Firepower Threat Defense 인터페이스 개요

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

관리/진단 인터페이스

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

관리 인터페이스

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

관리 인터페이스 대신 데이터 인터페이스를 사용하여 FTD를 관리할 수도 있습니다.

진단 인터페이스

논리적 진단 인터페이스는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** 화면에서 나머지 데이터 인터페이스와 함께 설정할 수 있습니다. 진단 인터페이스 사용은 선택 사항입니다(라우팅 및 투명 모드 구축 시나리오 참조). 진단 인터페이스는 관리 트래픽만 허용

하며 통과 트래픽은 허용하지 않습니다. SSH를 지원하지 않습니다. 데이터 인터페이스 또는 관리 인터페이스 사용 시에만 SSH를 사용할 수 있습니다. 진단 인터페이스는 SNMP 또는 시스템 로그 모니터링에 유용합니다.

인터페이스 모드 및 유형

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

일반 방화벽 모드

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

구성할 수 있는 방화벽 인터페이스의 유형은 디바이스의 방화벽 모드 집합이 라우팅인지 투명 모드인지에 따라 달라집니다. 자세한 내용은 Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드를 참조하십시오.

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

IPS 전용 모드

IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다.

IPS 전용 인터페이스는 다음과 같은 유형으로 구축할 수 있습니다.

- 필요에 따라 탭 모드가 가능한 인라인 집합 - 인라인 집합은 비활성 엔드포인트(bump in the wire)처럼 작동하며 두 인터페이스를 슬롯에 포함해 기존 네트워크에 바인딩합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 설정 없이 네트워크 환경에 FTD를 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

탭 모드에서는 FTD가 인라인으로 구축되지만, 네트워크 트래픽 플로우는 방해받지 않습니다. 대신 FTD는 패킷을 분석할 수 있도록 각 패킷의 복사본을 만듭니다. 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며, 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다. 인라인으로 구축된 FTD에서 탭 모드를 사용하는 데는 몇 가지 이점이 있습니다. 예를 들어, 디바이스가 인라인 상태인 것처럼 FTD와 네트워크 간에 케이블링을 설정할 수 있으며 FTD가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. FTD를 인라인으로 구축할 준비가 되면 FTD와 네트워크 간 케이블링을 다시 설정하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽을 삭제할 수 있습니다.

참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

참고 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 투명 방화벽 모드 또는 방화벽 유형 인터페이스와는 관련이 없습니다.

- 패시브 또는 ERSPAN 패시브 - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용해 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 패시브 구축으로 FTD를 설정한 경우, FTD에서 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며, 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 인터페이스는 여러 스위치를 통해 배포되는 소스 포트의 트래픽을 모니터링하고 GRE를 사용해 트래픽을 캡슐화합니다. ERSPAN 인터페이스는 FTD가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

보안 영역 및 인터페이스 그룹

각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당될 수 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어, "내부" 인터페이스는 "내부" 영역에, "외부" 인터페이스는 "외부" 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 인터페이스 또는 영역 이름 자체는 보안 정책과 관련하여 기본 동작을 제공하지 않습니다. 향후 설정에서 실수를 방지하려면 자체 설명 이름을 사용하는 것이 좋습니다. 올바른 이름은 논리적 세그먼트 또는 트래픽 사양을 나타냅니다. 예를 들면 다음과 같습니다.

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

일부 정책은 보안 영역만 지원하고 일부 정책은 영역 및 그룹을 지원합니다. 자세한 내용은 보안 영역.를 참조하십시오. 개체 페이지에서 보안 영역 및 인터페이스 그룹을 생성할 수 있습니다. 인터페이스를 구성하는 경우 영역을 추가할 수 있습니다. 패시브, 인라인, 라우팅, 스위치 영역 유형 등 인터페이스의 올바른 영역 유형에만 인터페이스를 추가할 수 있습니다.

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

진단/관리 인터페이스는 영역 또는 인터페이스 그룹에 속하지 않습니다.

Auto-MDI/MDIX 기능

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

인터페이스의 기본 설정

이 섹션에서는 인터페이스에 대한 기본 설정이 나열됩니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형에 따라 다릅니다.

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

기본 속도와 양방향

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

물리적 인터페이스 활성화 및 이더넷 설정

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화 기본적으로 물리적 인터페이스는 비활성화됩니다(진단 인터페이스의 경우는 제외).
- 특성 속도 및 양방향 설정 기본적으로 속도 및 양방향은 자동으로 설정되어 있습니다.

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

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

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

시작하기 전에

FMC에 추가한 후 디바이스의 물리적 인터페이스를 변경한 경우, **Interfaces(**인터페이스**)**의 왼쪽 상단에 있는 **Sync Interfaces from device(**디바이스의 인터페이스 동기화**)**를 클릭하여 인터페이스 목록을 새로 고쳐야 합니다.

프로시저

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

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

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

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

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** (선택 사항) **Hardware Configuration(**하드웨어 설정**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**)** - **Auto(**자동**)**를 선택하여 인터페이스가 듀플렉스를 협상하도록 하거나(Auto(자동)는 RJ-45 인터페이스에서만 사용 가능) 특정 **Half(**하프**)**, **Full(**풀**)** 듀플렉스를 선택합니다.
- **Speed(**속도**)** — **Auto(**자동**)**를 선택하여 인터페이스가 속도를 협상하도록 하거나(Auto(자동)는 RJ-45 인터페이스에서만 사용 가능), **10**, **100**, **1000**, **10000**Mbps 중에서 특정 속도를 선택합니다. SFP 인터페이스의 경우, 하드웨어에 따라 **No Negotiate(**협상 없음**)**를 선택하여 속도를 1000으로 설정하고 링크 협상을 비활성화할 수 있습니다.

단계 **6** 모드 드롭다운 목록에서 다음을 선택합니다.

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

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

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

Firepower Management Center를 사용한 동기화 인터페이스 변경

디바이스의 인터페이스 설정 변경은 FMC과 디바이스의 동기화 오류를 발생시킬 수 있습니다. FMC은 다음 방법 중 하나로 인터페이스 변경을 탐지할 수 있습니다.

- 디바이스에서 전송된 이벤트
- 에서 구축할 때 동기화 FMC

  FMC이 구축을 시도하지만 실패하는 경우 인터페이스 변경 사항을 탐지합니다. 먼저 인터페이스 변경 사항을 적용해야 합니다.

- 수동 동기화

FMC 외부에서 수행되는 두 가지 유형의 인터페이스 변경은 동기화되어야 합니다.

- 물리적 인터페이스 추가 또는 삭제 - 새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 FTD 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 FTD 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않

습니다. 논리적 디바이스에 영향을 주거나 FMC에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

FMC가 변경 사항을 탐지하는 경우 인터페이스 페이지는 각 인터페이스 왼쪽에 상태(제거, 변경, 추가)를 표시합니다.

- FMC 액세스 인터페이스 변경 - **configure network management-data-interface** 명령을 사용하여 FMC 관리용 데이터 인터페이스를 구성하는 경우 FMC에서 일치하는 구성 변경을 수동으로 수행한 다음 변경을 승인해야 합니다. 이러한 인터페이스 변경은 자동으로 수행할 수 없습니다.

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

시작하기 전에

- 모델 지원—FTD
- 사용자 역할:
  - 관리자
  - 액세스 관리자
  - Network Admin(네트워크 관리자)

프로시저

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

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

단계 **3** 변경 사항이 탐지되면 다음 단계를 참조하십시오.

물리적 인터페이스 추가 또는 삭제

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

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

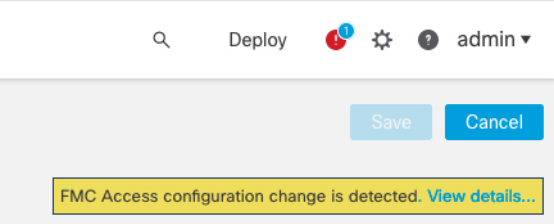
오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

c) **Save(**저장**)**를 클릭합니다.

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

FMC 액세스 인터페이스 변경

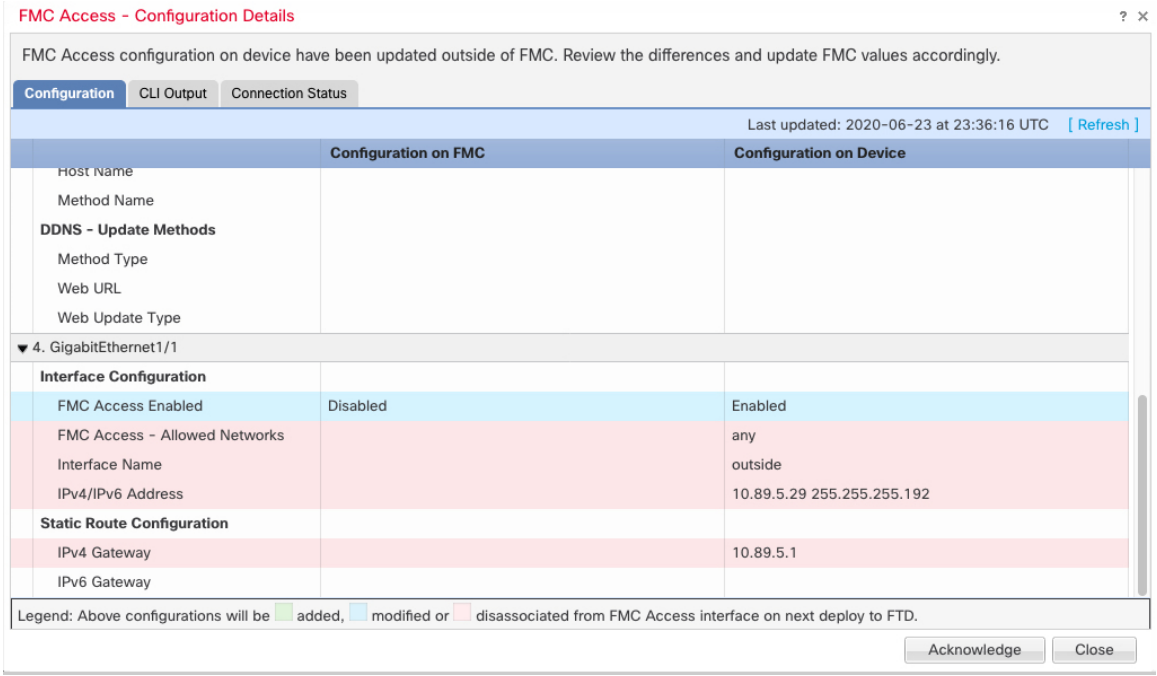
a) **Device(**디바이스**)** 페이지의 오른쪽 상단에 FMC 액세스 구성이 변경되었음을 나타내는 노란색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 세부 정보 보기 링크를 클릭합니다.



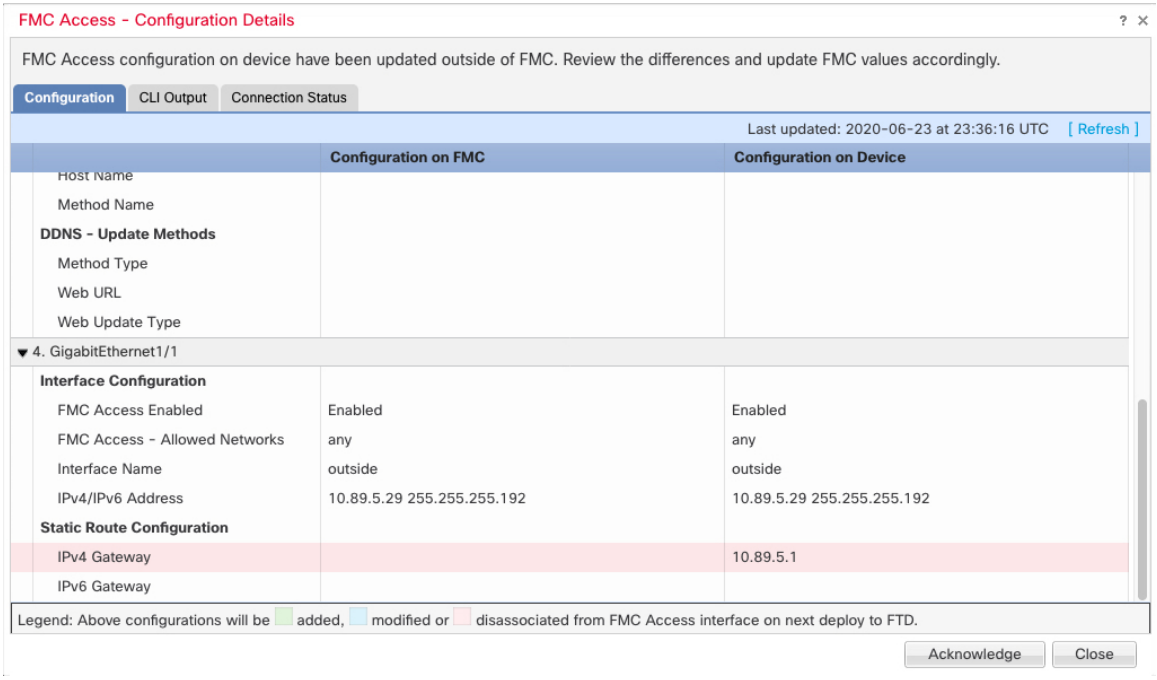
FMC Access - Configuration Details(FMC 액세스 - 구성 세부 정보**)** 대화 상자가 열립니다.

b) 강조 표시된 모든 구성, 특히 빨간색으로 강조 표시된 구성을 확인합니다. FMC에서 수동으로 값을 구성하여 FTD의 값을 일치시켜야 합니다.

예를 들어 아래의 분홍색 강조 표시는 FTD에는 있지만 아직 FMC에는 없는 구성을 보여줍니다.



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



c) **Acknowledge(**승인**)**를 클릭합니다.

FMC 구성을 완료하고 구축 준비가 완료될 때까지 **Acknowledge(**승인**)**를 클릭하지 않는 것이 좋습니다. **Acknowledge(**승인**)**를 클릭하면 구축시 차단이 제거됩니다. 다음에 구축할 때 FMC 컨피그레이션은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 컨피그레이션을 수동으로 수정하는 것은 사용자의 책임입니다.

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