思科安全防火牆/防火牆管理中心/自適應安全裝置指南 — 緊急不信任根和中間證書頒發機構

目錄

目的

以下是關於思科安全防火牆威脅防禦(FTD)、思科安全防火牆管理中心(FMC)和自適應安全裝置(ASA)的指南，針對木德拉根和中間證書頒發機構的緊急不信任。

FMC本地思科服務證書捆綁更新

FMC和FTD可以自動更新本地CA捆綁包，用於從裝置到思科服務的TLS連線，包括智慧許可和軟體、VDB、SRU和地理位置更新。系統在系統定義的時間每天進行檢查。從FMC/FTD 7.0.5、7.1.0.3、7.2.4和7.3.0+開始，思科文檔功能可用。這些是功能閾值，不是推薦的升級目標；使用確切的平台、來源版本、相容性要求和目前的思科版本指南選擇升級目標。[3、4]

在支援的FMC或FTD CLI上，`show cert-update`會報告自動更新狀態、每日排程和套件組合的上次修改時間。`configure cert-update test`將檢查本地捆綁包是否最新以及更新連線是否就緒。[4, 5, 6]

此思科服務捆綁包與SSL解密所使用的FTD已配置可信CA對象/組以及身份或VPN證書所用的裝置信任點分離。您將需要驗證這些證書是否均未手動新增到配置中。[5、6]

ASA CA trustpool自動匯入

在ASA上，CA信任池和命名信任點是獨立的證書管理功能。信任池儲存CA證書；信任點是用於證書身份和CA註冊的命名配置。ASA trustpool auto-import還獨立於上述FMC/FTD思科服務捆綁更新。[8、9]

對於只讀檢查，請運行`show crypto ca trustpool policy`以檢視trustpool證書計數、匯入狀態和結果、下一次計畫嘗試以及有效策略詳細資訊。運行`show run crypto ca trustpool policy`以檢視配置的信任池策略行。預設情況下，思科文檔自動匯入為關閉。啟用無覆蓋時，記錄的計畫每24小時22:00進行一次嘗試，並且使用預設的Cisco URL;配置的時間或URL可以更改這些值。檢查實際的ASA輸出，而不是假設啟用了自動匯入或使用預設計畫。[8、9]

這些檢查顯示策略和匯入狀態；它們不提供逐個證書的清單，也不確定已安裝、刪除或不信任任何命名的eMudra證書。不要從FMC/FTD `cert-update`推斷ASA行為，並且不要將信任池狀態視為有關在特定信任點或其他應用程式信任儲存下配置的證書的證據。在確定是否需要任何產品特定操作之前，請確認確切的ASA版本和證書相關服務。[8、9]

使用FTD保護未修補裝置的潛在解決方法

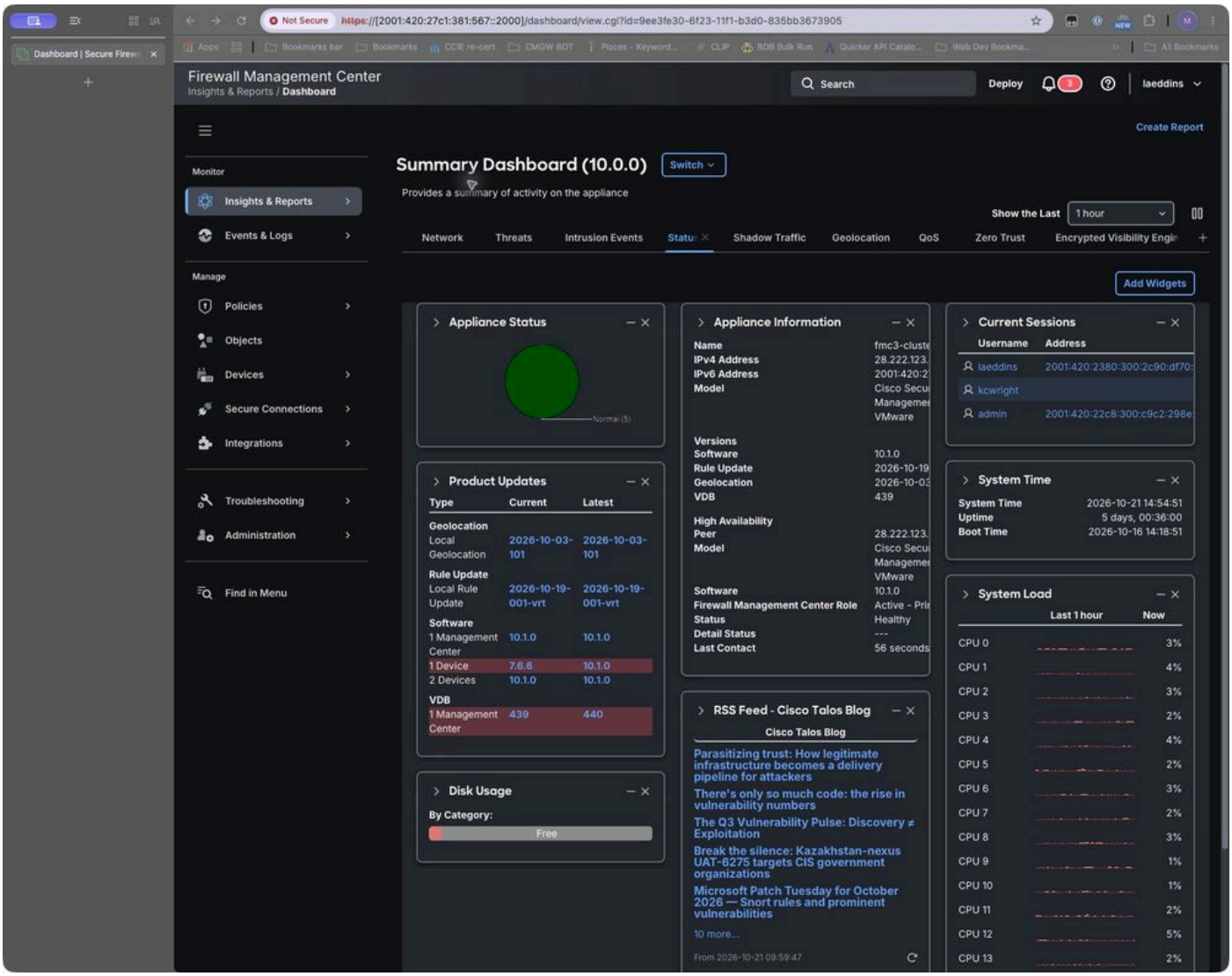
目的

使用Cisco Secure Firewall Management Center(FMC)配置TLS策略規則，該策略規則阻止具有已知受影響的eMudra頒發者名稱的伺服器證書。此控制元件可以減少無頭客戶端和伺服器的風險，這些客戶端和伺服器的應用程式信任儲存尚未收到所需的更新，但並非在所有情況下都阻止連線。 繼續信任儲存補救和證書替換。不要將受危害的CA匯入此過程的受信任CA。

必要條件

本文中的配置螢幕是在FMC 10.1.0上捕獲的。儀表板列出了10.0.0上的兩個受管裝置和7.6.6上的一個受管裝置。未執行流量測試。在執行驗證之前，請記錄目標FTD版本、Snort引擎、執行模式、訪問控制策略和TLS策略。確認受影響的出站流量達到預期策略。

圖1. FMC 10.1.0和受管裝置軟體清單。



配置頒發者匹配

Cisco記錄頒發者 — DN匹配頒發伺服器證書的CA的條件。在規則編輯器中新增DN對象並新增到頒發者。可用導航和標籤取決於版本。[1、2]

1建立對象

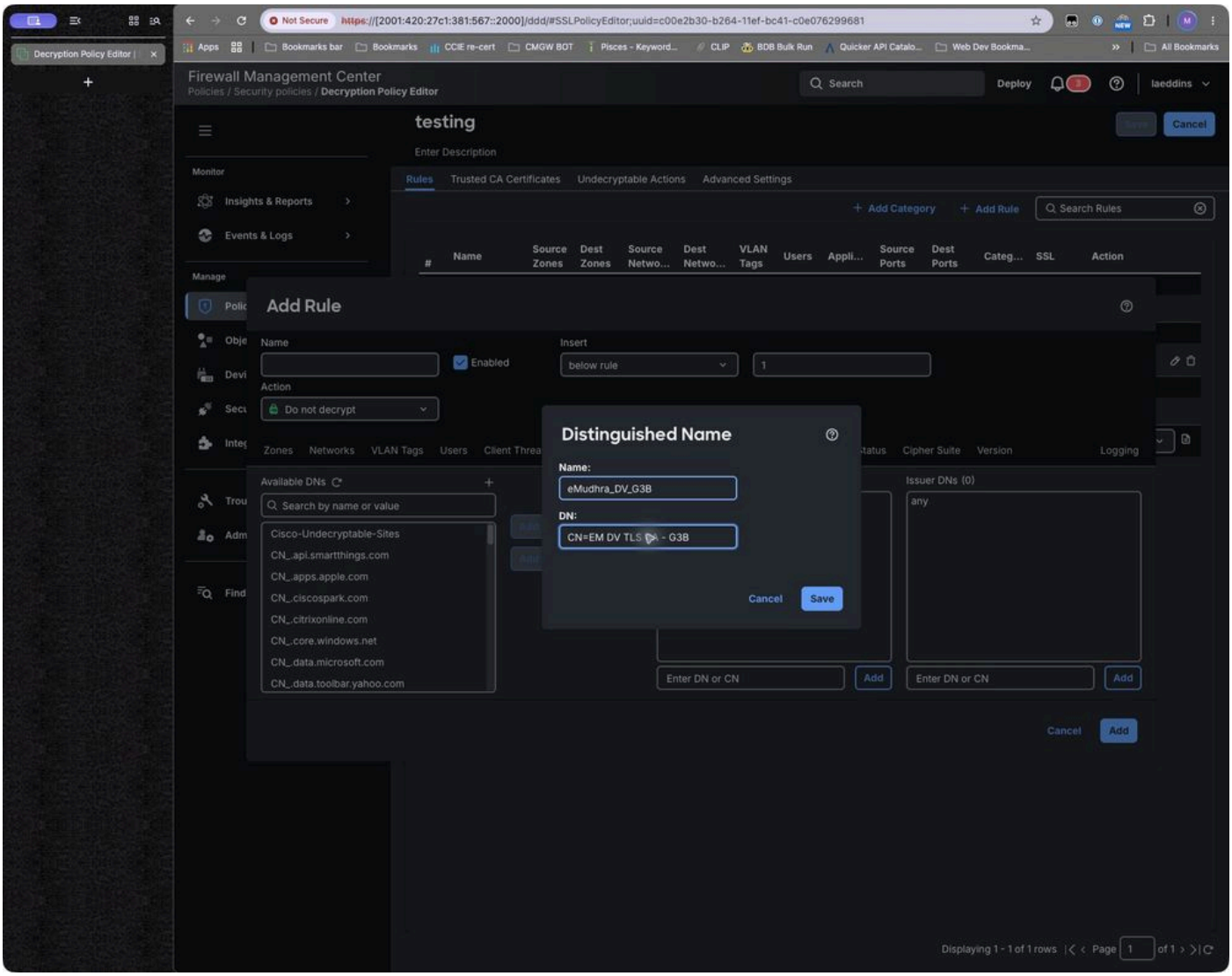
對象表

DN	建議的DN對象名稱
CN=EM DV TLS CA - G3B	eMudhra_DV_G3B

DN	建議的DN對象名稱
CN=EM DV TLS CA - G3C	eMudhra_DV_G3C
CN=EM EV TLS CA - G3B	eMudhra_EV_G3B
CN=EM EV TLS CA - G3C	eMudhra_EV_G3C
CN=EM OVER TLS CA - G3B	eMudhra_OV_G3B
CN=EM OVER TLS CA - G3C	eMudhra_OV_G3C

為上表中的每個對象建立一個縮小範圍的DN對象。

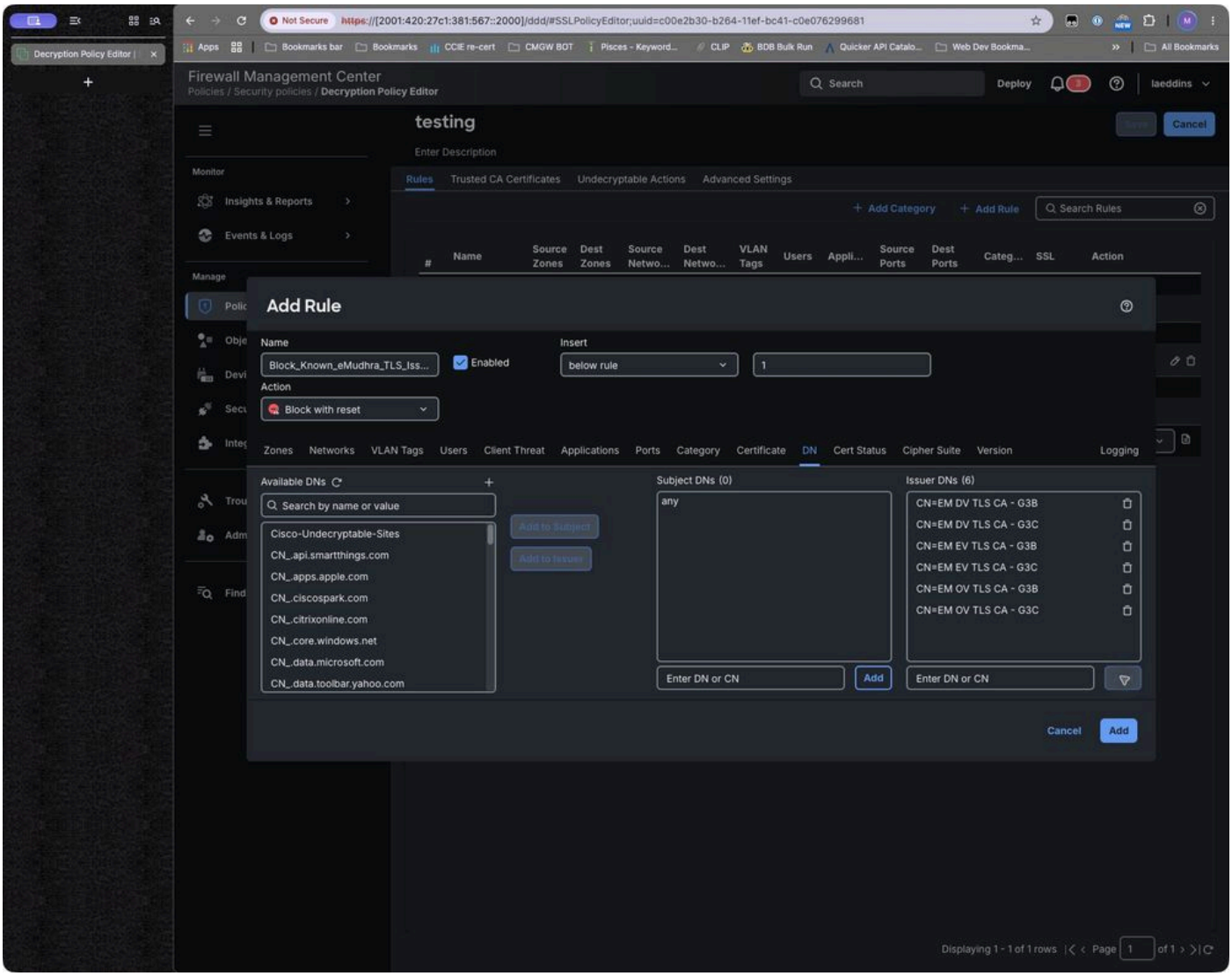
圖2.顯示Name和DN欄位的Distinguished Name表單。輸入示例值進行說明；完成後按一下「儲存」。



2建立阻止規則

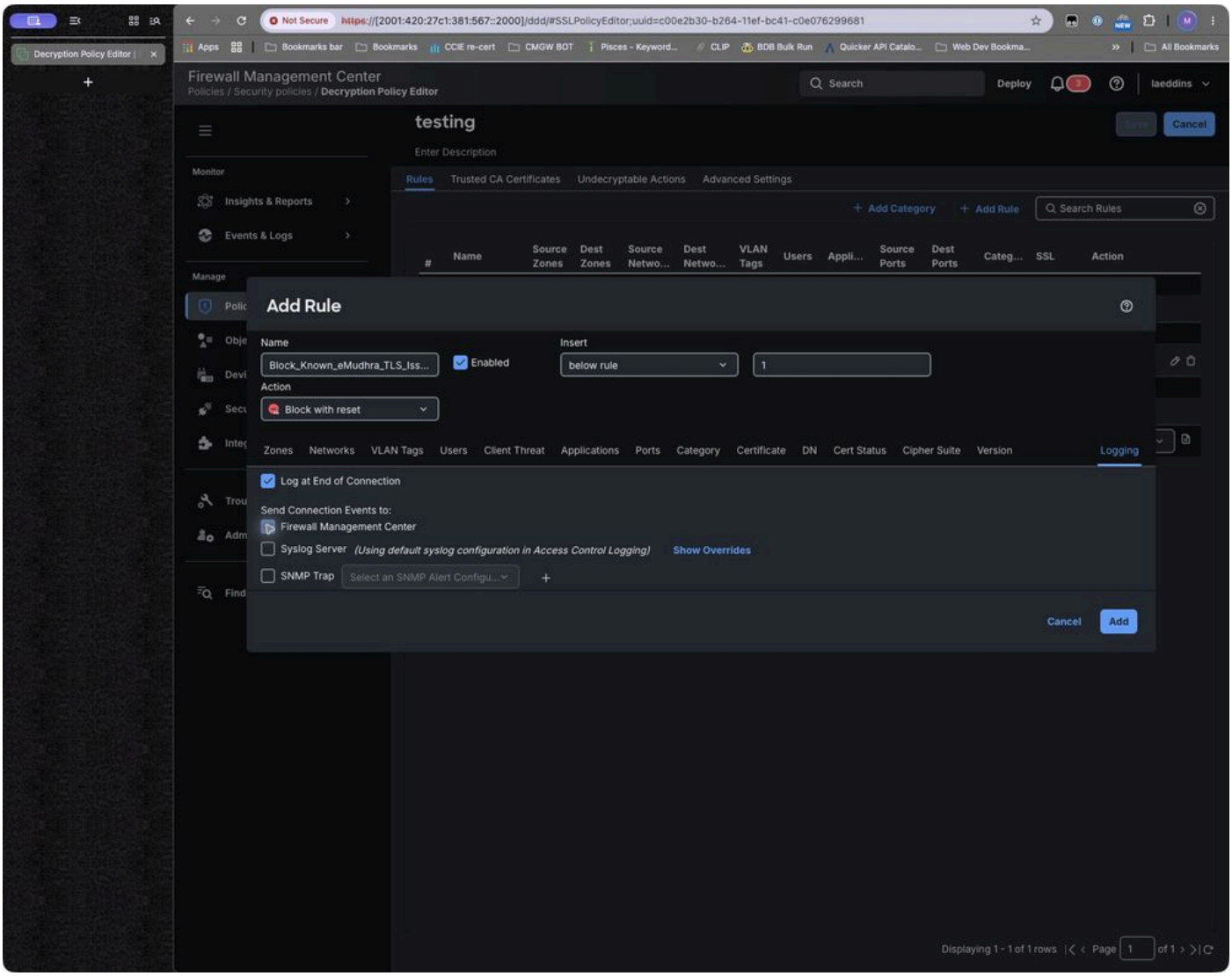
在FMC 10.1.0中，選擇Policies > Security policies > Decryption，開啟適用的策略，然後點選Add Rule。將規則命名為Block_Known_eMudhra_TLS_Issuers。開啟DN頁籤。使用「新增到頒發者」新增已驗證對象，或在標籤為「輸入DN或CN」的「頒發者DN」欄位中輸入DN，然後按一下其「新增」按鈕。確認名稱顯示在頒發者DN中，而不是主題DN中。

圖3.顯示帶重置的阻止、DN頁籤、六個頒發者DN和無主題DN約束的規則。完成後，點選Add。



選擇Block或Block with reset。將源區域或網路限制在協定範圍內。如果需要，在Logging頁籤上，選擇Log at End of Connection並驗證已選中Firewall Management Center。請勿新增「有效=是」要求：目標頒發者塊不得依賴於通過信任驗證的證書。

圖4.顯示已選擇「Log at End of Connection and Firewall Management Center（連線結束和防火牆管理中心登入）」的規則。完成後按一下Add



3稽核規則順序和策略關聯

將規則置於可先處理相同流量的更廣泛規則之前。確認TLS策略與分配給目標裝置的訪問控制策略的關聯。在測試之前檢查預過濾器和其他旁路路徑。

圖5.現有的測試策略規則表。這僅顯示了訂購介面。

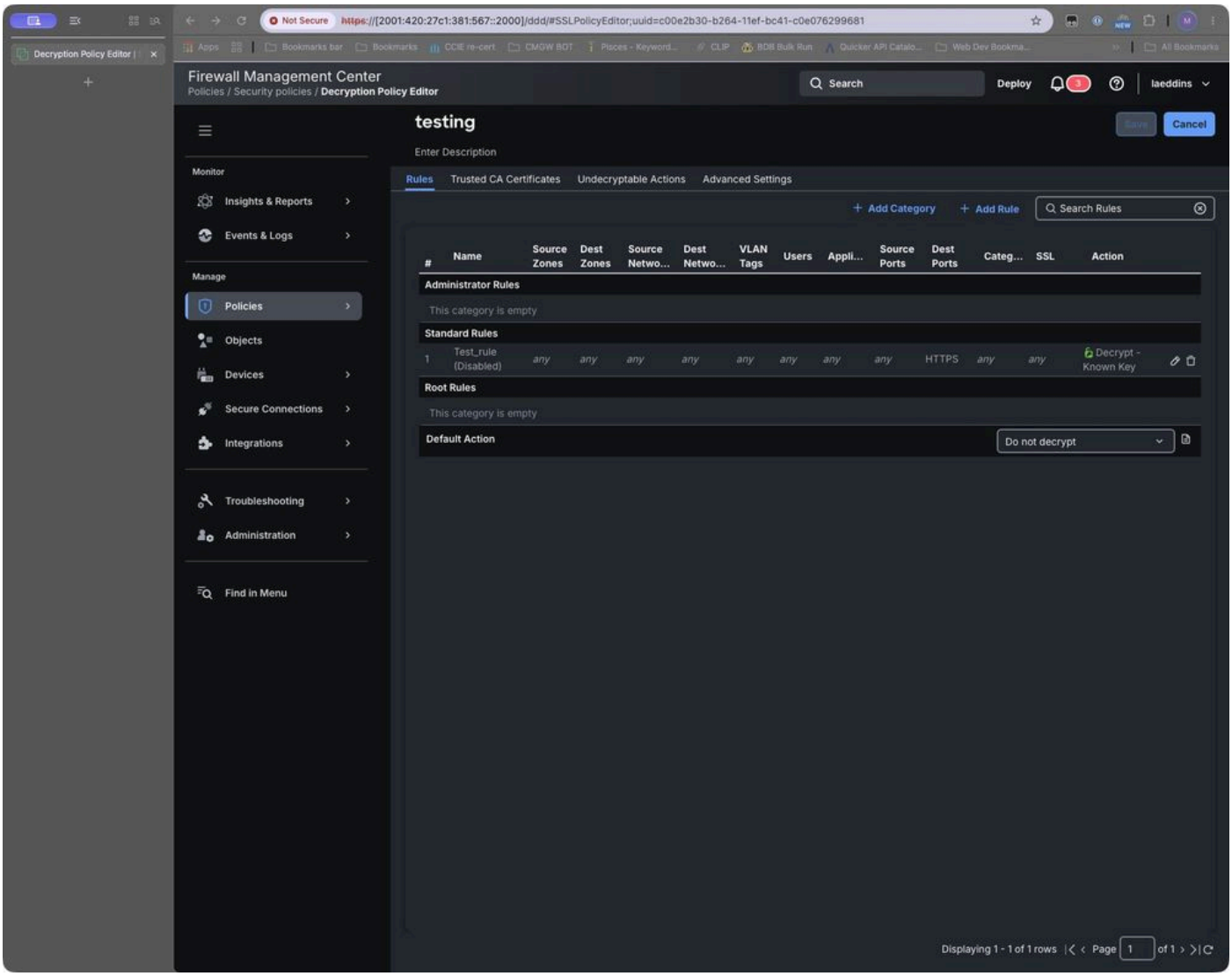
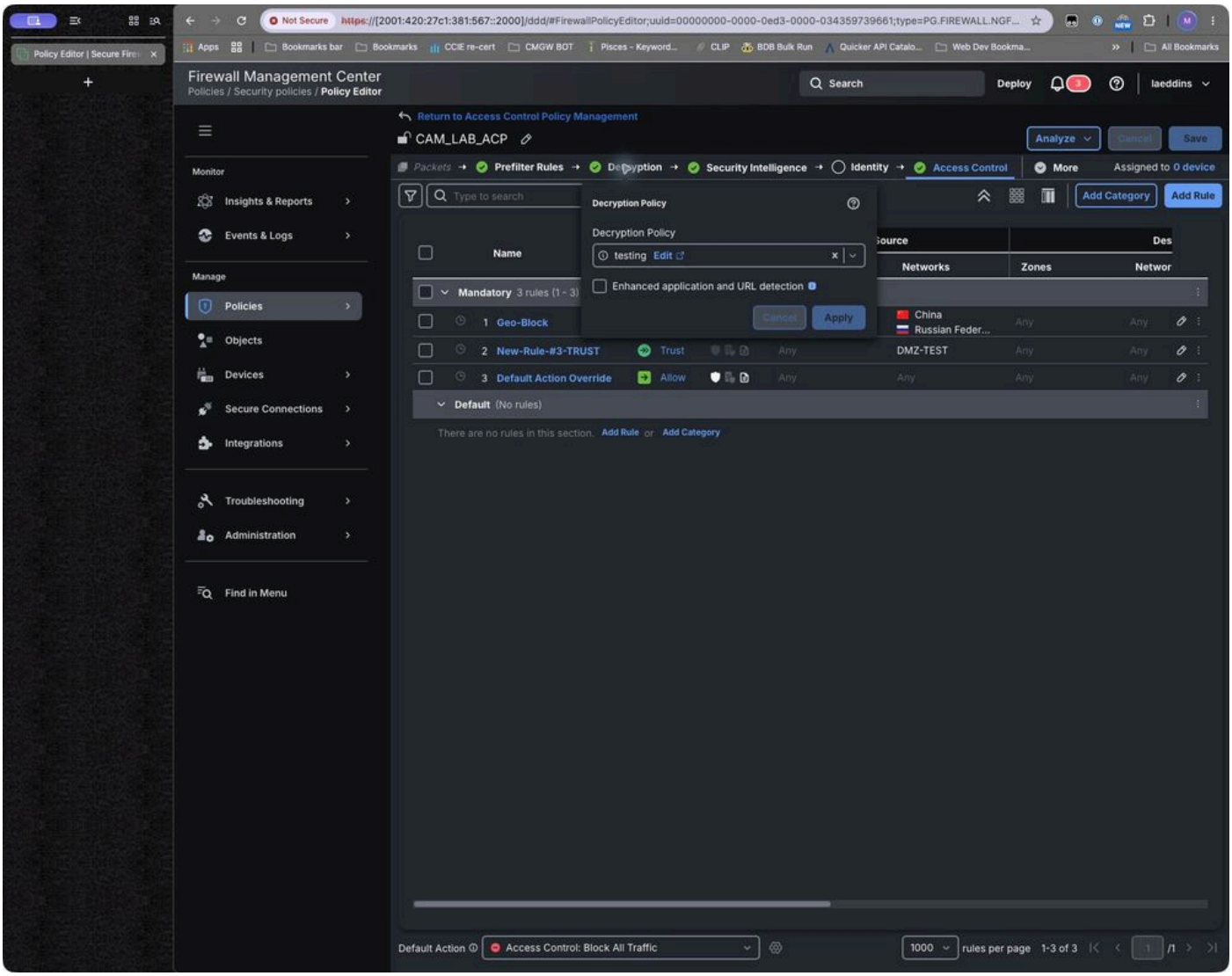


圖5b.現有的CAM_LAB_ACP策略引用測試解密策略。



部署和驗證

將更改部署到相關裝置。如果可用，請使用您知道正在使用相關CA之一頒發的證書的網站進行測試。

排除意外結果故障

如果流量通過，請檢查部署狀態、流量範圍、策略關聯、規則順序、頒發者拼寫和欄位編碼，以及裝置是否有證書資訊。確定另一個規則或旁路路徑是否處理了流。在申請等效覆蓋範圍之前，檢視測試版本上的TLS 1.3可見性。

其他TLS 1.3驗證：在FMC 7.6上，TLS 1.3解密是一個單獨的解密策略高級設定；如果禁用，則解密規則僅適用於TLS 1.2或更低版本。啟用TLS 1.3解密啟用自適應伺服器身份探測，並且頒發者DN條件可以在未快取證書時觸發探測。相關的訪問控制策略的TLS 1.3伺服器身份發現設定優先。

思科表示，這些高級設定在7.1之前的裝置或運行Snort 2的裝置上會被忽略，並且部署到AWS的FTDv不支援自適應身份發現。在申請TLS 1.3覆蓋範圍之前驗證目標軟體/平台和證書可見性。規則的TLS版本選擇器本身列出了SSL 3.0到TLS 1.2;不依賴TLS 1.3選擇器。[7]

如果不相關的流量失敗，請識別實際的匹配規則和頒發者。根據需要縮小DN或流量範圍，然後重複受影響和未受影響的測試。不要禁用證書驗證作為解決方法。

覆蓋範圍和操作限制

此解決方案不會阻止每個場景，也不會取代更新其他服務的需要。

回退和規則報廢

如果規則導致不可接受的影響，請通過正常的更改過程禁用新規則並重新部署。儲存事件和測試證據。在停用之前，確認受影響的工作負載強制執行當前信任策略，重複負面的證書驗證測試，並獲得更改所有者的批准以刪除臨時限制。

參考資料

[1] FMC 7.2解密規則

[2] FMC 10.x基於規則的解密規則

[3]按版本提供的安全防火牆管理中心新功能

[4]配置FMC和FDM的CA捆綁的自動更新

[5] FMC 7.6證書

[6] FDM 7.6證書

[7] FMC 7.6解密策略和TLS 1.3指南

[8] Cisco Secure Firewall ASA 9.22常規操作CLI配置指南 — 數位證書

[9] Cisco Secure Firewall ASA Series Command Reference — crypto ca trustpool policy

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）。