가능한 장치**)**에서 디바이스 그룹에 추가할 하나 이상의 디바이스를 선택합니다. 여러 디바이스를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다.

단계 **5** 디바이스 그룹에서 선택한 디바이스를 포함하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** 선택적으로 디바이스 그룹에서 디바이스를 제거하려면 제거하려는 디바이스 옆의 제거(**Delete(**삭제**)** ( ))를 클릭합니다.

단계 **7** 디바이스 그룹에 추가하려면 **OK(**확인**)**를 클릭합니다.

디바이스 종료 또는 재시작

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 방화벽이 정상적으로 종료되지 않는다는 점에 유의하십시오.

시스템을 올바르게 종료하거나 재시작하려면 다음 작업을 참고하십시오.

참고 디바이스를 재시작한 후 관리 연결을 재설정할 수 없다는 오류가 표시될 수 있습니다. 경우에 따라 디바이스의 관리 인터페이스가 준비되기 전에 연결이 시도됩니다. 연결은 자동으로 재시도되며 15분 이내에 시작됩니다.

프로시저

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

단계 **2** 다시 시작할 디바이스 옆의 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 디바이스를 다시 시작하려면:

a) **Restart Device(**디바이스 재시작**)**( ) 버튼을 클릭합니다.
b) 메시지가 표시되면 디바이스 다시 시작을 확인합니다.

단계 **5** 디바이스를 종료하려면:

a) **System(**시스템**)** 섹션에서 **Shut Down Device(**디바이스 종료**)**( )을 클릭합니다.
b) 메시지가 표시되면 디바이스 종료를 확인합니다.
c) 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

콘솔에 연결되지 않은 경우 시스템이 종료될 때까지 약 3분 동안 기다리십시오.

ISA 3000의 경우 종료가 완료되면 시스템 LED가 꺼집니다. 전원을 제거하기 전에 10초 이상 기다립니다.

디바이스 설정 구성

Device(디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서는 다양한 정보와 옵션을 제공합니다.

- View By(보기 기준) - 그룹, 라이선스, 모델, 버전 또는 액세스 제어 정책을 기준으로 디바이스를 보려면 이 옵션을 사용합니다.
- Device State(디바이스 상태) - 상태에 따라 디바이스를 볼 수도 있습니다. 상태 아이콘을 클릭하면 해당 아이콘에 속한 디바이스를 볼 수 있습니다. 상태에 속하는 디바이스의 수는 대괄호 안에 제공됩니다.
- Search(검색) - 디바이스 이름, 호스트 이름 또는 IP 주소를 제공하여 구성된 디바이스를 검색할 수 있습니다.
- 옵션 추가 - 디바이스, 고가용성 쌍, 클러스터 및 그룹을 추가할 수 있습니다.

- 편집 및 기타 작업 - 구성된 각 디바이스에 대해 **Edit(**수정**)** ( ) 아이콘을 사용하여 디바이스 매개변수 및 속성을 편집합니다. 추가 ( ) 아이콘을 클릭하고 다른 작업을 실행합니다.
  - Access Control Policy(액세스 제어 정책) - Access Control Policy(액세스 제어 정책) 열의 링크를 클릭하여 디바이스에 구축된 정책을 확인합니다.
  - Delete(삭제) - 디바이스를 삭제합니다.
  - Packet Tracer(패킷 트레이서) - 시스템에 모델 패킷을 삽입하여 디바이스의 정책 구성을 검토할 수 있는 패킷 트레이서 페이지로 이동합니다.
  - Packet Capture(패킷 캡처) - 패킷을 처리하는 동안 시스템이 수행하는 판정 및 작업을 볼 수 있는 패킷 캡처 페이지로 이동합니다.
  - Revert Upgrade(업그레이드 되돌리기) - 마지막 업그레이드 이후의 업그레이드 및 구성 변경 사항을 되돌립니다. 이 작업을 수행하면 디바이스가 업그레이드 이전 버전으로 복원됩니다.
  - Health Monitor(상태 모니터) - 디바이스의 상태 모니터링 페이지로 이동합니다.
  - Troubleshooting Files(문제 해결 파일) - 보고서에 포함할 데이터 유형을 선택할 수 있는 문제 해결 파일을 생성합니다.
  - Firepower 4100/9300 시리즈 디바이스의 경우, 섀시 관리자 웹 인터페이스로 연결되는 링크.

디바이스를 클릭하면 여러 탭이 있는 디바이스 속성 페이지가 나타납니다. 탭을 사용하여 디바이스 정보를 보고 라우팅, 인터페이스, 인라인 집합 및 DHCP를 구성할 수 있습니다.

일반 설정 편집

Device(디바이스**)** 페이지의 **General(**일반**)** 섹션은 아래 표의 설정을 표시합니다.

표 *2:* 일반 섹션 표 필드

필드	설명
이름	management center에 표시되는 디바이스의 이름입니다.
패킷 전송	관리되는 디바이스가 management center에 이벤트 및 패킷 데이터를 전송할지 여부를 표시합니다.
모드	디바이스에 대한 관리 인터페이스 모드로 라우팅 또는 투명을 선택할 수 있습니다.
컴플라이언스 모드	디바이스에 대한 보안 인증서 컴플라이언스를 표시합니다. 유효한 값은 CC, UCAPL, None(없음)입니다.
성능 프로파일	그러면 플랫폼 설정 정책에 구성된 대로 디바이스에 대한 코어 할당 성능 프로파일이 표시됩니다.
TLS 암호화 가속:	TLS 암호화 가속의 활성화 여부를 표시합니다.

필드	설명
디바이스 컨피그레이션	구성을 복사, 내보내기 또는 가져올 수 있습니다. 다른 디바이스에 구성 복사, 35 페이지 및 디바이스 구성 내보내기 및 가져오기, 37 페이지를 참조하십시오.

이 섹션에서 이러한 설정 중 일부를 편집할 수 있습니다.

프로시저

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

단계 **2** 수정할 디바이스 옆의 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 일반 섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

a) 매니지드 디바이스의 이름을 입력합니다.

b) 패킷 데이터를 management center에 이벤트와 함께 저장하려면 **Transfer Packets(**패킷 전송**)**을 선택합니다.

c) 디바이스에 현재 정책 및 디바이스 설정의 구축을 강제로 구축하려면 **Force Deploy(**강제 구축**)**을 클릭합니다.

참고 강제 구축은 threat defense에 구축할 정책 규칙의 완전한 생성을 포함하므로 일반 구축보다 더 많은 시간을 소비합니다.

단계 **5** 디바이스 구성 작업은 다른 디바이스에 구성 복사, 35 페이지 및 디바이스 구성 내보내기 및 가져오기, 37 페이지의 내용을 참조하십시오.

단계 **6** **Deploy(**구축**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

다른 디바이스에 구성 복사

새로운 디바이스가 네트워크에 구축되면 새 디바이스를 수동으로 다시 구성하는 대신 사전 구성된 디바이스에서 설정 및 정책을 쉽게 복사할 수 있습니다.

시작하기 전에

다음을 확인합니다.

- 소스 및 대상 threat defense 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어가 실행 중입니다.
- 소스는 독립형 Secure Firewall Threat Defense 디바이스 또는 Secure Firewall Threat Defense 고가용성 쌍입니다.
- 대상 디바이스는 독립형 threat defense 디바이스입니다.
- 소스 및 대상 threat defense 디바이스에는 동일한 수의 물리적 인터페이스가 있습니다.
- 소스 및 대상 threat defense 디바이스는 동일한 방화벽 모드(라우팅됨 또는 투명)를 사용합니다.
- 소스 및 대상 threat defense 디바이스는 동일한 보안 인증 규정 준수 모드 상태에 있습니다.
- 소스 및 대상 threat defense 디바이스가 동일한 도메인에 있습니다.
- 소스 및 대상 threat defense 디바이스에서 구성 구축이 진행되고 있지 않습니다.

프로시저

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

단계 **2** 수정할 디바이스 옆의 **Edit(**수정**)** ( )를 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 일반 섹션에서 다음 중 하나를 수행합니다.

- **Get Device Configuration(**디바이스 컨피그레이션 가져오기**)**( )를 클릭하여 다른 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 가져오기 페이지의 디바이스 선택 드롭다운 목록에서 소스 디바이스를 선택합니다.
- **Push Device Configuration(**디바이스 컨피그레이션 푸시**)**( )를 클릭하여 현재 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 푸시 페이지의 대상 디바이스 드롭다운 목록에서 설정을 복사할 대상을 선택합니다.

단계 **5** (선택 사항) 정책을 복사하려면 **Include shared policies configuration(**공유 정책 구성 포함**)** 확인란을 선택합니다.

AC 정책, NAT, 플랫폼 설정 및 FlexConfig 정책 같은 공유 정책은 여러 디바이스에 공유할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

메시지 센터의 작업에서 디바이스 설정 작업 복사 상태를 모니터링할 수 있습니다.

디바이스 설정 복사 작업이 시작되면 대상 디바이스의 설정을 삭제하고 소스 디바이스의 설정을 대상 장치에 복사합니다.

경고! 디바이스 설정 복사 작업을 완료하면 대상 디바이스를 원래 설정으로 되돌릴 수 없습니다.

디바이스 구성 내보내기 및 가져오기

디바이스별 구성을 내보낼 수 있습니다.

- 인터페이스
- 인라인 세트
- 라우팅
- DHCP
- 연결된 개체

그런 후에 다음 사용 사례에서 동일한 디바이스에 대해 저장된 구성을 가져올 수 있습니다.

- 디바이스를 다른 management center로 이동 - 먼저 원본 management center에서 디바이스를 삭제한 다음 새 management center에 추가합니다. 그런 다음 저장된 구성을 가져올 수 있습니다.
- 도메인 간 디바이스 이동 - 도메인 간에 디바이스를 이동하는 경우 지원 개체(예: 보안 영역에 대한 인터페이스 그룹)가 새 도메인에 존재하지 않으므로 일부 디바이스별 구성이 유지되지 않습니다. 도메인 이동 후 구성을 가져오면 해당 도메인에 필요한 모든 개체가 생성되고 디바이스 구성이 복원됩니다.
- 이전 구성 복원 - 디바이스 작동에 부정적인 영향을 미치는 변경 사항을 구축한 경우, 작동 중인 알려진 구성의 백업 복사본을 가져와 이전 작동 상태로 복원할 수 있습니다.
- 디바이스 다시 등록 - management center에서 디바이스를 삭제한 다음 다시 추가하려는 경우 저장된 구성을 가져올 수 있습니다.

다음 지침을 참조하십시오.

- 동일한 디바이스로만 구성을 가져올 수 있습니다(UUID가 일치해야 함). 동일한 모델이더라도 다른 디바이스로 구성을 가져올 수 없습니다.
- 내보내기와 가져오기 작업 도중 디바이스에서 실행 중인 버전을 변경하지 마십시오. 버전이 일치해야 합니다.
- 디바이스를 다른 management center로 이동할 경우 대상 management center 버전이 소스 버전과 동일해야 합니다.
- 개체가 없는 경우 생성됩니다. 개체가 존재하지만 값이 다른 경우 아래를 참조하십시오.

표 ***3:*** 개체 가져오기 작업

시나리오	가져오기 작업
동일한 이름과 값의 개체가 이미 존재합니다.	기존 개체 재사용

시나리오	가져오기 작업
이름은 같지만 값이 다른 개체가 있습니다.	• 네트워크 및 포트 개체 - 이 디바이스에 대한 개체 오버라이드를 생성합니다. 개체 재정의의 내용을 참조하십시오. • 인터페이스 개체 - 새 개체를 생성합니다. 예를 들어 유형(보안 영역 또는 인터페이스 그룹)과 인터페이스 유형(예: 라우팅 또는 스위치드)이 모두 일치하지 않으면 새 개체가 생성됩니다. • 기타 모든 개체 - 값이 달라도 기존 개체를 재사용합니다.
개체가 존재하지 않습니다.	새 개체 생성

프로시저

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

단계 **2** 편집하려는 디바이스 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

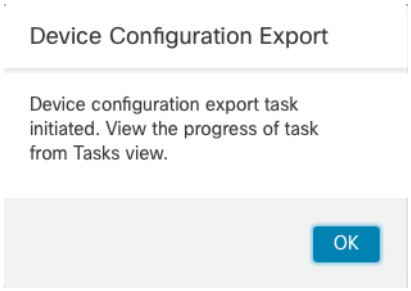
단계 **4** 구성을 내보냅니다.

a) **General(**일반**)** 영역에서 **Export(**내보내기**)**를 클릭합니다.

그림 ***11:*** 디바이스 구성 내보내기

내보내기를 승인하라는 프롬프트가 표시됩니다. **OK(**확인**)**를 클릭합니다.

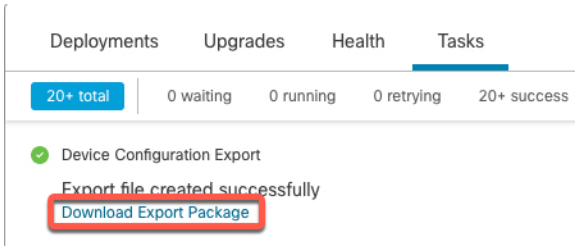
그림 *12:* 내보내기 승인



Tasks(작업**)** 페이지에서 내보내기 진행 상황을 볼 수 있습니다.

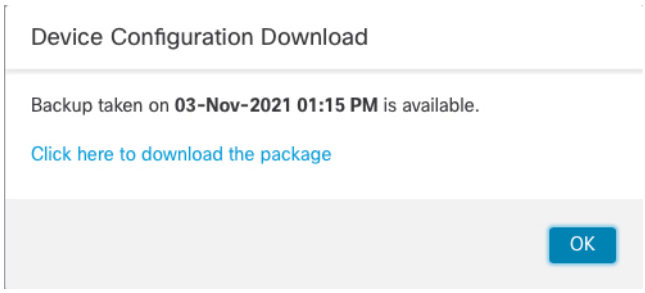
b) **Notifications(**알림**)** > **Tasks(**작업**)** 페이지에서 내보내기가 완료되었는지 확인합니다. **Download Export Package(**패키지 내보내기**)**를 클릭합니다. 또는 **General(**일반**)** 영역에서 **Download(**다운로드**)** 버튼을 클릭할 수 있습니다.

그림 *13:* 내보내기 작업



패키지를 다운로드하라는 프롬프트가 표시됩니다. **Click here to download package(**패키지를 다운로드하려면 여기를 클릭**)**를 클릭하고 파일을 로컬에 저장한 다음 **OK(**확인**)**를 클릭하여 대화 상자를 종료합니다.

그림 *14:* 패키지 다운로드



단계 **5** 구성 가져오기.

a) **General(**일반**)** 영역에서 **Import(**가져오기**)**를 클릭합니다.

그림 *15:* 디바이스 구성 가져오기

현재 구성이 교체될 것임을 확인하는 프롬프트가 표시됩니다. **Yes(**예**)**를 클릭한 다음 접미사가 .sfo인 구성 패키지로 이동합니다. 이 파일은 Backup/Restore 파일과 다릅니다.

그림 *16:* 패키지 가져오기

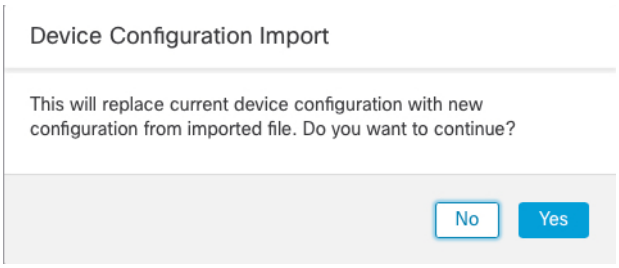
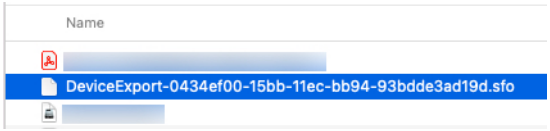
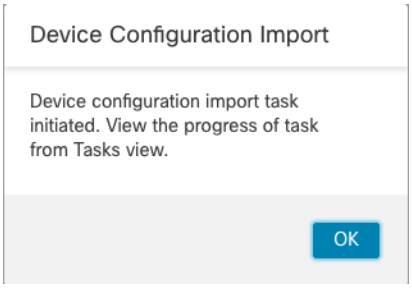


그림 *17:* 패키지로 이동



가져오기를 승인하라는 프롬프트가 표시됩니다. **OK(**확인**)**를 클릭합니다.

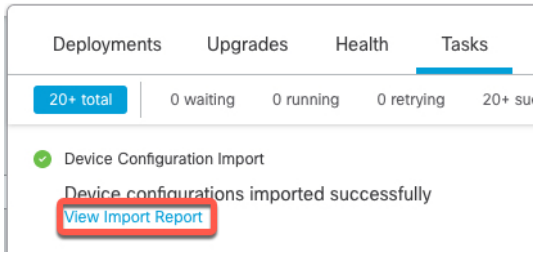
그림 *18:* 가져오기 승인



Tasks(작업**)** 페이지에서 가져오기 진행 상황을 볼 수 있습니다.

b) 가져온 항목을 확인할 수 있도록 가져오기 보고서를 봅니다. 가져오기 작업에 대한 **Notifications(**알림**)** > **Tasks(**작업**)** 페이지에서 **View Import Report(**가져오기 보고서 보기**)**를 클릭합니다.

그림 *19:* 가져오기 보고서 보기



Device Configuration Import Reports(디바이스 구성 가져오기 보고서**)** 페이지는 사용 가능한 보고서에 대한 링크를 제공합니다.

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

라이선스 설정 편집

디바이스 페이지의 라이선스 섹션은 장치에 대해 활성화된 라이선스를 표시합니다.

management center에 사용 가능한 라이선스가 있으면 디바이스에서 라이선스를 활성화할 수 있습니다.

프로시저

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

단계 **2** 라이선스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 라이선스 섹션 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** 관리되는 디바이스에서 활성화 또는 비활성화 하려는 라이선스 옆의 체크 박스를 선택하거나 선택 취소합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

시스템 정보 보기

디바이스 페이지의 시스템 섹션은 다음 표에 나타난 시스템 정보의 읽기 전용 표를 표시합니다.

디바이스를 종료하거나 다시 시작할 수 있습니다.

표 *4:* 시스템 섹션 표 필드

필드	설명
모델	관리되는 디바이스의 모델 이름 및 번호입니다.
일련 번호	관리되는 디바이스의 섀시의 일련 번호입니다.
시간	디바이스의 현재 시스템 시간입니다.
시간대	표준 시간대를 표시합니다.
버전	매니지드 디바이스에 현재 설치된 소프트웨어 버전입니다.
시간 기반 규칙에 대한 표준 시간대 설정	디바이스 플랫폼 설정에 지정된 표준 시간대의 디바이스의 현재 시스템 시간입니다.

검사 엔진 활성화

Device(디바이스**)** 페이지의 Inspection Engine(검사 엔진) 섹션에는 디바이스에서 Snort2를 사용하는지 Snort3을 사용하는지가 표시됩니다. 검사 엔진을 전환하려면 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 를 참조하십시오 Cisco Secure Firewall Management Center Snort 3 구성 가이드.

상태 정보 보기

Device(디바이스**)** 페이지의 **Health(**상태**)** 섹션은 아래 표에서 설명한 정보를 표시합니다.

표 *5:* 상태 섹션 표 필드

필드	설명
상태	디바이스의 현재 상태를 나타내는 아이콘 아이콘을 클릭하면 어플라이언스에 대한 상태 모니터가 표시됩니다.
정책	디바이스에 현재 구축된 상태 정책에 대한 읽기 전용 링크입니다.

필드	설명
제외됨	상태 제외 모듈을 활성화하거나 비활성화할 수 있는 상태 제외 페이지의 링크입니다.

관리 설정 편집

Management(관리**)** 영역에서 관리 설정을 편집할 수 있습니다.

Management Center에서 호스트 이름 또는 IP 주소 업데이트

디바이스의 호스트 이름 또는 IP 주소를 (디바이스의 CLI 등을 사용해) management center에 추가했다면, 아래의 절차를 사용하여 관리 management center의 호스트 이름 또는 IP 주소를 수동으로 업데이트해야 할 수 있습니다.

디바이스에서 디바이스 관리 IP 주소를 변경하려면를 참조하십시오.CLI에서 Threat Defense 관리 인터페이스 수정, 61 페이지

디바이스를 등록할 때 NAT ID만 사용하는 경우에는 이 페이지에서 IP가 **NO-IP**로 표시되며 IP 주소/호스트 이름을 업데이트할 필요가 없습니다.

Threat Defense 기능 기록**:**

- 7.3 - 이중화 관리자 액세스 데이터 인터페이스

프로시저

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

단계 **2** 관리 옵션을 수장할 디바이스 옆의 **Edit(**수정**)** ( )를 클릭합니다.

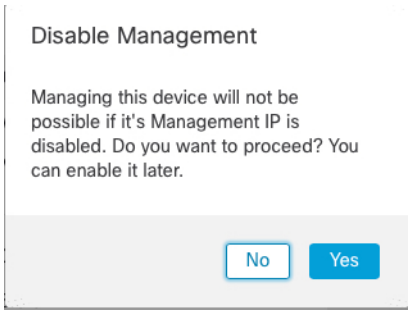
다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭하고 **Management(**관리**)** 영역을 확인합니다.

단계 **4** ( )이(가) 비활성화되도록 슬라이더를 클릭하여 관리를 일시적으로 비활성화합니다.

그림 ***20:*** 관리 비활성화

관리 비활성화를 진행하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.



관리를 비활성화하면 management center와 디바이스 간 연결이 차단되지만 management center에서 디바이스가 삭제되지는 않습니다.

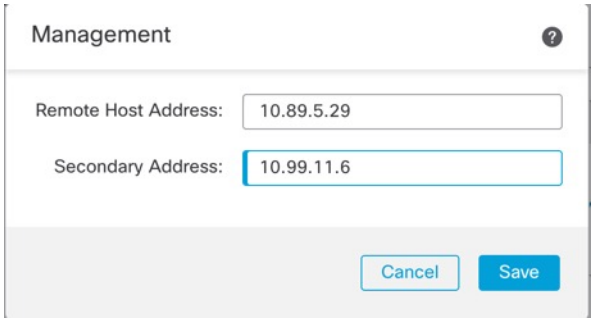
단계 **5** **Remote Host Address(**원격 호스트 주소**)** IP address(IP 주소) 및 선택 사항인 **Secondary Address(**보조 주소**)**(이중화 데이터 인터페이스를 사용하는 경우) 또는 **Edit(**수정**)** ( )를 클릭하여 호스트 이름을 편집합니다.

그림 ***21:*** 관리 주소 편집

단계 **6** **Management(**관리**)** 대화 상자의 **Remote Host Address(**원격 호스트 주소**)** 필드 및 선택 사항 **Secondary Address(**보조 주소**)** 필드에서 이름 또는 IP 주소를 수정하고 **Save(**저장**)**를 클릭합니다.

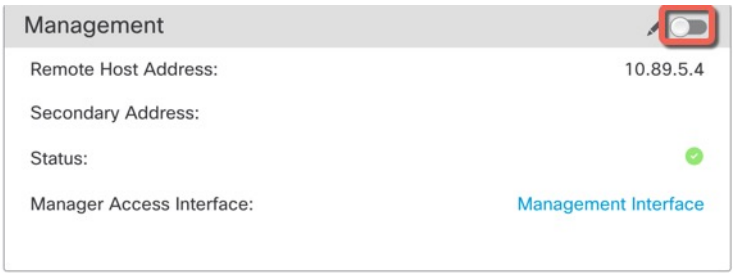
보조 관리자 액세스 데이터 인터페이스 사용에 대한 자세한 내용은 이중화 관리자 액세스 데이터 인터페이스 구성, 52 페이지 섹션을 참조하십시오.

그림 ***22:*** 관리 ***IP*** 주소



단계 **7** ( )이(가) 비활성화되도록 슬라이더를 클릭하여 관리를 비활성화합니다.

그림 *23:* 관리 연결 활성화



관리에서 데이터로 **Manager** 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 threat defense를 관리할 수 있습니다. 디바이스를 management center에 추가한 후 관리자 액세스 인터페이스를 변경하려면 다음 단계에 따라 관리 인터페이스에서 데이터 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 데이터에서 관리로 Manager 액세스 인터페이스 변경, 49 페이지의 내용 참조하십시오.

관리에서 데이터로의 관리자 액세스 마이그레이션을 시작하면 management center가 구축시 threat defense에 차단을 적용합니다. 블록을 제거하려면 데이터 인터페이스에서 관리자 액세스를 활성화합니다.

데이터 인터페이스에서 관리자 액세스를 활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

프로시저

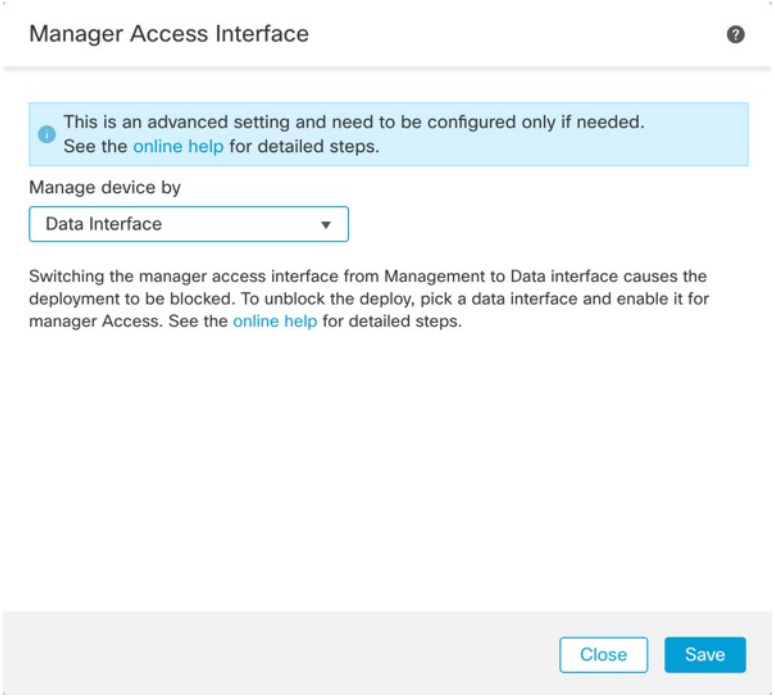
단계 **1** 인터페이스 마이그레이션을 시작합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대해 **Edit(**수정**)** ( )을 클릭합니다.

b) **Device(**디바이스**)** > **Management(**관리**)** 섹션으로 이동하여 **Manager Access Interface(**관리자 액세스 인터페이스**)** 링크를 클릭합니다.

Manager Access Interface(관리자 액세스 인터페이스**)** 필드에는 현재 관리 인터페이스가 표시됩니다. 링크를 클릭하면 **Manage device by(**디바이스 관리 기준**)** 드롭 다운 목록에서 새 인터페이스 유형 인 **Data Interface(**데이터 인터페이스**)**를 선택합니다.

그림 ***24:*** 관리자 액세스 인터페이스



c) **Save(**저장**)**를 클릭합니다.

이제 데이터 인터페이스에서 관리자 액세스를 활성화하려면 이 절차의 나머지 단계를 완료해야 합니다. 이제 **Management(**관리**)** 영역에 **Manager Access Interface: Data Interface(**데이터 인터페이스**)** 및 **Manager Access Details: Configuration(**관리자 액세스 세부 정보**:** 구성**)**이 표시됩니다.

그림 ***25:*** 관리자 액세스

Configuration(구성**)**을 클릭하면 **Manager Access - Configuration Details(**관리자 액세스 **-** 구성 세부 정보**)** 대화 상자가 열립니다. **Manager Access Mode(**관리자 액세스 모드**)**에 Deploy pending(구축 보류 중) 상태가 표시됩니다.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 편집**)** > **Manager Access(**관리자 액세스**)**페이지에서 데이터 인터페이스에 대한 관리자 액세스를 활성화합니다.

라우팅 모드 인터페이스 구성의 내용을 참조하십시오. 하나의 라우팅된 데이터 인터페이스와 선택적인 보조 인터페이스에서 관리자 액세스를 활성화 할 수 있습니다. 이러한 인터페이스가 이름과 IP 주소로 완전히 구성되어 있고 활성화되어 있는지 확인합니다.

이중화를 위해 보조 인터페이스를 사용하는 경우 추가 필수 구성은 이중화 관리자 액세스 데이터 인터페이스 구성, 52 페이지의 내용을 참조하십시오.

단계 **3** (선택 사항) 인터페이스에 DHCP를 사용하는 경우 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **DHCP** > **DDNS** 페이지에서 웹 유형 DDNS 방법을 활성화합니다.

동적 DNS 구성를 참조하십시오. DDNS는 FTD의 IP 주소가 변경될 경우 management center가 FQDN(Fully-Qualified Domain Name)에서 threat defense에 연결할 수 있도록 합니다.

단계 **4** threat defense가 데이터 인터페이스를 통해 management center로 라우팅될 수 있는지 확인합니다. **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**고정 경로**)**에서 필요한 경우 고정 경로를 추가합니다.

고정 경로 추가의 내용을 참조하십시오.

단계 **5** (선택 사항) 플랫폼 설정 정책에서 DNS를 구성하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 이 디바이스에 적용합니다.

DNS를 참조하십시오. DDNS를 사용하는 경우 DNS가 필요합니다. 보안 정책에서 FQDN에 대해 DNS를 사용할 수도 있습니다.

단계 **6** (선택 사항) 플랫폼 설정 정책에서 데이터 인터페이스에 대해 SSH를 활성화하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Secure Shell(**보안 셸**)**에서 이 디바이스에 적용합니다.

Secure Shell를 참조하십시오. SSH는 데이터 인터페이스에서 기본적으로 활성화되어 있지 않으므로 SSH를 사용하여 threat defense를 관리하려면 명시적으로 허용해야 합니다.

단계 **7** 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

management center는 현재 관리 인터페이스를 통해 구성 변경 사항을 구축합니다. 구축 후에는 데이터 인터페이스를 사용할 수 있지만 관리에 대한 원래 관리 연결은 계속 활성화됩니다.

단계 **8** 콘솔 포트의 threat defense CLI에서 관리 인터페이스가 고정 IP 주소를 사용하도록 설정하고 게이트웨이가 데이터 인터페이스를 사용하도록 설정합니다.

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask*-관리 인터페이스를 사용하지 않더라도 게이트웨이를 데이터 인터페이스로 설정할 수 있도록 고정 IP 주소(예: 개인 주소)를 설정해야 합니다(다음 글머리표 참조). 데이터 인터페이스여야 하는 기본 경로가 DHCP 서버에서 수신한 경로로 덮어 쓰여질 수 있으므로 DHCP를 사용할 수 없습니다.
- **data-interfaces** - 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 관리자 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.

관리 인터페이스 네트워크 설정을 변경하면 SSH 세션의 연결이 끊어 지므로 SSH 연결 대신 콘솔 포트를 사용하는 것이 좋습니다.

단계 **9** 필요한 경우 데이터 인터페이스에서 management center에 연결할 수 있도록 threat defense를 다시 케이블로 연결합니다.

단계 **10** management center에서 관리 연결을 비활성화하고 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** 섹션에서 threat defense의 **Remote Host Address(**원격 호스트 주소**)** IP address(IP 주소) 및 선택 사항 **Secondary Address(**보조 주소**)**를 제거하고 연결을 다시 활성화합니다.

Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지의 내용을 참조하십시오. threat defense를 management center에 추가할 때 threat defense 호스트 네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

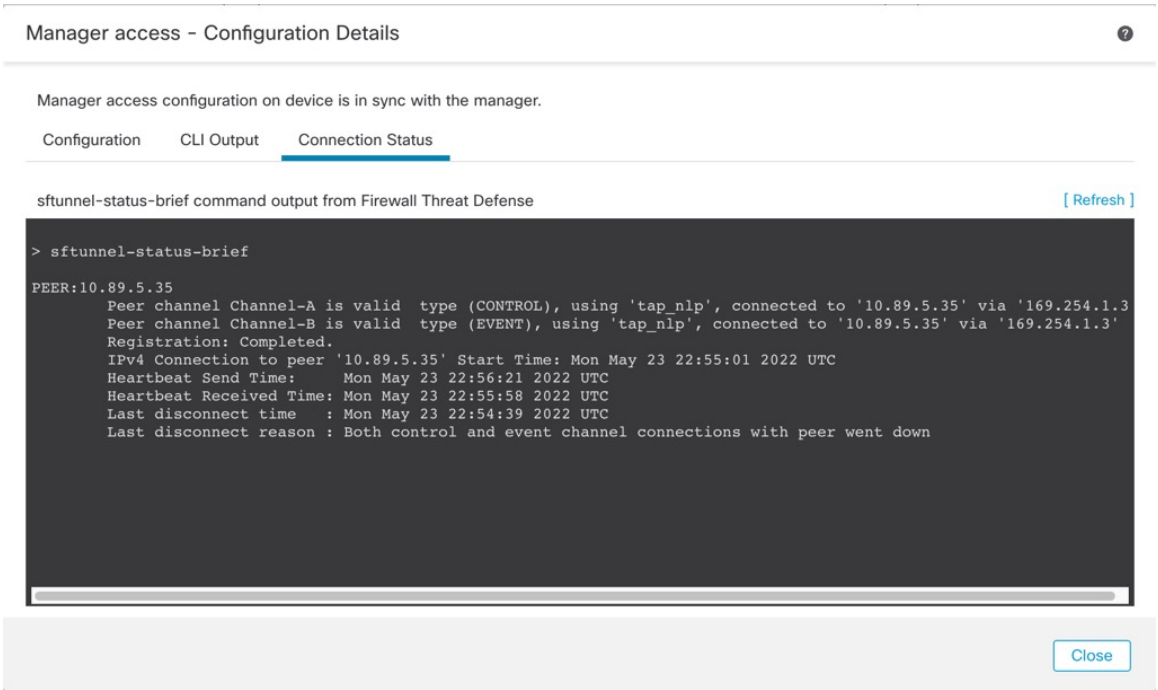
단계 **11** 관리 연결이 다시 설정되었는지 확인합니다.

management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

다음 상태는 내부 "tap_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.

그림 ***26:*** 연결 상태



연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 72 페이지의 내용을 참조하십시오.

데이터에서 관리로 Manager 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 threat defense를 관리할 수 있습니다. 디바이스를 management center에 추가한 후 관리자 액세스 인터페이스를 변경하려면 다음 단계에 따라 데이터 인터페이스에서 관리 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 관리에서 데이터로 Manager 액세스 인터페이스 변경, 45 페이지의 내용 참조하십시오.

데이터에서 관리로의 관리자 액세스 마이그레이션을 시작하면 management center가 구축시 threat defense에 차단을 적용합니다. 차단을 제거하려면 데이터 인터페이스에서 관리자 액세스를 비활성화해야 합니다.

데이터 인터페이스에서 관리자 액세스를 비활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

프로시저

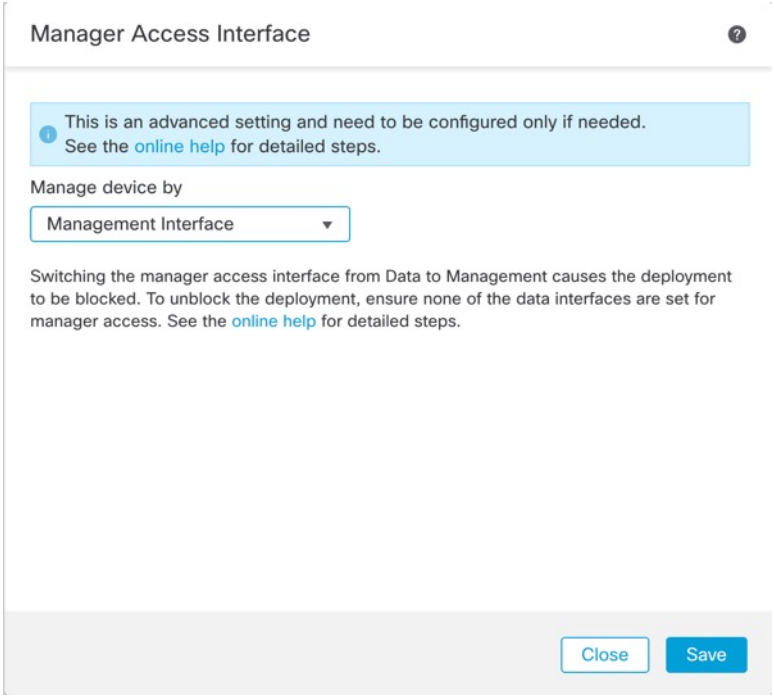
단계 **1** 인터페이스 마이그레이션을 시작합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대해 **Edit(**수정**)** ( )을 클릭합니다.

b) **Device(**디바이스**)** > **Management(**관리**)** 섹션으로 이동하여 **Manager Access Interface(**관리자 액세스 인터페이스**)** 링크를 클릭합니다.

Manager Access Interface(관리자 액세스 인터페이스**)** 필드는 현재 관리 인터페이스를 데이터로 표시합니다. 링크를 클릭할 때 **Manage device by(**디바이스 관리 기준**)** 드롭다운 목록에서 새 인터페이스 유형인 **Management Interface(**관리 인터페이스**)**를 선택합니다.

그림 ***27:*** 관리자 액세스 인터페이스



c) **Save(**저장**)**를 클릭합니다.

이제 이 절차의 나머지 단계를 완료하여 관리 인터페이스에서 관리자 액세스를 활성화해야 합니다. 이제 **Management(**관리**)** 영역에 **Manager Access Interface: Management Interface(**관리 인터페이스**)** 및 **Manager Access Details: Configuration(**관리자 액세스 세부 정보**:** 구성**)**이 표시됩니다.

그림 ***28:*** 관리자 액세스

Configuration(구성**)**을 클릭하면 **Manager Access - Configuration Details(**관리자 액세스 - 구성 세부 정보**)** 대화 상자가 열립니다. **Manager Access Mode(**관리자 액세스 모드**)**에 Deploy pending(구축 보류 중) 상태가 표시됩니다.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 편집**)** > **Manager Access(**관리자 액세스**)**페이지에서 데이터 인터페이스에 대한 관리자 액세스를 비활성화합니다.

라우팅 모드 인터페이스 구성를 참조하십시오. 이 단계에서는 구축 시 차단을 제거합니다.

단계 **3** 아직 수행하지 않은 경우, 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS 설정을 구성하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 해당 디바이스에 적용합니다.

DNS를 참조하십시오. 데이터 인터페이스에서 관리자 액세스를 비활성화하는 management center 구축은 로컬 DNS 설정을 제거합니다. 해당 DNS 서버가 액세스 규칙의 FQDN과 같은 보안 정책에서 사용되는 경우, management center를 통해 DNS 구성을 다시 적용해야 합니다.

단계 **4** 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

management center는 현재 데이터 인터페이스를 통해 구성 변경 사항을 구축합니다.

단계 **5** 필요한 경우, 관리 인터페이스에서 management center에 연결할 수 있도록 threat defense를 다시 케이블로 연결합니다.

단계 **6** threat defense CLI에서 고정 IP 주소 또는 DHCP를 사용하여 관리 인터페이스 IP 주소 및 게이트웨이를 설정합니다.

원래 관리자 액세스용 데이터 인터페이스를 설정하면 관리 게이트웨이가 데이터 인터페이스로 설정되었습니다. 이 인터페이스는 관리 트래픽을 백플레인을 통해 전달하여 관리자 액세스 데이터 인터페이스를 통해 라우팅할 수 있도록 지원했습니다. 이제 관리 네트워크에서 게이트웨이의 IP 주소를 설정해야 합니다.

고정 **IP** 주소**:**

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **dhcp**

단계 **7** management center에서 관리 연결을 비활성화하고 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** 섹션에서 threat defense의 **Remote Host Address(**호스트 주소 제거**)** IP address(IP 주소)를 업데이트하고 선택 사항 **Secondary Address(**보조 주소**)**를 제거하고 연결을 다시 활성화합니다.

Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지의 내용을 참조하십시오. threat defense를 management center에 추가할 때 threat defense 호스트 네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

단계 **8** 관리 연결이 다시 설정되었는지 확인합니다.

management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Status(**상태**)** 필드에서 관리 연결 상태를 확인하거나 management center에서 알림을 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 72 페이지의 내용을 참조하십시오.

이중화 관리자 액세스 데이터 인터페이스 구성

관리자 액세스를 위해 데이터 인터페이스를 사용할 때 기본 인터페이스가 다운될 경우 관리 기능을 수행하도록 보조 데이터 인터페이스를 구성할 수 있습니다. 보조 인터페이스는 하나만 구성할 수 있습니다. 디바이스는 SLA 모니터링을 사용하여 정적 경로 및 두 인터페이스를 모두 포함하는 ECMP 영역의 실행 가능성을 추적하므로 관리 트래픽이 두 인터페이스를 모두 사용할 수 있습니다.

시작하기 전에

- 보조 인터페이스는 기본 인터페이스와 별도의 보안 영역에 있어야 합니다.
- 기본 인터페이스에 적용되는 것과 동일한 요구 사항이 모두 보조 인터페이스에 적용됩니다. 관리를 위한 Threat Defense 데이터 인터페이스 사용, 4 페이지을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대해 **Edit(**수정**)** ( ) 을 클릭합니다.

단계 **2** 보조 인터페이스에 대한 관리자 액세스를 활성화합니다.

이 설정은 인터페이스 활성화, 이름 설정, 보안 영역 설정, 고정 IPv4 주소 설정 등의 표준 인터페이스 설정에 추가됩니다.

a) **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 편집**)** > **Manager Access(**관리자 액세스**)**를 선택합니다.

b) **Enable management on this interface for the Manager(**관리자를 위해 이 인터페이스에서 관리 활성화**)**를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

두 인터페이스 모두 인터페이스 목록에 **(Manager Access(**관리자 액세스**))**로 표시됩니다.

그림 ***29:*** 인터페이스 목록

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

단계 **3** **Management(**관리**)** 설정에 보조 주소를 추가합니다.

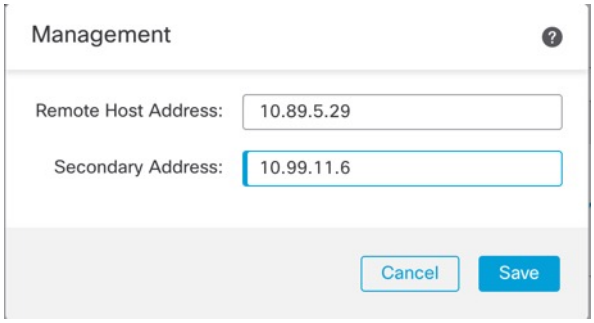
a) **Device(**디바이스**)**를 클릭하고 **Management(**관리**)** 영역을 확인합니다.

b) **Edit(**수정**)** (✎)를 클릭합니다.

그림 ***30:*** 관리 주소 편집

c) **Management(**관리**)** 대화상자에서 **Secondary Address(**보조 주소**)** 필드의 이름 또는 IP 주소를 수정합니다.

그림 ***31:*** 관리 ***IP*** 주소

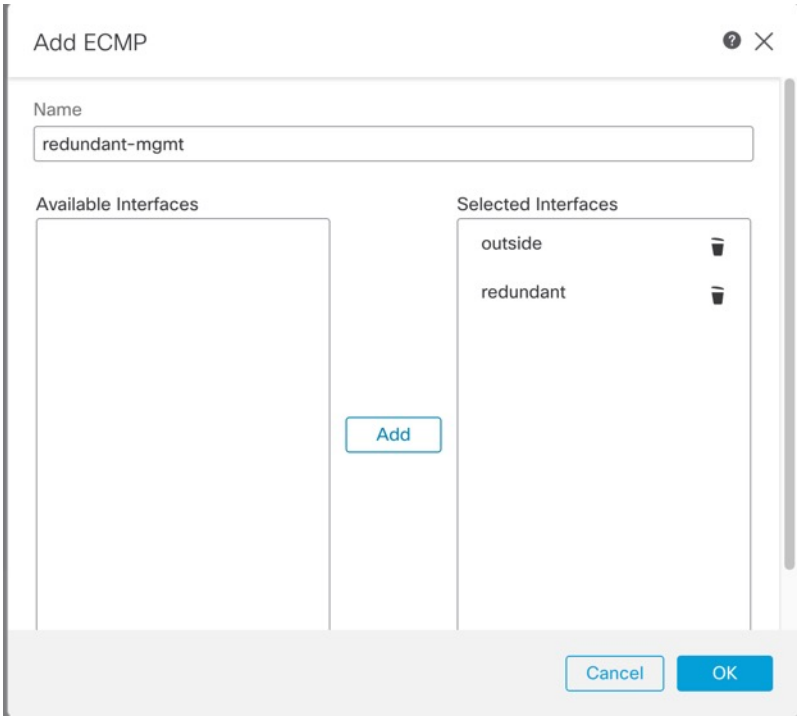


d) **Save(**저장**)**를 클릭합니다.

단계 **4** 두 인터페이스가 모두 포함된 ECMP 영역을 생성합니다.

a) **Routing(**라우팅**)**을 클릭합니다.
b) 가상 라우터 드롭다운에서 기본 및 보조 인터페이스가 있는 가상 라우터를 선택합니다.
c) **ECMP**를 클릭한 다음 **Add(**추가**)**를 클릭합니다.
d) ECMP 영역의 **Name(**이름**)**을 입력합니다.
e) **Available Interface(**사용 가능한 인터페이스**)** 상자에서 기본 및 보조 인터페이스를 선택한 다음 **Add(**추가**)**를 클릭합니다.

그림 ***32: ECMP*** 영역 추가

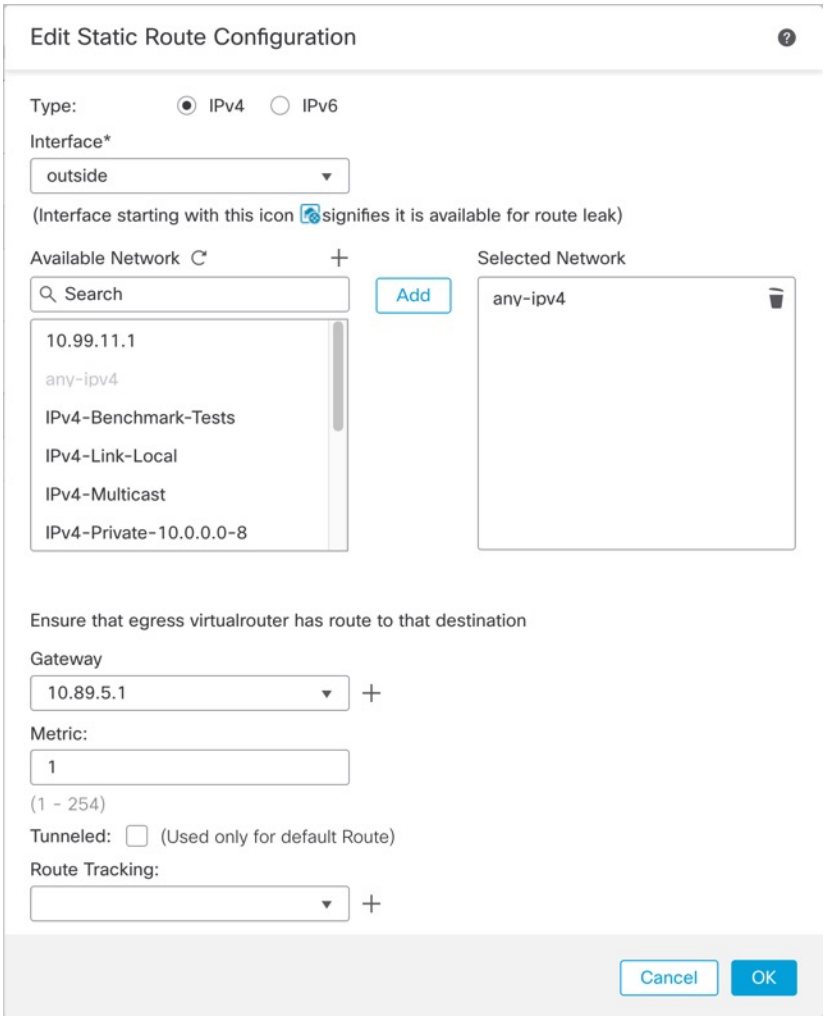


f) **OK(**확인**)**를 클릭한 다음 **Save(**저장**)**를 클릭합니다.

단계 **5** 두 인터페이스 모두에 대해 동일한 비용의 기본 고정 경로를 추가하고 두 인터페이스 모두에서 SLA 추적을 활성화합니다.

경로는 게이트웨이를 제외하고 동일해야 하며 둘 다 메트릭 1을 가져야 합니다. 기본 인터페이스에는 수정할 수 있는 기본 경로가 이미 있어야 합니다.

그림 ***33:*** 정적 경로 추가/편집



a) **Static Route(**정적 경로**)**를 클릭합니다.

b) **Add Route(**경로 추가**)**를 클릭하여 새 경로를 추가하거나 기존 경로에 대해 **Edit(**수정**)** ( )를 클릭합니다.

c) **Interface(**인터페이스**)** 드롭다운에서 인터페이스를 선택합니다.

d) 대상 네트워크에 대해 **Available Networks(**사용 가능한 네트워크**)** 상자에서 **any-ipv4**를 선택하고 **Add(**추가**)**를 클릭합니다.

e) 기본 게이트웨이를 입력합니다.

f) **Route Tracking(**경로 추적**)**의 경우 **Add(**추가**)** ( )을 클릭하여 새 SLA 모니터 개체를 추가합니다.

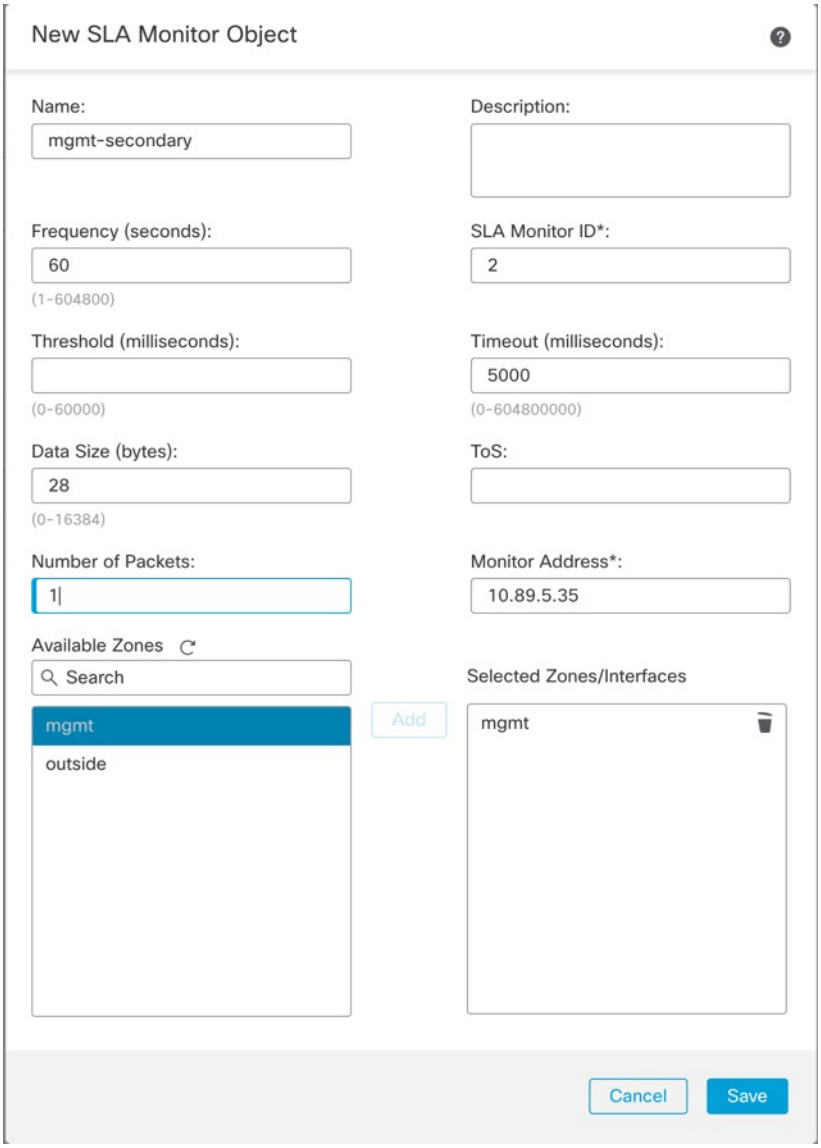
g) 다음을 포함한 필수 매개변수를 입력합니다.

- **Monitor Address(**모니터 주소**)** 를 management center IP 주소로.

- **Available Zones(**사용 가능한 영역**)**의 기본 또는 보조 관리 인터페이스에 대한 영역입니다. 예를 들어 기본 인터페이스 개체에 대해서는 외부 영역을 선택하고 보조 인터페이스 개체에 대해서는 관리 영역을 선택합니다.

자세한 내용은 SLA 모니터링을 참조하십시오.

그림 ***34: SLA*** 모니터 추가



h) **Save(**저장**)**를 클릭한 다음 **Route Tracking(**경로 추적**)** 드롭다운 목록에서 방금 생성한 SLA 개체를 선택합니다.

i) **OK(**확인**)**를 클릭한 다음 **Save(**저장**)**를 클릭합니다.

j) 다른 관리 인터페이스의 기본 경로에 대해 반복합니다.

단계 **6** 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

이 기능에 대한 구축의 일환으로 management center는 관리 트래픽에 대해 자동 생성된 정책 기반 라우팅 구성을 포함하여 관리 트래픽에 대한 보조 인터페이스를 활성화하여 올바른 데이터 인터페이스로 이동합니다. management center는 **configure network management-data-interface** 명령의 두 번째 인스턴스도 구축합니다. CLI에서 보조 인터페이스를 수정하는 경우, 게이트웨이를 구성하거나 기본 경로를 변경할 수 없습니다. 이 인터페이스의 정적 경로는 management center에서만 수정할 수 있습니다.

데이터 인터페이스 관리를 위한 **Manager** 액세스 세부 정보 보기

모델 지원—Threat Defense

전용 관리 인터페이스를 사용하는 대신 management center 관리용 데이터 인터페이스를 사용하는 경우, management center에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경할 수도 있습니다. 이렇게 하려면 management center에서 이러한 변경 사항을 수동으로 조정해야 합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(Manager** 액세스 - 구성 세부 정보**)** 대화 상자를 사용하면 management center와 threat defense 로컬 구성 간의 불일치를 해결할 수 있습니다.

일반적으로 management center에 threat defense를 추가하기 전에 초기 threat defense 설정의 일부로 Manager 액세스 데이터 인터페이스를 구성합니다. management center에 threat defense를 추가하면 management center는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버의 경우 구성이 등록 중에 검색된 경우 로컬로 유지되지만 management center의 플랫폼 설정 정책에 추가되지 않습니다.

threat defense를 management center에 추가한 후 **configure network management-data-interface** 명령을 사용하여 threat defense의 데이터 인터페이스 설정을 로컬로 변경하면 management center는 구성 변경 사항을 탐지하고 threat defense에 대한 구축을 차단합니다. management center는 다음 방법 중 하나를 사용하여 구성 변경을 탐지합니다.

- threat defense에 구축합니다. management center는 구축하기 전에 구성 차이를 탐지하고 구축을 중지합니다.
- **Interface(**인터페이스**)** 페이지의 **Sync(**동기화**)** 버튼
- **Manager Access - Configuration Details(Manager** 액세스 - 구성 세부 정보**)**대화 상자의 **Refresh**(새로 고침) 버튼.

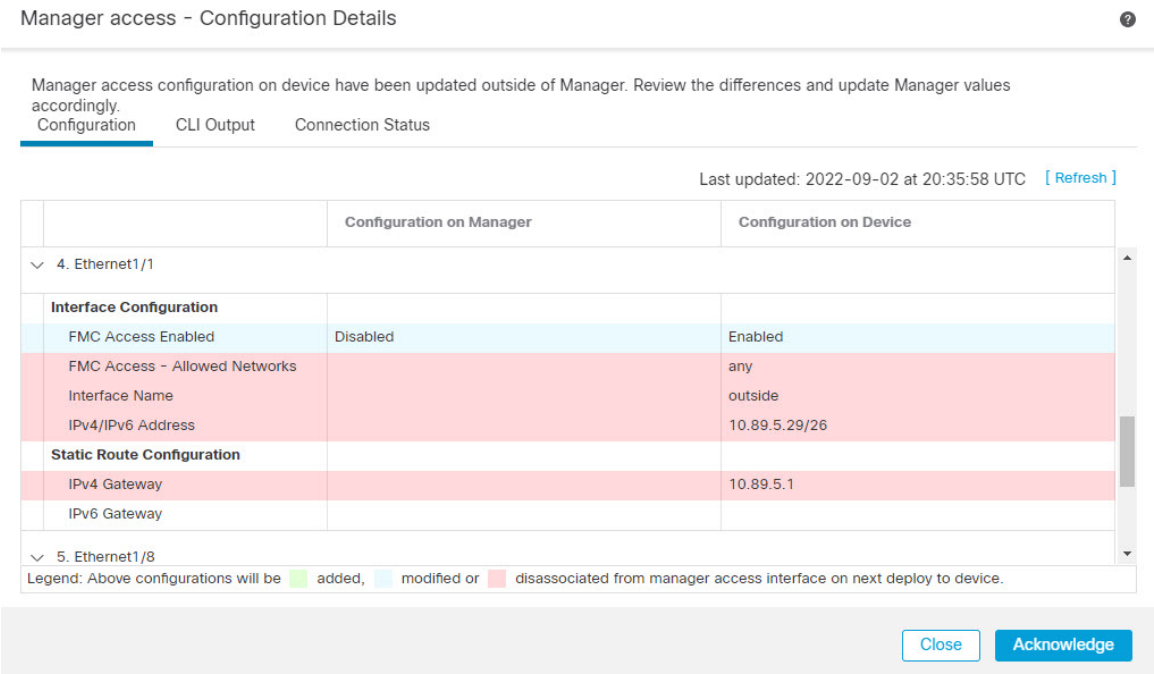
블록을 제거하려면 **Manager Access - Configuration Details(Manager** 액세스 - 구성 세부 정보**)** 대화 상자로 이동하고 **Acknowledge(**확인**)**를 클릭합니다. 다음에 구축할 때 management center 구성은 threat defense의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 management center에서 구성을 수동으로 수정하는 것은 사용자의 책임입니다.

이 대화 상자에서 다음 페이지를 참조하십시오.

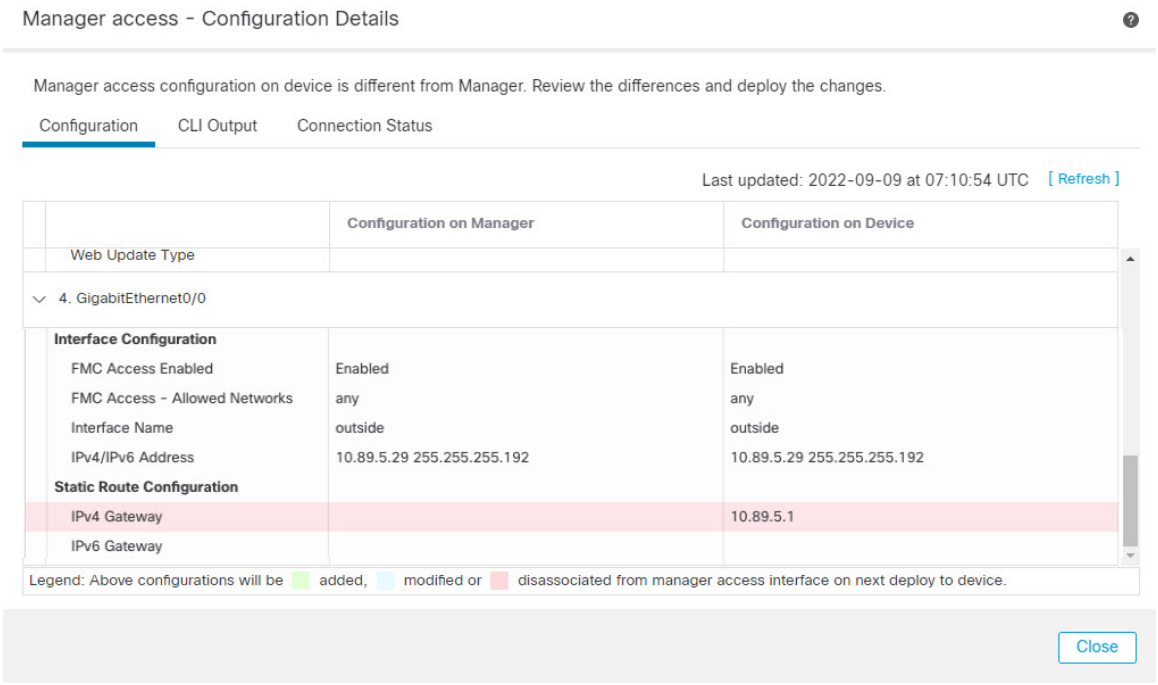
컨피그레이션

management center 및 threat defense에서 Manager 액세스 데이터 인터페이스의 구성 비교를 확인합니다.

다음 예에서는 threat defense에서 **configure network management-data-interface** 명령이 입력된 threat defense의 구성 세부 사항을 보여줍니다. 분홍으로 강조 표시된 부분은 차이점을 **Acknowledge(확인)** 하지만 management center의 구성과 일치하지 않으면 threat defense 구성이 제거됨을 나타냅니다. 파란색으로 강조 표시된 부분은 threat defense에서 수정될 구성을 보여줍니다. 녹색으로 강조 표시된 부분은 threat defense에 추가될 구성을 보여줍니다.



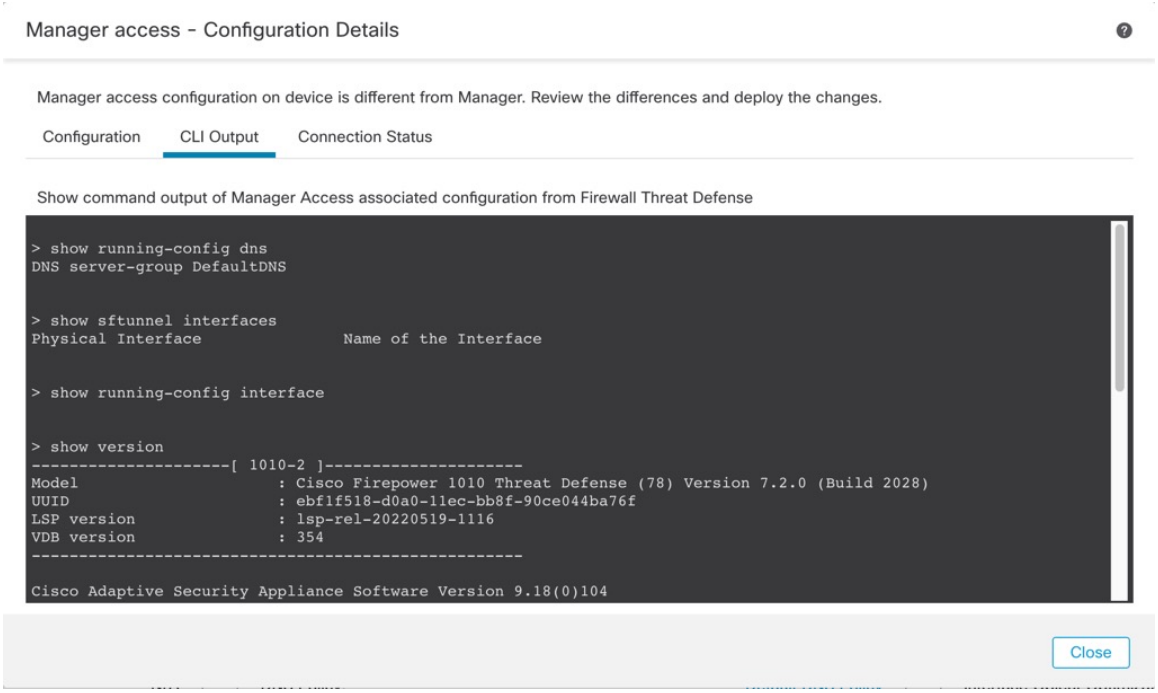
다음 예는 management center에서 인터페이스를 구성한 후의 이 페이지를 보여줍니다. 인터페이스 설정이 일치하고 분홍색 강조 표시가 제거되었습니다.



CLI 출력

관리자 액세스 데이터 인터페이스의 CLI 구성을 확인합니다. 이는 기본 CLI에 익숙한 경우 유용합니다.

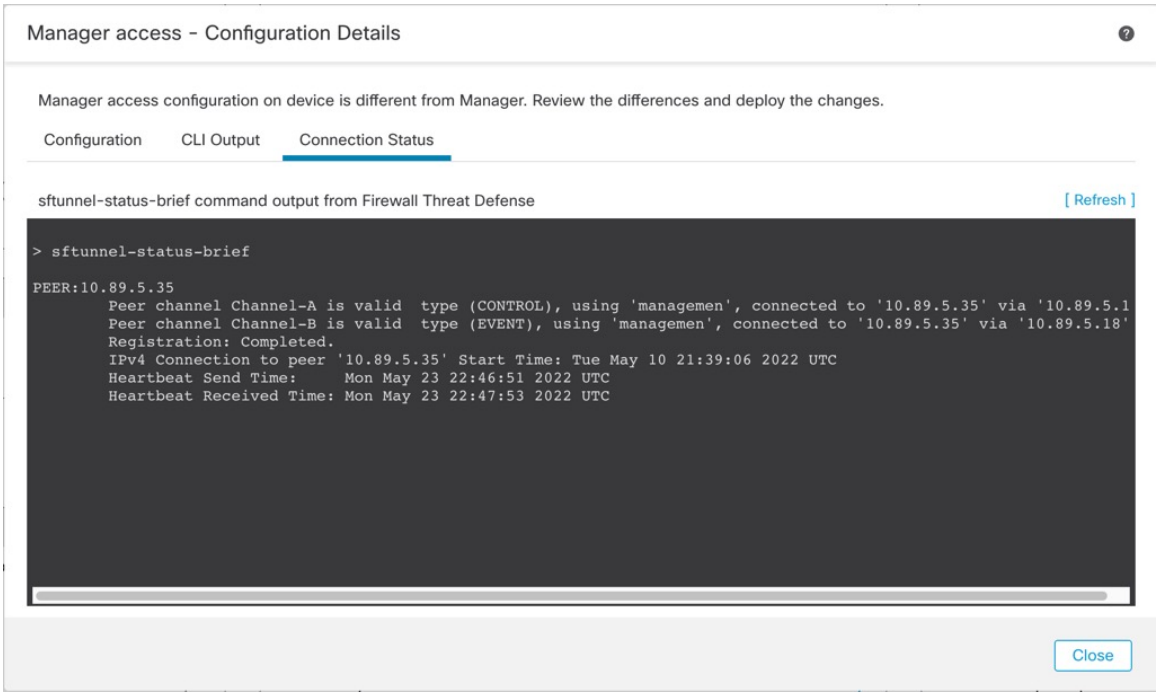
그림 ***35: CLI*** 출력



연결 상태

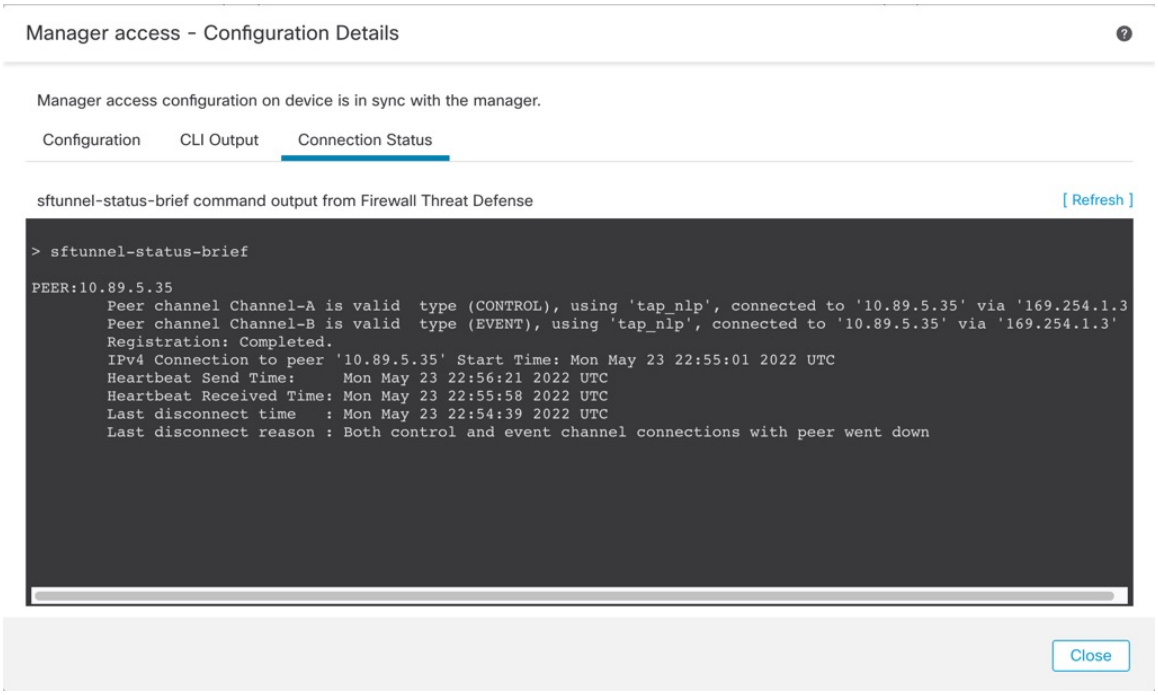
관리 연결 상태를 봅니다. 다음 예는 관리 연결이 여전히 관리 "management0" 인터페이스를 사용하고 있음을 보여줍니다.

그림 ***36:*** 연결 상태



다음 상태는 내부 "tap_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.

그림 *37:* 연결 상태



작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

CLI에서 Threat Defense 관리 인터페이스 수정

CLI를 사용하여 매니지드 디바이스의 관리 인터페이스 설정을 수정합니다. 이러한 설정 중 대부분은 초기 설정을 수행할 때의 설정입니다. 이 절차를 통해 해당 설정을 변경하고 모델에서 지원하는 경우 이벤트 인터페이스를 활성화하거나 정적 경로를 추가하는 등의 추가 설정을 지정할 수 있습니다.

참고 이 항목은 전용 관리 인터페이스에 적용됩니다. 관리를 위해 데이터 인터페이스를 설정할 수도 있습니다. 해당 인터페이스의 네트워크 설정을 변경하려면 CLI가 아닌 management center 내에서 변경해야 합니다. 중단된 관리 연결을 문제 해결해야 하고 threat defense에서 직접 변경해야 하는 경우 CLI에서 관리에 사용되는 Threat Defense 데이터 인터페이스 수정, 68 페이지의 내용을 참조하십시오.

threat defense CLI에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

참고 SSH를 사용하여 관리 인터페이스를 변경할 때는 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 디바이스 콘솔 포트에 액세스해야 합니다.

참고 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령(신규 Management Center 식별, 93 페이지 참조)을 사용하여 초기 디바이스 설정 중에 management center를 식별한 방법에 따라 management center 연결에 대한 다음 작업을 참조하십시오.

- **IP address(IP 주소)** - 작업이 없습니다**.** 연결 가능한 IP 주소를 사용하여 management center를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 management center에 표시되는 디바이스 IP 주소도 변경하는 것이 좋습니다. Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 management center IP 주소를 지정한 경우 아래의 NAT ID 절차를 참조하십시오.
- **NAT ID**만 - 수동으로 연결을 재설정합니다**.** NAT ID만 사용하여 management center를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지에 따라 management center에서 디바이스 관리 IP 주소를 변경합니다.

참고 고가용성 management center 구성에서 디바이스 CLI 또는 management center의 관리 IP 주소를 수정하면 보조 management center는 HA 동기화가 끝나도 변경 사항을 반영하지 않습니다. 보조 management center도 업데이트되게 하려면 두 management center의 역할을 바꿔 보조 management center를 액티브 유닛으로 설정해야 합니다. 현재 액티브 management center의 디바이스 관리 페이지에 등록한 디바이스의 관리 IP 주소를 수정합니다.

시작하기 전에

- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 사용자 계정을 생성할 수 있습니다. CLI에서 내부 사용자 추가의 내용을 참조하십시오. 외부 인증에 따라 AAA 사용자를 구성할 수도 있습니다.

프로시저

단계 **1** 콘솔 포트 또는 SSH를 사용하여 디바이스 CLI에 연결합니다.

Threat Defense 디바이스의 명령줄 인터페이스에 로그인, 11 페이지의 내용을 참조하십시오.

단계 **2** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **3** (Firepower 4100/9300만 해당) 두 번째 관리 인터페이스를 이벤트 전용 인터페이스로 활성화합니다.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

항상 관리 트래픽용 데이터 관리 인터페이스가 필요합니다. 디바이스에 두 번째 관리 인터페이스가 있는 경우 이벤트 전용 트래픽에 대해 이를 활성화할 수 있습니다.

configure network management-interface disable-events-channel 명령을 사용하여 주 관리 인터페이스의 이벤트를 선택적으로 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.

별도의 이벤트 인터페이스를 사용하려면 management center에서 이벤트 인터페이스를 활성화해야 합니다. Cisco Secure Firewall Management Center 관리 가이드를 참조하십시오.

예제:

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

단계 **4** 관리 인터페이스 및/또는 이벤트 인터페이스의 IP 주소를 구성합니다.

management_interface 인수를 지정하지 않으면 기본 관리 인터페이스에 대한 네트워크 설정을 변경하면 됩니다. 이벤트 인터페이스를 구성할 때 *management_interface* 인수를 지정해야 합니다. 이벤트 인터페이스는 관리 인터페이스와 별도의 네트워크에 있거나 동일한 네트워크에 있을 수 있습니다. 구성 중인 인터페이스에 연결되어 있으면 연결이 끊어집니다. 새 IP 주소에 다시 연결할 수 있습니다.

a) IPv4 주소 구성:

- 수동 구성:

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  이 명령의 *gateway_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *gateway_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *gateway_ip*를 설정한 다음 **configure network**

static-routes 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

예**:**

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP(기본 관리 인터페이스에서만 지원됨):

  configure network ipv4 dhcp

b) IPv6 주소 구성:

- 상태 비저장 자동 구성:

  configure network ipv6 router [*management_interface*]

  예**:**

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 수동 구성:

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  이 명령의 *ipv6_gateway_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *ipv6_gateway_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *ipv6_gateway_ip*를 설정한 다음 **configure network static-routes** 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

  예**:**

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6(기본 관리 인터페이스에서만 지원됨):

  configure network ipv6 dhcp

단계 **5** IPv6의 경우 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 활성화하거나 비활성화합니다. 이러한 메시지는 기본적으로 활성화됩니다.

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.

예제:

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

단계 **6** 기본 관리 인터페이스의 DHCP 서버가 연결된 호스트에 IP 주소를 제공할 수 있게 활성화합니다.

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

예제:

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

관리 인터페이스 IP 주소를 수동으로 설정할 때만 DHCP 서버를 구성할 수 있습니다. 이 명령은 management center virtual에서 지원되지 않습니다. DHCP 서버 상태를 표시하려면 **show network-dhcp-server**:를 입력합니다.

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

단계 **7** management center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다.

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

기본 경로의 경우 이 명령을 사용하지 마십시오. **configure network ipv4** 또는 **ipv6** 명령을 사용할 때만 기본 경로 게이트웨이 IP 주소를 변경할 수 있습니다(4단계 참조).단계 4, 63 페이지

예제:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

정적 경로를 표시하려면 **show network-static-routes**를 입력합니다(기본 경로는 표시되지 않음).

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

단계 **8** 호스트네임 설정

configure network hostname *name*

예제**:**

```
> configure network hostname farscape1.cisco.com
```

시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.

단계 **9** 검색 도메인 설정:

configure network dns searchdomains *domain_list*

예제**:**

```
> configure network dns searchdomains example.com,cisco.com
```

디바이스에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

단계 **10** 쉼표로 구분하여 최대 3개의 DNS 서버를 설정합니다.

configure network dns servers *dns_ip_list*

예제**:**

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

단계 **11** management center와의 통신을 위한 원격 관리 포트를 설정합니다.

configure network management-interface tcpport *number*

예제**:**

```
> configure network management-interface tcpport 8555
```

management center 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **12** (Threat Defense 전용) 관리 또는 이벤트 인터페이스 MTU를 설정합니다. MTU는 기본적으로 1500바이트입니다.

configure network mtu [*bytes*] [*interface_id*]

- *bytes* - MTU를 바이트 단위로 설정합니다. 관리 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 1500이고 IPv6를 활성화하는 경우 값은 1280 ~ 1500입니다. 이벤트 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 9000이고 IPv6를 활성화하는 경우 값은 1280 ~ 9000입니다. IPv4 및 IPv6를 모두 활성화하는 경우 최소값은 1280입니다. 바이트를 입력하지 않으면 값을 입력하라는 프롬프트가 표시됩니다.
- *interface_id* — MTU를 설정할 인터페이스 ID를 지정합니다. 플랫폼에 따라 사용 가능한 인터페이스 ID(예: management0, management1, br1, eth0)를 보려면 **show network** 명령을 사용합니다. 인터페이스를 지정하지 않으면 관리 인터페이스가 사용됩니다.

예제**:**

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

단계 **13** HTTP 프록시를 구성합니다. 디바이스는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다. 명령을 실행하면 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부에 대한 프롬프트가 표시되며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호의 확인에 대한 프롬프트가 표시됩니다.

참고 threat defense의 프록시 비밀번호의 경우, A~Z, a~z, 0~9 문자만 사용할 수 있습니다.

configure network http-proxy

예제**:**

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

단계 **14** 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령(신규 Management Center 식별, 93 페이지 참조)을 사용하여 초기 디바이스 설정 중에 management center를 식별한 방법에 따라 management center 연결에 대한 다음 작업을 참조하십시오.

- **IP address(IP** 주소**)** - 작업이 없습니다**.** 연결 가능한 IP 주소를 사용하여 management center를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 management center에 표시되는 디바이스 IP 주소도 변경하는 것이 좋습니다. Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 management center IP 주소를 지정한 경우 Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지을(를) 사용하여 연결을 수동으로 다시 설정해야 합니다.
- **NAT ID**만 - 수동으로 연결을 재설정합니다**.** NAT ID만 사용하여 management center를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지에 따라 management center에서 디바이스 관리 IP 주소를 변경합니다.

CLI에서 관리에 사용되는 Threat Defense 데이터 인터페이스 수정

threat defense와 management center 간의 관리 연결이 중단된 상태에서 기존 인터페이스를 대체할 새 데이터 인터페이스를 지정하려는 경우 threat defense CLI를 사용하여 새 인터페이스를 설정합니다. 이 절차에서는 동일한 네트워크에서 기존 인터페이스를 새 인터페이스로 교체하려 한다고 가정합니다. 관리 연결이 활성 상태이면 management center를 사용하여 기존 데이터 인터페이스를 변경해야 합니다. 데이터 관리 인터페이스의 초기 설정에 대해서는 CLI로 Threat Defense 초기 구성 완료, 18 페이지에서 **configure network management-data-interface** 명령을 참조하십시오.

참고 이 항목은 전용 관리 인터페이스가 아니라 관리용으로 설정한 데이터 인터페이스에 적용됩니다. 관리 인터페이스의 네트워크 설정을 변경하려면 CLI에서 Threat Defense 관리 인터페이스 수정, 61 페이지의 내용을 참조하십시오.

threat defense CLI에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

시작하기 전에

- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 사용자 계정을 생성할 수 있습니다. CLI에서 내부 사용자 추가의 내용을 참조하십시오. 외부 인증에 따라 AAA 사용자를 구성할 수도 있습니다.

프로시저

단계 **1** 데이터 관리 인터페이스를 새 인터페이스로 변경하는 경우 현재 인터페이스 케이블을 새 인터페이스로 이동합니다.

단계 **2** 디바이스 CLI에 연결합니다.

이러한 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 초기 설정을 수행하는 경우 관리 인터페이스에서 연결이 끊어질 수 있습니다. 관리 연결이 중단되어 구성을 수정하는 경우 전용 관리 인터페이스에 대한 SSH 액세스 권한이 있는 경우 해당 SSH 연결을 사용할 수 있습니다.

Threat Defense 디바이스의 명령줄 인터페이스에 로그인, 11 페이지의 내용을 참조하십시오.

단계 **3** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **4** 설정을 재구성할 수 있도록 인터페이스를 비활성화합니다.

configure network management-data-interface disable

예제:

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

단계 **5** 관리자 액세스용 새 데이터 인터페이스의 이름을 구성합니다

configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

데이터 관리 인터페이스를 동일한 네트워크의 새 인터페이스로 변경할 때는 인터페이스 ID를 제외하고 이전 인터페이스와 동일한 설정을 사용합니다. 또한, 적용하기 전에 모든 디바이스 구성을 지우시겠습니까**? (y/n) [n]:** 옵션에 대해 **y**를 선택합니다. 이 옵션을 선택하면 이전 데이터 관리 인터페이스 구성이 지워지므로 새 인터페이스에서 IP 주소 및 인터페이스 이름을 성공적으로 재사용할 수 있습니다.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **6** (선택 사항) 특정 네트워크에서 management center에 대한 데이터 인터페이스 액세스를 제한합니다.

configure network management-data-interface client *ip_address netmask*

기본적으로 모든 네트워크가 허용됩니다.

단계 **7** 연결은 자동으로 재설정되지만 management center에서 연결을 비활성화했다가 다시 활성화하면 연결을 더 빠르게 재설정하는 데 도움이 됩니다. Management Center에서 호스트 이름 또는 IP 주소 업데이트, 43 페이지을 참조하십시오.

단계 **8** 관리 연결이 재설정되었는지 확인합니다.

sftunnel-status-brief

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

단계 **9** management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 - 구성 세부 사항**)**를 선택하고 **Refresh(**새로 고침**)**를 클릭합니다.

management center는 인터페이스 및 기본 경로 구성 변경을 탐지하고 threat defense에 대한 구축을 차단합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경하는 경우 management center에서 수동으로 변경 사항을 조정해야 합니다. **Configuration(**구성**)** 탭에서 management center와 threat defense 간의 불일치를 볼 수 있습니다.

단계 **10** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택하고 다음을 변경합니다.

a) 이전 데이터 관리 인터페이스에서 IP 주소와 이름을 제거하고 이 인터페이스에 대해 관리자 액세스를 비활성화합니다.

b) 이전 인터페이스(CLI에서 사용한 인터페이스)의 설정으로 새 데이터 관리 인터페이스를 설정하고 관리자 액세스를 활성화합니다.

단계 **11** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**고정 경로**)**를 선택하고 기존 데이터 관리 인터페이스에서 새 경로로 기본 경로를 변경합니다.

단계 **12** **Manager Access - Configuration Details(Manager** 액세스 - 구성 세부 정보**)** 대화 상자로 돌아가 **Acknowledge(**확인**)**를 클릭하여 구축 블록을 제거합니다.

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

"Config was cleared(구성이 지워졌습니다)" 및 "Manager(관리자) Access changed and acknowledged(액세스가 변경되어 승인되었습니다)"라는 메시지가 표시됩니다.

Management Center에서 연결을 상실할 경우 구성을 수동으로 롤백

threat defense 관리를 위해 FTD에서 데이터 인터페이스를 사용하고 네트워크 연결에 영향을 주는 management center 구성 변경 사항을 배포하는 경우 관리 연결을 복원할 수 있도록 threat defense의 구성 을 마지막으로 배포된 구성으로 롤백할 수 있습니다. 그런 다음 네트워크 연결이 유지되도록 management center에서 구성 설정을 조정하고 다시 배포할 수 있습니다. 연결이 끊기지 않아도 롤백 기능을 사용할 수 있습니다. 이는 이 문제 해결 상황으로 제한되지 않습니다.

또는 구축 후 연결이 끊길 경우 구성의 자동 롤백을 활성화할 수 있습니다. 배포 설정 편집, 83 페이지 참조.

다음 지침을 참조하십시오.

- 이전 배포만 threat defense에서 로컬로 사용할 수 있습니다. 이전 배포으로 롤백할 수 없습니다.
- 고가용성에서는 롤백이 지원되지만 클러스터링 배포에서는 롤백이 지원되지 않습니다.
- 롤백은 management center에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 threat defense CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 management center 배포 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 배포된 management center 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 배포 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.

프로시저

단계 **1** threat defense CLI에서 이전 구성으로 롤백합니다.

configure policy rollback

롤백 후 threat defense는 롤백이 성공적으로 완료되었음을 management center에 알립니다. management center에서 배포 화면에는 구성이 롤백되었음을 알리는 배너가 표시됩니다.

참고 롤백에 실패하고 management center 관리가 복원된 경우, 일반적인 배포 문제에 대한 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html을 참조하십시오. 경우에 따라 management center 관리 액세스가 복원된 후 롤백이 실패할 수 있습니다. 이 경우 management center 구성 문제를 해결하고 management center에서 다시 배포할 수 있습니다.

예제:

관리자 액세스를 위해 데이터 인터페이스를 사용하는 threat defense의 경우:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?
```

```
Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

단계 **2** 관리 연결이 재설정되었는지 확인합니다.

management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 - 설정 세부 사항**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 72 페이지의 내용을 참조하십시오.

데이터 인터페이스에서 관리 연결성 문제 해결

전용 관리 인터페이스를 사용하는 대신 관리자 데이터 인터페이스를 사용하는 경우, management center에서 threat defense에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. management center에 threat defense를 추가한 후 관리 인터페이스 유형을 데이터에서 관리로 또는 관리에서 데이터로 변경하는 경우, 인터페이스 및 네트워크 설정이 올바르게 설정되지 않으면 관리 연결이 끊어질 수 있습니다.

이 주제는 관리 연결 끊김 문제를 해결하는 데 도움이 됩니다.

관리 연결 상태 보기

management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다. **sftunnel-status** 명령을 사용하여 전체 정보를 볼 수도 있습니다.

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

threat defense 네트워크 정보 보기

threat defense CLI에서 관리 및 FMC 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
```

```
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

threat defense가 **management center**에 등록되었는지 확인합니다**.**

threat defense CLI에서 management center 등록이 완료되었는지 확인합니다. 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

show managers

```
> show managers
Type                     : Manager
Host                     : 10.10.1.4
Display name             : 10.10.1.4
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

management center ping하기

FTD CLI에서 threat defense 다음 명령을 사용하여 데이터 인터페이스에서 management center를 ping합니다.

ping *fmc_ip*

threat defenseCLI에서 다음 명령을 사용하여 관리 인터페이스에서 management center를 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅되어야 합니다.

ping system *fmc_ip*

threat defense 내부 인터페이스에서 패킷 캡처

threat defense CLI에서 내부 백플레인 인터페이스(nlp_int_tap)의 패킷을 캡처하여 관리 패킷이 전송되는지 확인합니다.

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture *name* **trace detail**

내부 인터페이스 상태**,** 통계 및 패킷 수 확인

threat defense CLI에서 내부 백플레인 인터페이스, nlp_int_tap에 대한 정보를 참조하십시오.

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
```

```
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

라우팅 및 **NAT** 확인

threat defense CLI에서 기본 경로(S *)가 추가되었고 관리 인터페이스(nlp_int_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
```

```
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

다른 설정 확인

다른 모든 설정이 있는지 확인하려면 다음 명령을 참조하십시오. management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 컨피그레이션 디테일**)** > **CLI Output(CLI** 출력**)** 페이지에서 이러한 명령을 많이 볼 수 있습니다.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

성공적인 **DDNS** 업데이트 확인

threat defense CLI에서 DDNS 업데이트에 성공했는지 확인합니다.

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

업데이트가 실패하면 **debug http** 및 **debug ssl** 명령을 사용합니다. 인증서 검증에 실패한 경우, 다음을 통해 루트 인증서가 디바이스에 설치되어 있는지 확인합니다.

show crypto ca certificates *trustpoint_name*

DDNS 작업을 확인하려면 다음 명령을 사용하십시오.

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

management center 로그 파일 확인

https://cisco.com/go/fmc-reg-error를 참조하십시오.

재고 목록 세부 정보 보기

Device(디바이스**)** 페이지의 **Inventory Details(**재고 목록 세부 정보**)** 섹션에는 CPU 및 메모리와 같은 섀시 세부 정보가 표시됩니다.

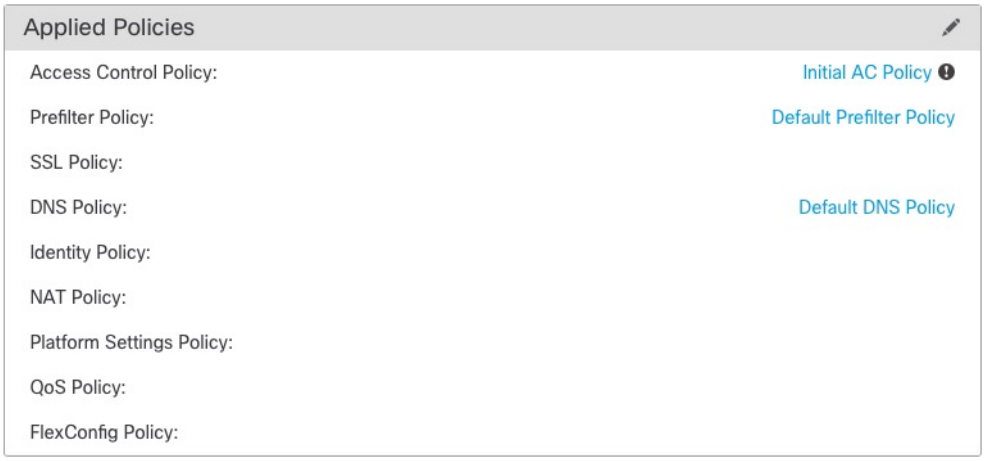
그림 ***38:*** 재고 목록 세부 정보

정보를 업데이트하려면 **Refresh(**새로 고침**)(**)를 클릭합니다.

적용된 정책 편집

Device(디바이스**)** 페이지의 **Applied Policies(**적용된 정책**)** 섹션에는 방화벽에 적용된 다음 정책이 표시됩니다.

그림 **39:** 정책 적용



링크가 있는 정책의 경우 링크를 클릭하여 정책을 볼 수 있습니다.

Access Control Policy(액세스 제어 정책)의 경우, 느낌표( ) 아이콘을 클릭하여 **Access Policy for Troubleshooting(**문제 해결을 위한 액세스 정책 정보**)**대화 상자를 확인합니다. 이 대화 상자는 액세스 규칙을 ACE(Access Control Entry)로 확장하는 방법을 보여줍니다.

그림 **40:** 트러블슈팅을 위한 액세스 정책 정보

Device Management(디바이스 관리**)** 페이지에서 개별 디바이스에 정책을 할당할 수 있습니다.

프로시저

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

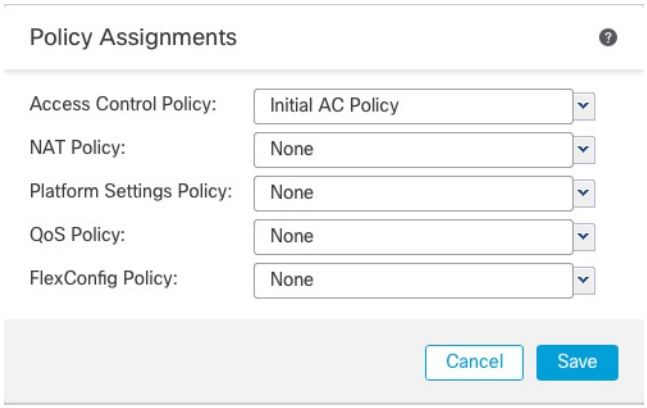
단계 **2** 정책을 할당할 디바이스 옆의 **Edit(**수정**)** ( )를 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** **Applied Polides(**적용된 살충제**)** 섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

그림 ***41:*** 정책 할당



단계 **5** 각 정책 유형에 대해 드롭다운 메뉴에서 정책을 선택합니다. 기존 정책만 나열됩니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

고급 설정 편집

Device(디바이스**)** 페이지의 **Advanced Settings(**고급 설정**)** 섹션은 아래 표에 설명된 대로 고급 구성 설정을 표시합니다. 이러한 설정은 편집할 수 있습니다.

표 ***6:*** 고급 섹션 표 필드

필드	설명
애플리케이션 우회	디바이스에서 Automatic Application Bypass의 상태
우회 임계값	밀리초로 나타낸 Automatic Application Bypass(자동 애플리케이션 우회) 임계값입니다.

필드	설명
개체 그룹 검색	디바이스에서 개체 그룹 검색의 상태입니다. 작동하는 동안 FTD 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 컨텐츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 Firepower 디바이스 관리자에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다. 참고 관리 센터에서 처음으로 위협 방어를 추가하면 기본적으로 **Object Group Search(**개체 그룹 검색**)**이 활성화됩니다.
인터페이스 개체 최적화	디바이스에서 인터페이스 개체 최적화의 상태입니다. 구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, **Object Group Search(**개체 그룹 검색**)** 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.

다음 주제에서는 고급 디바이스 설정을 편집하는 방법에 대해 설명합니다.

참고 패킷 전송 설정에 대한 자세한 내용은 일반 설정 편집, 34 페이지를 참고하십시오.

AAB(Automatic Application Bypass) 구성

AAB(Automatic Application Bypass)를 사용하면 Snort가 다운된 경우 또는 클래식 디바이스의 경우 패킷 처리에 시간이 너무 오래 걸리는 경우 패킷이 탐지를 우회할 수 있습니다. AAB는 장애 발생 후 10분 이내에 Snort를 재시작하고, Snort 장애의 원인을 조사하기 위해 분석할 수 있는 문제 해결 데이터를 생성합니다.

주의 AAB 활성화는 Snort 프로세스를 일부 재시작하여 일부 패킷의 검사를 일시적으로 중단합니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오.

다음 동작을 참조하십시오.

FTD 동작: Snort가 중단된 경우 지정된 타이머 기간 후에 AAB가 트리거됩니다. Snort가 작동하면 패킷 처리가 설정된 타이머를 초과하더라도 AAB가 트리거되지 않습니다.

기본 디바이스 동작: AAB는 인터페이스를 통해 패킷을 처리하는 데 허용되는 시간을 제한합니다. 패킷 처리 지연을 패킷 대기 시간을 위한 네트워크의 허용 오차와 균형을 맞춥니다.

이 기능은 모든 배포에서 기능하지만, 인라인 배포에서 특히 유용합니다.

일반적으로 레이턴시 임계값이 초과된 후 빠른 경로 패킷에 대한 침입 정책에서 Rule Latency Thresholding을 사용합니다. 규칙 레이턴시 임계값은 엔진을 종료하거나 문제 해결 데이터를 생성하지 않습니다.

탐지가 우회되면 디바이스는 상태 모니터링 알림을 생성합니다.

기본적으로 AAB는 비활성화되어 있습니다. AAB를 활성화하려면 단계 설명을 따릅니다.

프로시저

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

단계 **2** 고급 디바이스 설정을 수정할 디바이스 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **3** **Device(**디바이스**)** 탭을 클릭한 다음 **Advanced Settings(**고급 설정**)**섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** **AAB(Automatic Application Bypass)**를 선택합니다.

단계 **5** 250~60000밀리초 사이의 우회 임계값을 입력합니다. 기본 설정은 3000밀리초(ms)입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

개체 그룹 검색 구성

작동하는 동안 threat defense 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 컨텐츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 management center에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다.

개체 그룹 검색을 활성화하면 네트워크 또는 인터페이스 개체를 포함하는 액세스 컨트롤 정책에 대한 메모리 요구 사항이 감소합니다. 그러나 개체 그룹 검색은 또한 규칙 조회 성능을 저하시켜 CPU

사용률이 증가한다는 점에 유의해야 합니다. 특정 액세스 컨트롤 정책에 대한 감소된 메모리 요구 사항에 대한 CPU 영향의 균형을 유지해야 합니다. 대부분의 경우, 개체 그룹 검색을 활성화하면 네트워크 운영이 개선됩니다.

기본적으로 개체 그룹 검색은 management center에서 처음 추가되는 위협 방어 디바이스에 대해 활성화됩니다. 업그레이드된 디바이스의 경우 디바이스가 비활성화된 개체 그룹 검색으로 구성된 경우 수동으로 활성화해야 합니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며 전역적으로 활성화할 수 없습니다. 네트워크 또는 인터페이스 개체를 사용하는 액세스 규칙을 구축하는 모든 디바이스에서 이 기능을 활성화하는 것이 좋습니다.

참고 개체 그룹 검색을 활성화한 다음 잠시 동안 디바이스를 구성하고 작동할 경우 나중에 기능을 비활성화하면 원하지 않는 결과가 발생할 수 있습니다. 개체 그룹 검색을 비활성화할 경우 디바이스의 실행 중인 구성에서 기존 액세스 제어 규칙이 확장됩니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다. 디바이스가 정상적으로 작동중인 경우 활성화한 개체 그룹 검색을 비활성화해서는 안 됩니다.

시작하기 전에

- 모델 지원—Threat Defense
- 각 디바이스에서 트랜잭션 커밋도 활성화하는 것이 좋습니다. 디바이스 CLI에서 **asp rule-engine transactional-commit access-group** 명령을 입력합니다.
- 이 설정을 변경하면 디바이스가 ACL을 다시 컴파일하는 동안 시스템 작동이 중단될 수 있습니다. 유지 보수 기간 중에 이 설정을 변경하는 것이 좋습니다.

프로시저

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

단계 **2** 규칙을 설정하려는 threat defense 디바이스 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭한 다음 **Advanced Settings(**고급 설정**)**섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 개체 그룹 검색을 선택합니다.

단계 **5** 네트워크 개체 외에 인터페이스 개체에서도 개체 그룹 검색을 수행하려면 **Interface Object Optimization(**인터페이스 개체 최적화**)**을 선택합니다.

Interface Object Optimization(인터페이스 개체 최적화**)**을 선택하지 않으면 시스템은 각 소스/인터페이스 쌍에 대해 별도의 규칙을 구축합니다. 규칙에 사용되는 보안 영역 및 인터페이스 그룹을 사용합니다. 이는 인터페이스 그룹을 개체 그룹 검색 처리에 사용할 수 없음을 의미합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

인터페이스 개체 최적화 구성

구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, **Object Group Search(**개체 그룹 검색**)** 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.

인터페이스 개체 최적화는 기본적으로 비활성화되어 있습니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며, 전역적으로 활성화할 수 없습니다.

참고 인터페이스 개체 최적화를 비활성화하면 인터페이스 개체를 사용하지 않고 기존 액세스 제어 규칙이 구축되므로 구축 시간이 더 오래 걸릴 수 있습니다. 또한 개체 그룹 검색을 활성화하면 인터페이스 개체에 이점이 적용되지 않으며, 디바이스의 실행 중인 설정에서 액세스 제어 규칙이 확장되어 표시될 수 있습니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다.

시작하기 전에

모델 지원—Threat Defense

프로시저

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

단계 **2** 규칙을 설정하려는 FTD 디바이스 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭한 다음 **Advanced Settings(**고급 설정**)**섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** **Interface Object Optimization(**인터페이스 개체 최적화**)**을 확인합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

배포 설정 편집

디바이스 페이지의 디바이스 설정 섹션은 아래 표에서 설명한 정보를 표시합니다.

그림 ***42:*** 배포 설정

표 *7:* 배포 설정

필드	설명
연결 실패 시 자동 롤백 배포	Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다. 배포의 결과로 관리 연결이 실패하는 경우 자동 롤백을 활성화할 수 있습니다. 특히 관리 센터 액세스를 위해 데이터를 사용하고 데이터 인터페이스를 잘못 구성하는 경우
연결성 모니터 간격(분)	구성을 롤백하기 전에 대기하는 시간을 표시합니다.

디바이스 관리 페이지에서 배포 설정을 지정할 수 있습니다. 배포 설정에는 배포의 결과로 관리 연결이 실패할 경우 배포의 자동 롤백 활성화가 포함됩니다. 특히 관리 센터 액세스를 위해 데이터를 사용하고 데이터 인터페이스를 잘못 구성하는 경우 그렇습니다 **configure policy rollback** 명령을 사용하여 수동으로 구성을 롤백할 수도 있습니다(Management Center에서 연결을 상실할 경우 구성을 수동으로 롤백, 71 페이지 참조).

다음 지침을 참조하십시오.

- 이전 배포만 threat defense에서 로컬로 사용할 수 있습니다. 이전 배포으로 롤백할 수 없습니다.
- 고가용성에서는 롤백이 지원되지만 클러스터링 배포에서는 롤백이 지원되지 않습니다.
- 롤백은 management center에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 threat defense CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 management center 배포 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 배포된 management center 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 배포 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.

프로시저

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

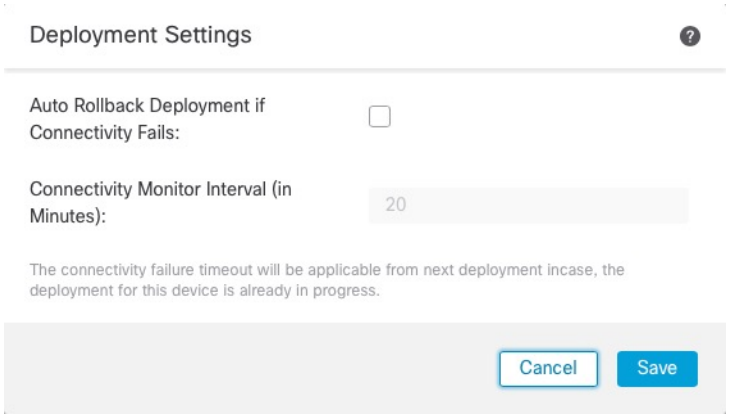
단계 **2** 정책을 할당할 디바이스 옆의 **Edit(**수정**)** ( )를 클릭합니다.

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** **Deployment Settings(**구축 설정**)** 섹션에서 **Edit(**수정**)** ( )를 클릭합니다.

그림 **43:** 배포 설정



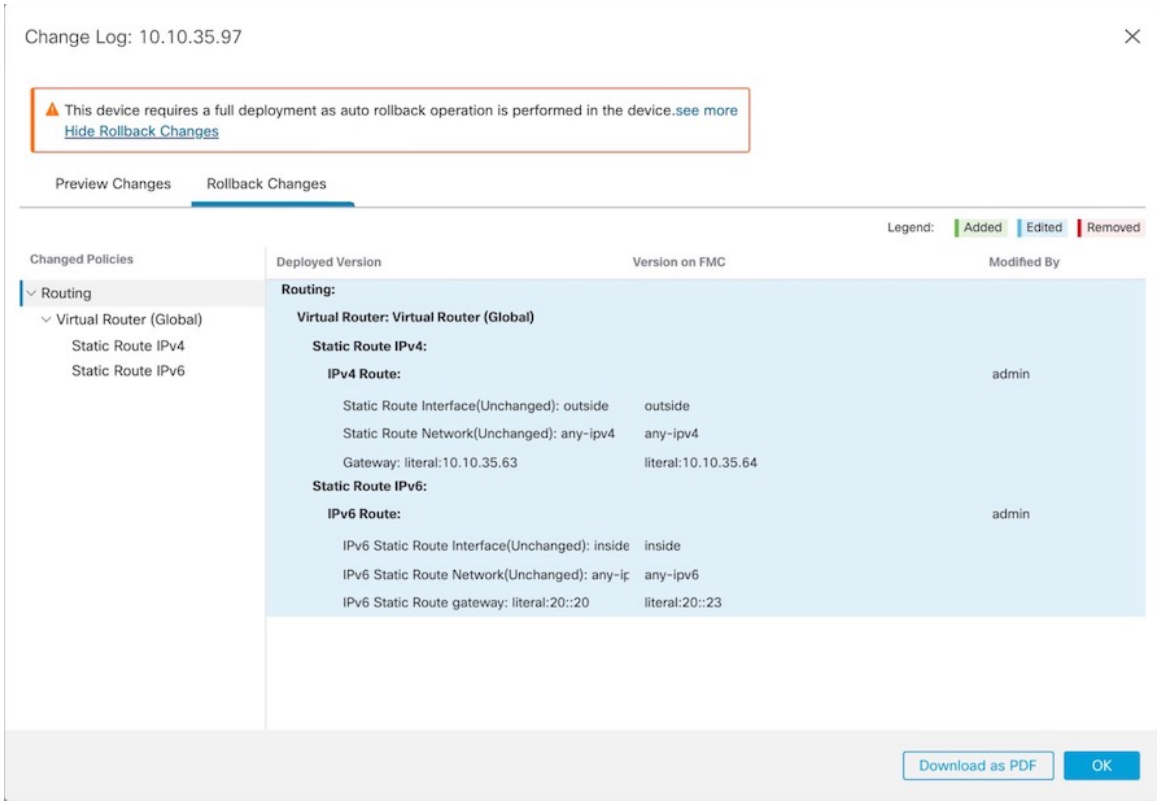
단계 **5** 자동 롤백을 활성화하려면 연결 실패 시 자동 롤백 구축을 선택합니다.

단계 **6** 구성을 롤백하기 전에 대기할 시간을 설정하려면 연결성 모니터 간격**(**분**)**을 설정합니다. 기본값은 20분입니다.

단계 **7** 롤백이 발생하는 경우 다음 단계를 참조하십시오.

- 자동 롤백에 성공한 경우 전체 배포을 수행하라는 성공 메시지가 표시됩니다.
- **Deployment(**구축**)** 화면으로 이동하여 **Preview(**미리보기**)**( ) 아이콘을 클릭하여 롤백된 구성의 일부를 볼 수도 있습니다(구축 미리보기 참조). **Show Rollback Changes(**롤백 변경 사항 표시**)**를 클릭하여 변경 사항을 확인하고 **Hide Rollback Changes(**롤백 변경 사항 숨기기**)**를 클릭하여 변경 사항을 숨깁니다.

그림 **44:** 롤백 변경 사항



- Deployment History Preview(배포 기록 미리 보기)에서 롤백 변경 사항을 볼 수 있습니다. 구축 히스토리 프리뷰 보기을 참조하십시오.

단계 **8** 관리 연결이 재설정되었는지 확인합니다.

management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 72 페이지의 내용을 참조하십시오.

클러스터 상태 모니터링 설정 편집

Cluster(클러스터**)** 페이지의 **Cluster Health Monitor Settings(**클러스터 상태 모니터링 설정**)** 섹션은 아래 표의 설정을 표시합니다.

그림 **45:** 클러스터 상태 모니터링 설정

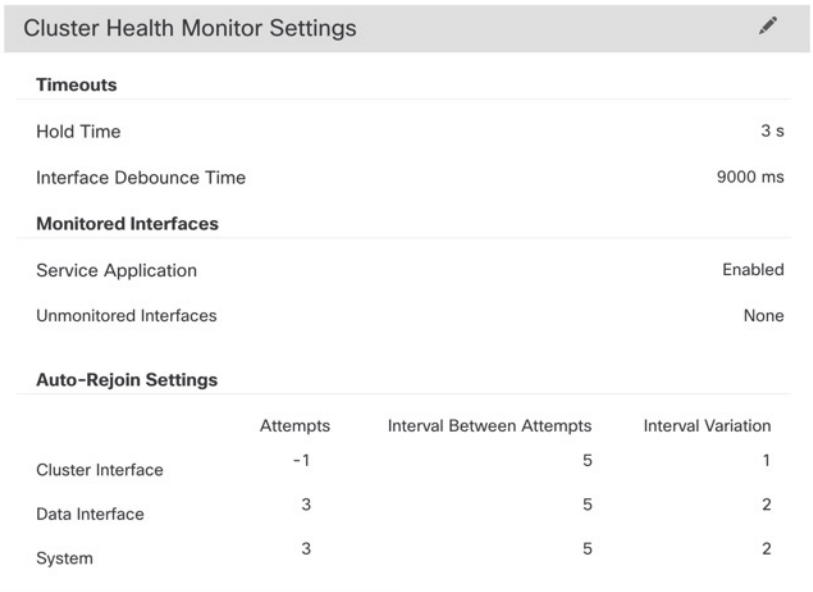


표 **8:** 클러스터 상태 모니터링 설정 섹션 표 필드

필드	설명
시간 초과	
보류 시간	노드 시스템 상태를 확인하기 위해 클러스터 노드에서는 다른 노드에 대한 클러스터 제어 링크에서 하트비트 메시지를 보냅니다. 노드가 피어 노드의 하트비트 메시지를 대기 시간 내에 수신하지 않을 경우, 해당 피어 노드는 응답하지 않거나 중지된 상태로 간주됩니다.
인터페이스 디바운스 시간	인터페이스 디바운스 시간은 노드가 인터페이스에 장애가 발생한 것으로 간주하고 노드가 클러스터에서 제거되기 전까지의 시간입니다.
모니터링 인터페이스	인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 노드에서 오류가 발생했지만 다른 노드에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 노드는 클러스터에서 제거됩니다. 노드에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 노드가 설정된 노드인지 또는 클러스터에 참가하는지에 따라 달라집니다.
서비스 애플리케이션	Snort 및 disk-full 프로세스의 모니터링 여부를 표시합니다.
모니터링되지 않는 인터페이스	모니터링되지 않는 인터페이스를 표시합니다.
자동 재연결 설정	

필드	설명
클러스터 인터페이스	클러스터 제어 링크 장애에 대한 자동 다시 참가 설정을 표시합니다.
데이터 인터페이스	데이터 인터페이스 실패에 대한 자동 다시 참가 설정을 표시합니다.
시스템	내부 오류에 대한 자동 다시 참가 설정을 표시합니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등

참고 시스템 상태 확인을 비활성화하면 시스템 상태 확인이 비활성화되었을 때 적용되지 않는 필드가 표시되지 않습니다.

이 섹션에서 이러한 설정을 할 수 있습니다.

모든 포트 채널 ID, 단일 물리적 인터페이스 ID는 물론 Snort 및 디스크 전체 프로세스도 모니터링할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.

프로시저

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

단계 **2** 수정할 클러스터 옆의 **Edit(**수정**)** ( )을 클릭합니다.

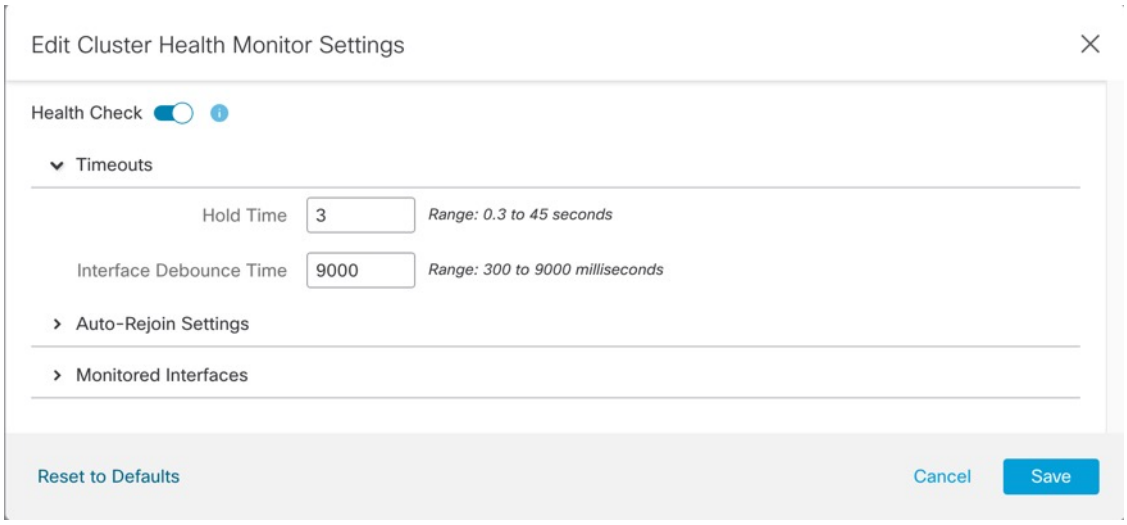
다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Cluster(**클러스터**)**를 클릭합니다.

단계 **4** **Cluster Health Monitor Settings(**클러스터 상태 모니터링 설정**)** 섹션에서 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Health Check(**상태 확인**)** 슬라이더를 클릭하여 시스템 상태 확인을 비활성화합니다.

그림 **46:** 시스템 상태 확인 비활성화



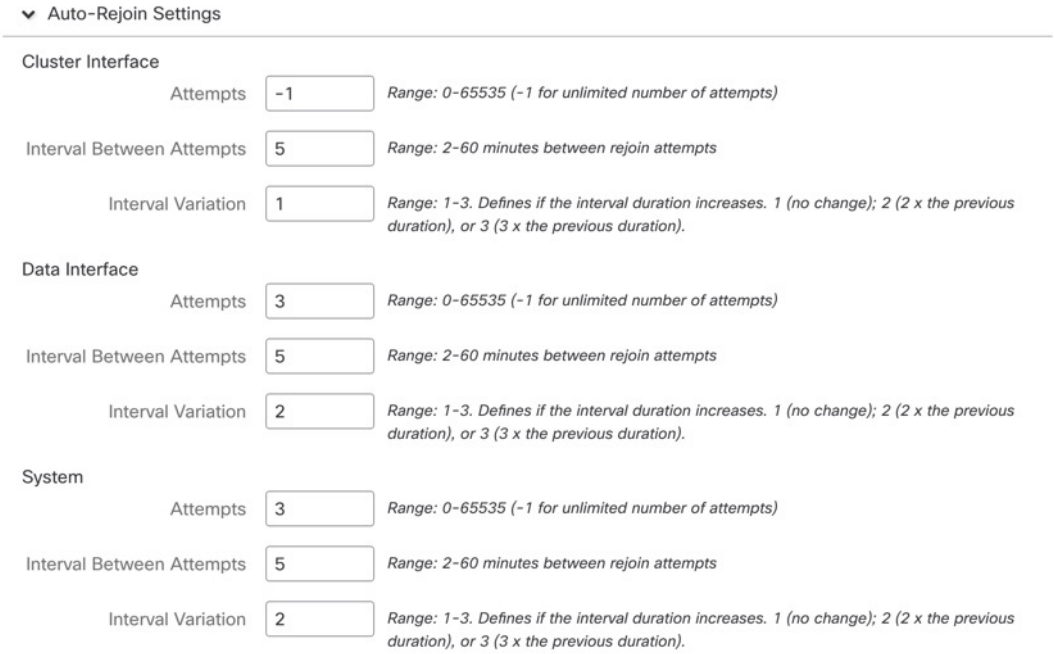
토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, 노드 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 시스템 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 노드와 동기화되면 시스템 상태 검사 기능 및 모니터링되는 인터페이스를 다시 활성화할 수 있습니다.

단계 **6** 보류 시간 및 인터페이스 디바운스 시간을 구성합니다.

- 보류 시간—노드 하트비트 상태 메시지 사이의 시간을 결정하는 보류 시간을 0.3초에서 45초 사이로 설정합니다. 기본값은 3초입니다.
- **Interface Debounce Time(**인터페이스 디바운스 시간**)**—디바운스 시간을 300~9000밀리초 범위에서 설정합니다. 기본값은 500ms입니다. 값이 낮을수록 인터페이스 오류 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 노드가 클러스터에서 제거되기 전에 노드는 지정되어 있는 밀리초 동안 대기합니다. 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 노드가 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 노드에서 실패한 것으로 표시되는 것을 방지할 수 있습니다.

단계 **7** 상태 검사에 실패한 후에 자동 다시 참가 클러스터 설정을 맞춤화합니다.

그림 ***47:*** 자동 재연결 설정 구성

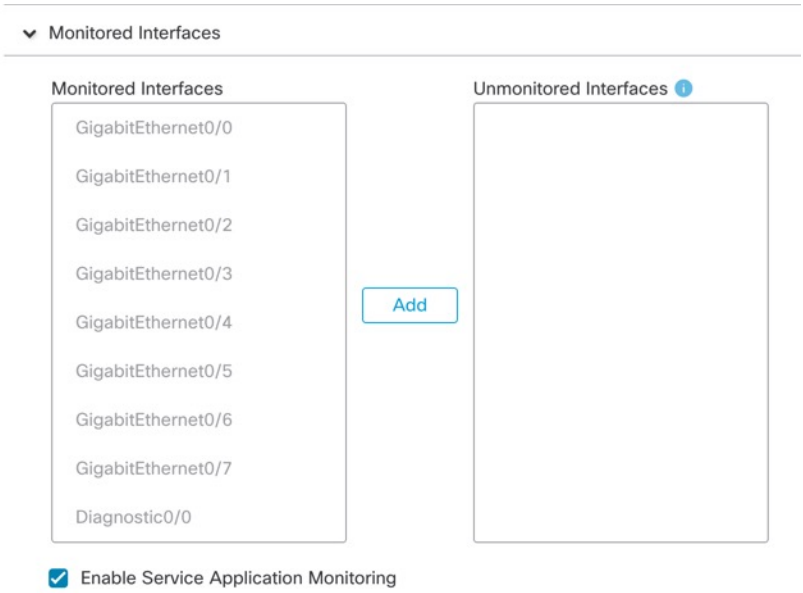


Cluster Interface(클러스터 인터페이스**)**, **Data Interface(**데이터 인터페이스**)** 및 **System(**시스템**)**에 대해 다음 값을 설정합니다(내부 장애에는 애플리케이션 동기화 시간 초과, 일관되지 않은 애플리케이션 상태 등이 포함됨).

- **Attempts(**시도 횟수**)** — 다시 참가 시도 횟수를 -1~65535 범위에서 설정합니다. **0**은 자동 다시 참가를 비활성화합니다. **Cluster Interface(**클러스터 인터페이스**)**의 기본값은 -1(무제한)입니다. **Data Interface(**데이터 인터페이스**)** 및 **System(**시스템**)**의 기본값은 3입니다.
- **Interval Between Attempts(**시도 간의 간격**)**—다시 참가 시도 간의 간격 기간(분)을 2~60분 사이로 정의합니다. 기본값은 5분입니다. 노드가 클러스터에 다시 조인하려고 시도하는 최대 총 시간은 마지막 장애 시간으로부터 14400분(10일)으로 제한됩니다.
- **Interval Variation(**간격 변동**)**—간격 기간이 증가하는지 여부를 정의합니다. 1~3 사이의 값 설정: **1**(변경 없음), **2**(2 x 이전 기간) 또는 **3**(3 x 이전 기간)입니다. 예를 들어, 간격 기간을 5분으로 설정하고 변수를 2로 설정하면 첫 번째 시도가 5분 후에 일어나고 두 번째 시도는 10분(2 x 5), 세 번째 시도는 20분(2 x 10) 후에 일어납니다. 기본값은 **Cluster Interface(**클러스터 인터페이스**)**의 경우 **1**이고 **Data Interface(**데이터 인터페이스**)** 및 **System(**시스템**)**의 경우 **2**입니다.

단계 **8** **Monitored Interfaces(**모니터링된 인터페이스**)** 또는 **Unmonitored Interfaces(**모니터링되지 않는 인터페이스**)** 창에서 인터페이스를 이동하여 모니터링되는 인터페이스를 구성합니다. 또한 **Enable Service Application Monitoring(**서비스 애플리케이션 모니터링 활성화**)**을 선택하거나 선택 취소하여 Snort 및 디스크 꽉 찬 프로세스의 모니터링을 활성화하거나 비활성화할 수 있습니다.

그림 **48:** 모니터링되는 인터페이스 구성



인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 노드에서 오류가 발생했지만 다른 노드에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 노드는 클러스터에서 제거됩니다. 노드에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 노드가 설정된 노드인지 또는 클러스터에 참가하는지에 따라 달라집니다. 상태 검사는 모든 인터페이스와 Snort 및 디스크 풀 프로세스에 대해 기본적으로 활성화됩니다.

필수가 아닌 인터페이스(예: 진단 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, 노드 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 시스템 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 노드와 동기화되면 시스템 상태 검사 기능 및 모니터링되는 인터페이스를 다시 활성화할 수 있습니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

단계 **10** 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

디바이스의 관리자 변경

다음과 같은 상황에서는 디바이스에서 관리자를 변경해야 할 수 있습니다.

- 디바이스의 Management Center IP 주소 또는 호스트네임 편집, 92 페이지 - FMC IP 주소 또는 호스트네임을 변경하는 경우, 디바이스의 새 IP 주소 또는 호스트네임과 일치하는 것이 좋습니다.

- 신규 Management Center 식별, 93 페이지- 이전 FMC에서 디바이스가 있다면 이를 삭제한 후 새 FMC에 대해 디바이스를 구성한 다음 FMC에 추가할 수 있습니다.
- Device Manager에서 Management Center 전환, 94 페이지- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FDM에서 FMC로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.
- Management Center에서 Device Manager로 전환, 99 페이지- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FMC에서 FDM으로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.

디바이스의 **Management Center IP** 주소 또는 호스트네임 편집

management center IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 management center IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 management center에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 management center IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다

프로시저

단계 **1** threat defense CLI에서 management center 식별자를 확인합니다.

show managers

예제**:**

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

단계 **2** threat defense CLI에서 management center IP 주소 또는 호스트네임을 편집합니다.

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

management center가 원래 **DONTRESOLVE** 및 NAT ID로 식별된 경우 이 명령을 사용하여 값을 호스트네임 또는 IP 주소로 변경할 수 있습니다. IP 주소 또는 호스트네임은 **DONTRESOLVE**으로 변경할 수 없습니다.

관리 연결이 중단된 다음 다시 설정됩니다. **sftunnel-status** 명령을 사용하여 연결 상태를 모니터링할 수 있습니다.

예제**:**

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

신규 Management Center 식별

이 절차에서는 매니지드 디바이스의 새 management center를 식별하는 방법을 보여줍니다. 새 management center에서 이전 management center의 IP 주소를 사용하는 경우에도 이러한 단계를 수행해야 합니다.

프로시저

단계 **1** 기존 management center에서 매니지드 디바이스를 삭제합니다. Management Center에서 디바이스 삭제(등록 해제), 31 페이지의 내용을 참조하십시오.

management center와의 활성 연결이 있는 경우 management center IP 주소를 변경할 수 없습니다.

단계 **2** 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 **3** 새 management center를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—management center 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE**—management center에서 주소를 직접 지정할 수없는 경우 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다. 이 디바이스를 management center에 추가할 때는 디바이스 IP 주소와 *nat_id*를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.
- *regkey*—등록 시 management center와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. threat defense를 추가하는 경우 management center에 동일한 키를 입력합니다.
- *nat_id* - management center와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. threat defense를 추가할 때 management center에 동일한 NAT ID를 지정합니다.
- *display_name* — **show managers** 명령과 함께 이 관리자를 표시하기 위한 표시 이름을 제공합니다. 이 옵션은 CDO를 기본 관리자 및 분석 전용 management center 온프레미스로 식별하는 경우 유용합니다. 이 인수를 지정하지 않으면 방화벽은 다음 방법 중 하나를 사용하여 표시 이름을 자동으로 생성합니다.

- *hostname* | *IP_address*(**DONTRESOLVE** 키워드를 사용하지 않는 경우)
- **manager-***timestamp*

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

단계 **4** management center에 디바이스를 추가합니다. Management Center에 디바이스 추가 , 27 페이지의 내용을 참조하십시오.

Device Manager에서 Management Center 전환

device manager에서 management center로 전환하면 관리 인터페이스 및 관리자 액세스 설정 외에 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 구성 설정은 유지되지 않습니다.

management center로 전환한 후에는 더 이상 device manager를 사용하여 threat defense 디바이스를 관리할 수 없습니다.

시작하기 전에

방화벽이 고가용성으로 구성된 경우에는 먼저 device manager(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 구성을 해제해야 합니다. 액티브 유닛에서 고가용성을 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** device manager에서 Cisco Smart Software Manager에서 디바이스의 등록을 취소합니다.

단계 **2** (필요할 수 있음) 관리 인터페이스를 구성합니다.

관리자 액세스에 데이터 인터페이스를 사용하려는 경우에도 관리 인터페이스 구성을 변경해야 할 수 있습니다. device manager 연결을 위해 관리 인터페이스를 사용하는 경우 device manager에 다시 연결해야 합니다.

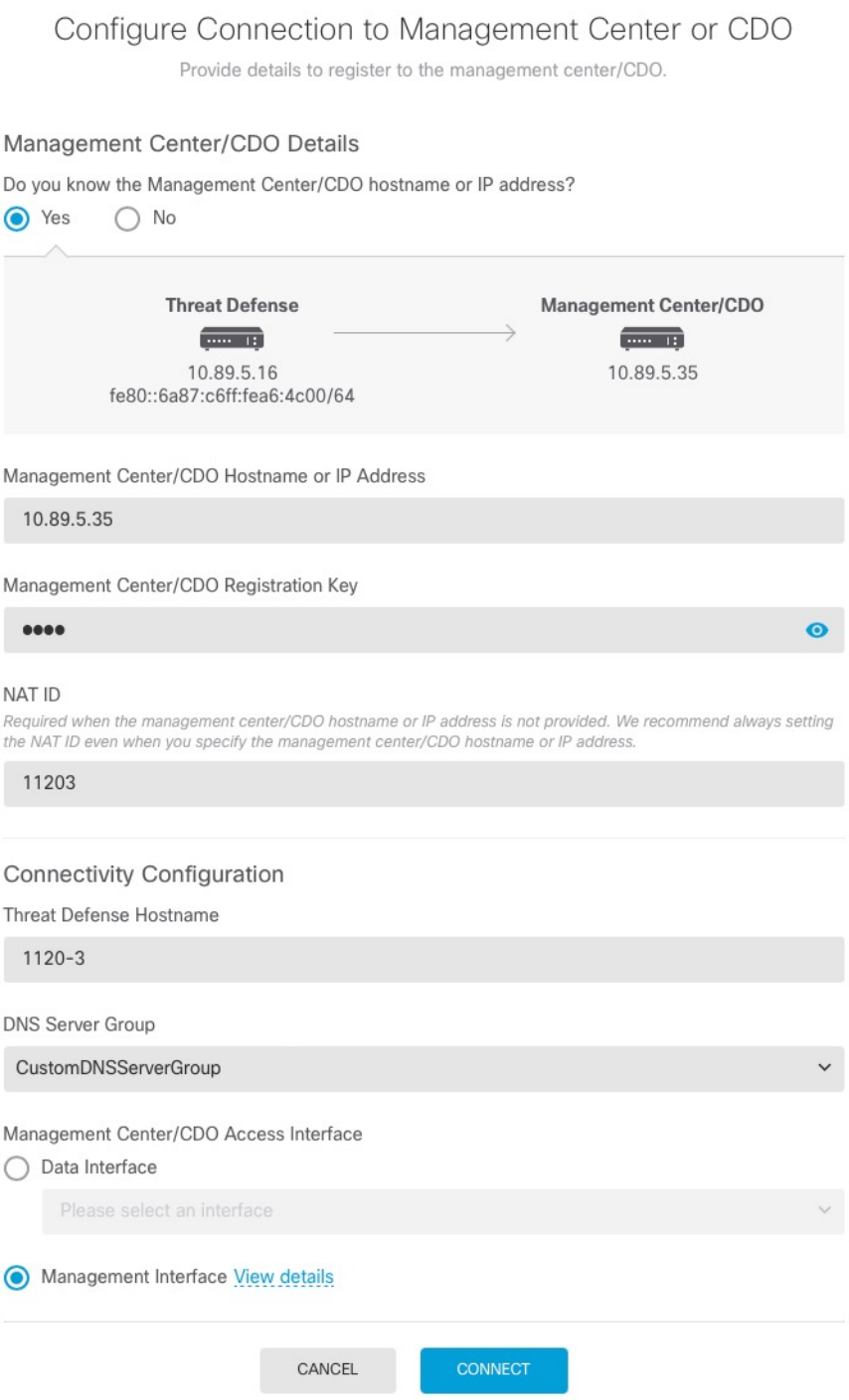
- 관리자 액세스용 데이터 인터페이스 - 관리 인터페이스에 데이터 인터페이스로 설정된 게이트웨이가 있어야 합니다. 기본적으로 관리 인터페이스는 DHCP에서 IP 주소 및 게이트웨이를 수신합니다. DHCP에서 게이트웨이를 수신하지 못한 경우(예: 이 인터페이스를 네트워크에 연결하지 않은 경우) 게이트웨이는 기본적으로 데이터 인터페이스로 설정되며, 아무것도 구성할 필요가 없습니다. DHCP에서 게이트웨이를 수신한 경우 대신 고정 IP 주소로 이 인터페이스를 구성하고 게이트웨이를 데이터 인터페이스로 설정해야 합니다.

- 관리자 액세스용 관리 인터페이스 - 고정 IP 주소를 구성하려면 기본 게이트웨이도 데이터 인터페이스 대신 고유한 게이트웨이로 설정해야 합니다. DHCP를 사용하는 경우 DHCP에서 게이트웨이를 성공적으로 가져오면 어떤 것도 구성할 필요가 없습니다.

단계 **3** **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Central Management(**중앙 관리**)**를 선택하고 **Proceed(**계속**)**을 눌러 management center 관리를 설정합니다.

단계 **4** **Management Center/CDO Details(**관리 센터**/CDO** 세부 정보**)**를 구성합니다.

그림 *49: Management Center/CDO* 세부 정보



a) **Do you know the Management Center/CDO hostname or IP address(**관리 센터**/CDO** 호스트 이름 또는 **IP** 주소를 알고 있습니까**)**에 대해 IP 주소 또는 호스트 이름을 사용하여 management center에 도달할 수 있으면 **Yes(**예**)**를, management center에 퍼블릭 IP 주소 또는 호스트 이름이 없거나 NAT 뒤에 있는 경우 **No(**아니요**)**를 클릭합니다.

하나 이상의 디바이스(management center 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다.

b) **Yes(**예**)**를 선택한 경우 **Management Center/CDO Hostname/IP Address(**관리 센터**/CDO** 호스트 이름**/IP** 주소**)**를 입력합니다.

c) **Management Center/CDO Registration Key(**관리 센터**/CDO** 등록 키**)**를 지정합니다.

threat defense 디바이스 등록 시에 management center에서 지정할 일회용 등록 키입니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 여러 디바이스에 사용할 수 있습니다.

d) **NAT ID**를 지정합니다.

이 ID는 management center에서 지정할 고유한 일회성 문자열을 지정합니다. 이 필드는 디바이스 중 하나의 IP 주소만 지정하는 경우 입력해야 합니다. 두 디바이스의 IP 주소를 모두 알고 있는 경우에도 NAT ID를 지정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다. NAT ID는 연결이 올바른 디바이스에서 오는지 확인하기 위해 IP 주소와 함께 사용됩니다. IP 주소/NAT ID 인증 후에만 등록 키가 확인됩니다.

단계 **5** 연결성 설정을 구성합니다.

a) **FTD** 호스트 이름을 지정합니다.

Management Center/CDO Access Interface 액세스를 위해 데이터 인터페이스를 사용하는 경우 이 FQDN이 이 인터페이스에 사용됩니다.

b) **DNS** 서버 그룹을 지정합니다.

기존 그룹을 선택하거나 새로 생성합니다. 기본 DNS 그룹은 **CiscoUmbrellaDNSServerGroup**이며, 여기에는 OpenDNS 서버가 포함됩니다.

관리 센터**/CDO** 액세스 인터페이스에 대한 데이터 인터페이스를 선택하려는 경우 이 설정은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 마법사를 사용하여 설정하는 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다. 관리 및 데이터 트래픽이 모두 외부 인터페이스를 통해 DNS 서버에 연결되므로 관리에 사용한 것과 동일한 DNS 서버 그룹을 선택할 수 있습니다.

management center에서 이 threat defense 디바이스에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center에 threat defense 디바이스를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense 디바이스에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center와 threat defense 디바이스를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center에 의해 유지됩니다.

FMC 액세스 인터페이스용관리 인터페이스를 선택하려는 경우 이 설정은 관리 DNS 서버를 구성합니다.

c) **Management Center/CDO Access Interface(**관리 센터**/CDO** 액세스 인터페이스**)**의 경우 구성된 인터페이스를 선택합니다.

threat defense 디바이스를 management center에 등록한 후 관리자 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.

단계 **6** (선택 사항) 데이터 인터페이스를 선택했는데 외부 인터페이스가 아닌 경우 기본 경로를 추가합니다.

인터페이스를 통과하는 기본 경로가 있는지 확인하라는 메시지가 표시됩니다. 외부를 선택한 경우 설정 마법사의 일부로 이 경로를 이미 구성한 것입니다. 다른 인터페이스를 선택한 경우 management center에 연결하기 전에 기본 경로를 수동으로 구성해야 합니다.

관리 인터페이스를 선택한 경우 이 화면에서 계속 진행하기 전에 게이트웨이를 고유한 게이트웨이로 구성해야 합니다.

단계 **7** (선택 사항) 데이터 인터페이스를 선택한 경우 **Add a Dynamic DNS (DDNS) method(**동적 **DNS(DDNS)** 메서드 추가**)**를 클릭합니다.

DDNS는 management center 의 IP 주소가 변경될 경우 threat defense 디바이스가 FQDN(Fully-Qualified Domain Name)에서 에 연결할 수 있도록 합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)**를 참조하여 DDNS를 구성합니다.

management center에 threat defense 디바이스를 추가하기 전에 DDNS를 구성할 경우 threat defense 디바이스가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 threat defense 디바이스가 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. Threat Defense는 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.

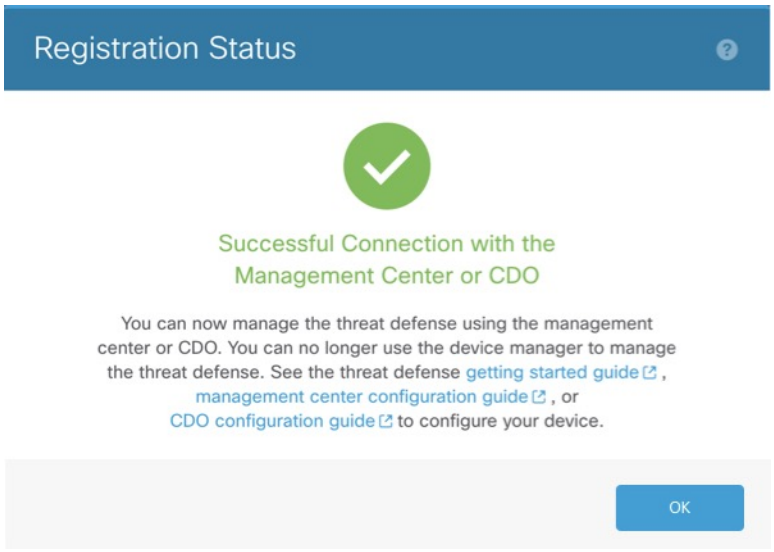
관리자 액세스용 관리 인터페이스를 사용할 때는 DDNS가 지원되지 않습니다.

단계 **8** **Connect(**연결**)**를 클릭합니다. 등록 상태**(Registration Status)** 대화 상자는 management center 전환에 대한 현재 상태를 보여줍니다. **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계에서 management center로 이동하여 방화벽을 추가합니다.

management center에 대한 전환을 취소하려면 **Cancel Registration(**등록 취소**)**을 클릭합니다. 아니면 **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계까지 device manager 브라우저를 닫지 마십시오. 이렇게 하면 프로세스가 일시 중지되며, device manager에 다시 연결할 때만 재개됩니다.

Save Management Center/CDO Registration Settings(관리 센터**/CDO** 등록 설정 저장**)** 단계를 수행한 후 device manager에 연결된 상태로 유지되는 경우, 마지막으로 **Successful Connection with Management Center or CDO(**관리 센터 또는 **CDO**와의 연결 성공**)** 대화 상자가 표시된 뒤 device manager으로부터 연결이 해제됩니다.

그림 50: 연결 성공



Management Center에서 Device Manager로 전환

대신 device manager를 사용하도록 온프레미스 또는 클라우드 제공management center에서 현재 관리 중인 threat defense 디바이스를 구성할 수 있습니다.

소프트웨어를 다시 설치하지 않고 management center에서 device manager로 전환할 수 있습니다. management center에서 device manager로 전환하기 전에 device manager에서 모든 구성 요건을 충족하는지 확인하십시오. device manager에서 management center로 전환하려면 Device Manager에서 Management Center 전환, 94 페이지의 내용을 참조하십시오.

⚠

주의 device manager 전환 시 디바이스 구성이 지워지며 시스템이 기본 구성으로 돌아갑니다. 하지만 관리 IP 주소 및 호스트 이름은 유지됩니다.

프로시저

단계 1 management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 방화벽을 삭제합니다.

단계 2 SSH 또는 콘솔 포트를 사용하여 threat defense CLI에 연결합니다. SSH의 경우 관리 **IP** 주소에 대한 연결을 열고, 관리자 사용자 이름(또는 관리자 권한이 있는 다른 사용자)을 사용하여 threat defense CLI에 로그인합니다.

콘솔 포트는 기본적으로 FXOS CLI를 사용합니다. **connect ftd** 명령을 사용하여 threat defense CLI에 연결합니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. **configure network ipv4/ipv6 manual** 명령을 사용하십시오.

단계 **3** 현재 원격 관리 모드 상태인지 확인합니다.

show managers

예제:

```
> show managers
Type                        : Manager
Host                        : 10.89.5.35
Display name                : 10.89.5.35
Identifier                  : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration                : Completed
```

단계 **4** 원격 관리자를 삭제하고 관리자 없음 모드를 설정합니다.

configure manager delete *uuid*

원격 관리에서 로컬 관리로 직접 이동할 수는 없습니다.둘 이상의 관리자가 정의된 경우 식별자(UUID 라고도 함, **show managers** 명령 참조)를 지정해야 합니다. 각 관리자 항목을 개별적으로 삭제합니다.

예제:

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **5** 로컬 관리자를 구성합니다.

configure manager local

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

예제:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Secure Firewall 3100에서 SSD 핫스왑

SSD 2개를 설치한 경우 부팅 시 RAID를 형성합니다. 방화벽의 전원이 켜져 있는 동안 threat defense CLI에서 다음 작업을 수행할 수 있습니다.

- SSD 중 하나를 핫 스왑 - SSD에 결함이 있는 경우 교체할 수 있습니다. SSD가 하나뿐인 경우 방화벽이 켜져 있는 동안에는 SSD를 제거할 수 없습니다.
- SSD 중 하나 제거 - SSD가 2개인 경우 하나를 제거할 수 있습니다.
- 두 번째 SSD 추가 - SSD가 한 개인 경우 두 번째 SSD를 추가하여 RAID를 구성할 수 있습니다.

⚠

주의 이 절차를 사용하여 RAID에서 SSD를 먼저 분리하지 않은 상태에서 SSD를 분리하지 마십시오. 데이터가 손실될 수 있습니다.

프로시저

단계 **1** SSD 중 하나를 분리합니다.

a) RAID에서 SSD를 분리합니다.

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 키워드는 RAID에서 SSD를 제거하고, 자체 암호화 디스크 기능을 비활성화하며, SSD의 보안 기반 초기화를 수행합니다. RAID에서 SSD만 제거하고 데이터를 그대로 유지하려는 경우 **remove** 키워드를 사용할 수 있습니다.

예제**:**

```
> configure raid remove-secure local-disk 2
```

b) SSD가 인벤토리에 더 이상 표시되지 않을 때까지 RAID 상태를 모니터링합니다.

show raid

SSD가 RAID에서 제거되면 작동성 및 드라이브 상태가 저하됨으로 표시됩니다. 두 번째 드라이브는 더 이상 멤버 디스크로 나열되지 않습니다.

예제**:**

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
```

```
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 섀시에서 SSD를 물리적으로 분리합니다.

단계 **2** SSD를 추가합니다.

a) SSD를 빈 슬롯에 물리적으로 추가합니다.

b) RAID에 SSD를 추가합니다.

configure raid add local-disk {**1** | **2**}

방화벽이 완전히 작동하는 동안 새 SSD를 RAID에 동기화하는 작업을 완료하는 데 몇 시간이 걸릴 수 있습니다. 재부팅해도 전원이 켜지면 동기화가 계속됩니다. **show RAID** 명령을 사용하여 상태를 표시합니다.

이전에 다른 시스템에서 사용된 SSD를 설치했지만 여전히 잠겨 있는 경우 다음 명령을 입력합니다.

configure raid add local-disk {**1** | **2**} *psid*

*PSID*는 SSD 후면에 부착된 레이블에 인쇄되어 있습니다. 또는 시스템을 재부팅할 수 있습니다. 그러면 SSD가 다시 포맷되고 RAID에 추가됩니다.

디바이스 관리 기본 사항 기록

기능	버전	세부정보
클러스터 상태 모니터링 설정	7.3	이제 클러스터 상태 모니터링 설정을 편집할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **Cluster Health Monitor Settings(**클러스터 상태 모니터링 설정**)** 참고 이전에 FlexConfig를 사용하여 이러한 설정을 구성한 경우 구축하기 전에 FlexConfig 구성을 제거해야 합니다. 그렇지 않으면 FlexConfig 구성이 관리 센터 구성을 덮어씁니다.
이중화 관리자 액세스 데이터 인터페이스	7.3	관리자 액세스를 위해 데이터 인터페이스를 사용할 때 기본 인터페이스가 다운될 경우 관리 기능을 수행하도록 보조 데이터 인터페이스를 구성할 수 있습니다. 디바이스는 SLA 모니터링을 사용하여 정적 경로 및 두 인터페이스를 모두 포함하는 ECMP 영역의 실행 가능성을 추적하므로 관리 트래픽이 두 인터페이스를 모두 사용할 수 있습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device** > **(**디바이스**) Management(**관리**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Devices(**디바이스**)** > **Interfaces(**인터페이스**)** > **Manager Access(**관리자 액세스**)**
종료를 위한 ISA 3000 시스템 LED 지원	7.0.5/7.3	ISA 3000을 종료하면 시스템 LED가 꺼집니다. 전원을 제거하기 전에 10초 이상 기다려야 합니다.
종료를 위한 ISA 3000 지원	7.0.2/7.2	이제 ISA 3000을 종료할 수 있습니다. 이전에는 디바이스를 리부팅만 할 수 있었습니다.

기능	버전	세부정보
고가용성을 위한 정책 롤백 지원	7.2	**configure policy rollback** 명령은 고가용성을 위해 지원됩니다.
다중 관리자 지원.	7.2	클라우드 제공 관리 센터를 도입했습니다. 클라우드 제공 관리 센터는 CDO(Cisco Defense Orchestrator) 플랫폼을 사용하며 여러 Cisco 보안 솔루션 전반에서 관리를 통합합니다. Cisco에서 관리자 업데이트를 처리합니다. 버전 7.2 이상을 실행하는 하드웨어 또는 가상 관리 센터는 클라우드 매니지드 디바이스를 "공동 관리"할 수 있지만 이벤트 로깅 및 분석 용도로만 사용됩니다. 하드웨어 또는 가상 관리 센터에서는 이러한 디바이스에 정책을 구축할 수 없습니다. 신규/수정된 threat defense 명령: **configure manager add**, **configure manager delete, configure manager edit** 및 **show managers** 신규/수정된 화면: • 클라우드 매니지드 디바이스를 하드웨어 또는 가상 관리 센터에 추가할 때 새 **CDO Managed Device(CDO** 매니지드 디바이스**)** 확인란을 사용하여 분석 전용으로 지정합니다. • **Devices(**디바이스**) > Device Management(**디바이스 관리**)**에서 분석 전용 디바이스를 확인합니다. 자세한 내용은 CDO 설명서를 참조하십시오.
개체 그룹 검색은 액세스 제어 규칙에 대해 기본적으로 활성화되어 있습니다.	7.2	개체 그룹 검색 설정은 버전 7.2.0부터 매니지드 디바이스에 대해 기본적으로 활성화됩니다. 이 옵션은 **Device Management(**디바이스 관리**)** 페이지에서 디바이스 설정을 편집할 때 **Advanced Settings(**고급 설정**)** 섹션에 있습니다.
관리 연결 손실을 유발하는 구축의 자동 롤백.	7.2	이제 구축으로 인해 관리 센터와 위협 방어 간의 관리 연결이 중단되는 경우 구성의 자동 롤백을 활성화할 수 있습니다. 이전에는 **configure policy rollback** 명령을 사용하여 수동으로만 구성을 롤백할 수 있었습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**장치**)** > **Deployment Settings(**구축 설정**)** • **Deploy(**구축**)** > **Advanced Deploy(**고급 구축**)** > **Preview(**미리 보기**)** • **Deploy(**구축**)** > **Deployment History(**구축 기록**)** > **Preview(**미리 보기**)**
Secure Firewall 3100의 SSD에 대한 RAID 지원.	7.1	SSD는 SED(자체 암호화 드라이브)이며, 2개의 SSD가 있는 경우 소프트웨어 RAID를 구성합니다. 신규/수정된 명령: **configure raid, show raid, show ssd**

기능	버전	세부정보
디바이스 구성 가져오기 및 내보내기	7.1	디바이스별 구성을 내보낸 후 다음과 같은 사용 사례에서 동일한 디바이스에 대해 저장된 구성을 가져올 수 있습니다: • 디바이스를 다른 FMC로 이동. • 기존 구성을 복원합니다. • 디바이스 재등록. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **General(**일반**)**
management center을 통한 threat defense 관리 구성을 위해 device manager를 사용합니다.	7.1.	device manager를 사용하여 초기 설정을 수행할 때 관리를 위해 management center로 전환하면 관리 및 관리자 액세스 설정 외에 device manager에서 완료된 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 기본 구성 설정은 유지되지 않습니다. management center CLI를 사용하는 경우 관리 및 관리자 액세스 설정만 유지됩니다(예: 기본 내부 인터페이스 구성은 유지되지 않음). management center로 전환한 후에는 더 이상 device manager를 사용하여 management center를 관리할 수 없습니다. 신규/수정된 device manager 화면: **System Settings(**시스템 설정**)** > **Management Center(**관리 센터**)**
업그레이드 상태별로 디바이스 필터링	6.7	이제 **Device Management(**디바이스 관리**)** 페이지에서는 디바이스의 업그레이드 여부(및 업그레이드 경로), 최종 업그레이드의 성공 또는 실패 여부 등 매니지드 디바이스에 대한 업그레이드 정보를 제공합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**
threat defense에서 management center IP 주소를 업데이트합니다.	6.7	management center IP 주소를 변경하는 경우 이제 threat defense CLI를 사용하여 디바이스를 업데이트할 수 있습니다. 신규/수정된 threat defense CLI 명령: **configure manager edit**

기능	버전	세부정보
데이터 인터페이스에서 threat defense 관리	6.7	이제 전용 관리 인터페이스를 사용하는 대신 데이터 인터페이스에서 threat defense의 management center 관리를 구성할 수 있습니다. 이 기능은 본사의 management center에서 브랜치 오피스에서 threat defense를 관리하고 외부 인터페이스에서 FTD를 관리해야 하는 경우의 원격 구축에 유용합니다. threat defense가 DHCP를 사용하여 공용 IP 주소를 수신하는 경우, 웹 유형 업데이트 방법을 사용하여 인터페이스에 대한 DDNS(동적 DNS)를 선택적으로 구성할 수 있습니다. DDNS는 threat defense의 IP 주소가 변경될 경우 management center가 FQDN(Fully-Qualified Domain Name)에서 threat defense에 연결할 수 있도록 합니다. 참고 데이터 인터페이스에 대한 management center 액세스는 클러스터링 또는 고가용성에서 지원되지 않습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **FMC Access(FMC** 액세스**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **DHCP** > **DDNS** > **DDNS Update Methods(DDNS** 업데이트 방법**)** 페이지 신규/수정된 threat defense CLI 명령: **configure network management-data-interface**, **configure policy rollback** 지원되는 플랫폼: threat defense
클릭 한 번으로 섀시 관리자에 액세스할 수 있습니다.	6.4	Firepower 4100/9300 시리즈 디바이스의 경우, Device Management(디바이스 관리) 페이지에서는 섀시 관리자 웹 인터페이스로 연결되는 링크를 제공합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**
상태 및 구축 상태별로 디바이스 필터링(버전 정보 보기)	6.2.3	이제 Device Management(디바이스 관리) 페이지에서는 매니지드 디바이스의 버전 정보와 상태 및 구축 상태를 기준으로 디바이스를 필터링하는 기능을 제공합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**

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.