FTD의 다중 도메인 환경에서의 상속

목차

소개

이 문서에서는 상속 및 다중 도메인 기능의 구성 및 작업에 대해 설명합니다. 또한 이 두 기능이 어떻게 연동되는지 확인하기 위한 실제 활용 사례에 중점을 둡니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- FMC(Firepower Management Center)
- FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMC(Firepower Management Center) 소프트웨어 버전 6.4
- FTD(Firepower Threat Defense) 소프트웨어 버전 6.4

참고:다중 도메인 및 상속 기능은 FMC/FTD에서 6.0 버전부터 지원됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 컨피그레이션의 잠재적인 영향을 이해해야 합니다.

배경 정보

정책 상속에서 액세스 제어 정책은 하위 정책이 보안 인텔리전스, HTTP 응답, 로깅 설정 등과 같은 ACP 설정을 비롯한 기본 정책에서 규칙을 상속받는 방식으로 중첩될 수 있습니다. 선택적으로 관리자는 하위 정책이 보안 인텔리전스, HTTP 응답, 로깅 설정 등의 ACP 설정을 재정의하도록 허용하거나 하위 정책이 재정의할 수 없도록 설정을 잠글 수 있습니다.이 기능은 다중 도메인 FMC 환경에서 매우 유용합니다.

다중 도메인 기능은 FMC의 관리되는 디바이스, 컨피그레이션 및 이벤트에 대한 사용자 액세스를 분할합니다.사용자는 권한에 따라 다른 도메인으로 전환/액세스할 수 있습니다.다중 도메인 기능이 구성되지 않은 경우 모든 관리되는 디바이스, 컨피그레이션 및 이벤트가 **전역** 도메인에 속합니다.

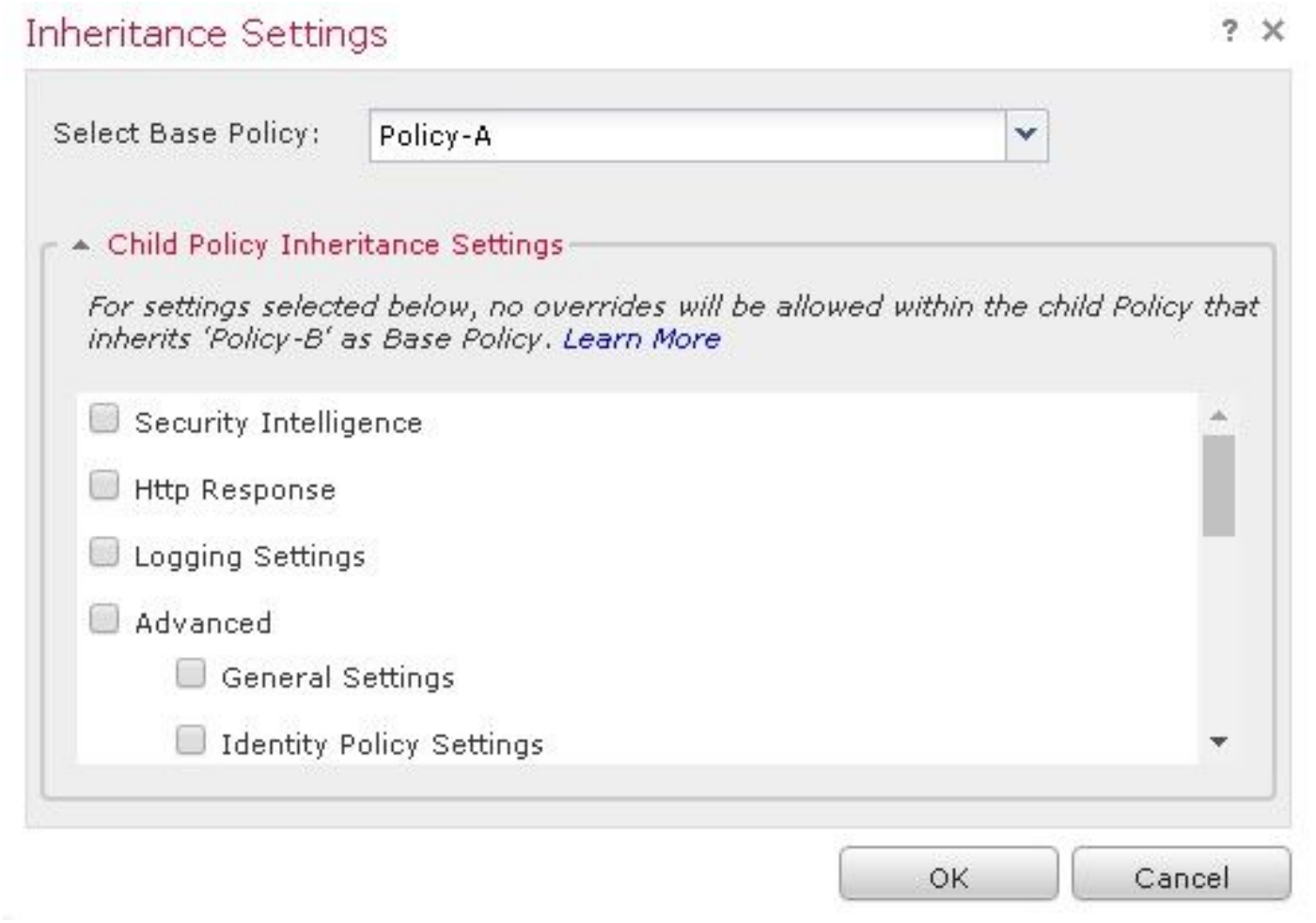
정책 상속 구성

리프 도메인은 추가 하위 도메인이 없는 도메인입니다.하위 도메인은 사용자/관리자가 현재 있는 도메인의 다음 수준 하위 도메인입니다.상위 도메인은 사용자/관리자가 현재 있는 도메인의 직접 상위 도메인입니다.

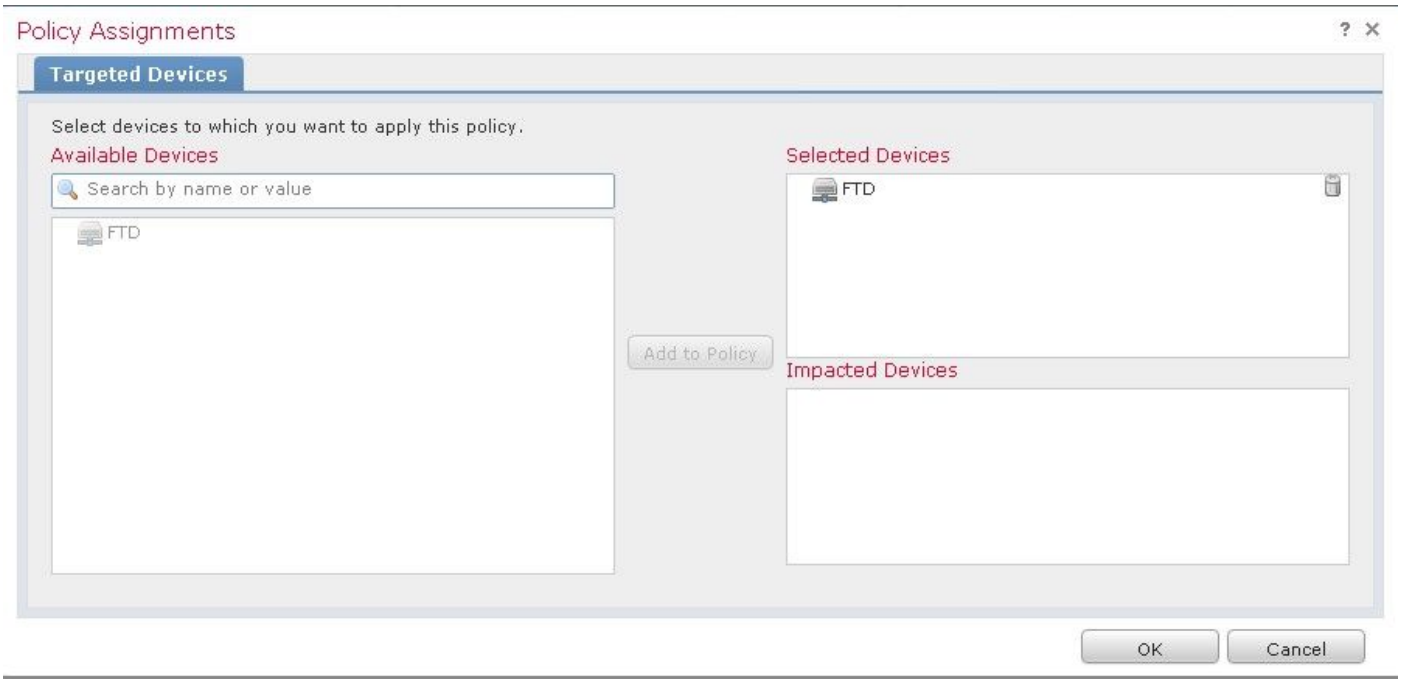
존재하는 정책에 대한 상속을 구성/활성화하려면

1. Policy-A가 기본 정책이 되고 Policy-B가 하위 정책이 되도록 합니다(Policy-B는 Policy-A에서 규칙을 상속).
2. **EDIT** Policy-B(정책-B 수정)를 클릭하고 이미지에 표시된 대로 Inheritance Settings(상속 설정)를 클릭합니다.

3. 아래 표시된 **Select Base Policy** 드롭다운 목록에서 Policy-A를 선택합니다.보안 인텔리전스, HTTP 응답, 로깅 설정 등의 기타 ACP 설정은 선택적으로 하위 정책의 설정을 재정의하기 위해 상속될 수 있습니다.

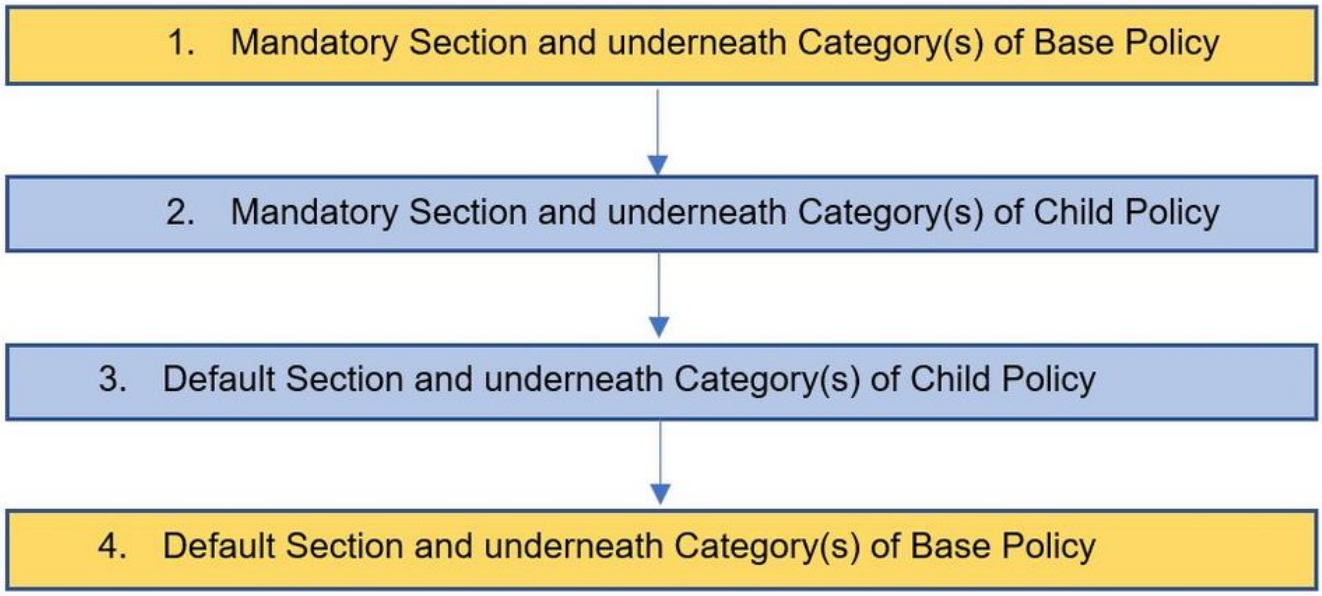


4. 대상 FTD 디바이스에 대해 하위 정책 Policy-B에 대한 **정책** 할당을 수행합니다.

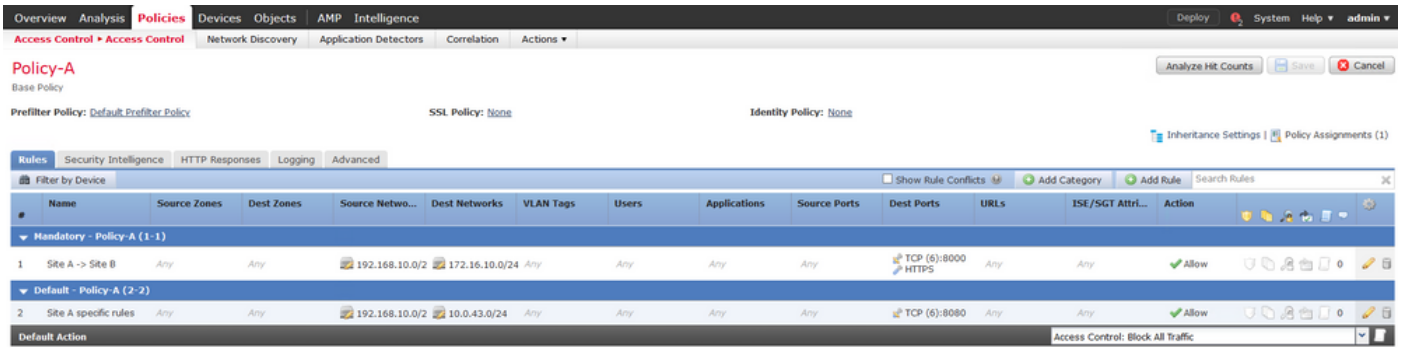


기본적으로 **Default Action** of Child Policy는 상속되고 이미지에 표시된 대로 **Inherit from base policy**로 설정됩니다.또한 사용자는 여기와 같이 시스템 제공 정책에서 **기본 작업**을 선택할 수 있습니다.

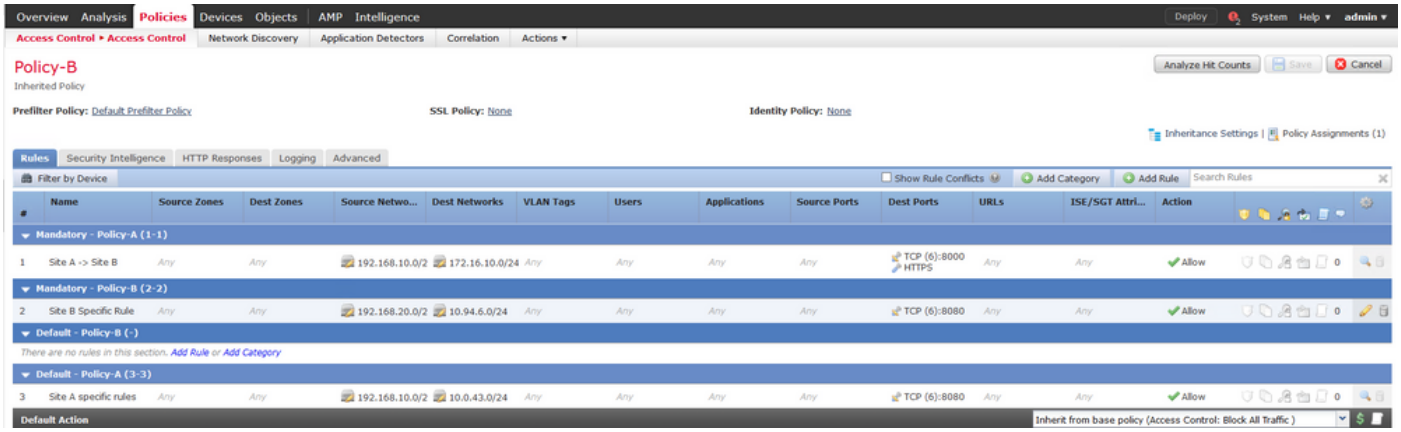
트래픽에 대한 조회 순서는 Mandatory(필수) 및 Default(기본) 섹션에 추가된 카테고리 수에 관계없이 항상 하향식 방식으로 유지됩니다.상속 **설정**을 적용한 후 이미지에 표시된 대로 하위 정책 Policy-B(하위 정책)에 대한 ACP 표현을 앞에서 설명한 **규칙 확인 순서**와 일치시킵니다.



이 이미지는 기본 정책인 Policy-A와 하위 정책인 Policy-B를 모두 FMC에 표시하는 방법을 보여줍니다.



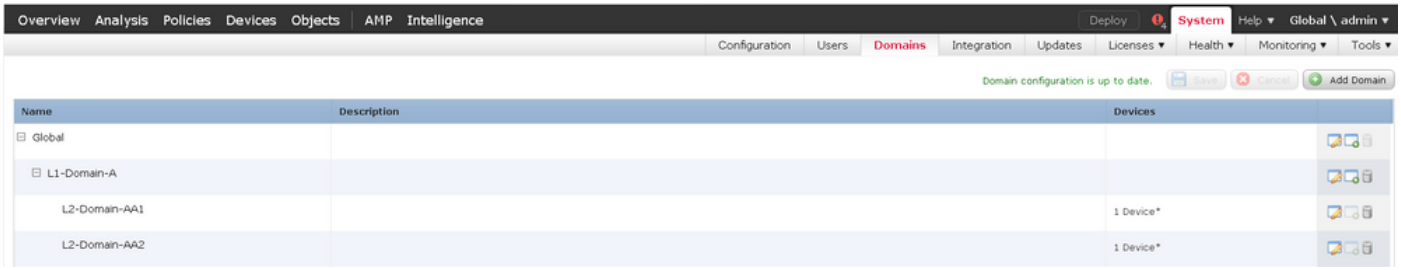
이 이미지는 Policy-B에서 Policy-A의 규칙은 물론 Policy-B 자체에 구성된 특정 규칙을 볼 수 있음을 보여줍니다.규칙의 구성 방법에 대해 주문을 염두에 두어야 합니다.



다중 도메인 FMC 환경의 FTD 관리

다중 도메인 기능은 관리되는 디바이스, 컨피그레이션 및 이벤트에 대한 사용자 액세스를 분할합니다.사용자는 권한에 따라 다른 도메인으로 전환할 수 있습니다.다중 도메인 기능이 구성되지 않은 경우 모든 관리되는 디바이스, 컨피그레이션 및 이벤트가 **전역** 도메인에 속합니다.

최대 3개 수준의 도메인은 레벨 1로 전역 도메인으로 구성할 수 있습니다. 모든 관리되는 디바이스는 리프 도메인에만 속해야 합니다.이는  (Add Sub Domain)은 이미지에 표시된 대로 리프 도메인에서 회색으로 표시됩니다.



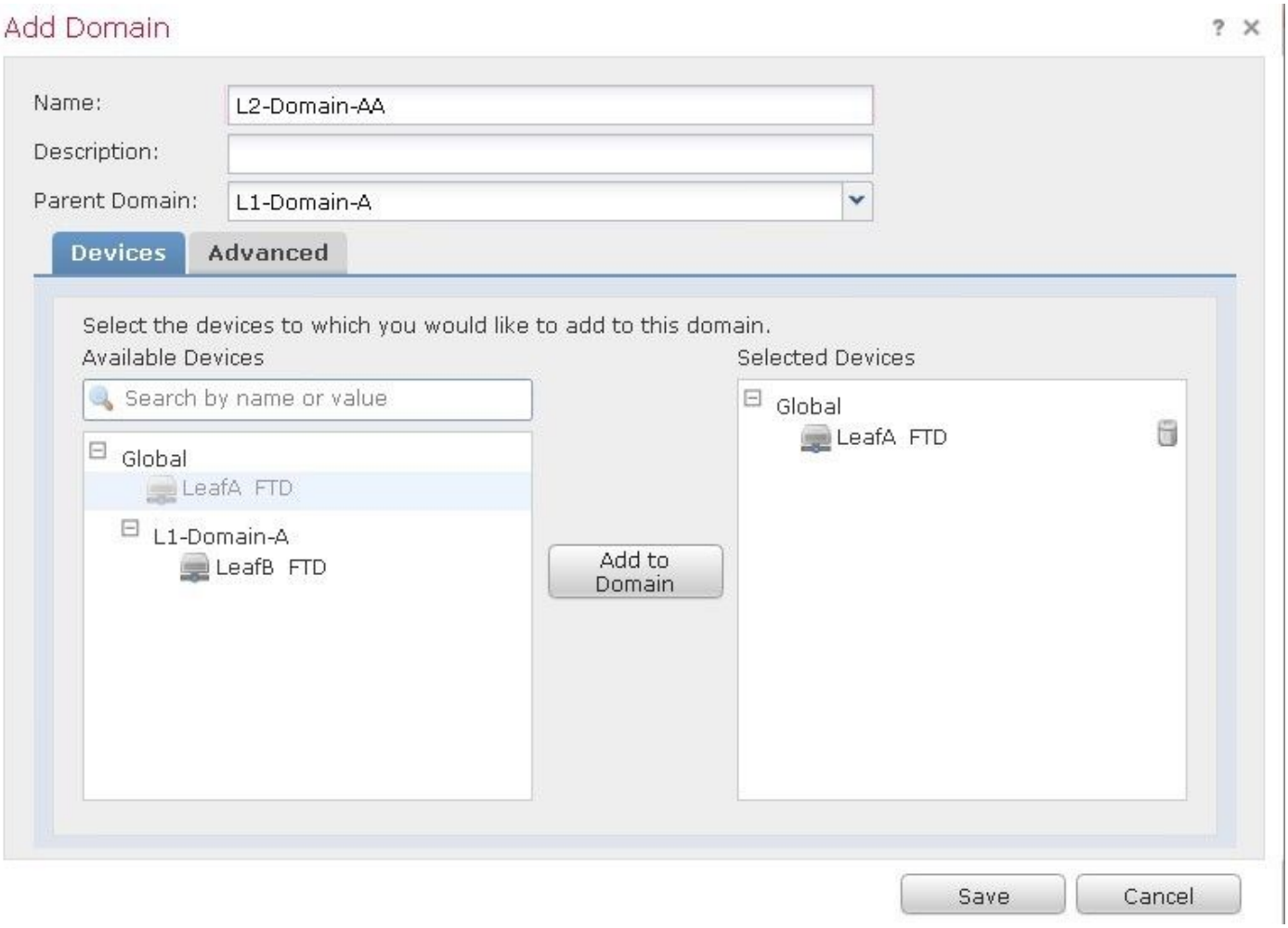
도메인 구성

도메인 컨피그레이션은 다음과 같이 수행할 수 있습니다.

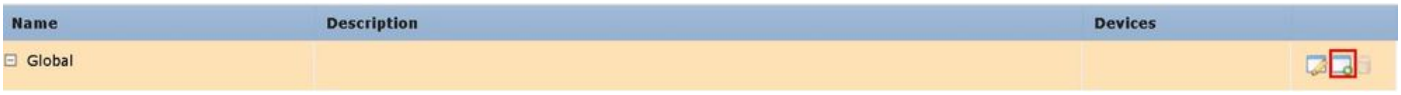
1. System(**시스템) > Domains(도메인)로 이동합니다**.기본적으로 **전역** 도메인이 있습니다.

2. 이미지에 표시된 대로 **Add Domain(도메인 추가)**을 클릭합니다.

3. Add **Domain** 대화 상자가 나타납니다.도메인 **이름**을 입력하고 **Parent Domain** from 드롭다운 목록을 선택합니다.리프 도메인인 경우 이미지에 표시된 대로 FTD 디바이스를 도메인에 추가해야 합니다.

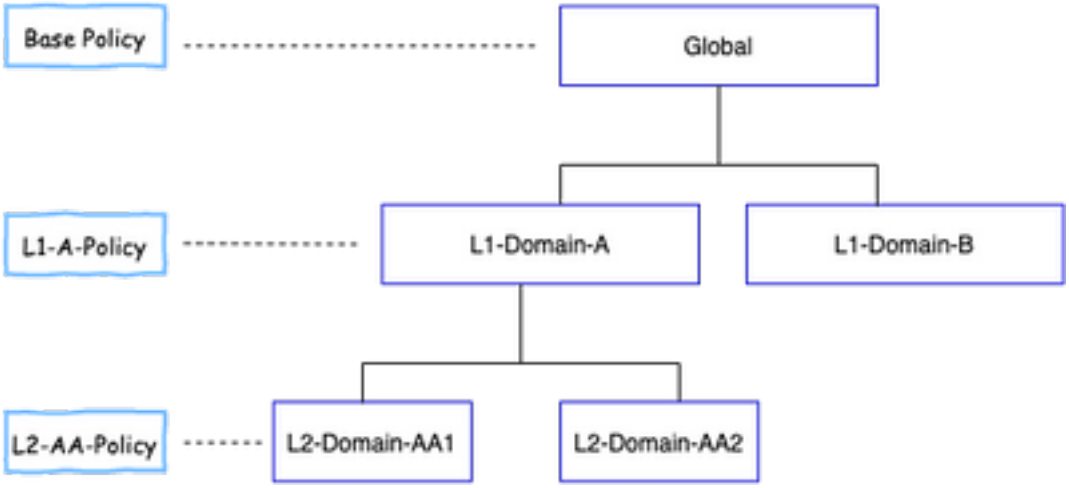


참고:도메인을 추가하려면 이미지에 표시된 대로 **Add Sub Domain**(하위 도메인 추가) 아이콘을 클릭합니다.상위 도메인이 이미 선택되어 있습니다.



다중 도메인 FMC 환경의 정책 가시성 및 제어

정책 가시성 및 제어는 **전역** 도메인 관리자를 제외한 각 도메인 사용자로 제한됩니다.이 예는 다음과 같이 계층을 기반으로 합니다.



가시성:이 이미지에 표시된 대로 기본 보기 **정책** 페이지에는 각 도메인 아래에 구성된 ACP(정책)가 나열됩니다.

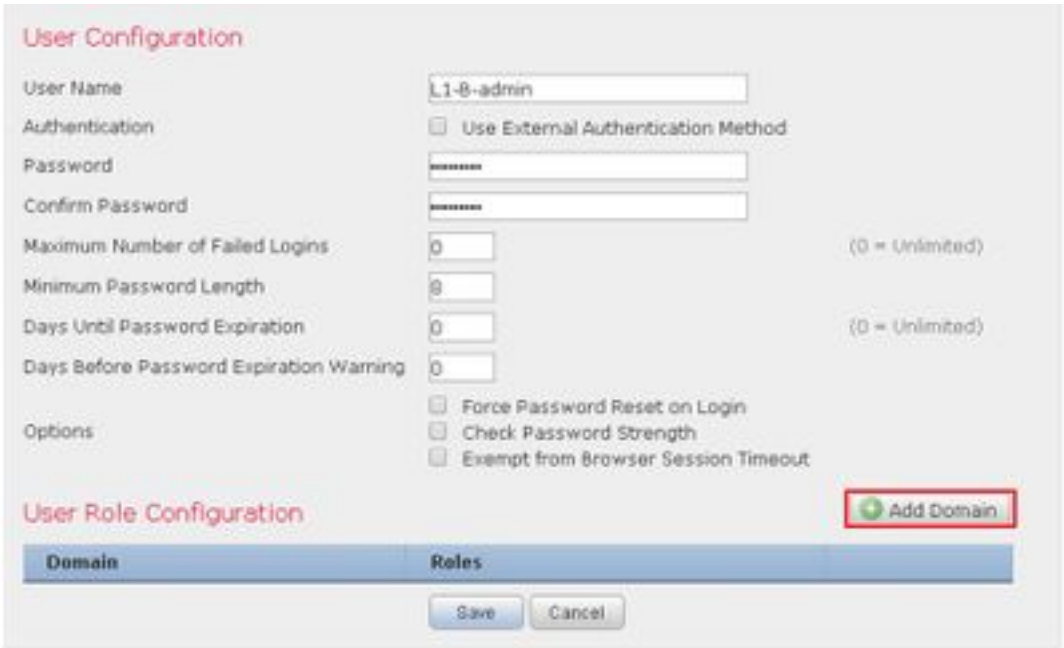
제어:각 도메인에 속한 관리자 사용자는 정책을 수정할 수 있습니다.상속의 일부로 다른 도메인에 속하는 정책을 수정하려면 도메인을 현재 도메인에서 정책이 구성된 도메인으로 전환해야 합니다 .**전역** 도메인 또는 L1 도메인에 속한 Admin 사용자만 정책 관리를 위해 하위 도메인을 전환할 수 있습니다.

도메인에 사용자 추가

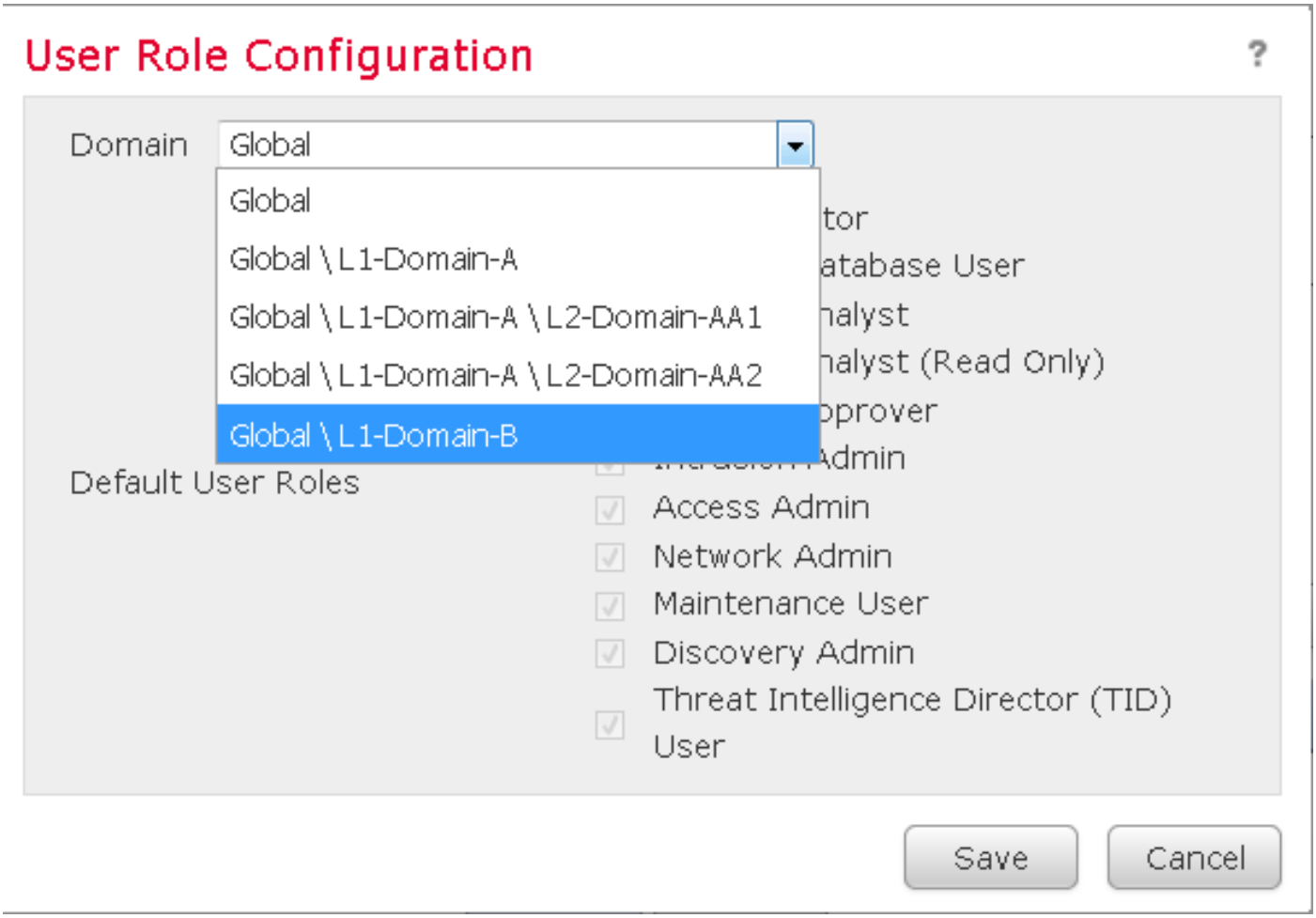
특정 도메인의 사용자를 추가하는 방법을 보여 줍니다.이 절차는 로컬 데이터베이스의 사용자에게 적용됩니다.

1. System(**시스템) >Users(사용자)로 이동합니다**.이미지에 표시된 대로 **Create User(사용자 생성)**를 클릭합니다.

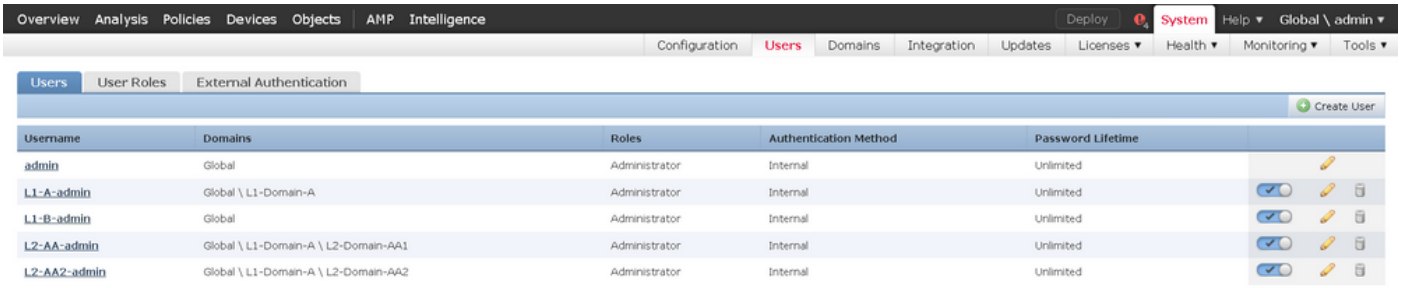
2. **User** Configuration 대화 상자가 나타납니다.**사용자 이름**과 **비밀번호(& 비밀번호 확인)를 입력합니다**. Add **Domain(도메인 추가)**을 클릭하여 이미지에 표시된 대로 지정된 도메인에 사용자를 추가합니다.



3. **도메인** 드롭다운 목록에서 사용자를 추가할 대상 도메인을 선택하고 이미지에 표시된 역할을 지정합니다.새 사용자를 자체 도메인 또는 하위 도메인에 추가할 수 있습니다.



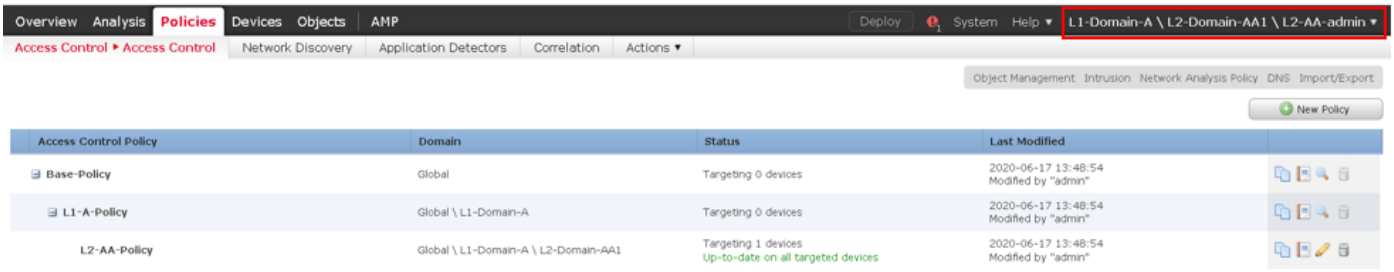
구성된 사용자는 다음 이미지에 표시됩니다.



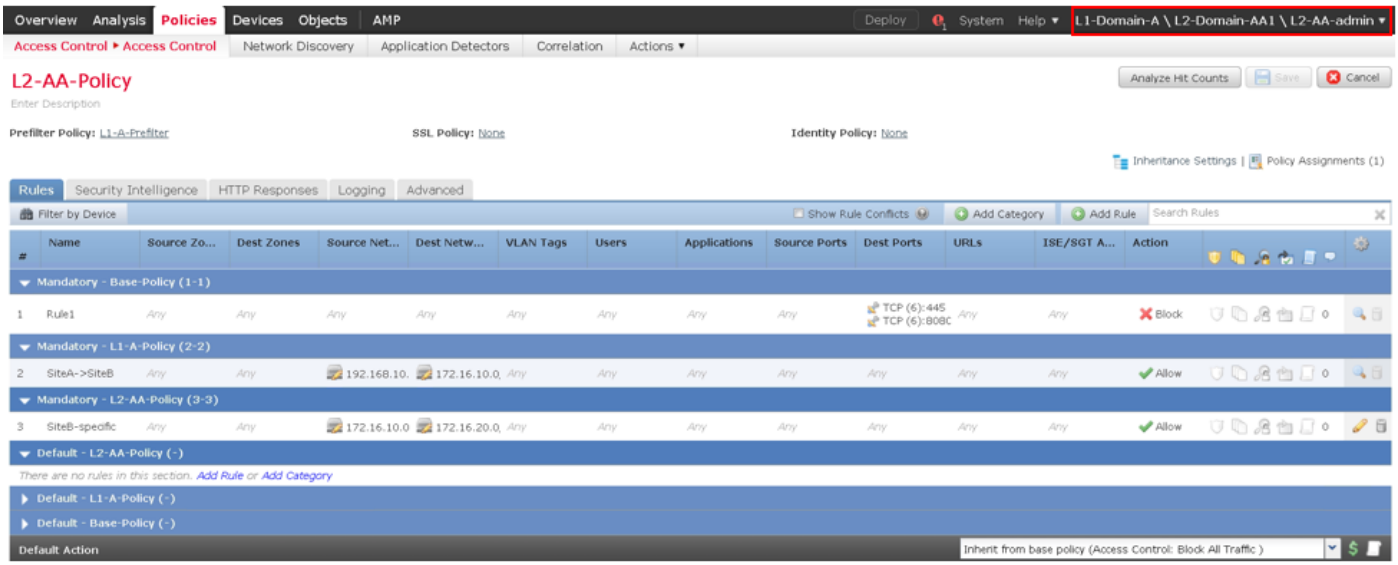
FMC의 리소스 액세스는 사용자가 속한 도메인으로 제한됩니다.아래 그림과 같이 user- **L1-A-admin**이 FMC UI에 로그인하면 사용자가 속한 Domain- **L1-Domain-A**와 사용자가 해당 하위 도메인으로 전환하면 하위 도메인으로 액세스가 제한됩니다.이 사용자는 **L1-Domain-A** 도메인에 정의된 정책과 자식 도메인으로 전환할 때 자식 도메인에 정의된 정책만 편집할 수 있습니다.또한 아래 예에서 **L1-A-Policy**가 전역 도메인(**Base-Policy**)에 정의된 정책을 상속하며,에서 볼 수 있는 수정 가능 서명상속 설정은 이미지에 표시된 대로 **Base-Policy**를 가리키도록 설정됩니다.

마찬가지로, **L2-Domain-AA1** 도메인에 속하는 사용자 **L2-AA-admin**은 이미지에 표시된 대로 도메인에 정의된 정책 **L2-AA-Policy**를 제어할 수 있습니다.**L2-AA-Policy**는 **L1-Domain-A**에 정의된 정책 **L1-A-Policy**를 상속하며, 이 정책은 전역 도메인에 정의된 **Base-Policy**를 상속합니다.또한 정책 **L2-**

AA-Policy는 서명사용자 L2-AA-admin은 상위 도메인(L1-Domain-A 또는 상위 도메인, 즉 전역 도메인으로 전환할 수 없습니다.



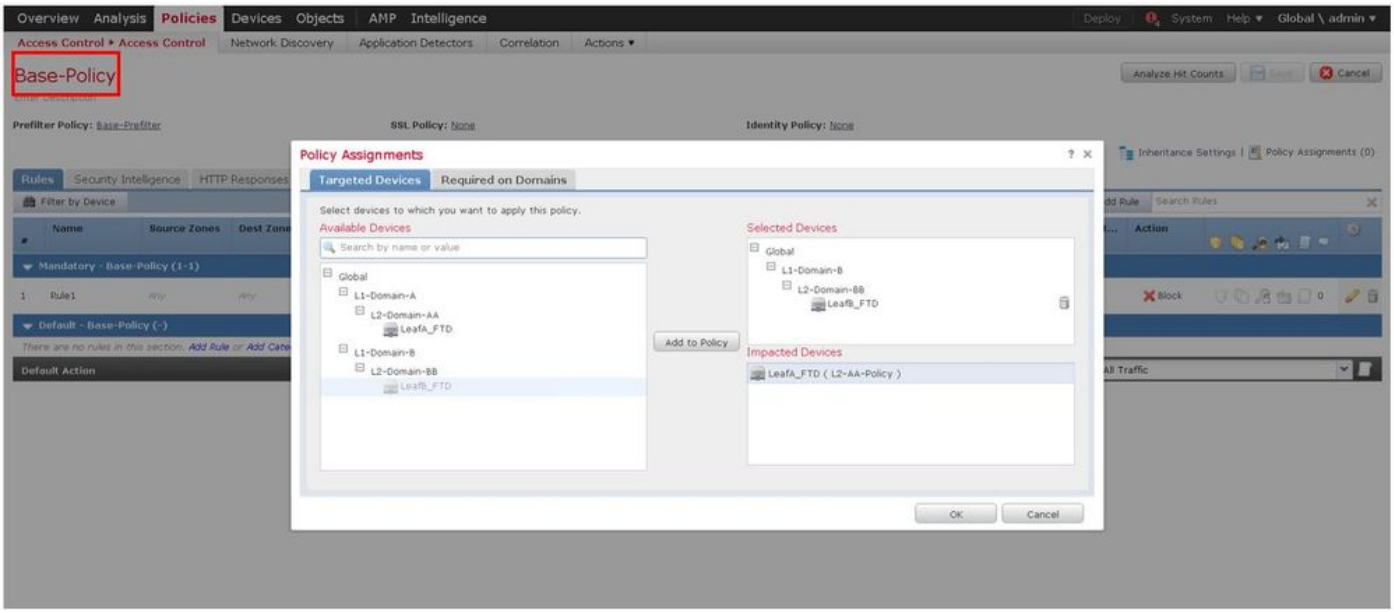
또한 L1-Domain-A에 속하는 사용자 **L1-A-admin은** L2-Domain-AA1로 전환하고 의 정책 **L2-AA-Policy**를 수정할 수 있습니다. 이미지에 표시된 대로 로그인합니다.이는 전역 도메인에 속한 사용자에게도 적용되며 하위 도메인으로 전환하고 특정 하위 도메인에 정의된 정책을 수정하는 경우에도 적용됩니다.



중요 사항:

- 비전역 도메인을 삭제하면 도메인에 속한 사용자가 자동으로 **전역** 도메인으로 이동됩니다.

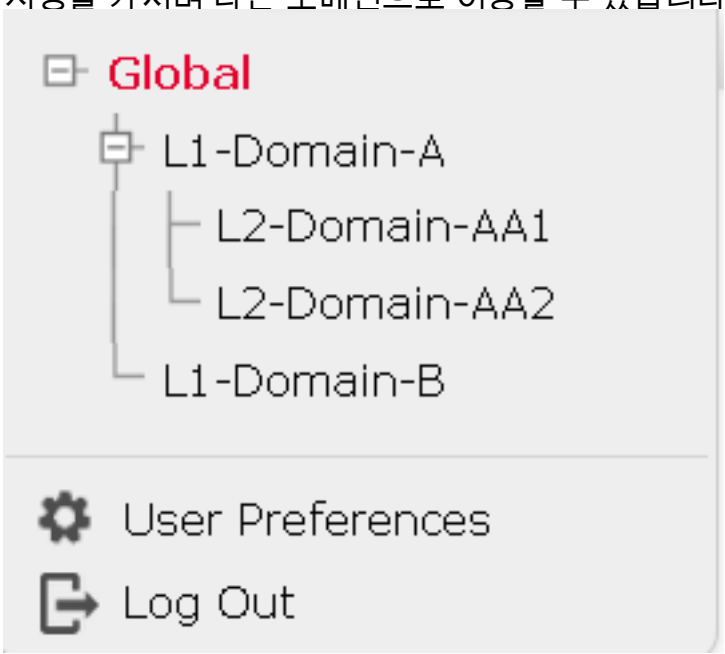
  FTD/s는 항상 리프 도메인에 정의되어 있습니다.이 경우 리프 도메인은 **L2-Domain**(예: L2-Domain-AA 및 L2-Domain-BB)입니다. **L2-도메인**에 속한 FTD는 **L1-Domain**의 정책 또는 **Global** Domain에서 정책에 할당할 수 있습니다.이 이미지에서 전역 도메인의 ACP는 L3 도메인에 정의된 FTD를 전역 도메인에 정의된 정책에 할당합니다.



- 전역 도메인의 사용자는 다른 사용자별 도메인으로 이동할 수 있지만 특정 도메인의 사용자는 자신의 도메인 및 하위 도메인에만 가시성이 있습니다.다음 표와 같이 전역 도메인 또는 기타 상위 도메인으로 이동할 수 없습니다.

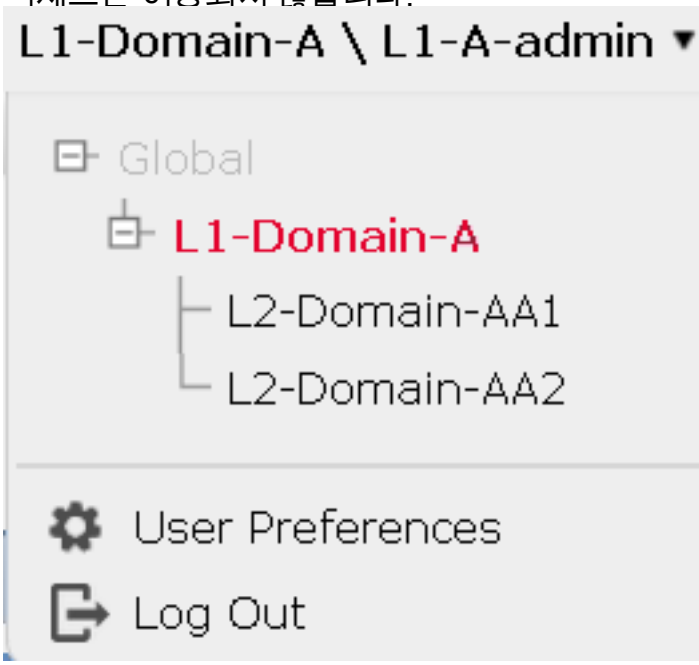
전역 도메인

전역 도메인의 사용자는 구성된 모든 도메인에 대한 가시성을 가지며 다른 도메인으로 이동할 수 있습니다.

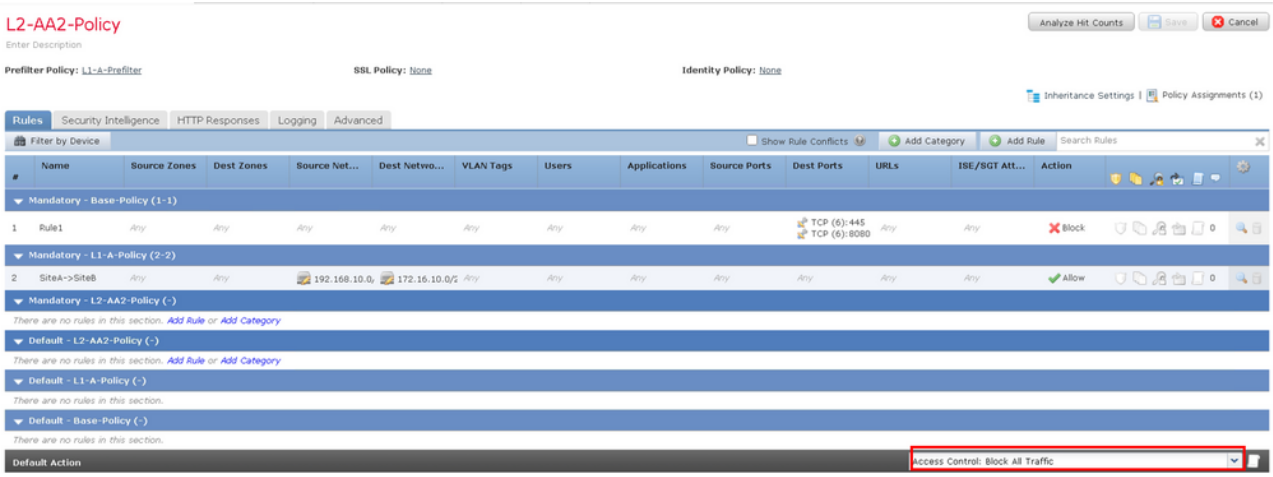


사용자별 도메인

L1-Domain-A의 사용자는 자체 및 해당 하위 도메
Domain-AA)에 대해서만 가시성을 가지며 **L2-Dom**
AA로 이동할 수 있습니다.상위 레벨 도메인(예: **전**
액세스는 허용되지 않습니다.



- 하위 정책의 기본 작업은 상위 정책에 의해 잠길 수 없으며 사용자는 이 이미지에 있는 것처럼 상위 정책의 기본 작업을 상속할 필요가 없습니다.



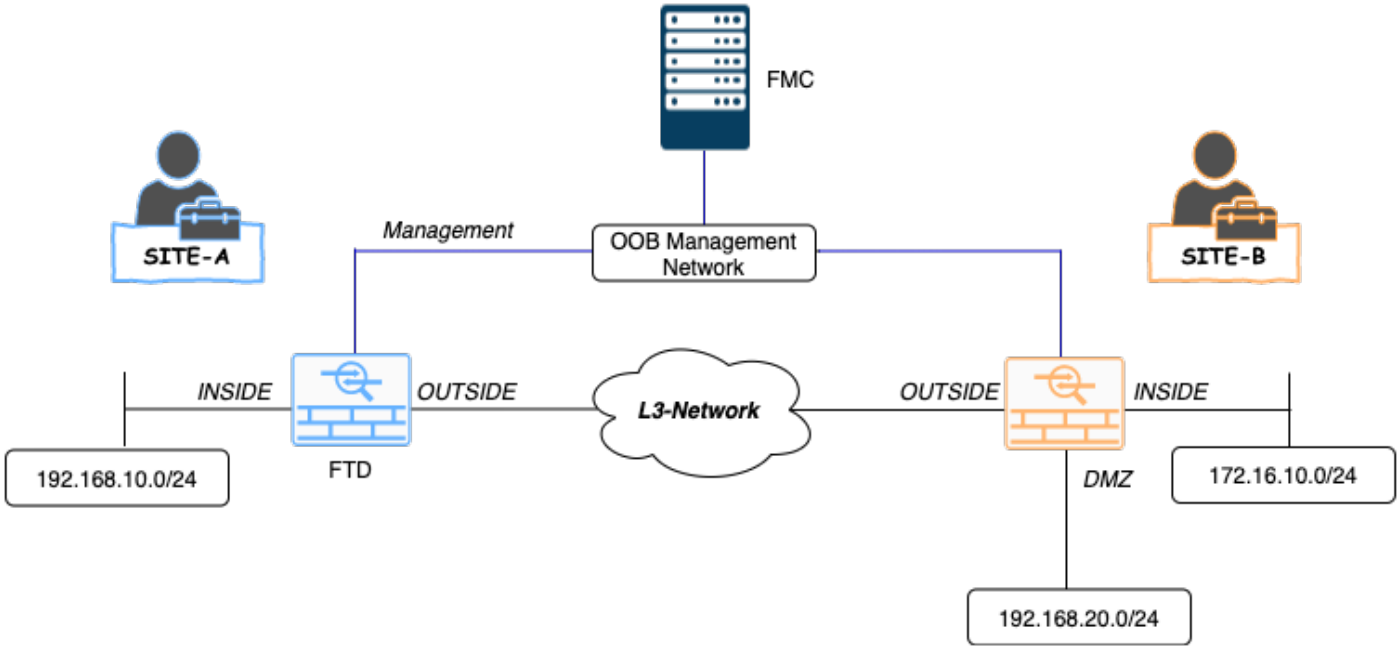
이 그림에서는 사용자가 기본 **정책**에서 상속: 기본 작업에 표시되지 않음에서 알 수 있는 상위**의** 기본 작업을 할당하지 않은 것을 볼 수 있습니다.

참고:사용자는 L1/L2 도메인 정책을 동시에 볼 수 없다는 점에 유의해야 합니다.사용자는 정책을 보고 편집하려면 원하는 도메인으로 전환해야 합니다. 예를 들면 다음과 같습니다.전역 도메인에 있는 사용자 **관리자**가 L1-Domain-A 및 L2-Domain-AA에 구성된 정책을 보려면 L1-A-Domain으로 전환하여 해당 도메인에 구성된 정책을 보고 수정한 다음 L2-Domain-AA로 전환하여 해당 정책을 보고 편집하되 동시에 둘 다 볼 수는 없습니다.또한 L1-Domain-A의 사용자는 전역 도메인(L1-A-Policy의 상위 정책인 Base Policy)에 정의된 정책을 편집하거나 삭제할 수 없으며, L2-Domain-AA의 사용자는 전역 및 L2-Domain-A 도메인에 정의된 Base Policy 및 L2-A-Policy라는 정책을 각각 수정하거나 삭제할 수 없습니다.

활용 사례 시나리오

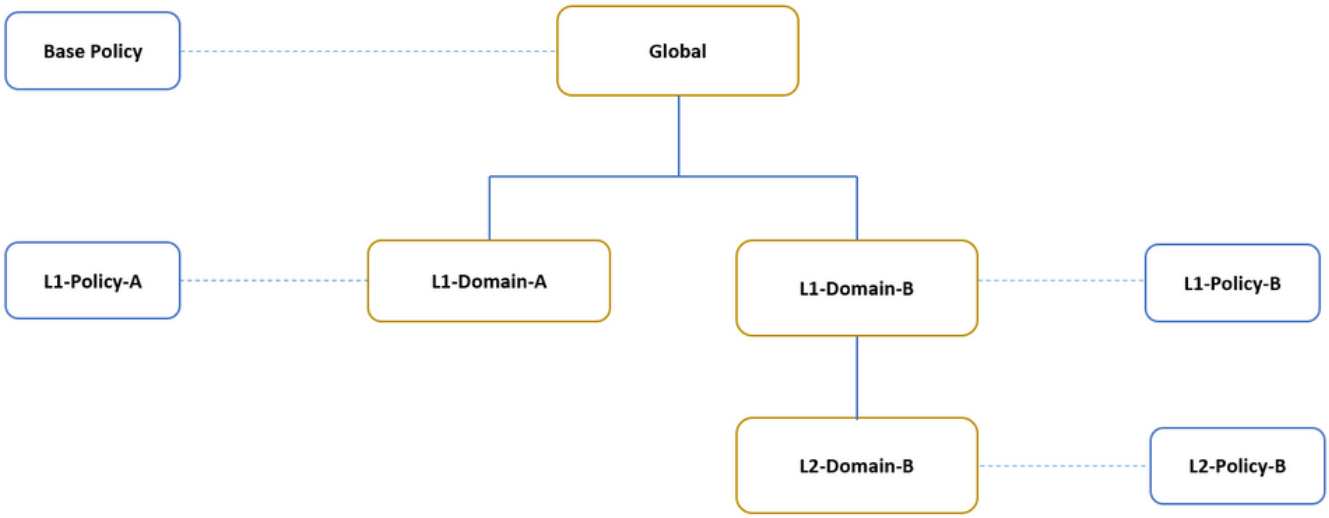
이미지에 표시된 시나리오, SITE-A(SiteA-FTD) 및 SITE-B(SiteB-FTD)의 FTD는 서로 다른 도메인(다중 도메인)을 통해 단일 FMC에 의해 관리되어 제어되는 액세스를 고려합니다.정책의 관점에서 볼 때 조직 수준에서 고려해야 할 정책 사항은 다음과 같습니다.

- SITE 또는 DOMAIN에 독립적인 모든 FTD에 적용할 수 있는 서비스 관련 BLOCK 규칙(Base-Policy)입니다.
- 사이트-A-사이트-B 액세스(L1-정책-A) 및 사이트-B-사이트-A 액세스(L1-정책-B)를 충족하기 위한 요구 사항을 충족하는 규칙
- Site-B FTD(L2-Policy-B)에 적용할 수 있는 규칙.



다중 도메인 환경에서 상속

위에서 언급한 활용 사례에 대해서는 다음 도메인/정책 계층 구조를 고려하십시오.SiteA-FTD 및 SiteB-FTD는 각각 리프-도메인 L1-Domain-A 및 L2-Domain-B의 일부입니다.

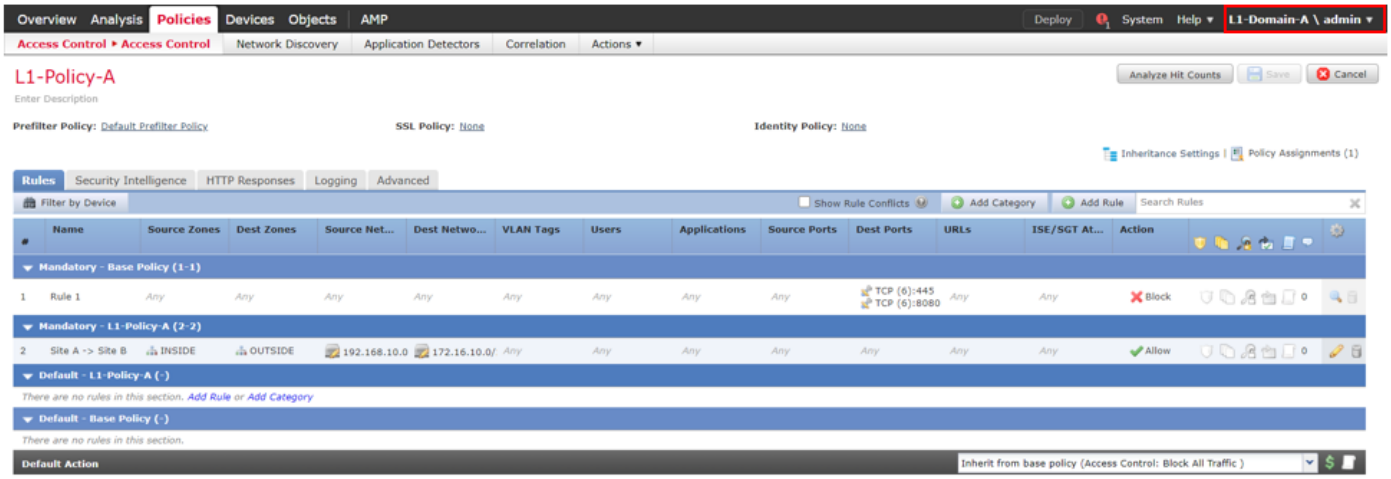


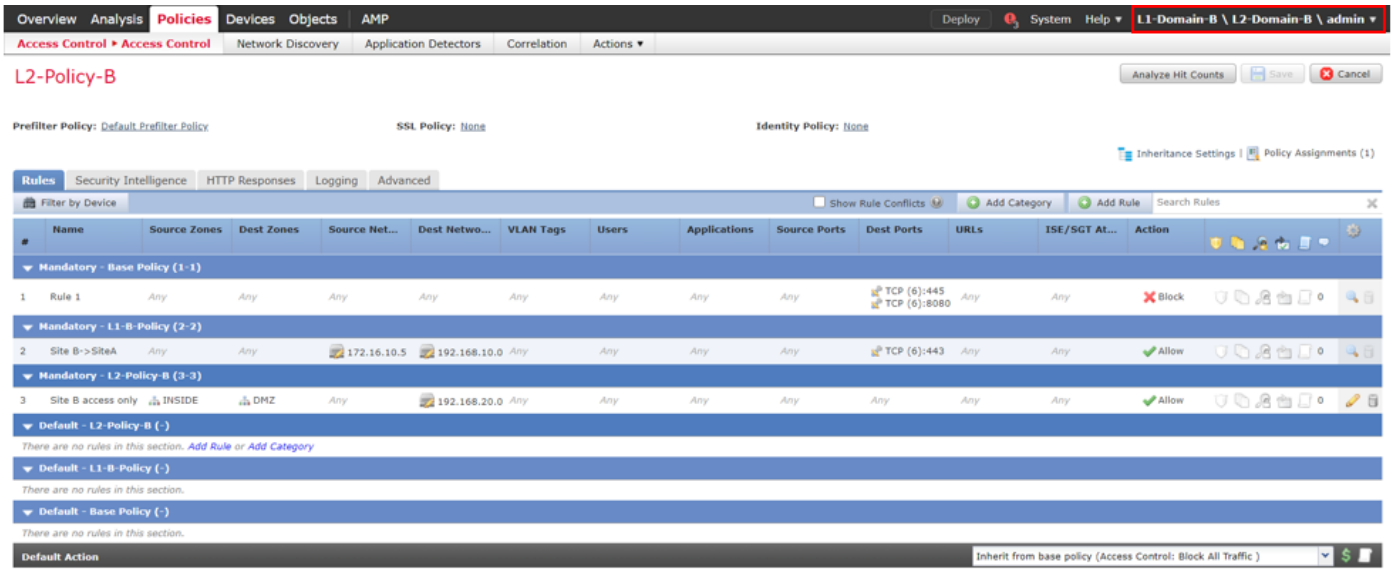
도메인 계층의 구조는 다음과 같습니다.

- **전역** 도메인**은 L1-Domain-A 및 L1-Domain-B의 상위 도메인입니다**.
- **전역** 도메인**은 L2-Domain-B**의 **상위 도메인입니다**.
- **L2-Domain-B**는 **L1-Domain-B**의 하위 항목입니다**.**
- **L2-Domain-B**는 자식 도메인이 없으므로 리프 도메인입니다.

이 그림에서는 FMC의 도메인 계층 구조를 보여 줍니다.

아래 스냅샷은 **L1-Policy-A** 및 **L2-Policy-B** w.r.t에서 위 시나리오에 대한 규칙을 어떻게 정의하는지 보여줍니다.





합법적인 트래픽을 차단하거나 원치 않는 트래픽을 허용하지 않도록 여러 도메인을 구성할 때는 항상 규칙과 상속을 고려해야 합니다.