

在安全防火牆管理中心(FMC)上配置身份策略

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[組態](#)

[驗證](#)

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

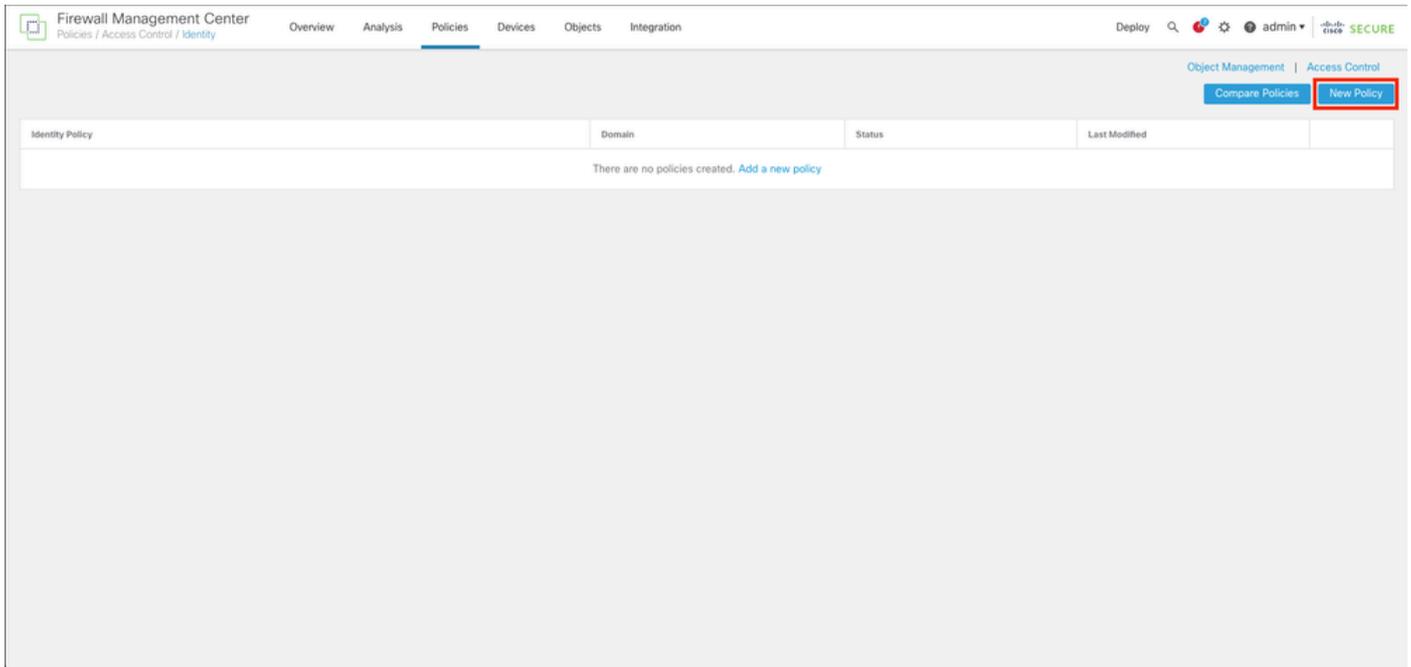
組態

第1步：在FMC GUI中，導航到策略>訪問控制>身份

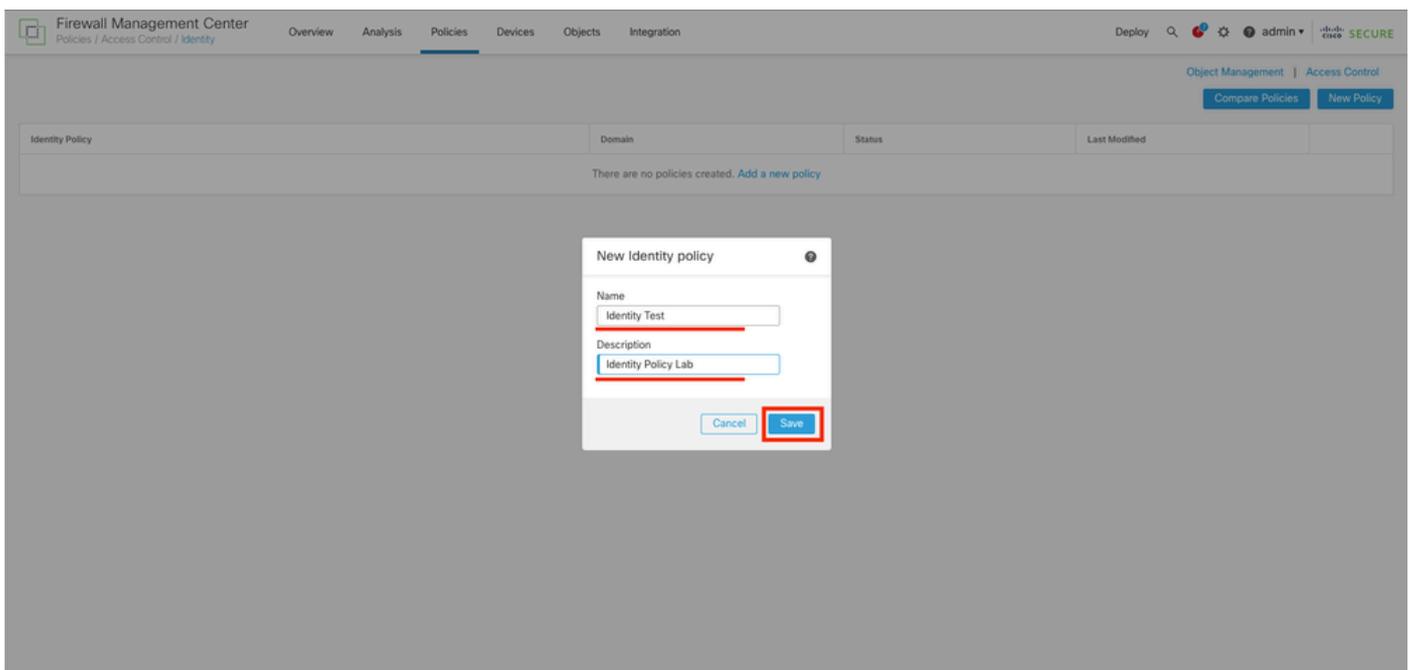
The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Policies' menu is open, showing a list of categories: Access Control, Network Discovery, Actions, Access Control, Application Detectors, Alerts, Intrusion, Correlation, Scanners, Malware & File, Groups, Modules, DNS, Identity (highlighted with a red box), Instances, SSL, and Prefilter. The main dashboard area shows a 'Summary Dashboard' with various widgets: 'Unique Applications over Time' (line graph), 'Traffic by Application Risk' (horizontal bar chart), 'Traffic by Business Relevance' (horizontal bar chart), 'Top Client Applications Seen' (table), 'Top Server Applications Seen' (No Data), and 'Top Operating Systems Seen' (No Data). The 'Top Client Applications Seen' table lists applications and their total bytes:

Application	Total Bytes (KB)
HTTP Tunnel	63.33
SMBv3-unencrypted	16.41
DCE/RPC	5.02
Emap	1.24
LDAP	0.92

步驟2. 按一下New Policy。

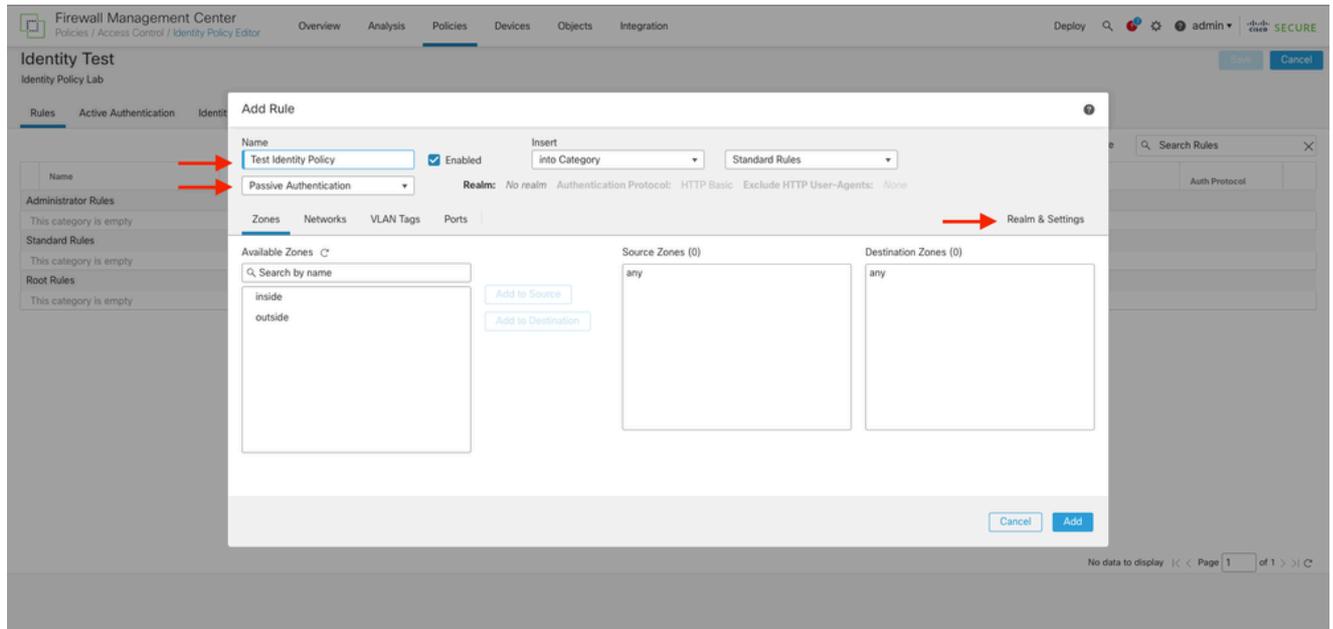


第3步：為新Identity Policy分配名稱和說明，然後按一下Save。

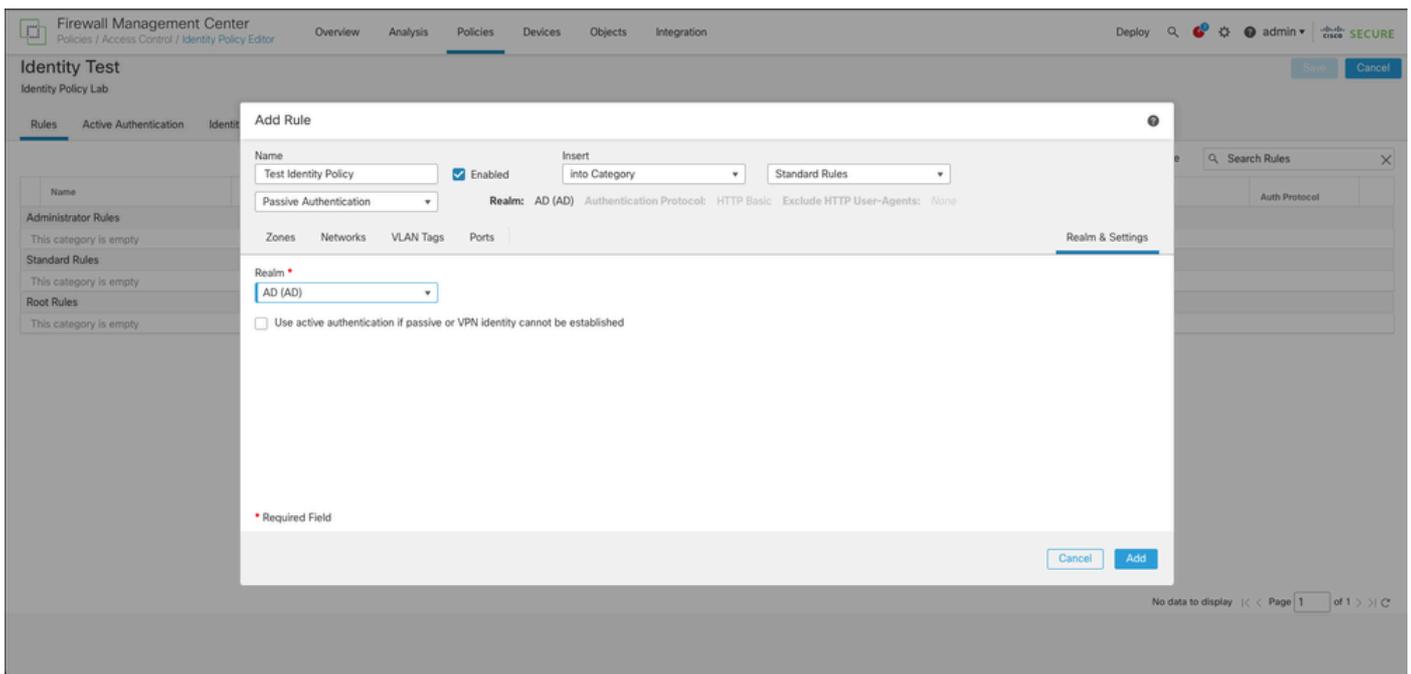


步驟 4. 點選+增加規則圖示。

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. 在螢幕右邊選取範圍與設定。

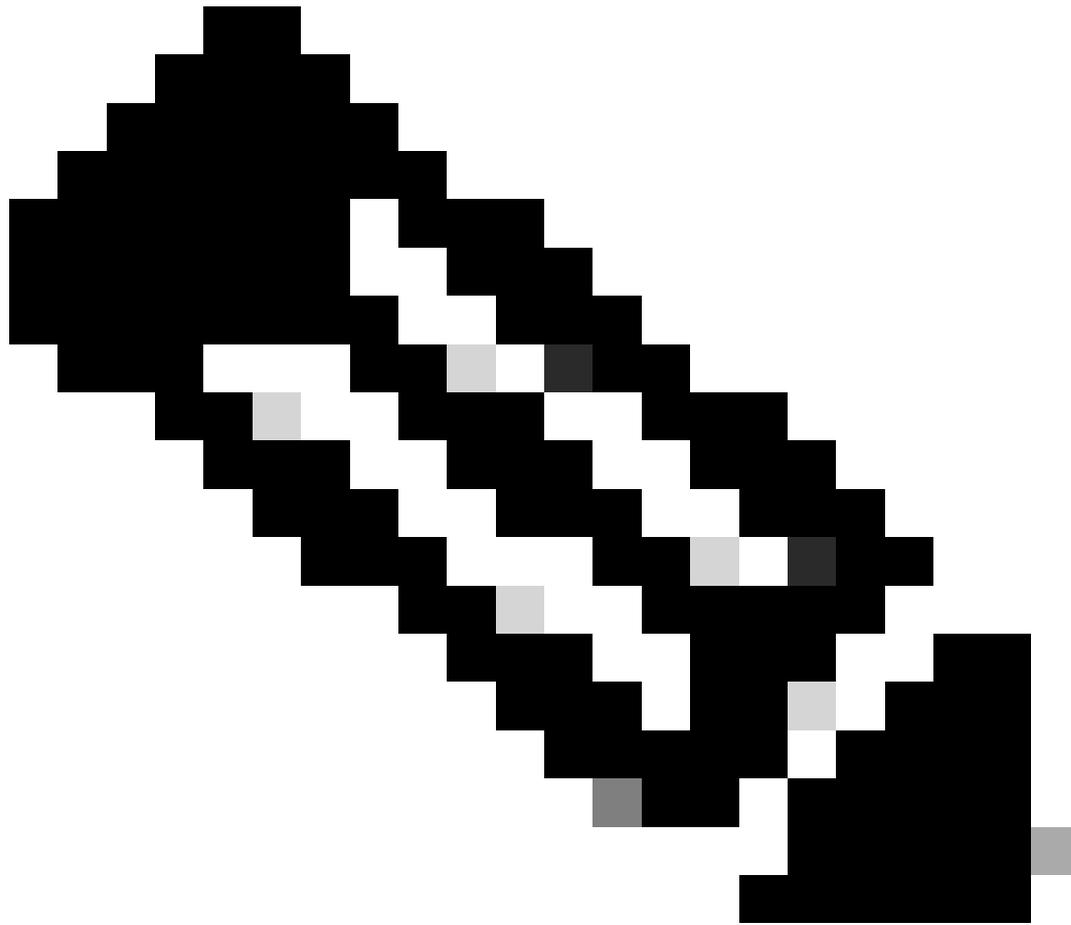


4. 從下拉式功能表中選取範圍。



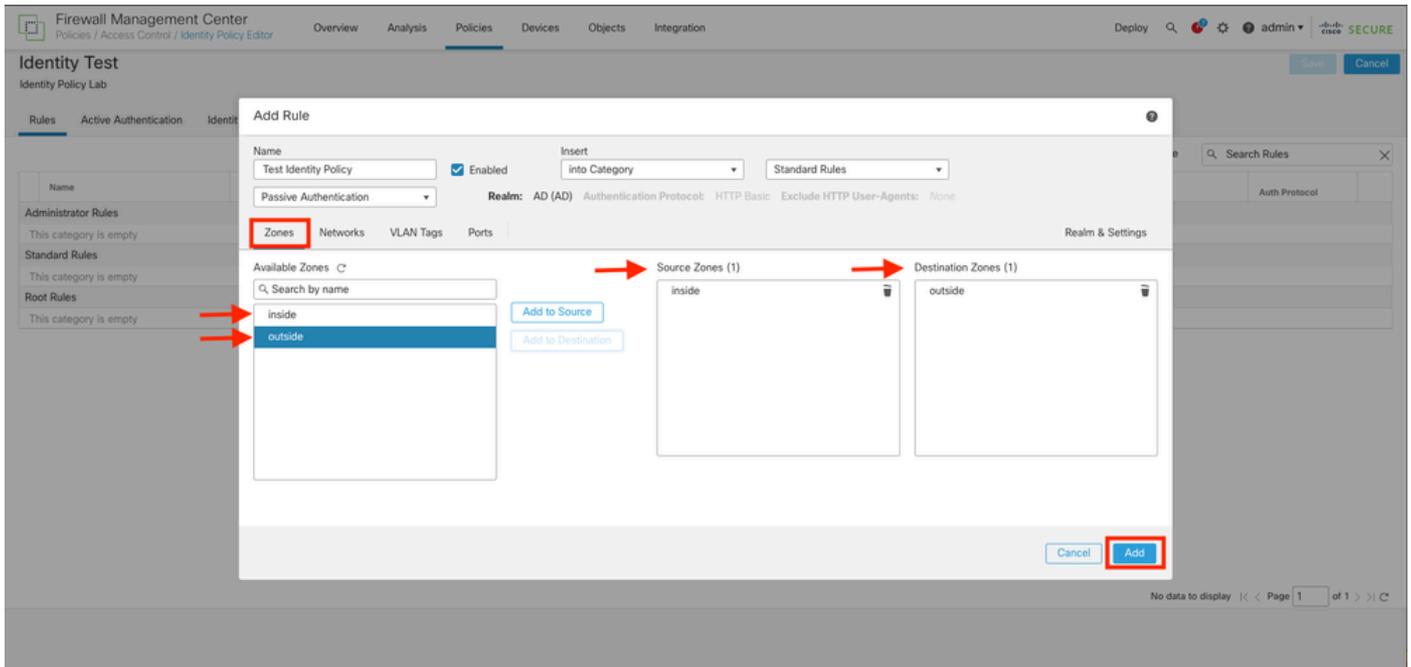
5. 按一下螢幕左側的Zones。

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。

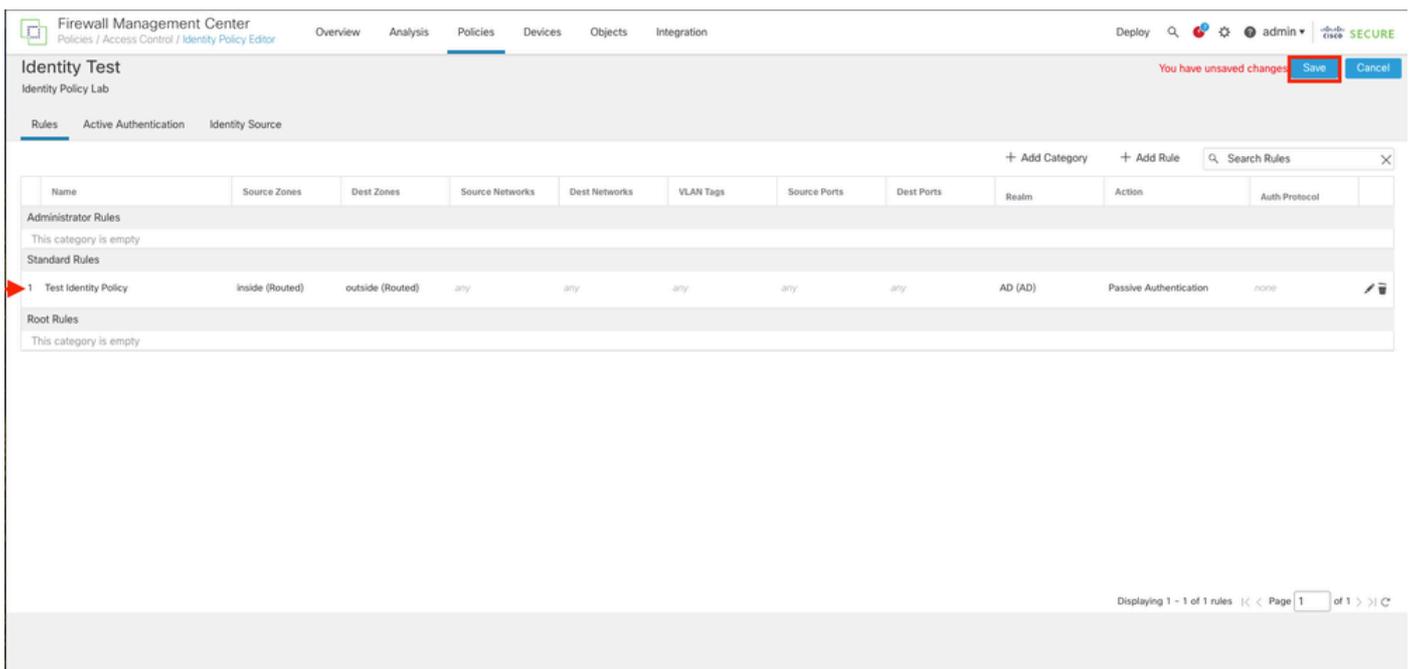


注意：在本文檔中，使用者檢測僅應用於來自內部區域的流量，並且該流量被轉發到外部區域。

7. 選擇增加和儲存。

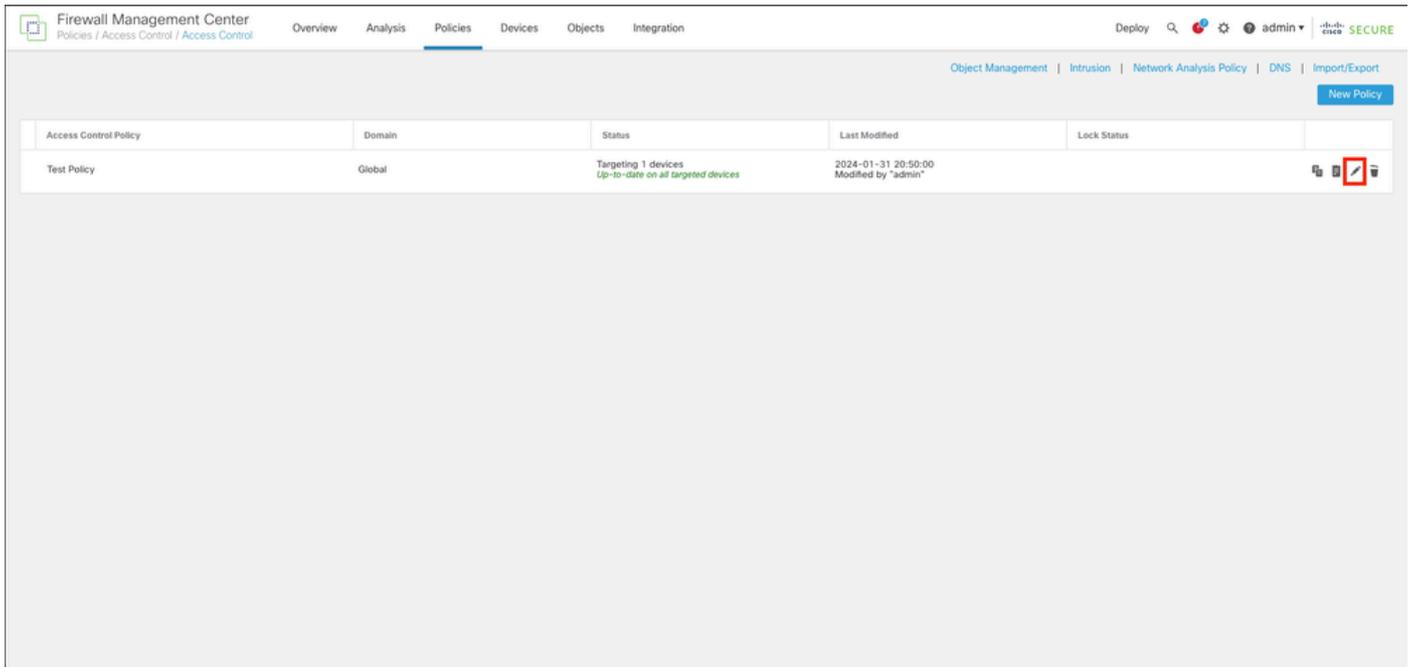


步驟 5. 驗證新規則是否在身份策略中，然後按一下Save。

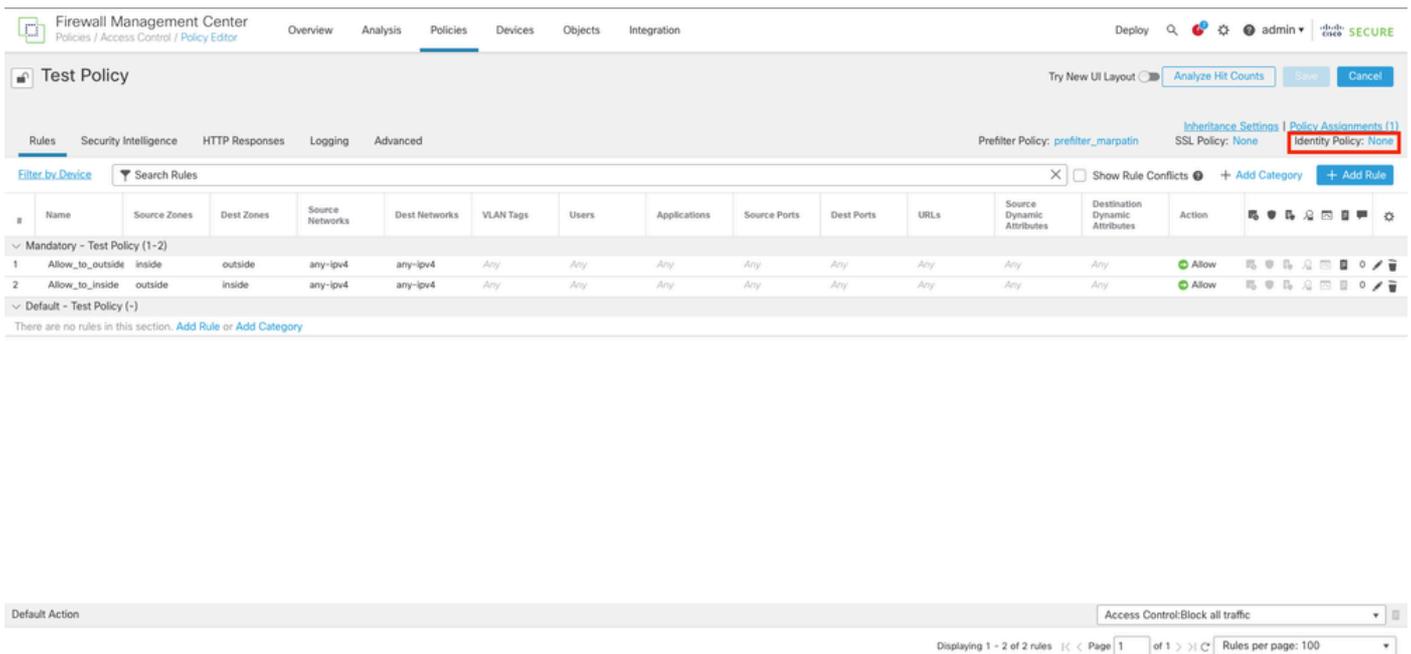


步驟 6. 導航到策略>訪問控制

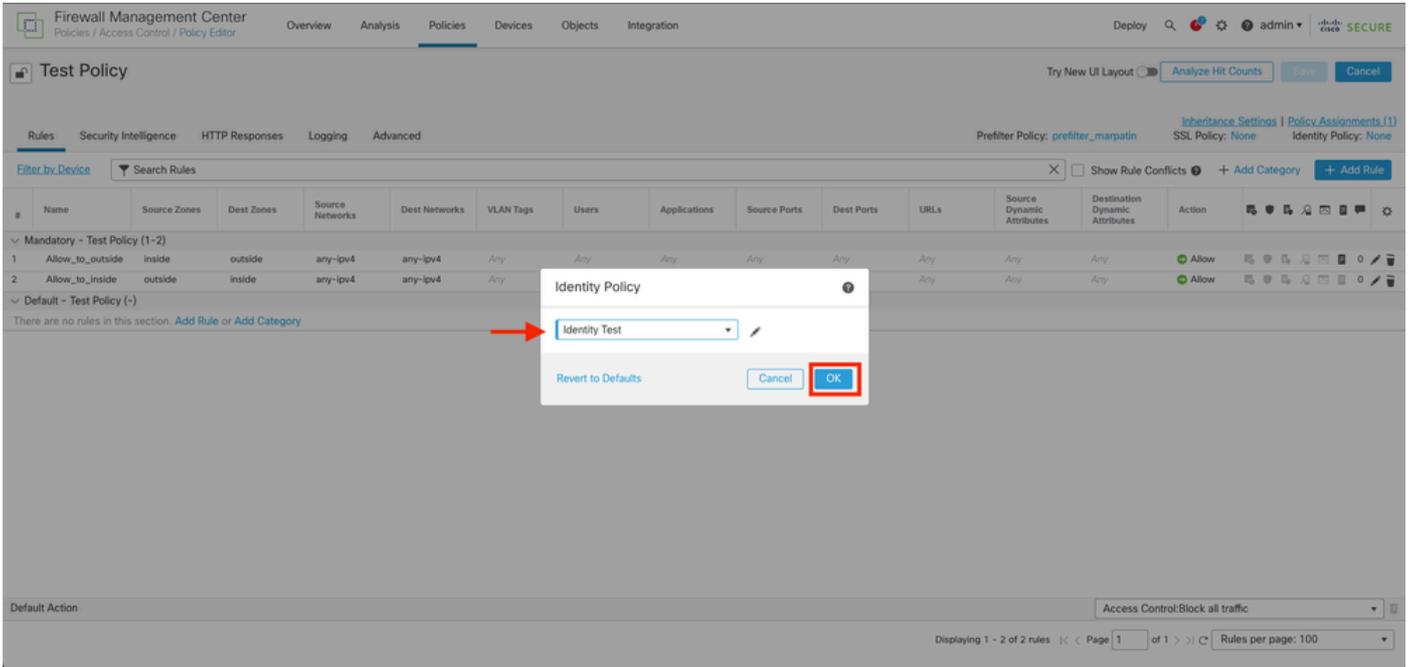
步驟 7. 確定它將在處理使用者流量的防火牆中部署的訪問控制策略，並按一下超過鉛筆圖示以編輯策略。



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

No Search Constraints (Edit Search)

Table View of Active Sessions Active Sessions

Jump to...

	Login Time x	Last Seen x	User x	Authentication Type x	Current IP x	Realm x	Username x	First Name x	Last Name x	E-Mail x	Department x	Phone x	Discovery Application x	Device x
▼	2024-01-09 15:20:06	2024-01-31 16:21:08	sfua (LDAP\sfua, LDAP)	Passive Authentication	10.4.23.129	LDAP	sfua	sfua		sfua@orgeju.local	users (orgeju)		LDAP	frepower

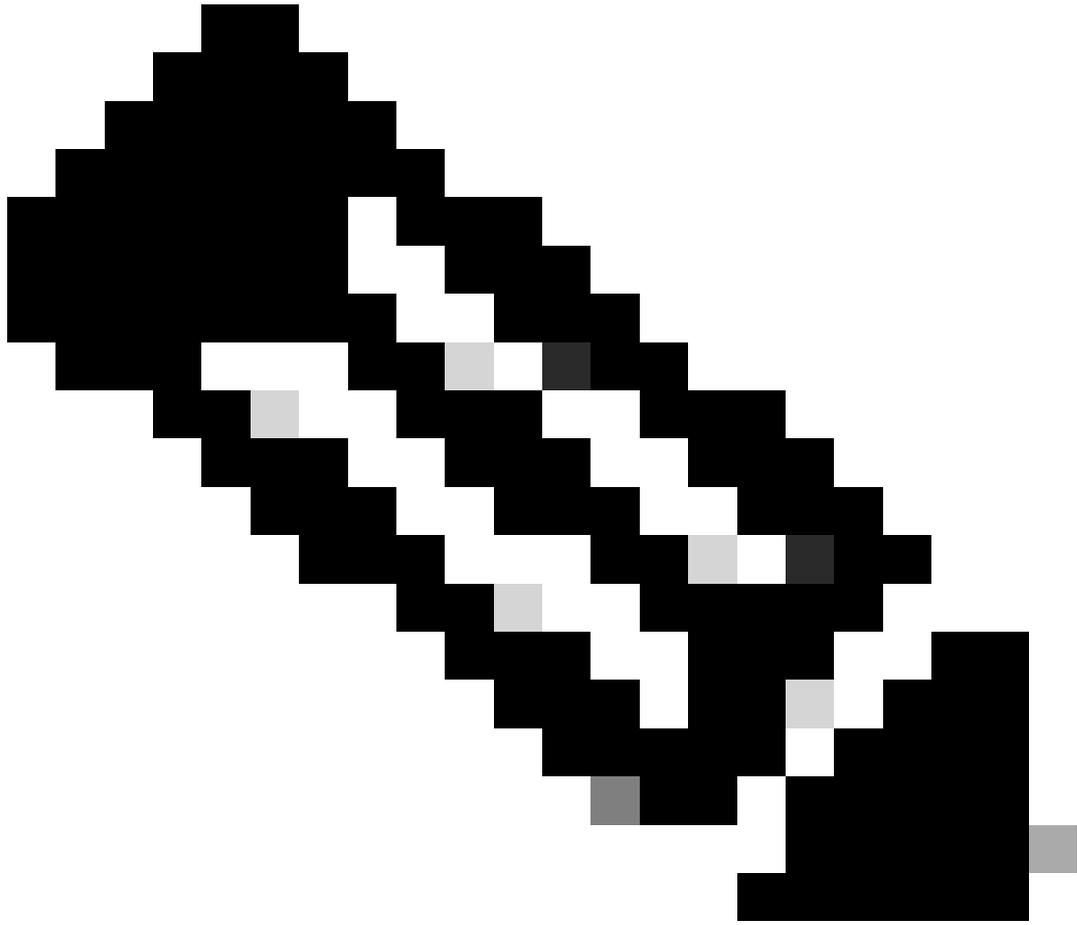
3. 從分析>連線>事件：連線事件的表格檢視進行驗證

Search Constraints (Edit Search Save Search)

Connections with Application Details Table View of Connection Events

Jump to...

	First Packet x	Last Packet x	Action x	Reason x	Initiator IP x	Initiator Country x	Initiator User x	Responder IP x	Responder Country x	Security Intelligence x Category	Ingress Security Zone x	Egress Security Zone x	Source Port / ICMP Type x	Destination Port / ICMP Code x	SSL Status x	Application Protocol x	Client x	CI Ve
▼	2024-01-31 16:26:46		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	10.6.11.5			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:45		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	10.6.11.4			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:44		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	10.6.11.3			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
▼	2024-01-31 16:26:23		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	10.6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	



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）。