為DAP證書引數評估配置LUA指令碼

目錄

簡介

本文檔介紹如何配置LUA指令碼以檢測使用者嘗試連線到VPN時必須具有的證書引數。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆管理中心(FMC)
- 遠端存取VPN組態(RAVPN)
- 基本LUA指令碼編碼
- 基本SSL憑證
- 動態存取原則(DAP)

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全防火牆版本7.7.0
- 安全防火牆管理中心版本7.7.0

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。

背景資訊

DAP是一項強大的功能，它允許網路管理員根據嘗試連線到網路的使用者和裝置的各種屬性來定義精細的訪問控制策略。DAP的主要功能之一是能夠建立策略來評估客戶端裝置上安裝的數位證書。這些證書用作驗證使用者身份和驗證裝置合規性的安全方法。

在Cisco Secure FMC介面中，管理員可以配置DAP策略以評估特定證書引數，例如：

- 主題
- 發行商
- 使用者替代名稱
- 序列號
- 證書儲存

但是，通過FMC GUI提供的證書評估選項僅限於這些預定義屬性。此限制意味著，如果管理員想要基於更詳細的或自定義的證書資訊（例如證書或自定義擴展中的特定欄位）實施策略，則無法僅使用標準DAP配置來實現此限制。

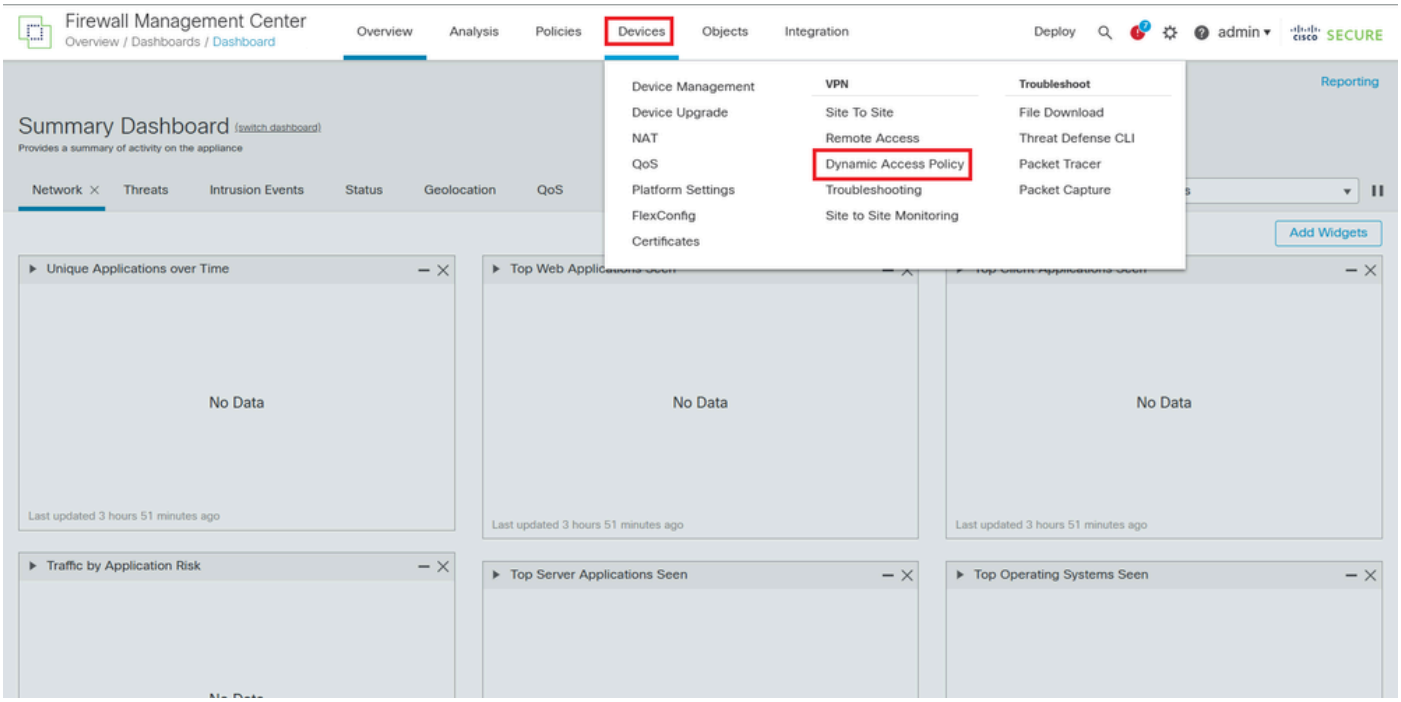
為了克服這一限制，思科安全防火牆支援在DAP中整合LUA指令碼。LUA指令碼提供了訪問和評估未通過FMC介面公開的其他證書屬性的靈活性。此功能使管理員能夠根據詳細的證書資料實施更完善和定製的訪問策略。

通過利用LUA指令碼，可以分析預設引數（如組織名稱、自定義擴展或其他證書後設資料）之外的證書欄位。這種擴展的評估功能允許策略精確地根據組織的要求進行定製，從而確保只有證書符合具體、詳細標準的客戶才能被授予訪問許可權，從而增強了安全性。

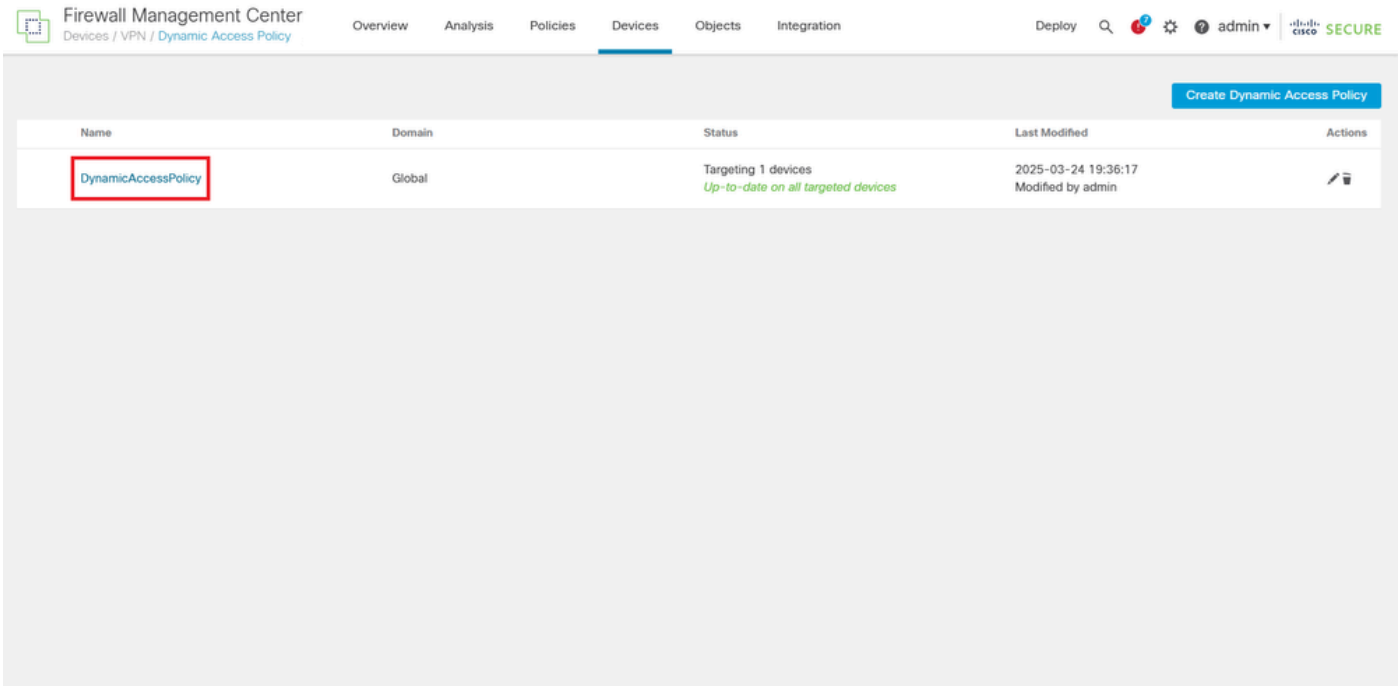
因此，在本文檔中，LUA指令碼配置為利用LUA指令碼功能評估客戶端證書中的Organization引數。

組態

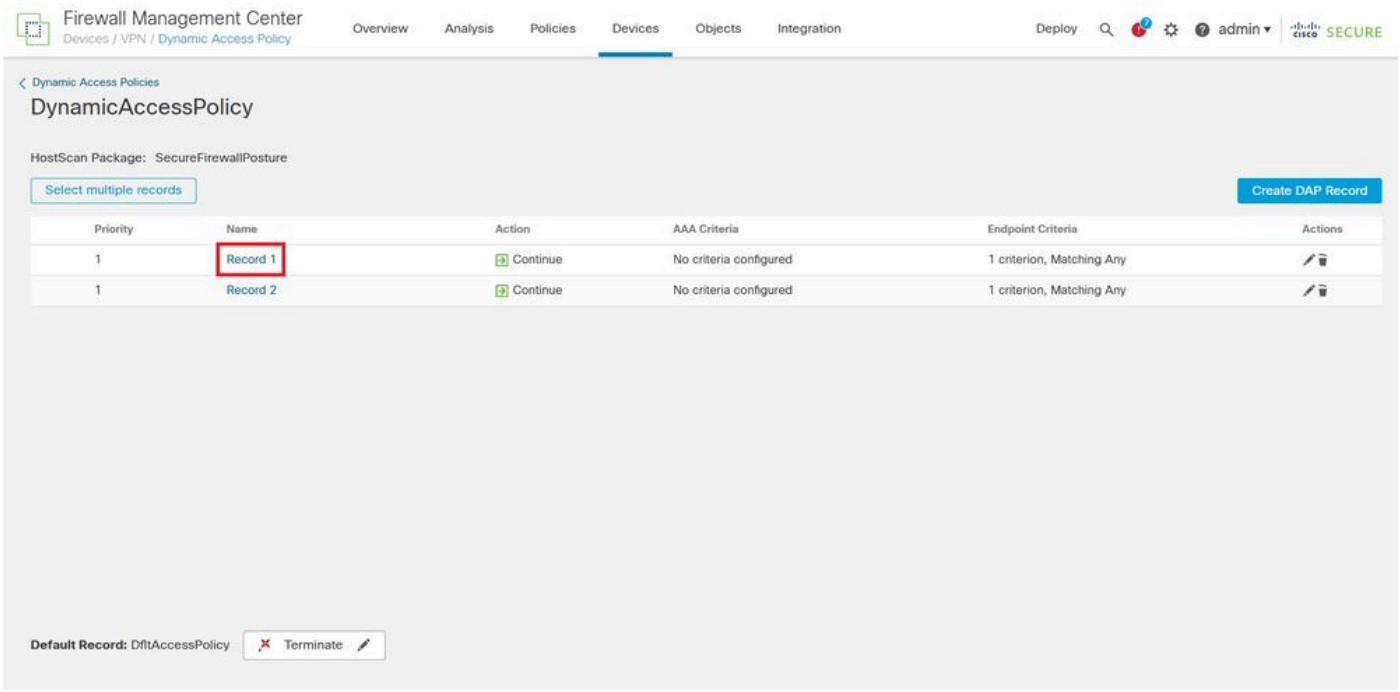
1.登入到FMC GUI，然後從儀表板導航到選單中的Devices > Dynamic Access Policy。



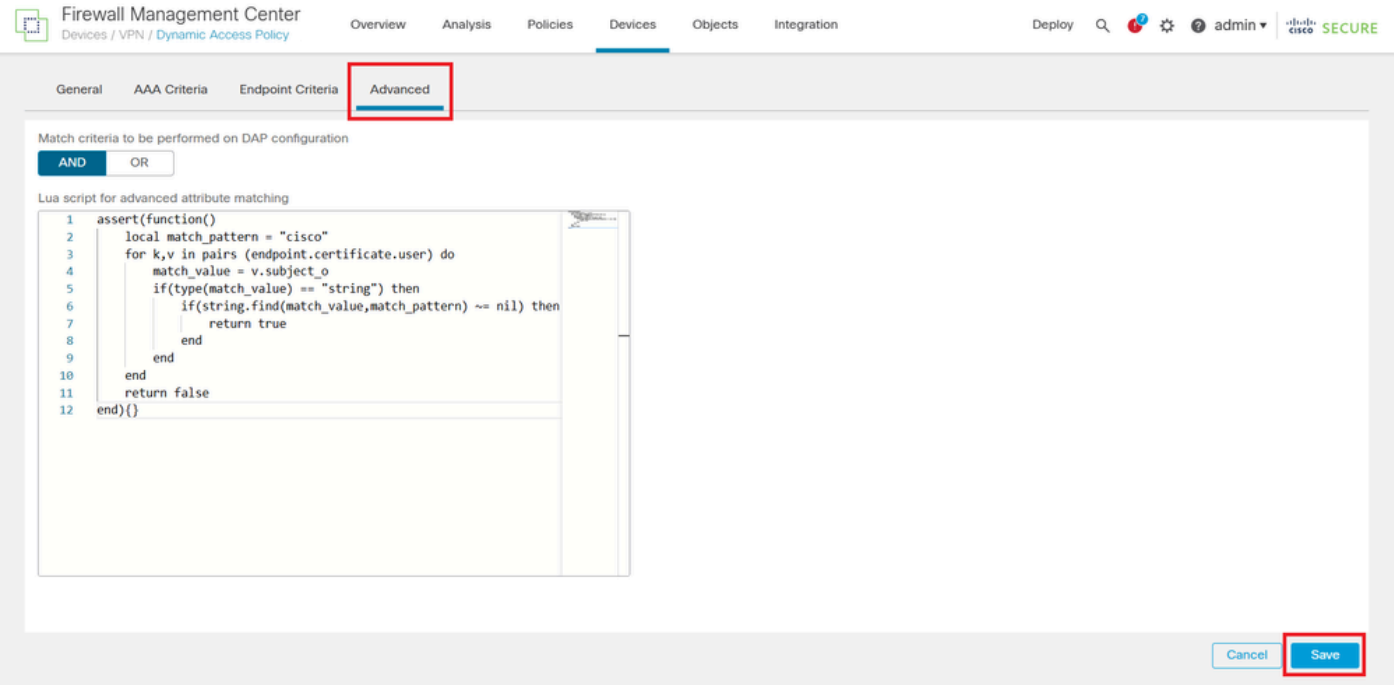
2.開啟應用於RAVPN配置的DAP策略。



3.通過按一下記錄名稱來編輯所需的記錄以配置LUA指令碼。



4.在選定的記錄中，定位至高級標籤以輸入用於評估所需證書引數的LUA指令碼。配置指令碼後，按一下Save以應用更改。在DAP記錄中儲存變更後，部署策略，將更新的組態推送到FTD裝置。



附註：本文中顯示的代碼用於評估客戶端裝置上安裝的證書，尤其是驗證是否存在其在Subject欄位中的Organization引數與值cisco匹配的證書。

<#root>

```
assert(function()
    local match_pattern = "
```

cisco

```
"
    for k,v in pairs (
```

endpoint.certificate.user

```
) do
        match_value =
```

v.subject_o

```
        if(type(match_value) == "string") then
            if(string.find(match_value,match_pattern) ~= nil) then
```

return true

```
            end
        end
    end
    return false
end){}
```

- 該指令碼定義一個設定為cisco的match_pattern變數，該變數是要查詢的目標組織名稱。
- 它使用for循環對終端上的所有可用使用者證書進行迭代。
- 對於每個證書，它提取組織欄位(subject_o)。

- 它檢查Organization欄位是否為字串，然後在其內搜尋match_pattern。
- 如果找到匹配項，指令碼將返回true，表示證書符合策略條件。
- 如果在檢查所有證書後未找到匹配的證書，指令碼將返回false，導致策略拒絕訪問。

此方法允許管理員在FMC GUI公開的標準引數之外實施自定義的證書驗證邏輯。

驗證

執行命令more dap.xml以驗證在FTD上的DAP配置中是否存在代碼。

<#root>

firepower#

more dap.xml

Record 1

and

```
assert(function()
        local match_pattern = "cisco"
        for k,v in pairs (endpoint.certificate.user) do
                match_value = v.subject_o
                if(type(match_value) == "string") then
                        if(string.find(match_value,match_pattern) ~= nil) then
                                return true
                        end
                end
        end
        return false
end) {}
```

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）。