在安全防火牆管理中心(FMC)上配置身份策略

目錄

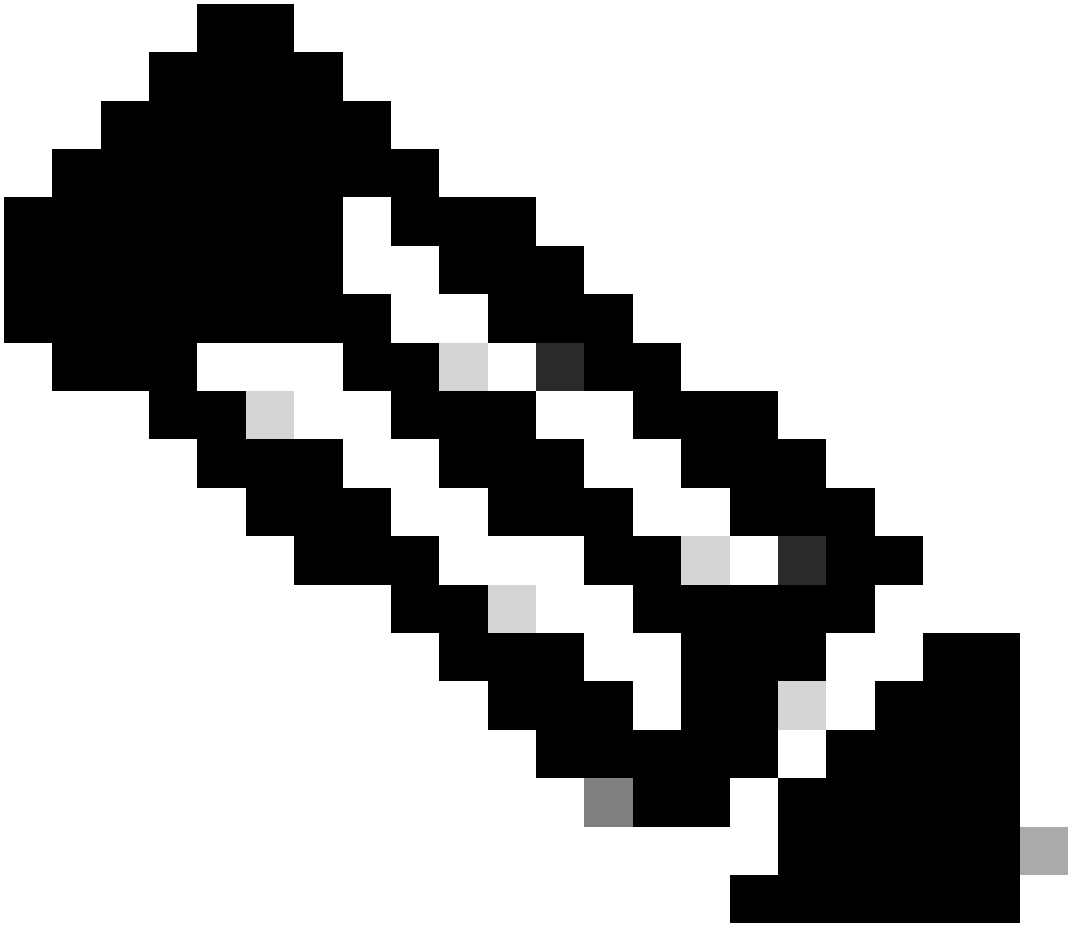
簡介

本檔案介紹如何透過安全FMC為安全FTD流量設定和部署辨識原則的程式。

必要條件

1. 已在FMC中配置領域。

2. 已配置身份源- ISE、ISE-PIC。



注意：ISE和領域配置說明不在本文檔的討論範圍之內。

需求

思科建議瞭解以下主題：

- 安全防火牆管理中心(FMC)
- 安全防火牆執行緒防禦(FTD)
- 思科身分辨識服務引擎(ISE)
- LDAP/AD伺服器
- 驗證方法

1. 被動身份驗證：使用外部身份使用者源，例如ISE
2. 主動身份驗證：將受管裝置用作身份驗證源（強制網路門戶或遠端VPN訪問）
3. 無身份驗證

採用元件

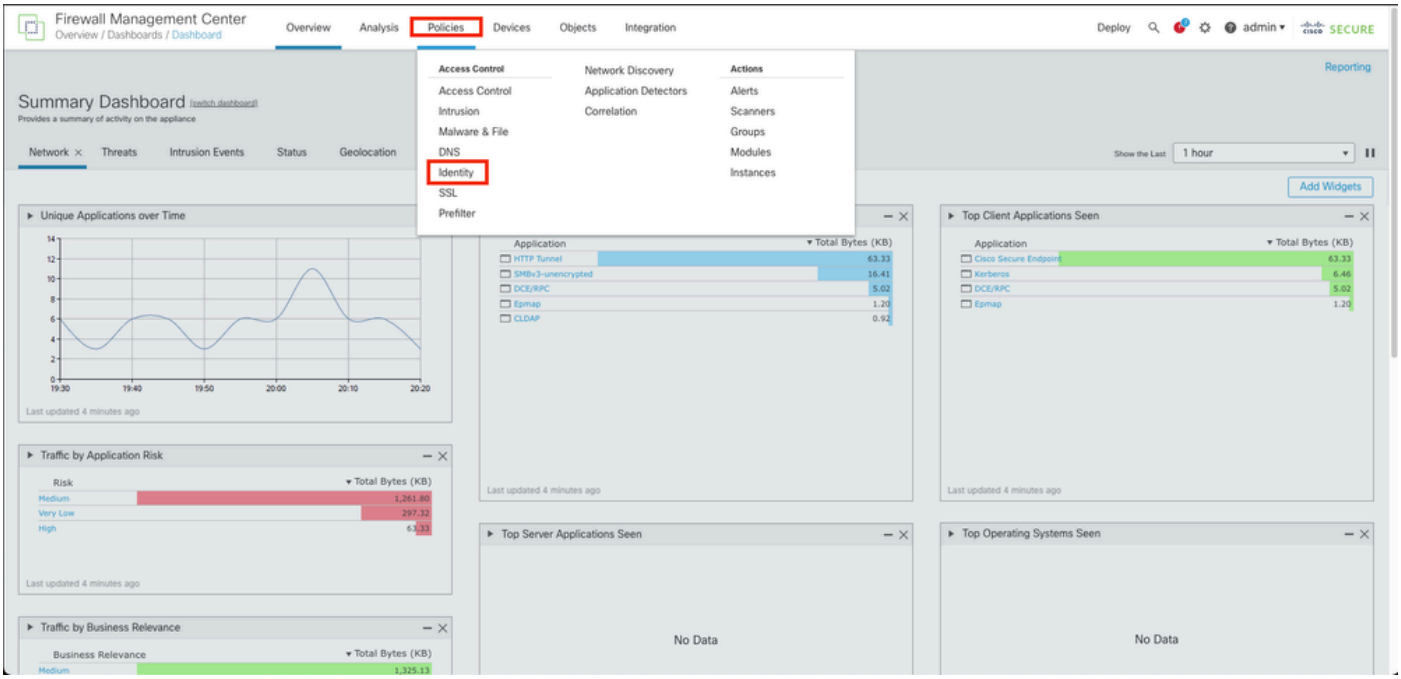
- 適用於VMWare v7.2.5的安全防火牆管理中心
- 適用於VMWare v7.2.4的思科安全防火牆威脅防禦
- Active Directory伺服器
- 思科身份服務引擎(ISE) v3.2修補4
- 被動驗證方法

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

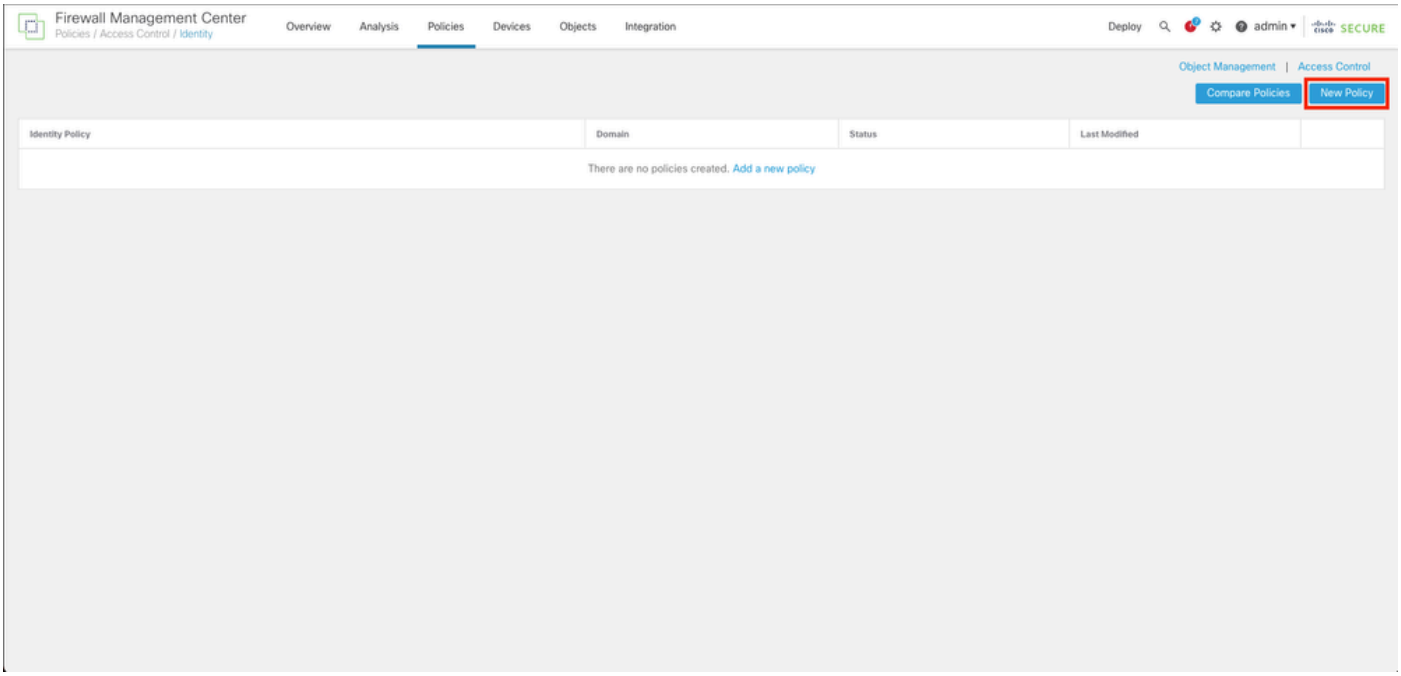
設定

組態

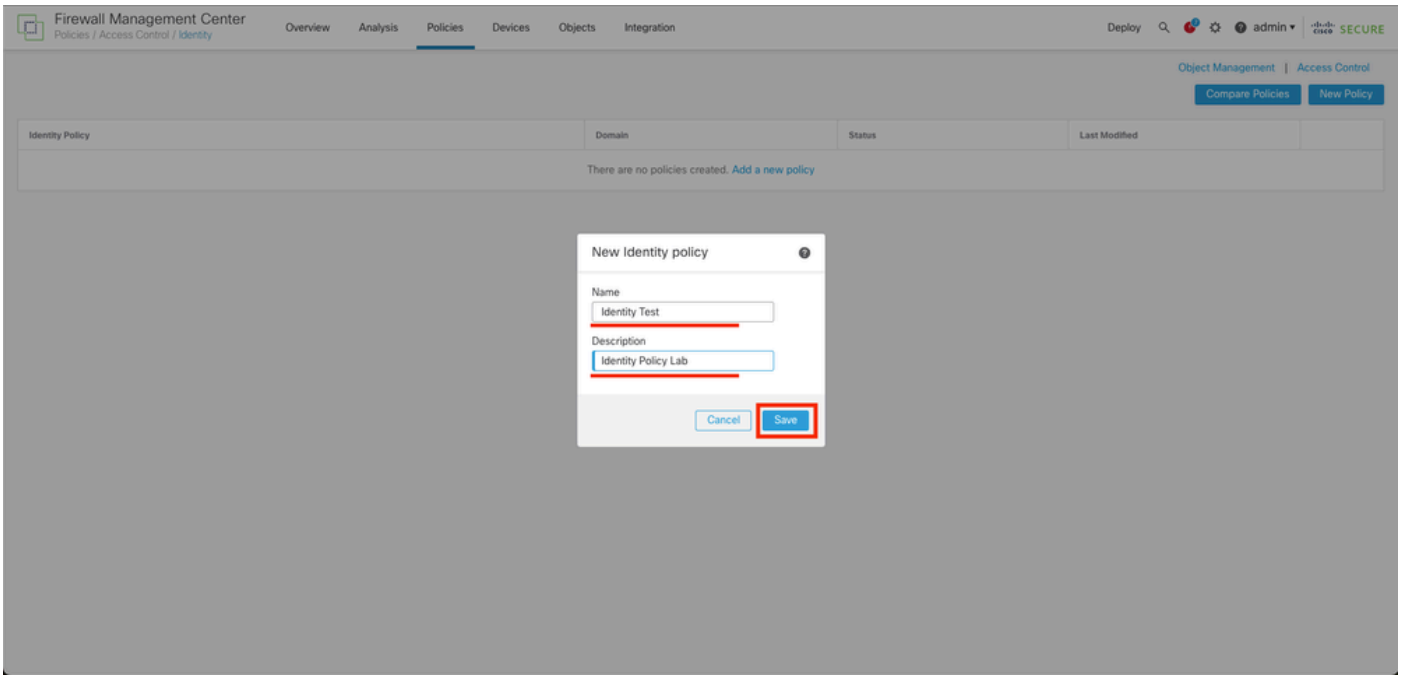
第1步：在FMC GUI中，導航到策略>訪問控制>身份



步驟2.按一下New Policy。

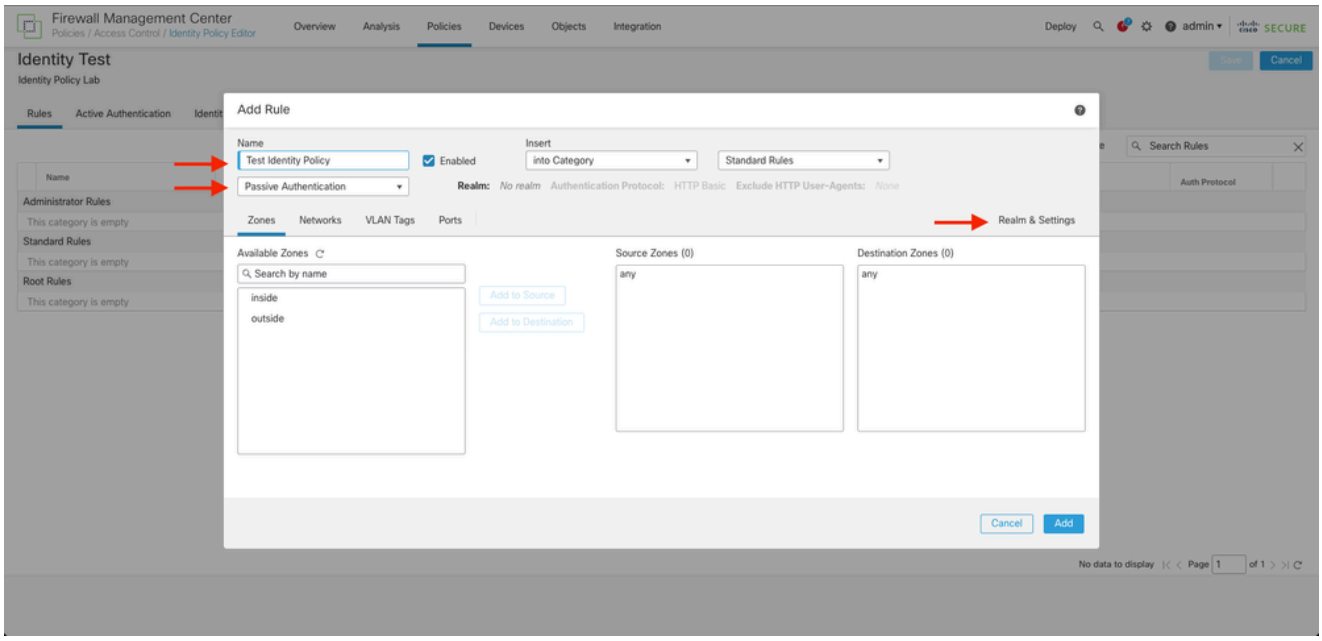


第3步：為新Identity Policy分配名稱和說明，然後按一下Save。

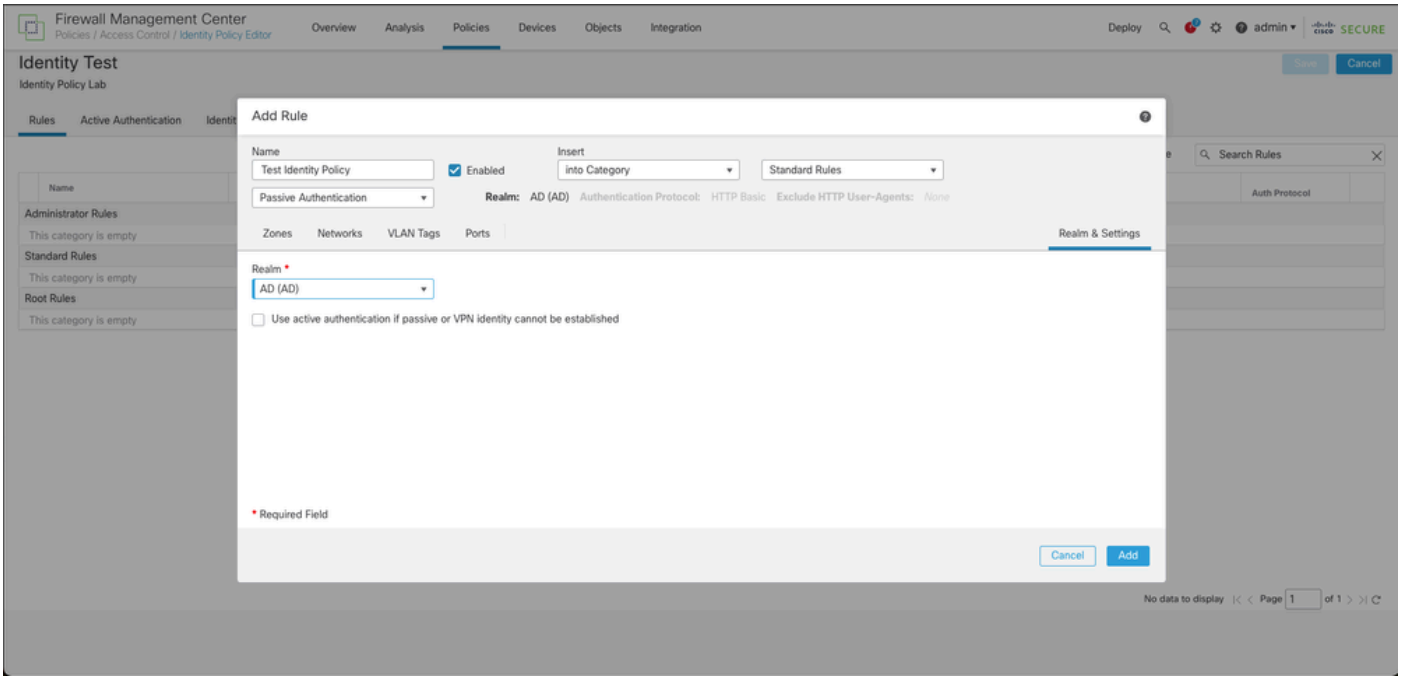


步驟 4.點選+增加規則圖示。

1. 為新規則指定名稱。
2. 在name欄位下，選擇身份驗證方法，選擇Passive Authentication。
3. 在熒幕右邊選取範圍與設定。

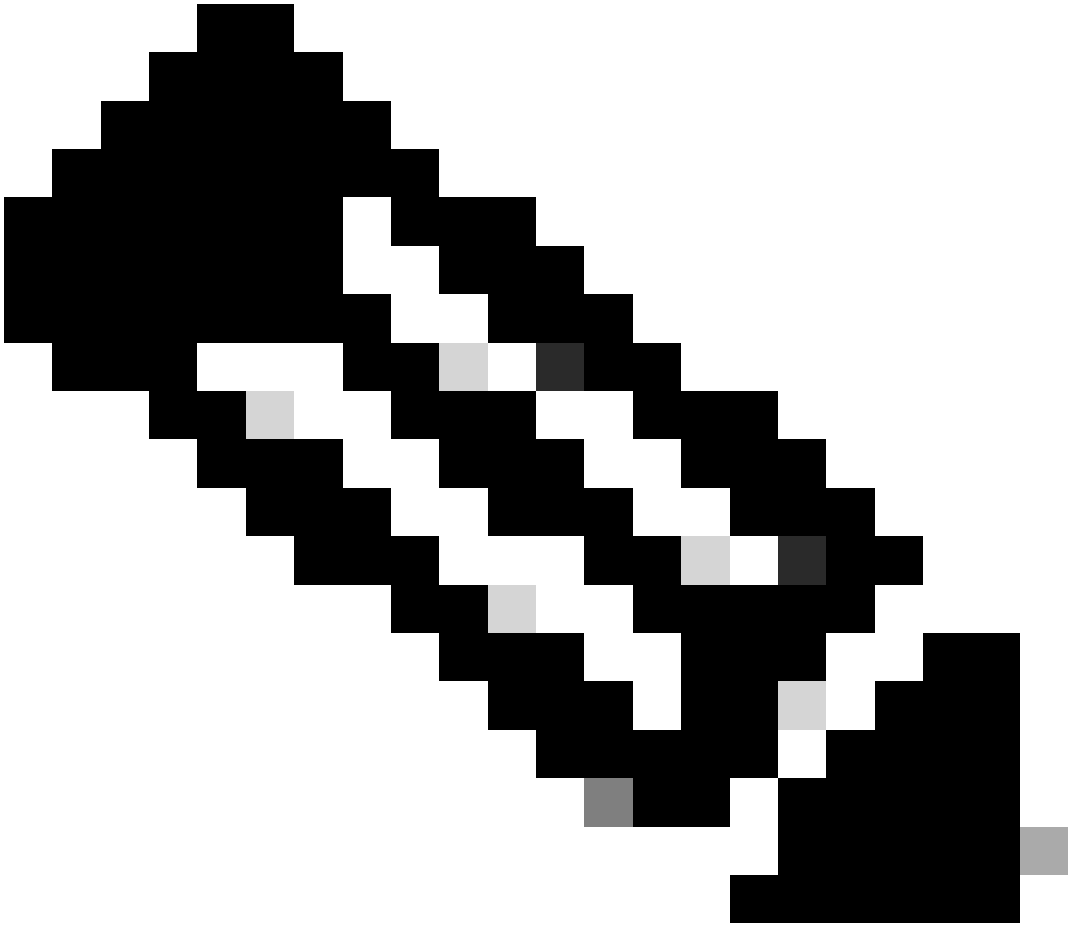


4.從下拉式功能表中選取範圍。



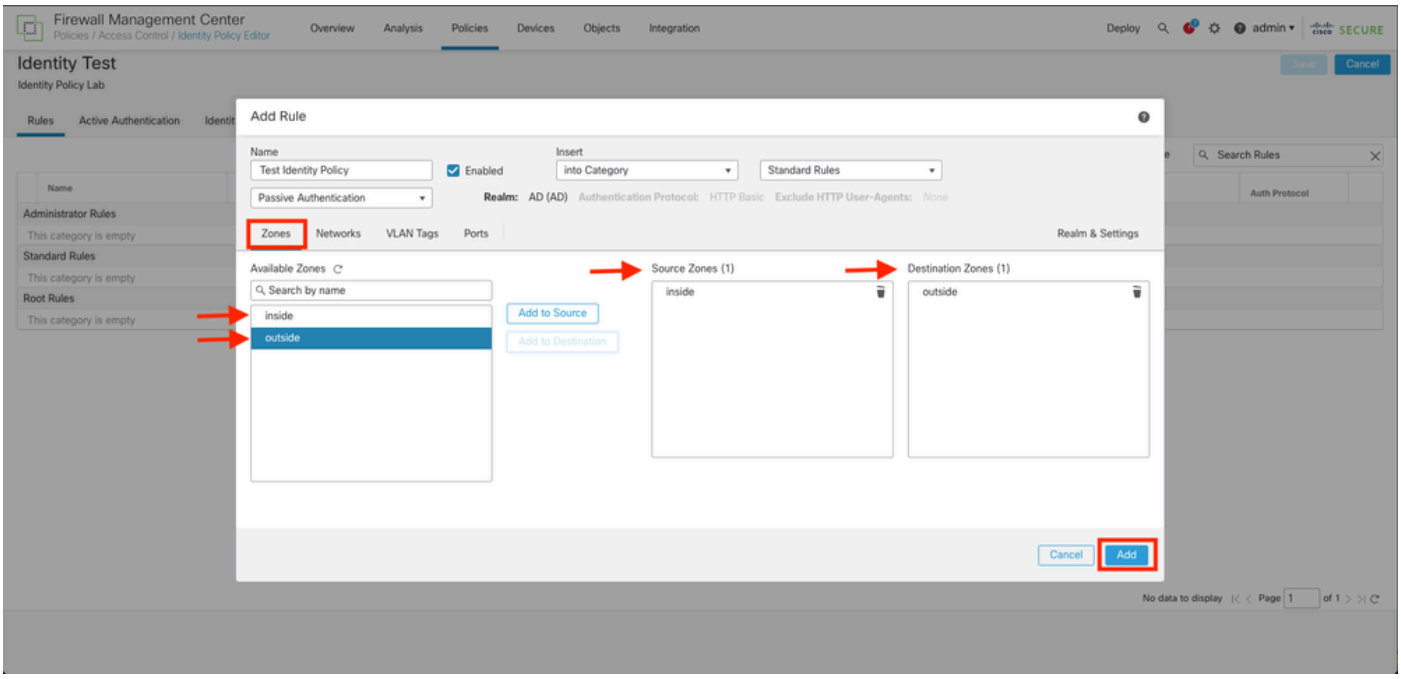
5. 按一下螢幕左側的Zones。

6. 從可用區域選單中，根據檢測使用者所需的流量路徑分配源和目標區域。要增加區域，請點選區域的名稱，然後根據具體情況，選擇Add to Source或Add to Destination。

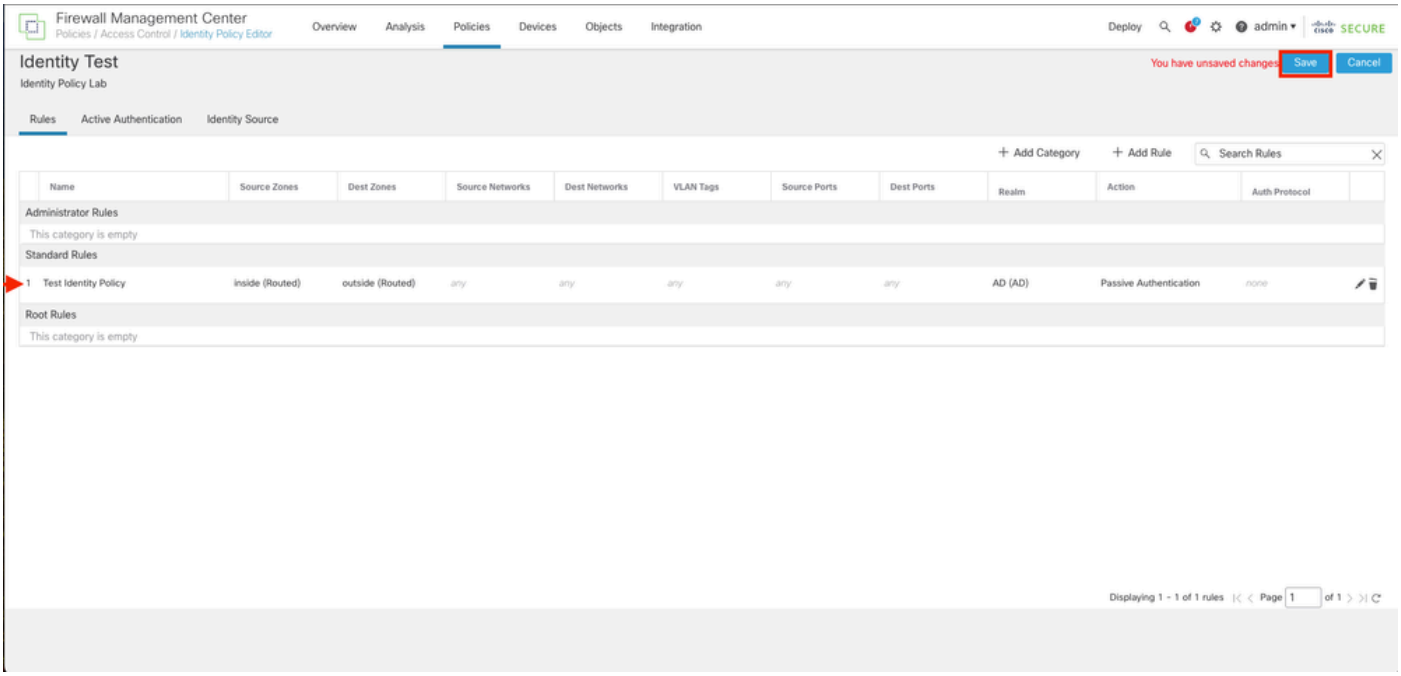


注意：在本文檔中，使用者檢測僅應用於來自內部區域的流量，並且該流量被轉發到外部區域。

7. 選擇增加和儲存。

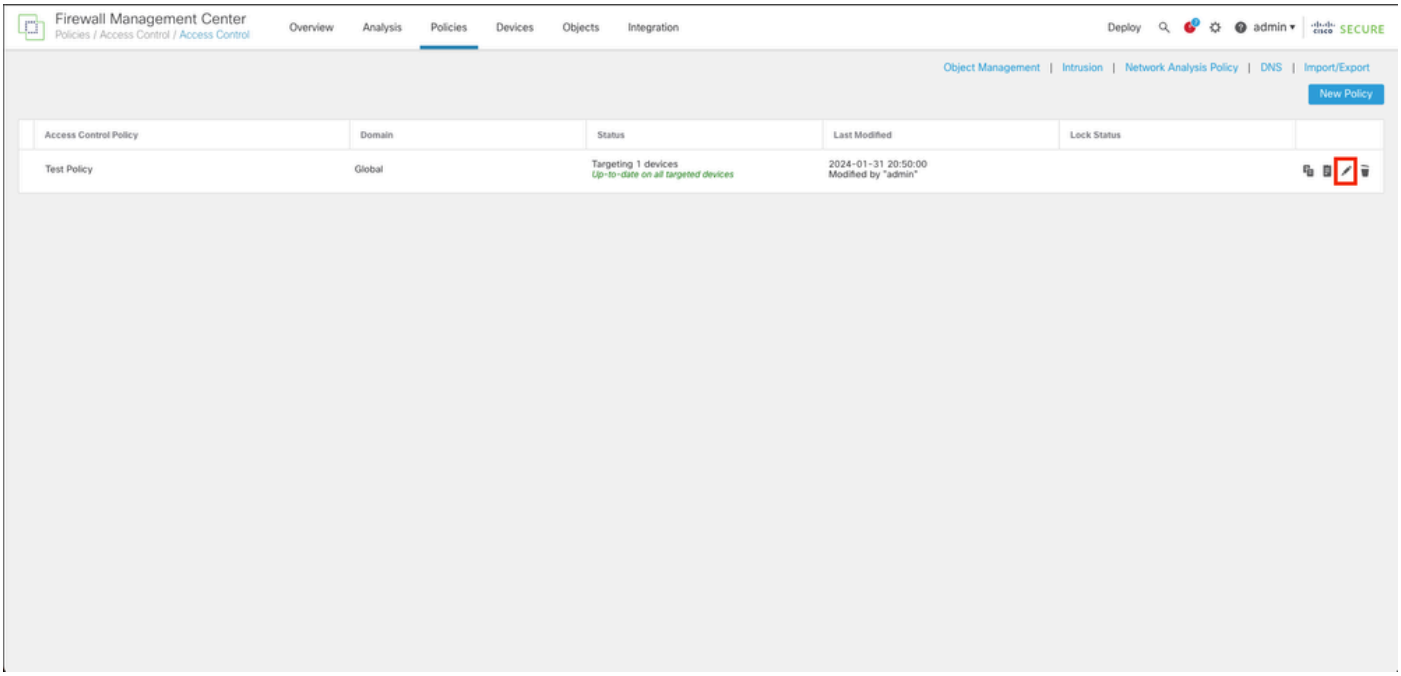


步驟 5.驗證新規則是否在身份策略中，然後按一下Save。

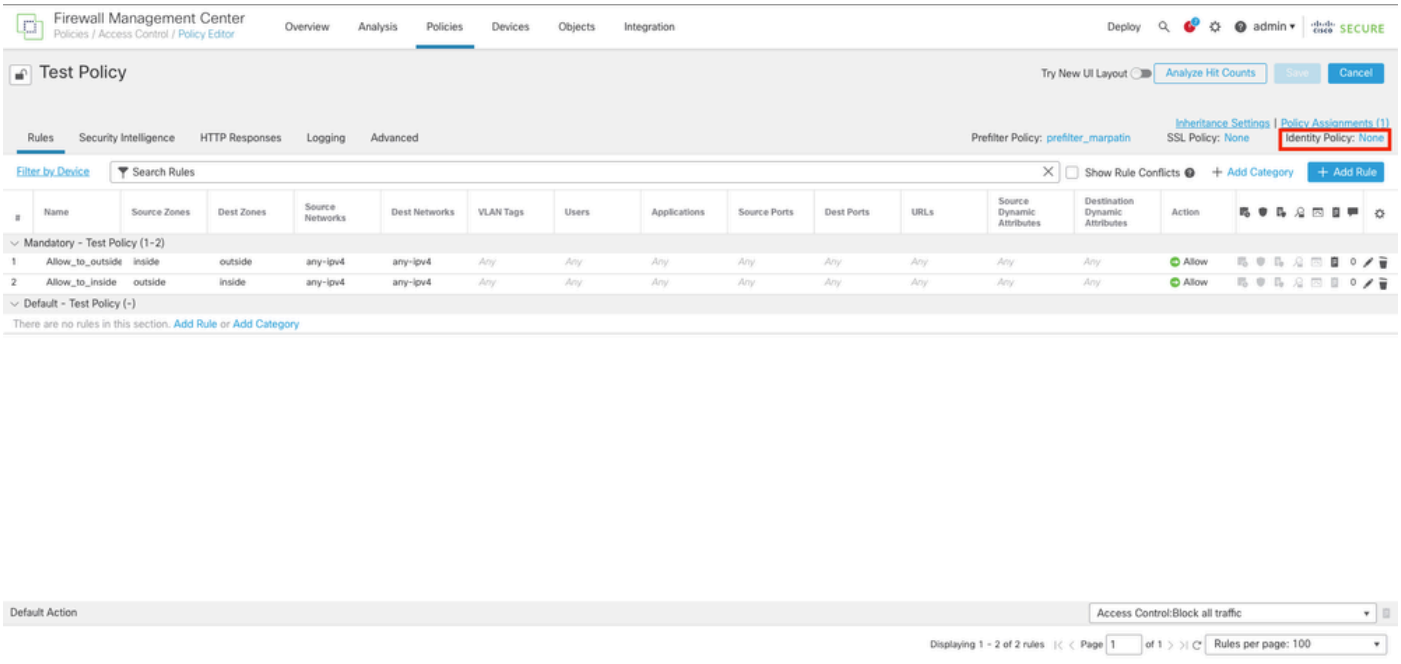


步驟 6. 導航到策略>訪問控制

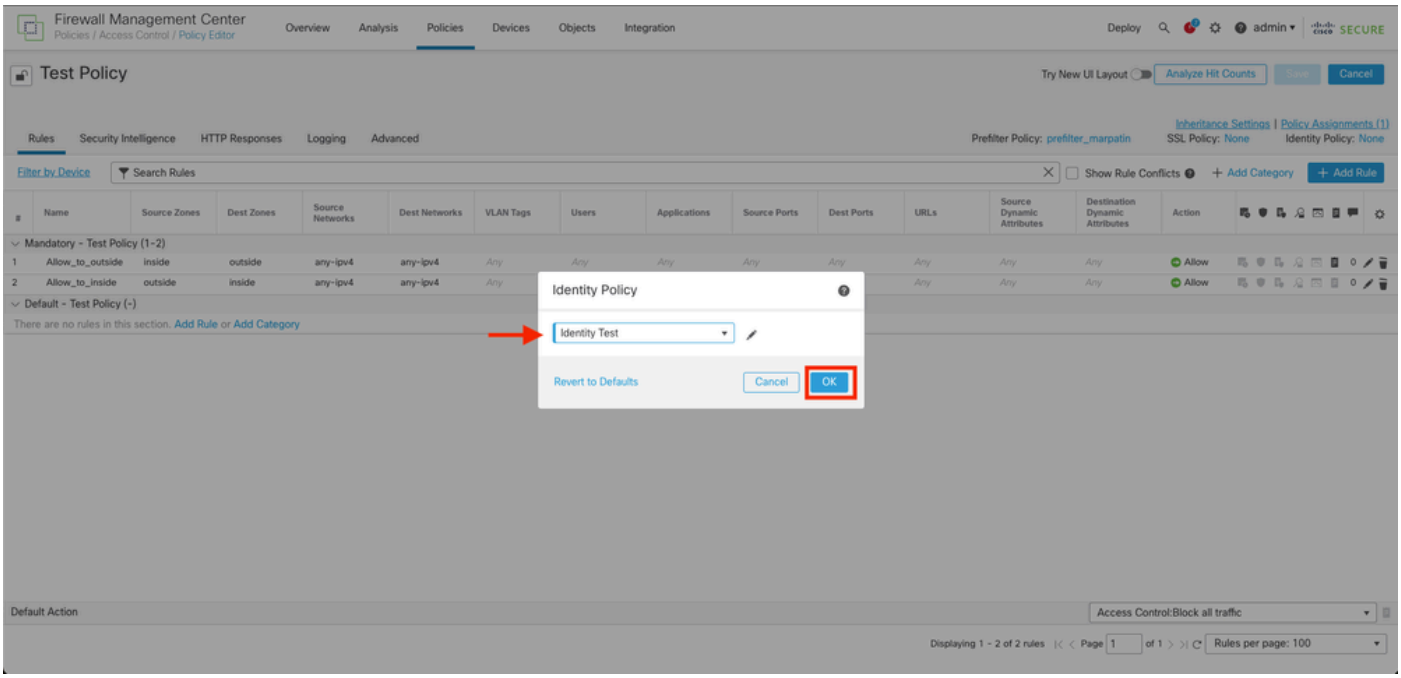
步驟 7.確定它將在處理使用者流量的防火牆中部署的訪問控制策略，並按一下超過鉛筆圖示以編輯策略。



步驟 6. 在Identity Policy欄位中按一下None。



步驟 7.從下拉選單中選擇之前在步驟3中建立的「Policy」，然後按一下OK以完成配置。

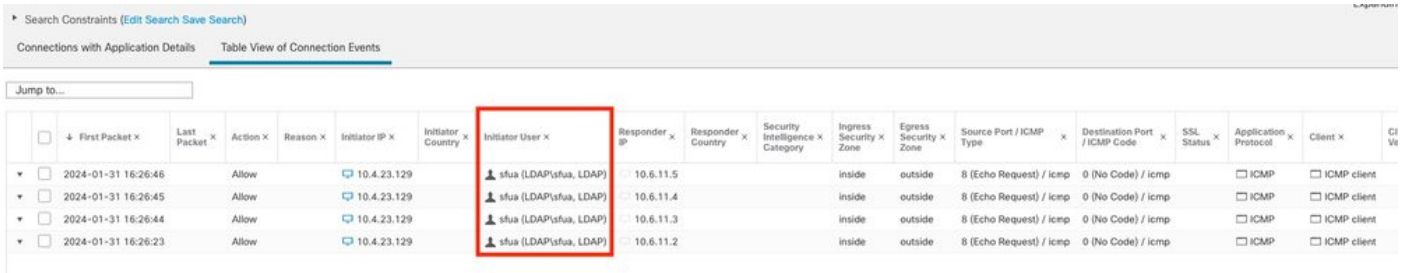


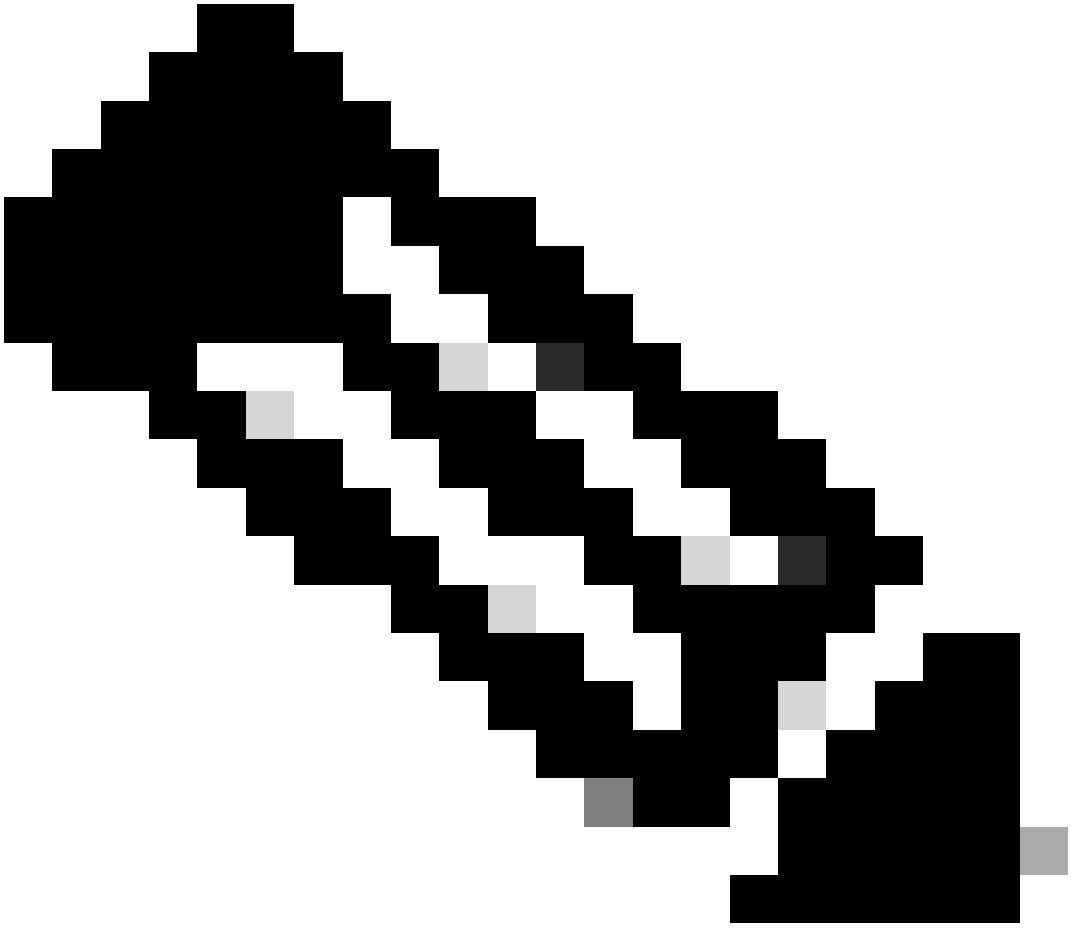
步驟8.儲存並部署組態至FTD。

驗證

1. 在FMC GUI中，導航至分析>使用者：活動會話

3. 從分析>連線>事件：連線事件的表格檢視進行驗證





注意：與「身份策略」和「訪問控制策略」的流量條件匹配的使用者在其使用者名稱欄位中顯示。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。