FTD中多網域環境中的繼承

目錄

簡介

本文檔介紹繼承功能和多域功能的配置和工作情況，並重點介紹一個真實的使用案例，以瞭解這兩個功能如何協同工作。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

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

採用元件

本檔案中的資訊是根據以下軟體版本：

- Firepower管理中心(FMC)軟體版本6.4
- Firepower威脅防禦(FTD)軟體版本6.4

附註：從6.0版本開始，FMC/FTD上提供多域和繼承功能支援。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何組態可能造成的影響。

背景資訊

在策略繼承中，可以巢狀訪問控制策略，其中子策略從基本策略繼承規則，包括安全情報、HTTP響應、日誌記錄設定等ACP設定。 管理員可以選擇允許子策略覆蓋ACP設定，如安全情報、HTTP響應、日誌記錄設定，或者鎖定設定，以便子策略無法覆蓋這些設定。此功能在多域FMC環境中非常有用。

多域功能使使用者能夠訪問FMC的受管裝置、配置和事件。使用者將能夠根據許可權切換到/訪問其他域。如果未配置多域功能，則所有受管裝置、配置和事件均屬於**全域性**域。

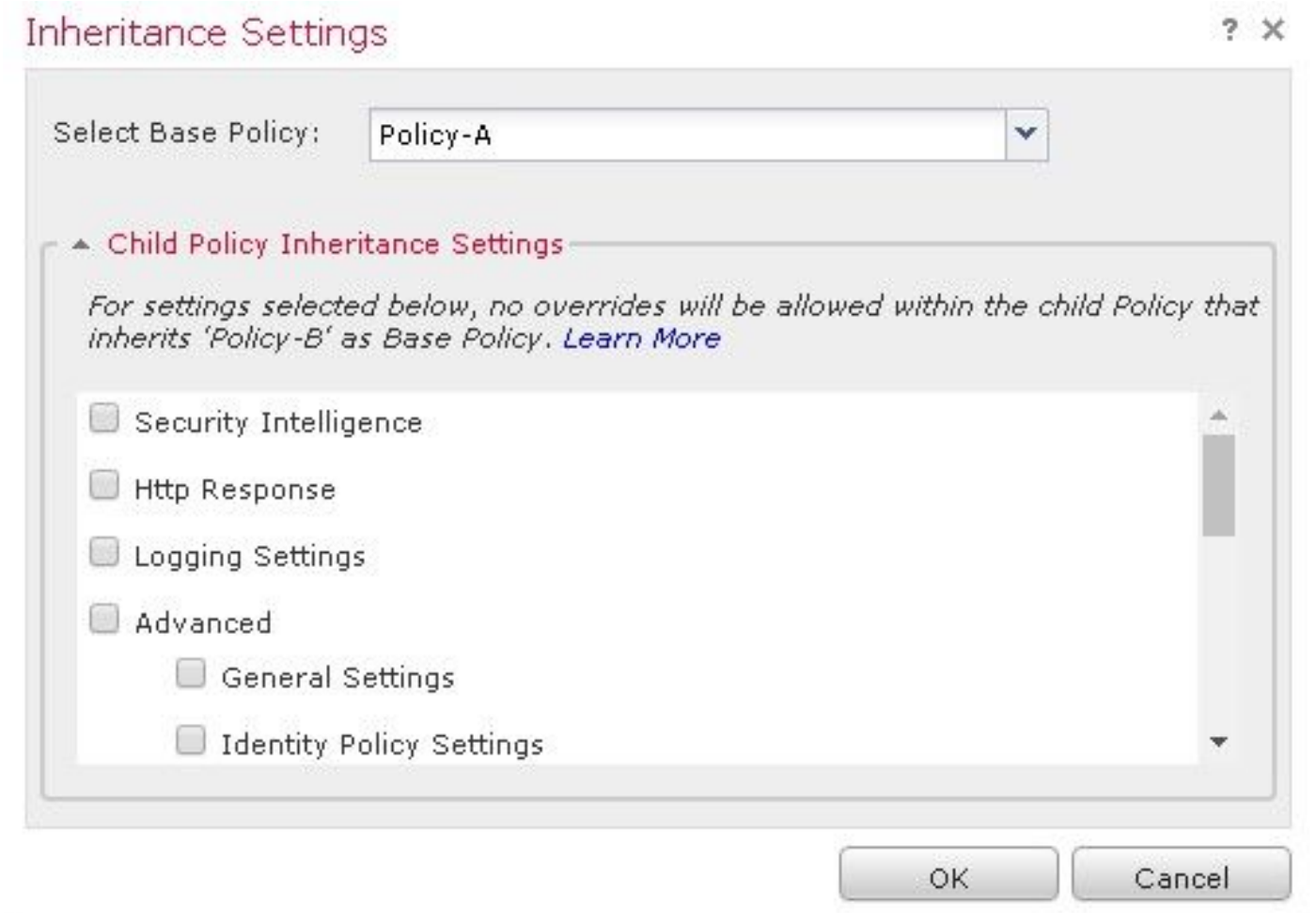
配置策略繼承

枝葉域是沒有其他子域的域。子域是使用者/管理員當前所在的域的下一個級別後代。父域是使用者/管理員當前所在的域的直接祖先。

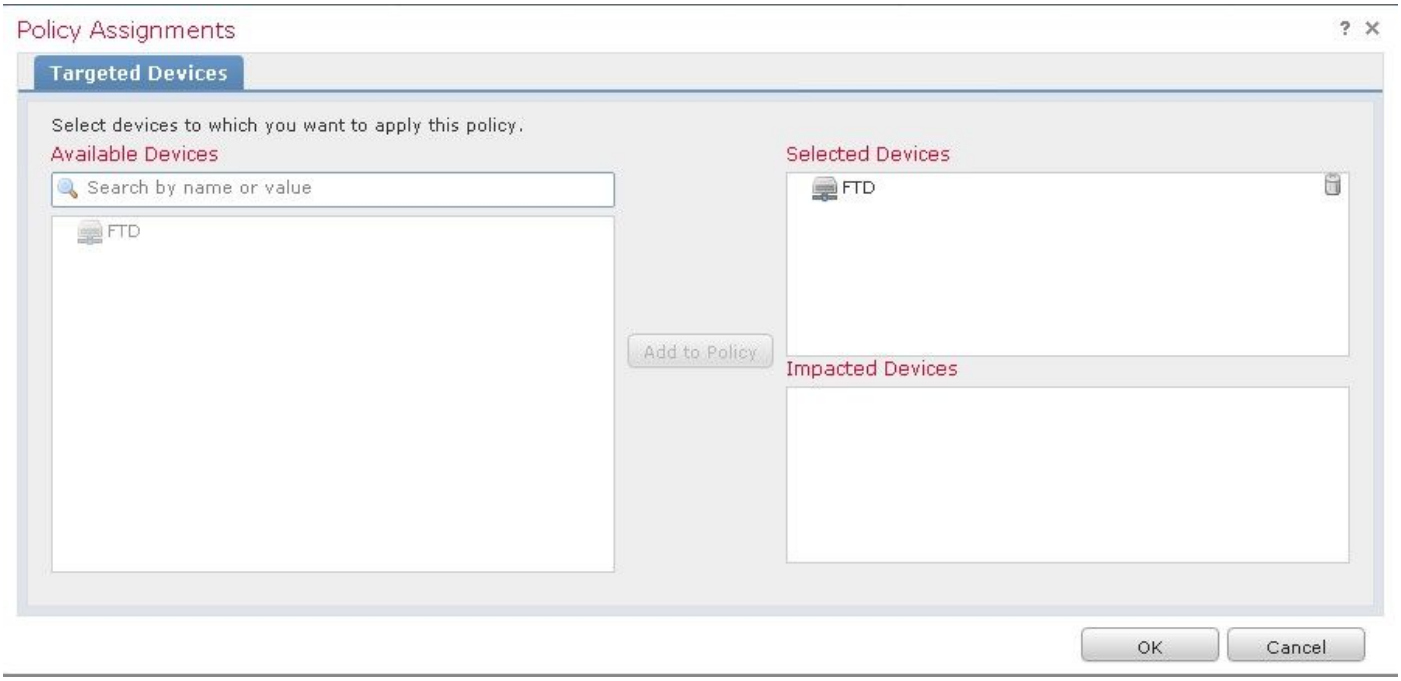
要配置/啟用現有策略的繼承，請執行以下操作：

1. 讓策略A成為基本策略，策略B成為子策略（策略B從策略A繼承規則）
2. **EDIT** Policy-B並按一下**Inheritance Settings**，如下圖所示。

3.從**Select Base Policy**下拉選單中選擇Policy-A，如下所示。其他ACP設定（如安全情報、HTTP響應、日誌記錄設定等）可以繼承，以選擇性地覆蓋子策略的設定。

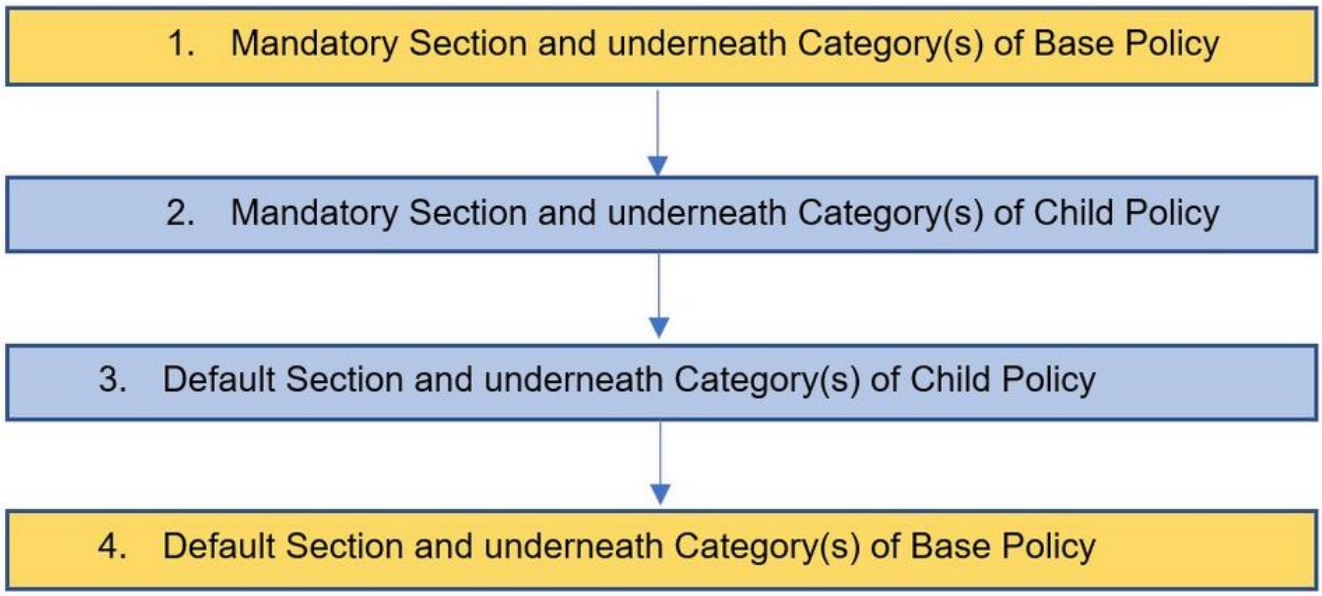


4.針對預期的目標FTD裝置，為子策略Policy-B執行**策略分配**:

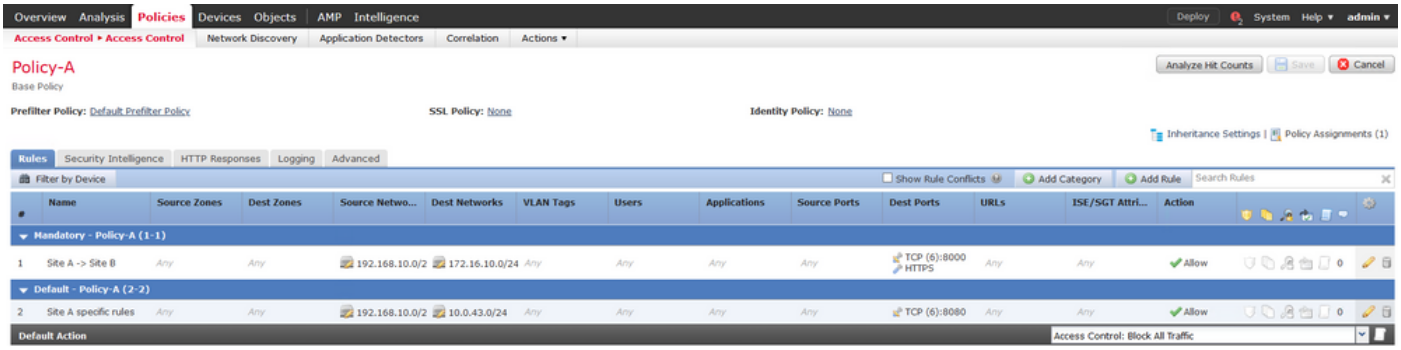


預設情況下，會繼承**Default Action** of Child Policy並設定為**Inherit from base policy**，如下圖所示。使用者還可以從系統提供的策略中選擇**Default Action**，如下圖所示。

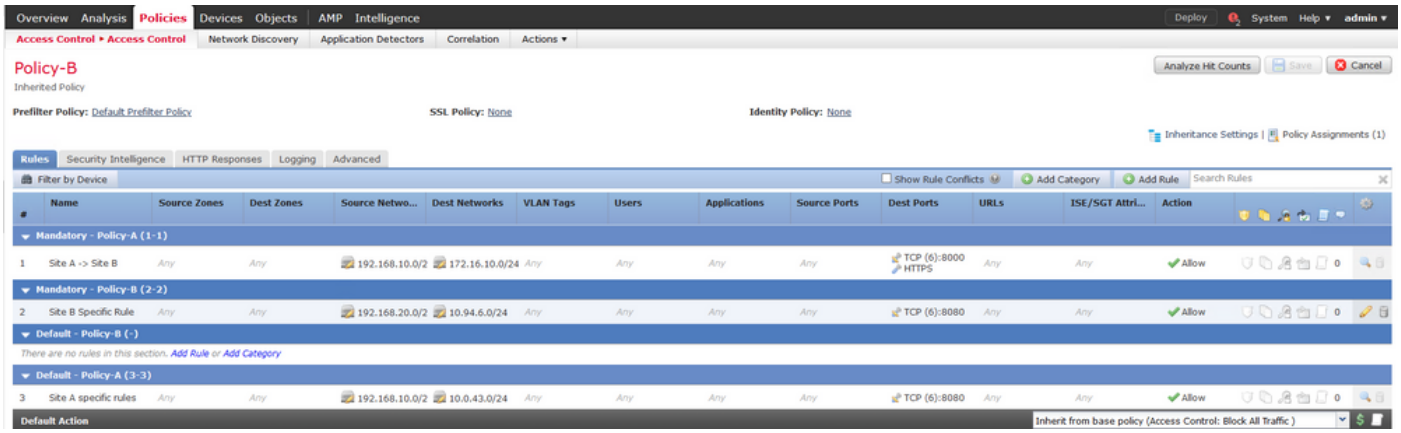
無論在「必備」和「預設」部分中新增的類別數如何，流量的查詢順序始終為自上而下。應用**繼承設定**後，子策略Policy-B（子策略）的ACP表示形式如圖所示，與前面提到的**Order of rule檢查**一致：



此圖顯示FMC中如何顯示策略（即作為基本策略的策略A和作為子策略並從策略A繼承的策略B）。



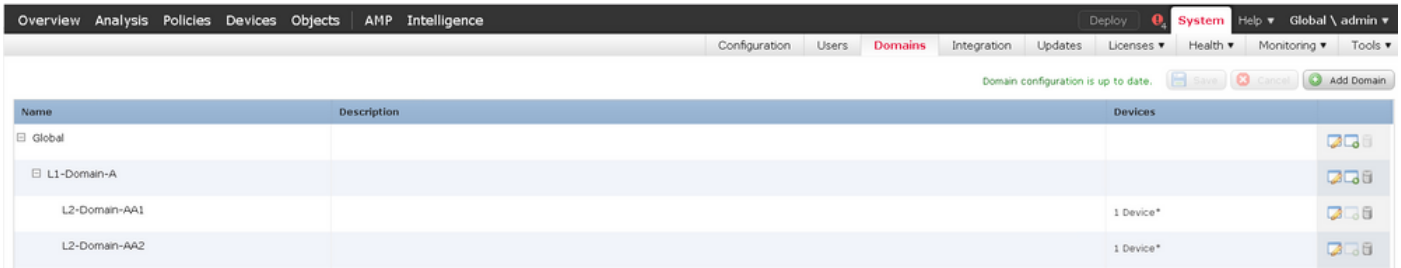
此圖顯示，在策略B中，可以看到來自策略A的規則，以及在策略B本身中配置的特定規則。應該注意規則的配置方式，要牢記順序。



多域FMC環境中的FTD管理

多域功能使使用者能夠訪問受管裝置、配置和事件。使用者將能夠根據許可權切換到其他域。如果未配置多域功能，則所有受管裝置、配置和事件均屬於**全域性**域。

最多可以將三級域配置為一級「全域性域」。所有受管裝置必須僅屬於枝葉域。這可以從以下符號確認  （新增子域）在枝葉域中呈灰色顯示，如下圖所示。



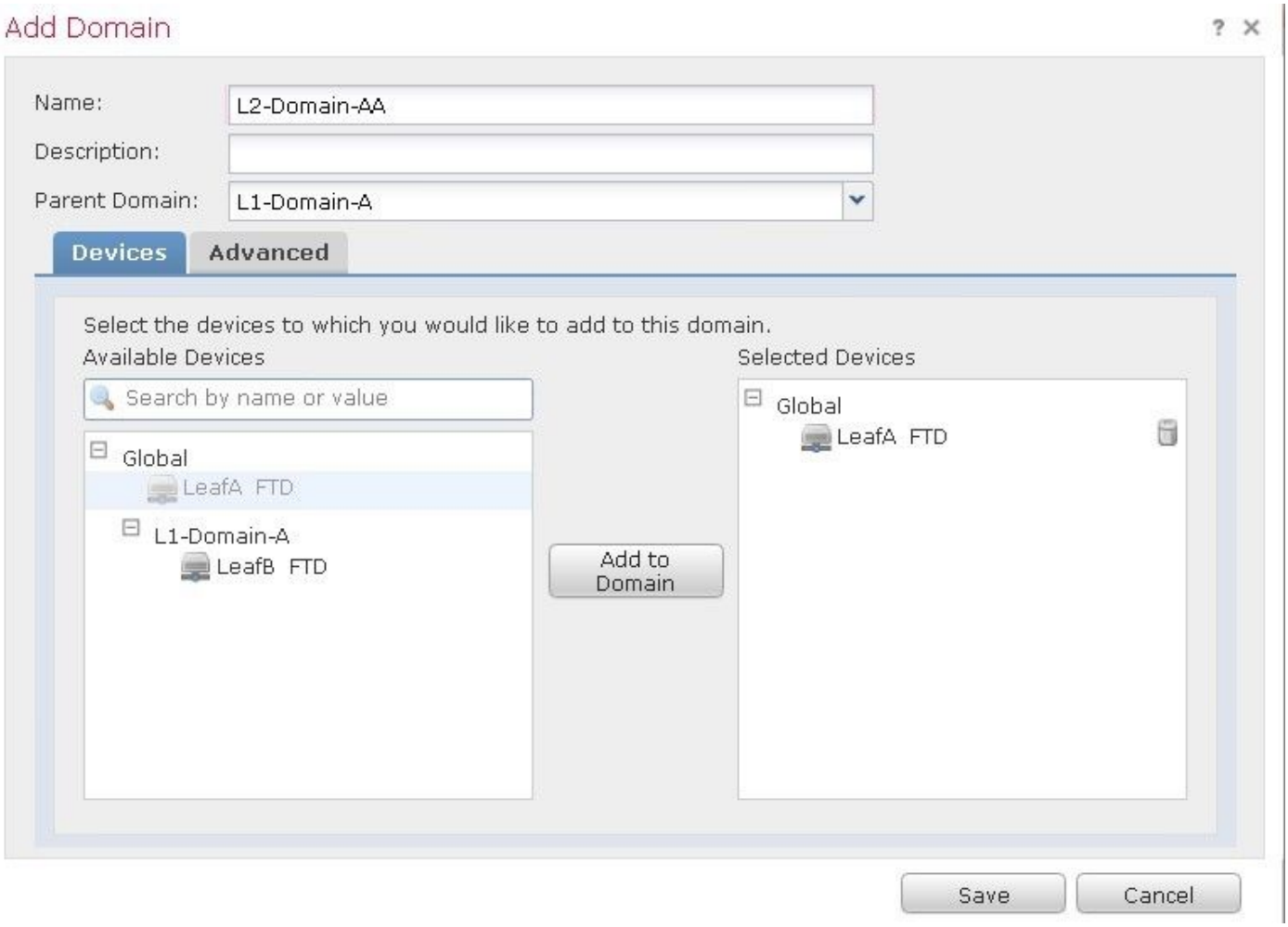
域配置

域配置可以按如下方式完成：

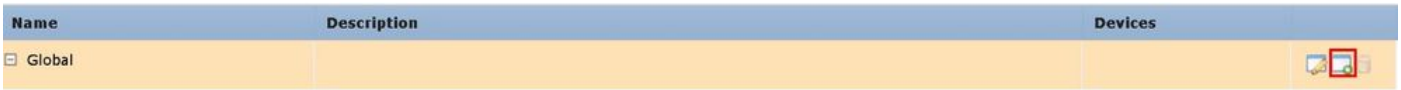
1. 導覽至**System > Domains**。預設情況下，**Global**域存在。

2. 按一下「**Add Domain**」，如下圖所示。

3.出現**Add Domain**對話方塊。鍵入域的**Name**，然後從下拉選單中選擇**Parent Domain**。如果這是枝葉域，則需要將FTD裝置新增到域中，如下圖所示。

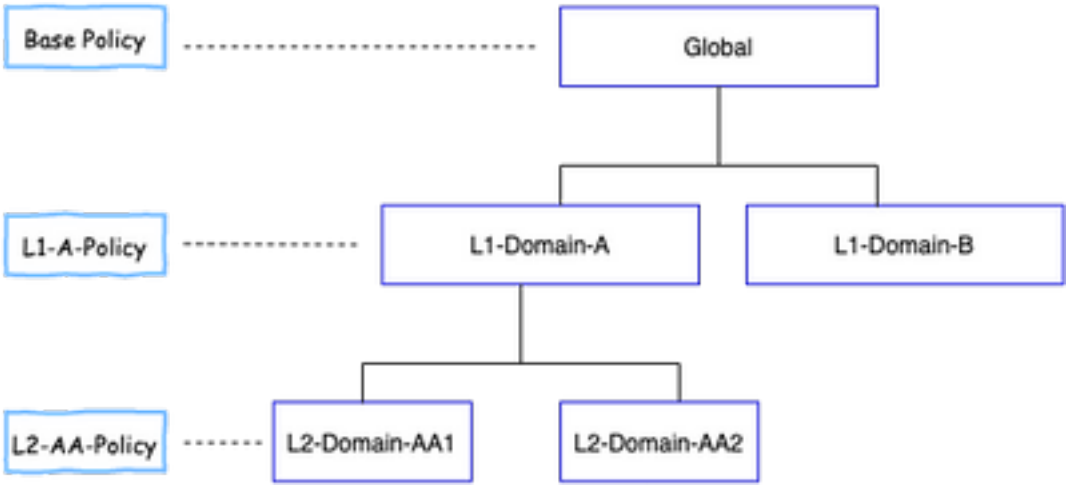


附註：要新增域，請按一下**新增子域**圖示，如下圖所示。已在此處選擇父域。



多域FMC環境中的策略可視性與可控性

策略可見性和控制僅限於各個域使用者，全域性域管理員除外。此示例基於以下層次：



可視性：如下圖所示，預設檢視**Policies**頁面列出在各自域下配置的策略(ACP)。

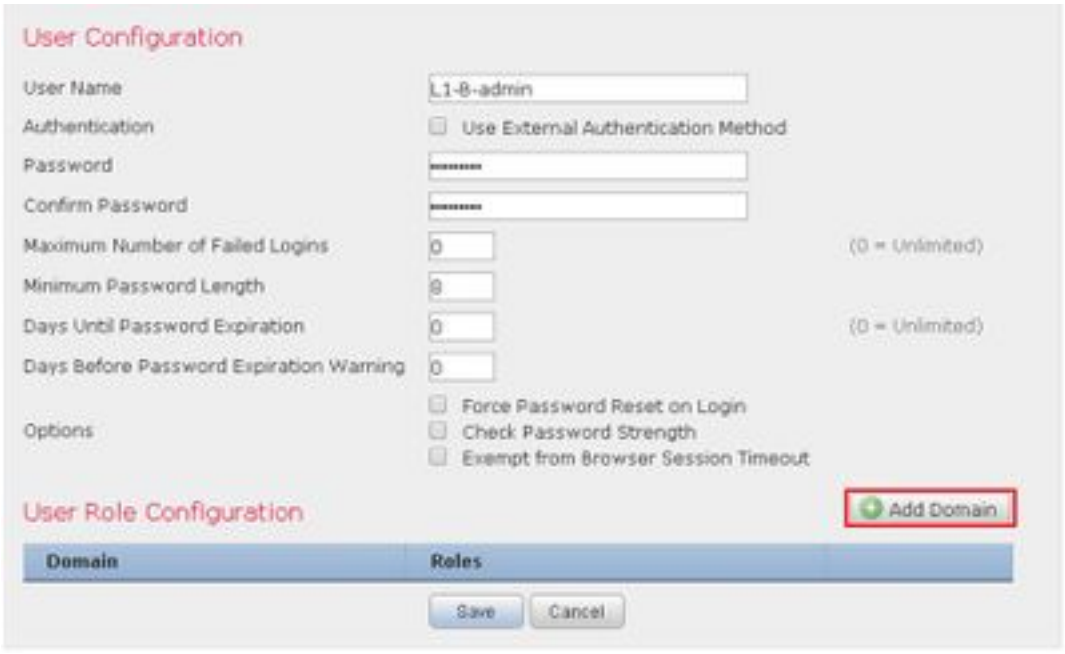
控制：**屬**於相應域的管理員使用者可以編輯策略。要編輯屬於其他域（例如作為繼承的一部分）的策略，必須將域從當前域切換到策略配置所在的域。只有屬於**Global**域或**L1**域的管理員使用者才能在較低的域之間切換以進行策略管理。

向域中新增使用者

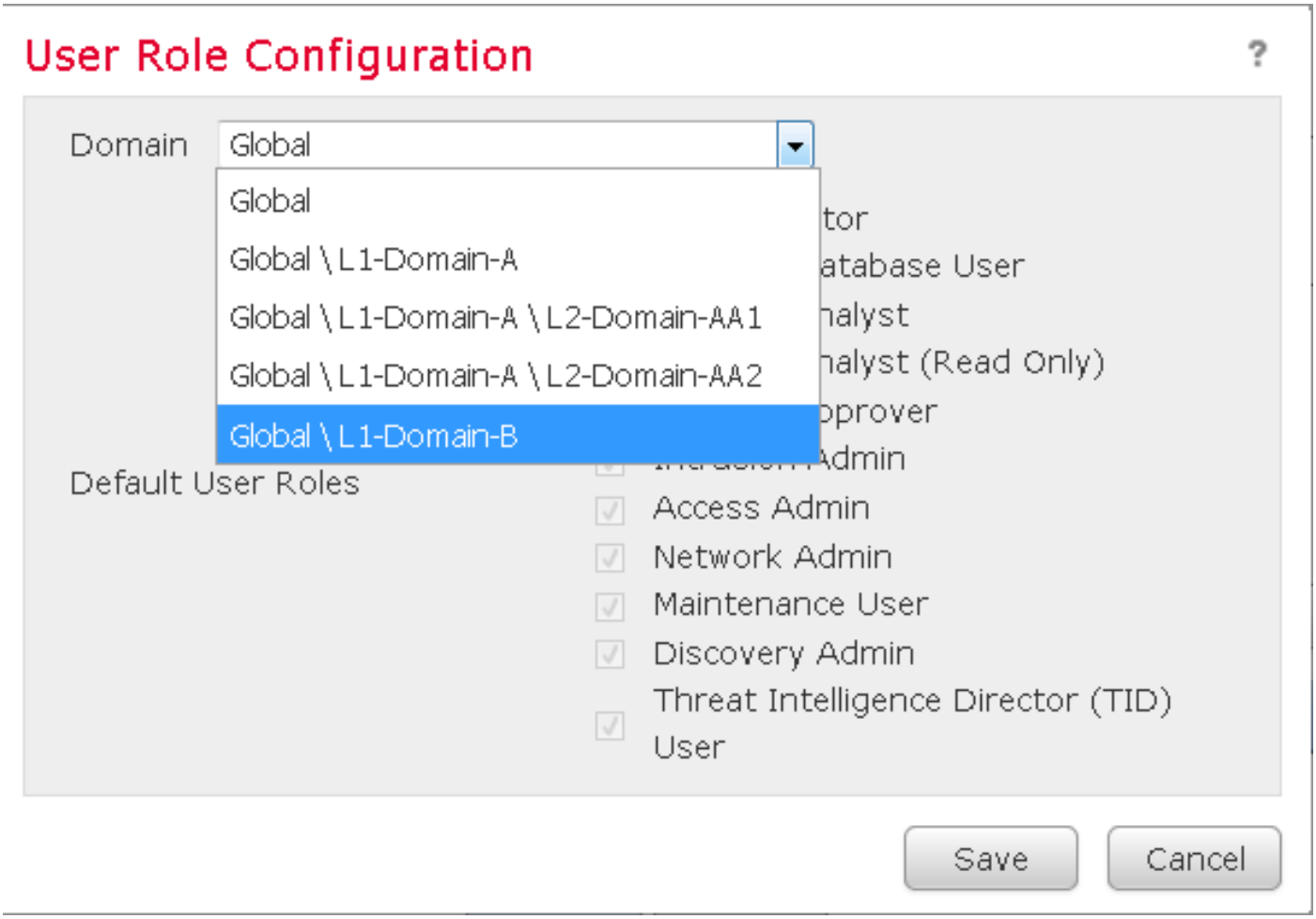
這顯示如何在特定域中新增使用者。此過程適用於本地資料庫中的使用者。

1. 導覽至**System > Users**。按一下「**Create User**」，如下圖所示。

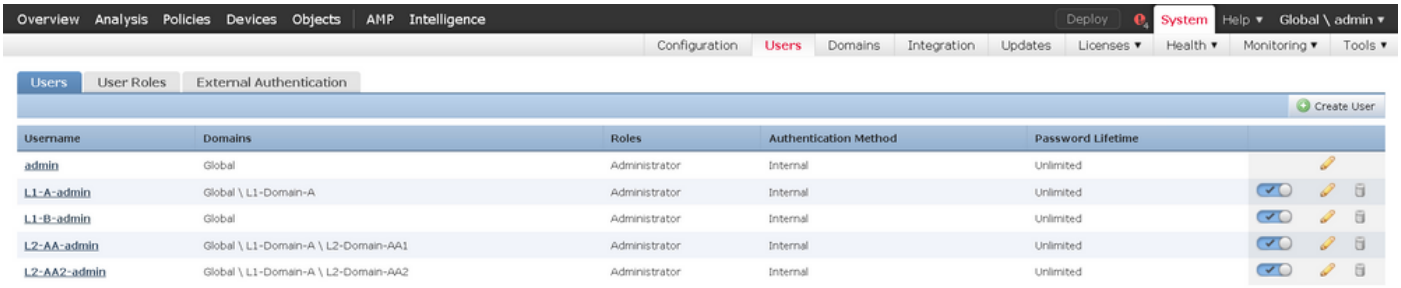
2.出現**User Configuration**對話方塊。填寫**使用者名稱**和密碼（**&確認密碼**）。 按一下「**Add Domain**」，將使用者新增到指定的網域，如下圖所示。



3.從**域**下拉選單中選擇要在其中新增使用者的目標域，並指定角色，如下圖所示。可以將新使用者新增到自己的域或子域。

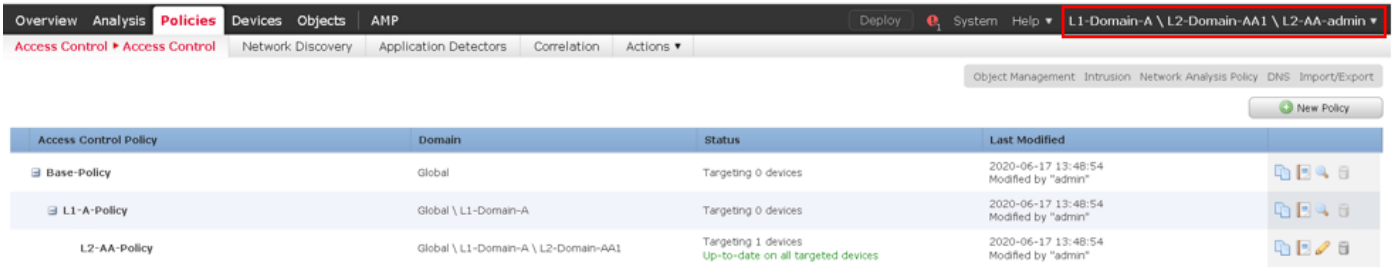


已設定的使用者如下圖所示：

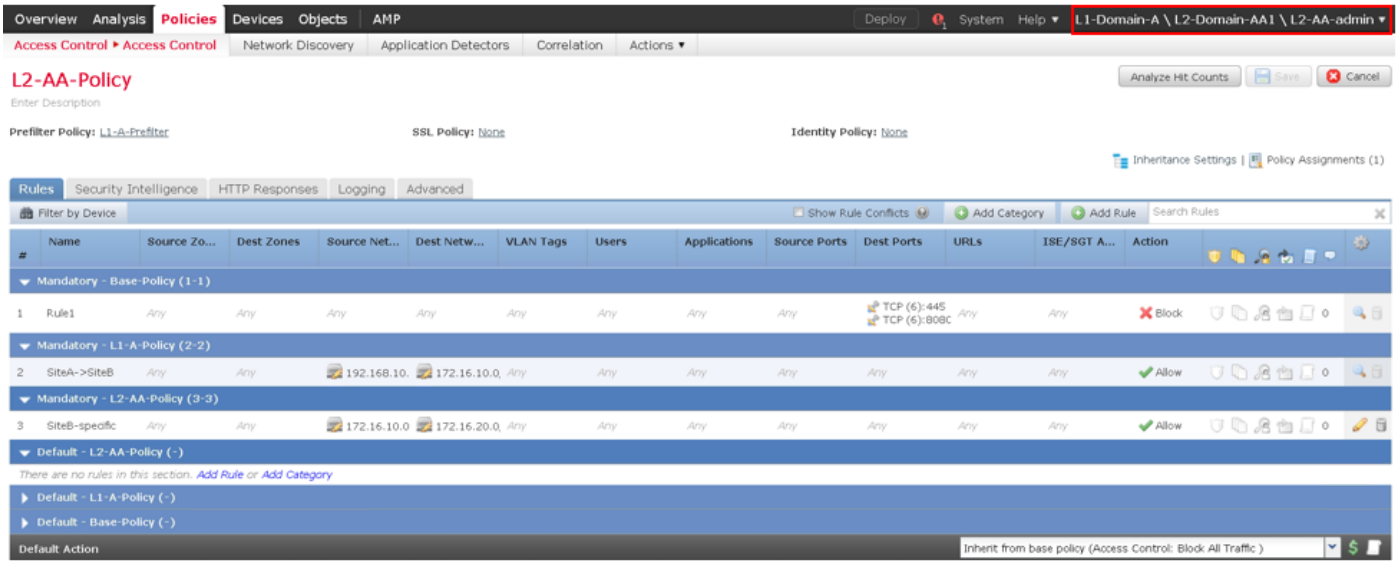


FMC上的資源訪問將限制於使用者所屬的域。如下圖所示，當使用者 — **L1-A-admin**登入FMC UI時，訪問限製為使用者所屬的Domain- **L1-Domain-A**，並在使用者切換到子域後訪問子域。當域切換至其子域時，此使用者只能編輯**L1-Domain-A**域中定義的策略和子域中定義的策略。此外，從下面的示例中可以看到，**L1-A-Policy**繼承在全域性域中定義的策略(即**Base-Policy**)，並且還可以進行編輯(可從  簽名。使繼承設定指向**Base-Policy**，如下圖所示。

類似地，屬於**L2-Domain-AA1**域的使用者**L2-AA-admin**僅控制在該域中定義的策略**L2-AA-Policy**，如下圖所示。**L2-AA-Policy**繼承在**L1-Domain-A**中定義的策略**L1-A-Policy**，後者又繼承在全域性域中定義的**Base-Policy**。此外，還可以編輯**策略L2-AA-Policy**，可從  簽名。使用者L2-AA-admin永遠無法切換到其父域L1-Domain-A或其祖先域global domain。



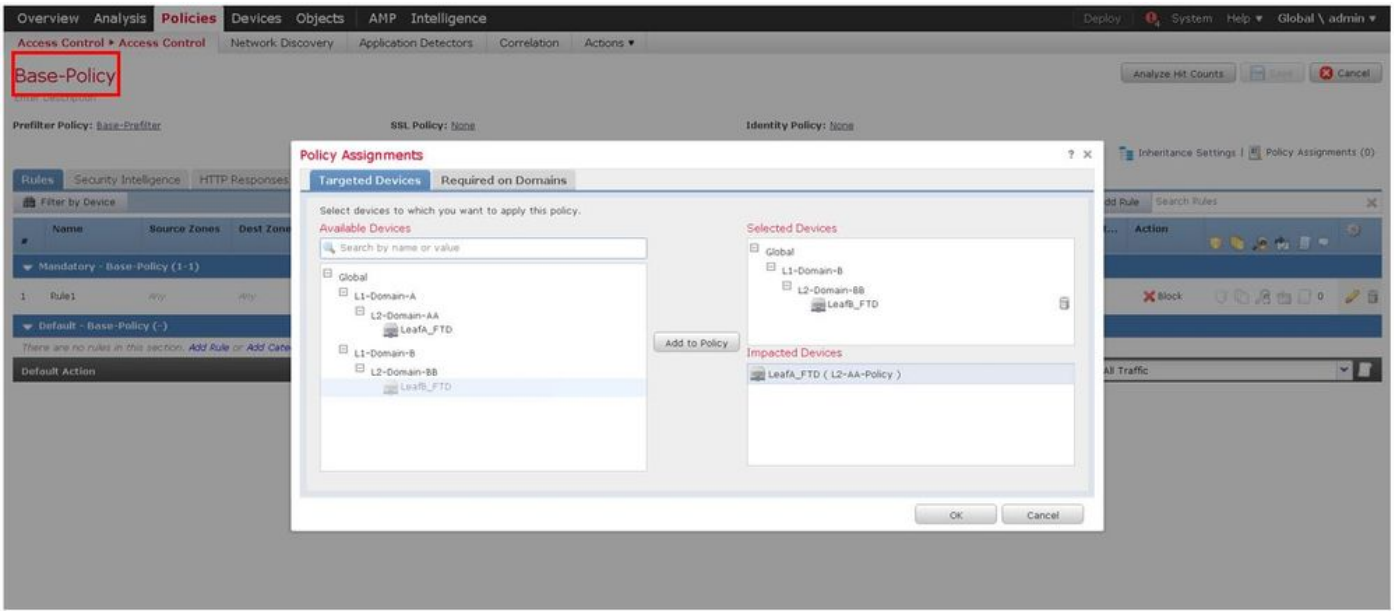
此外，屬於L1-Domain-A的使用者**L1-A-admin可以切換到L2-Domain-AA1並編輯策略L2-AA-Policy**，該策略可從  如圖所示進行簽名。這甚至適用於屬於全域性域並切換到子域並編輯特定子域中定義的策略的使用者。



需注意的重要事項：

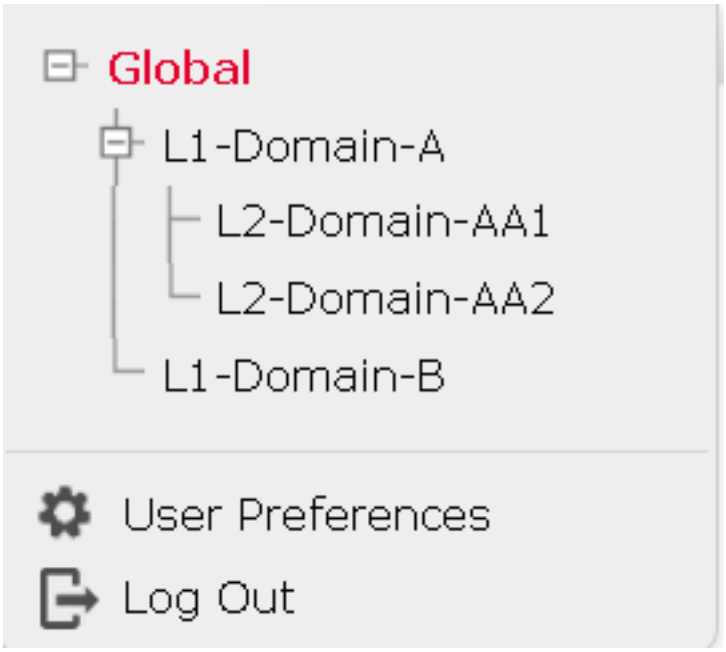
- 刪除非全域性域時，屬於這些域的使用者將自動移動到**全域性**域。

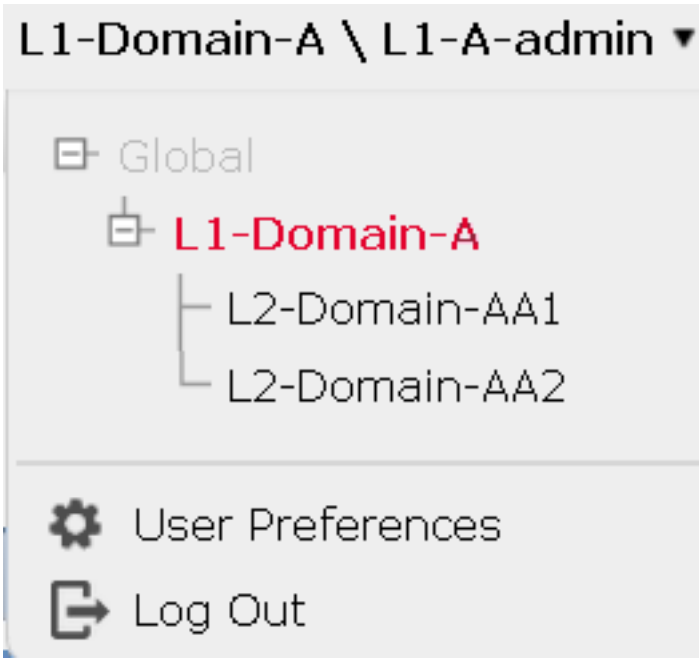
  FTD/s始終在枝葉域中定義。在這種情況下，枝葉域是**L2-Domain**（即L2-Domain-AA和L2-Domain-BB）。 屬於**L2-Domain的FTD**可以分配給**L1-Domain**或**Global** Domain中的策略。在此圖中，全域性域中的ACP將第3層域中定義的FTD分配給在全域性域中定義的策略。



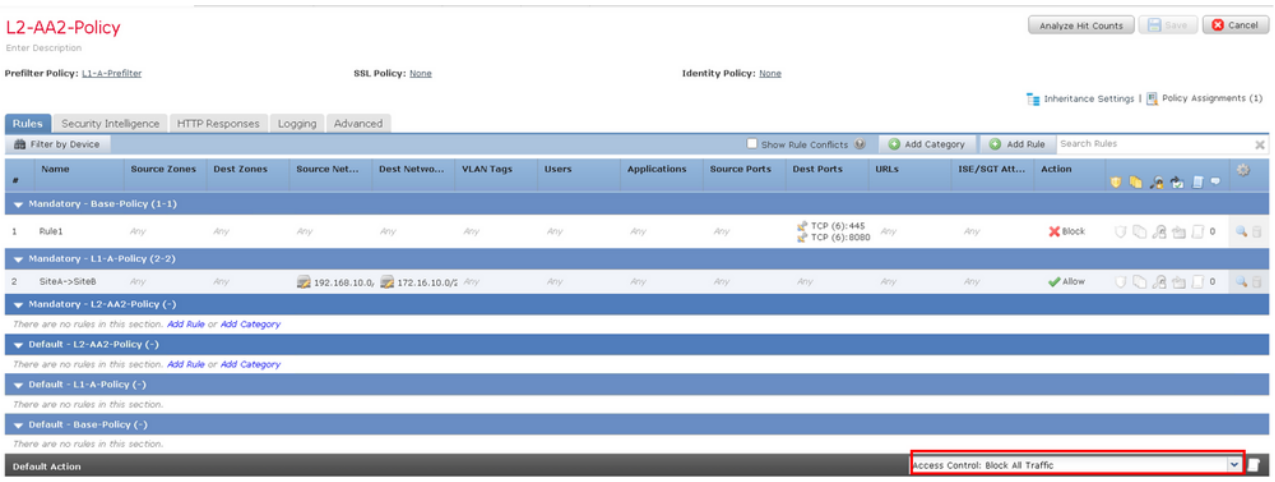
- 全域性域中的使用者可以導航到其他使用者特定的域，但特定域中的使用者僅在其自己的域及其子域中具有可見性。它們無法導航到全域性域或任何其他更高版本的域，如下表所示：

全域性域	**使用者特定的域**
全域性域中的使用者可以看到所有已配置的域，並且可以導航到其他域。	**L1-Domain-A**中的使用者只能看到自己及其子域(即**Domain-AA**)，並且可以導航到**L2-Domain-AA**。不更高級別的域(如**全域性**)訪問。





- 父策略無法鎖定子策略的預設操作，使用者無需繼承父策略的預設操作，如本圖所示。



在此圖中，可以看到使用者沒有將預設操作指定為父操作的預設操作，這從**Inherit from base policy：未在預設操作中顯**示。

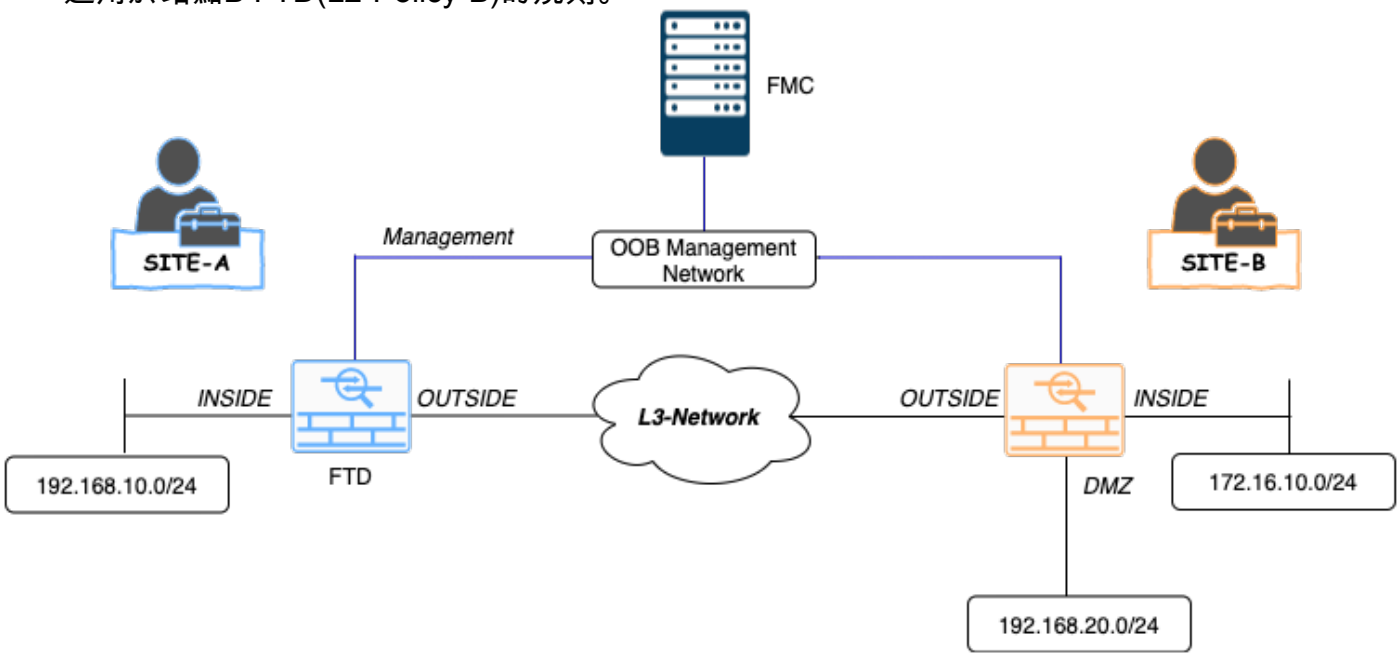
附註：應牢記，使用者不能同時檢視L1/L2域策略。使用者需要切換到所需域才能檢視和編輯策略。例如：如果全域性域中的使用者**admin**想要檢視L1-Domain-A和L2-Domain-AA中配置的策略，則使用者可以通過切換到L1-A-Domain檢視和編輯該域中配置的策略，然後切換到L2-Domain-AA檢視和編輯相應的策略，但不能同時檢視這兩個策略。此外，L1-Domain-A中的使用者不能編輯或刪除全域性域中定義的策略，即作為L1-A-Policy父策略的基本策略，而L2-Domain-AA中的使用者不能分別編輯或刪除全域性域和L2-Domain-A域中定義的基本策略和L2-A-Policy。

用例場景

考慮圖中所描述的方案，站點A（站點A-FTD）和站點B（站點B-FTD）的FTD由單個FMC通過不同的域（多域）進行管理，以提供受控訪問。從策略角度來看，這些是組織層面的策略考慮因素：

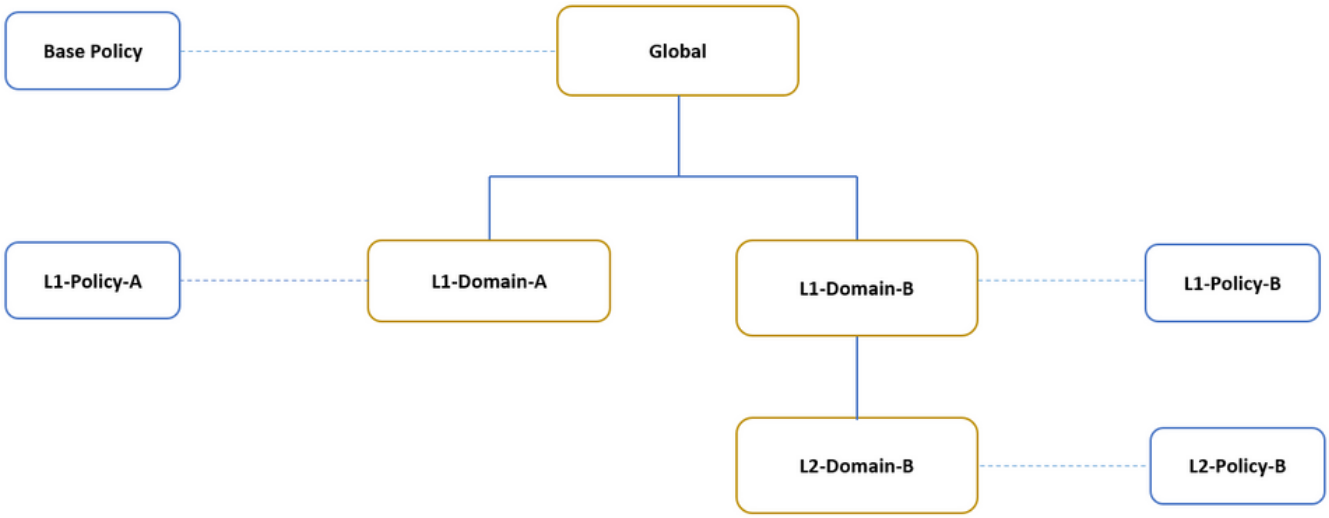
- 適用於所有FTD且獨立於站點或域所屬的服務特定阻止規則(Base-Policy)。
- 滿足站點A到站點B訪問(L1-Policy-A)和站點B到站點A訪問(L1-Policy-B)的要求的規則。

- 適用於站點B FTD(L2-Policy-B)的規則。



多域環境中的繼承

對於上述使用案例，請考慮以下域/策略層次結構。SiteA-FTD和SiteB-FTD分別是葉域L1 — 域A和L2 — 域B的一部分。

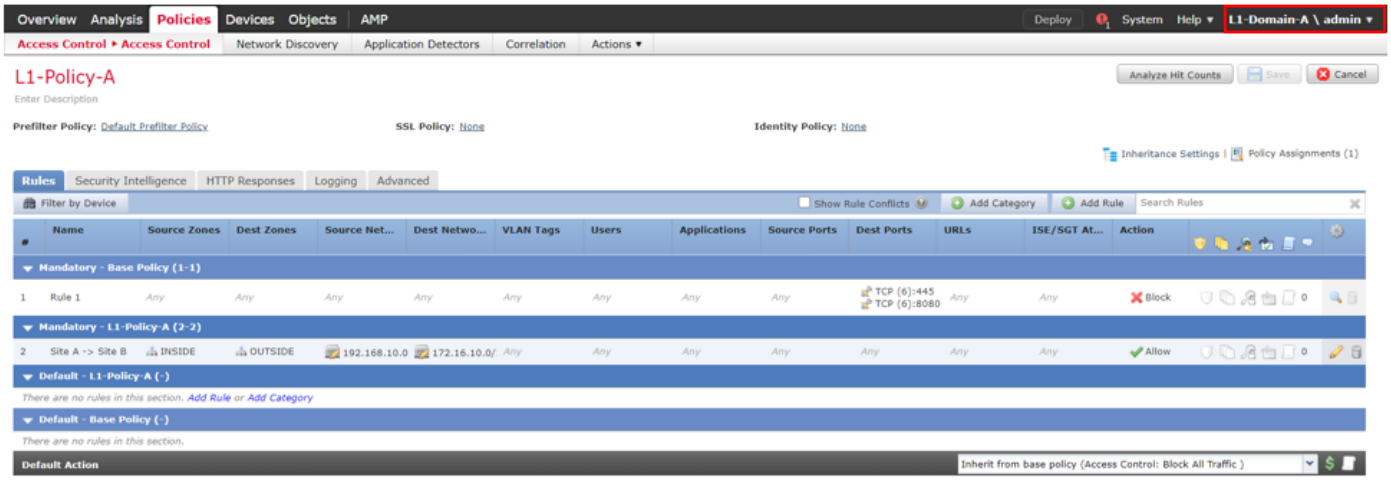


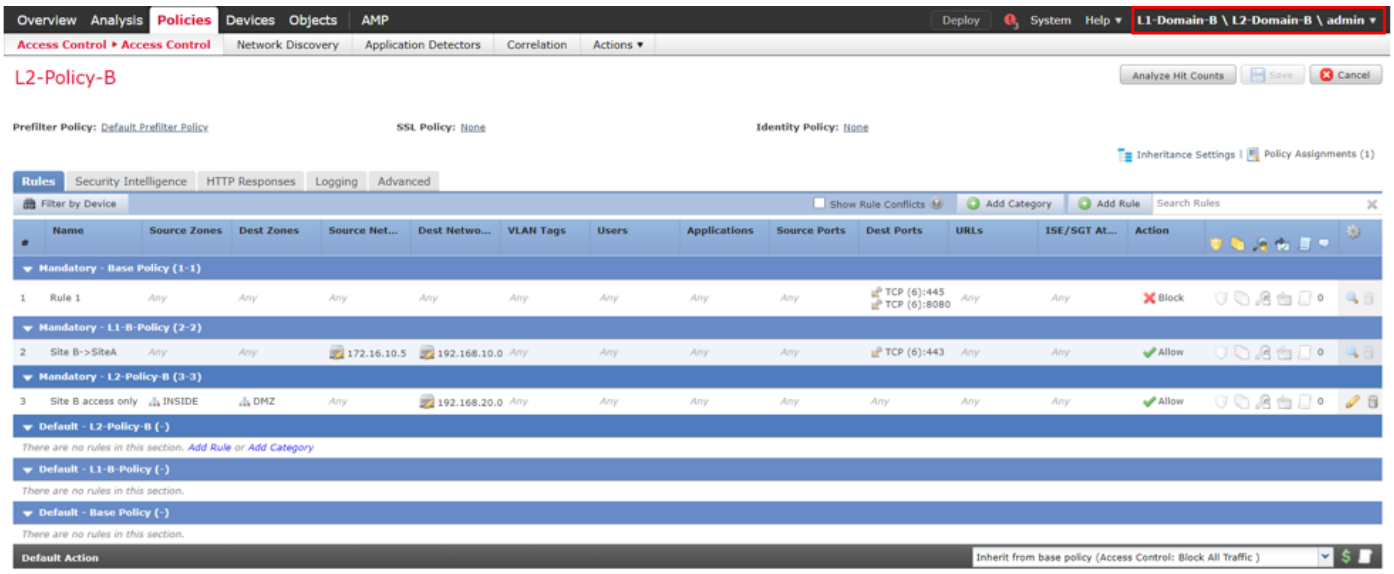
域層次的結構如下：

- **全局網域是L1-Domain-A 和L1-Domain-B的父網域。**
- **全局網域是L2-Domain-B的祖先。**
- **L2-Domain-B是L1-Domain-B的子項**
- **L2-Domain-B是**枝葉域，因為它沒有子域。

該圖顯示了從FMC中看到的域層次結構。

以下快照顯示了如何在**L1-Policy-A**和**L2-Policy-B** w.r.t中針對上述方案定義規則。





配置多個域時，應始終注意規則及其繼承，以避免阻止合法流量或允許不需要的流量。