在FMC上配置關聯策略

目錄

簡介

本文檔介紹配置關聯策略以連線事件並檢測網路上異常的過程。

必要條件

需求

思科建議您瞭解以下產品：

- 安全防火牆管理中心(FMC)
- 安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於VMware的Firepower威脅防禦7.6.0版

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

關聯策略透過配置不同型別的事件來辨識網路上的潛在安全威脅，並用於補救、條件警報和流量策略。

設定

配置關聯規則

步驟 1.導航到策略>關聯，選擇規則管理。

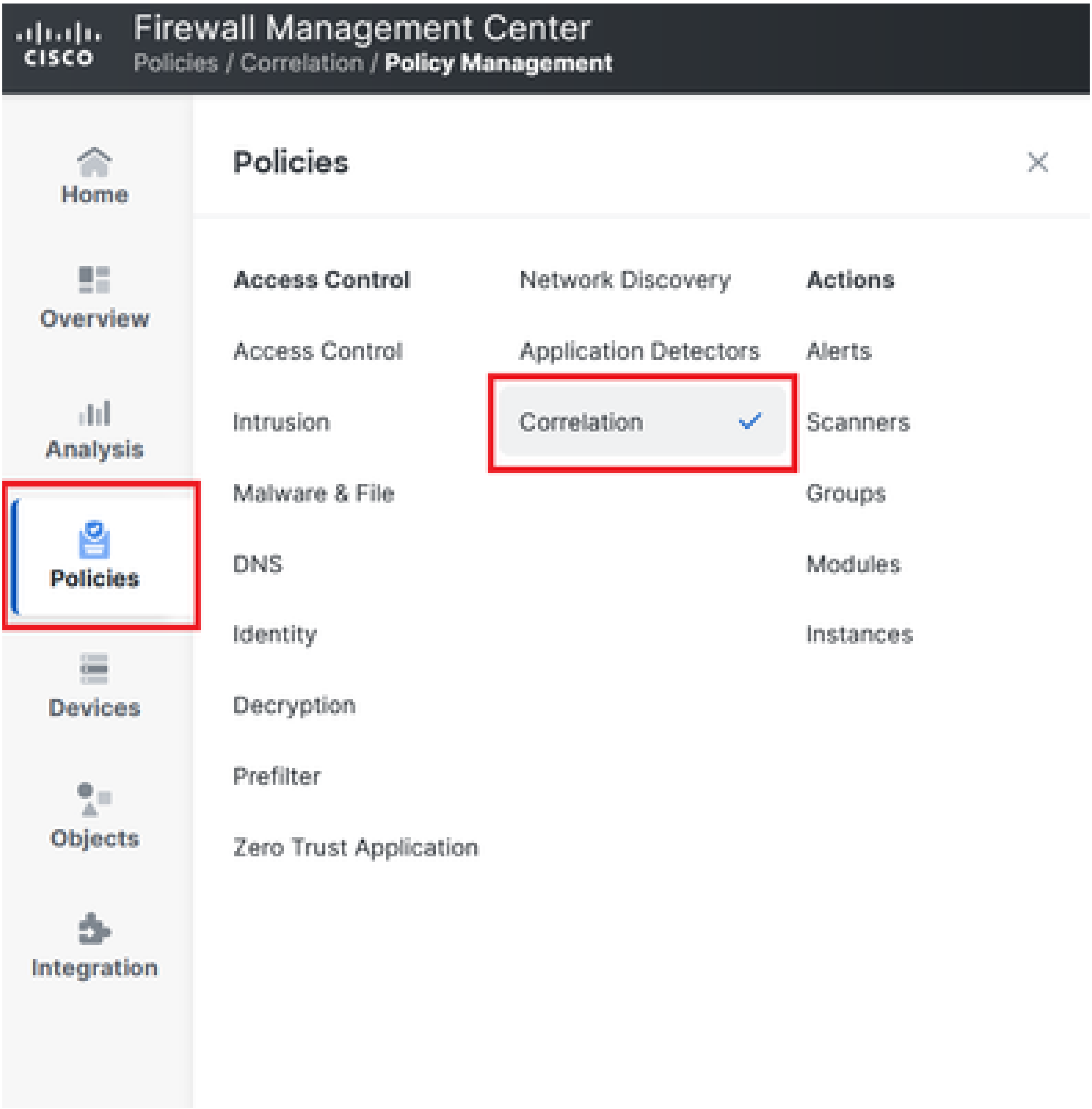
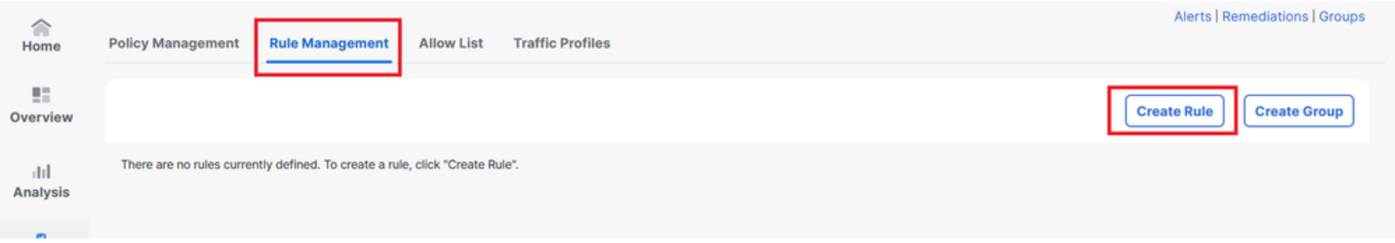


圖1.導航到關聯策略選單

步驟 2.選取建立規則來建立新的規則。

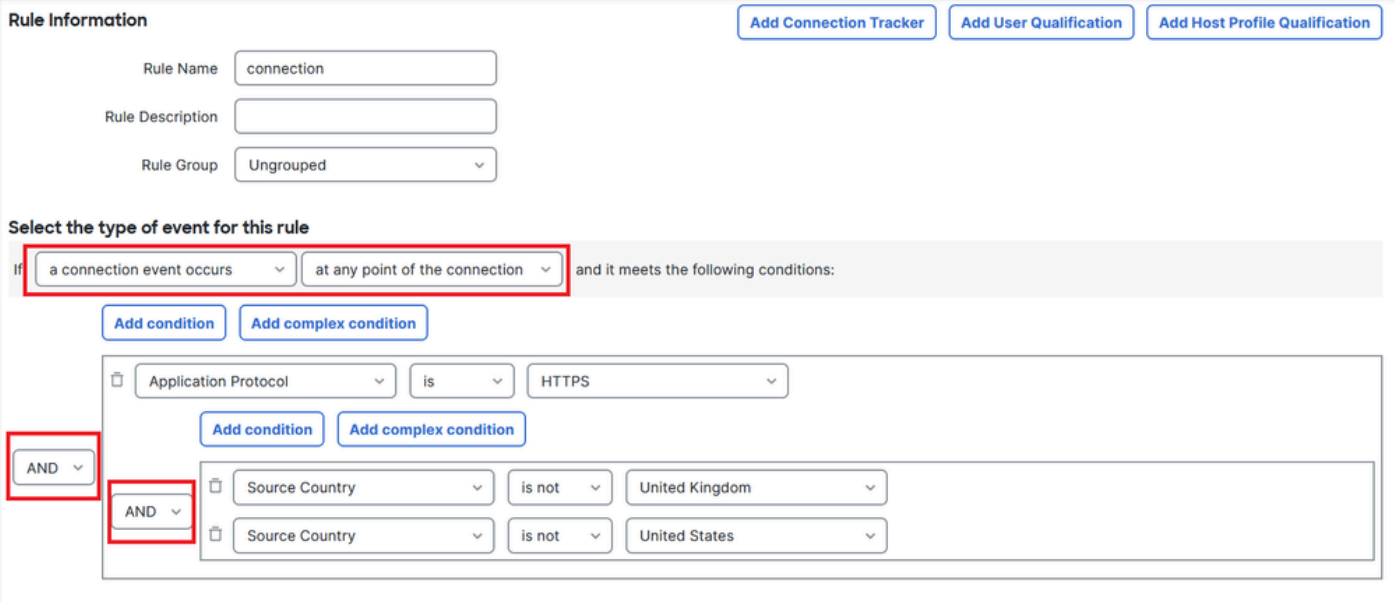


There are no rules currently defined. To create a rule, click "Create Rule".

圖2.規則管理功能表上的規則建立

步驟 3. 選取事件型別和符合規則的條件。

當規則包含多個條件時，必須使用AND或OR運算子將其連結。



Rule Information

Rule Name: connection

Rule Description:

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at any point of the connection and it meets the following conditions:

AND

- Application Protocol is HTTPS
- AND
  - Source Country is not United Kingdom
  - Source Country is not United States

圖3.規則建立功能表

注意：關聯規則不能是通用的，如果規則經常由正常流量觸發，則這可能會佔用額外的CPU並影響FMC效能。

設定警示

步驟 1. 導航到策略>操作>警報。

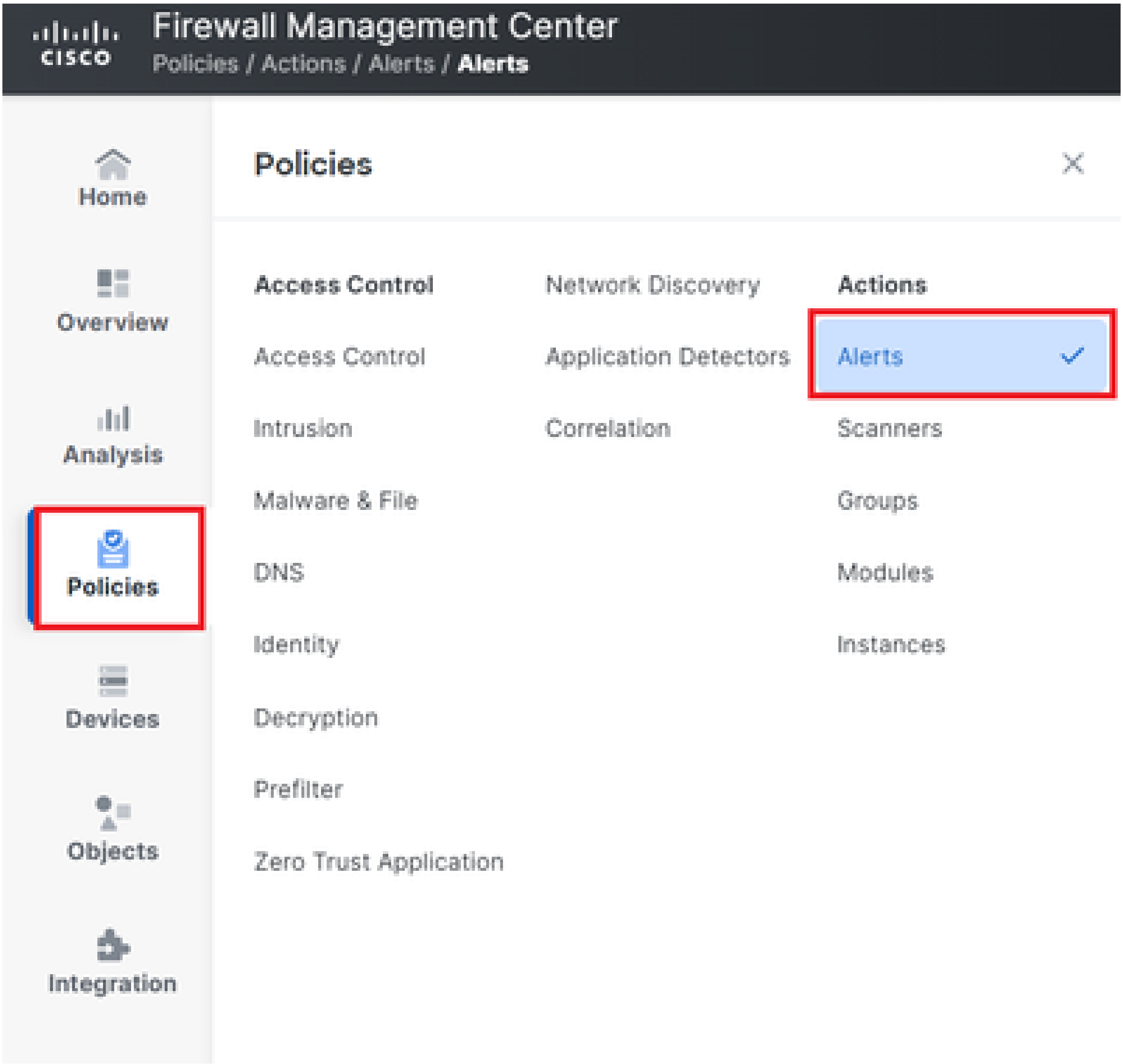
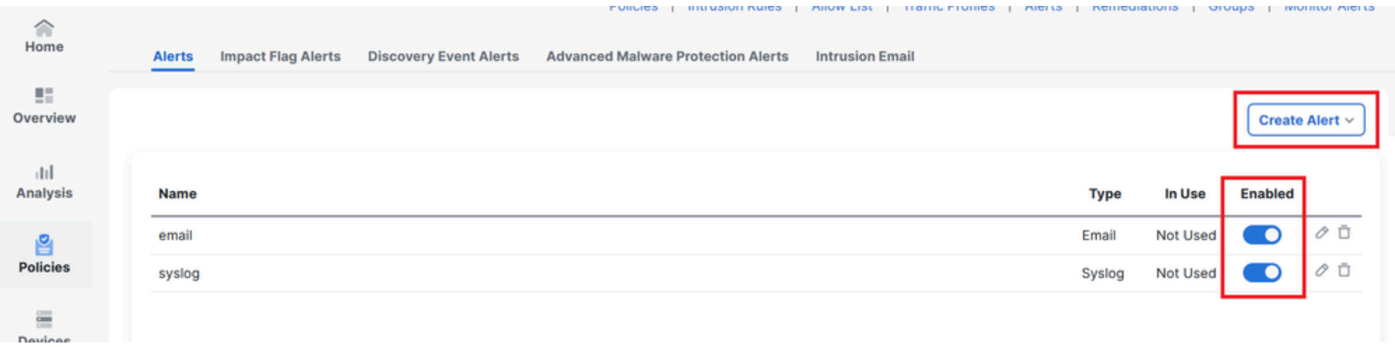


圖4.導航到「警報」選單

步驟 2. 選擇Create Alert，並建立Syslog、SNMP或email alert。


Policies | Intrusion Rules | Allow List | Traffic Profiles | Alerts | Remediations | Groups | Monitor Alerts
Home
Overview
Analysis
Policies
Devices
Alerts
Impact Flag Alerts
Discovery Event Alerts
Advanced Malware Protection Alerts
Intrusion Email
Create Alert

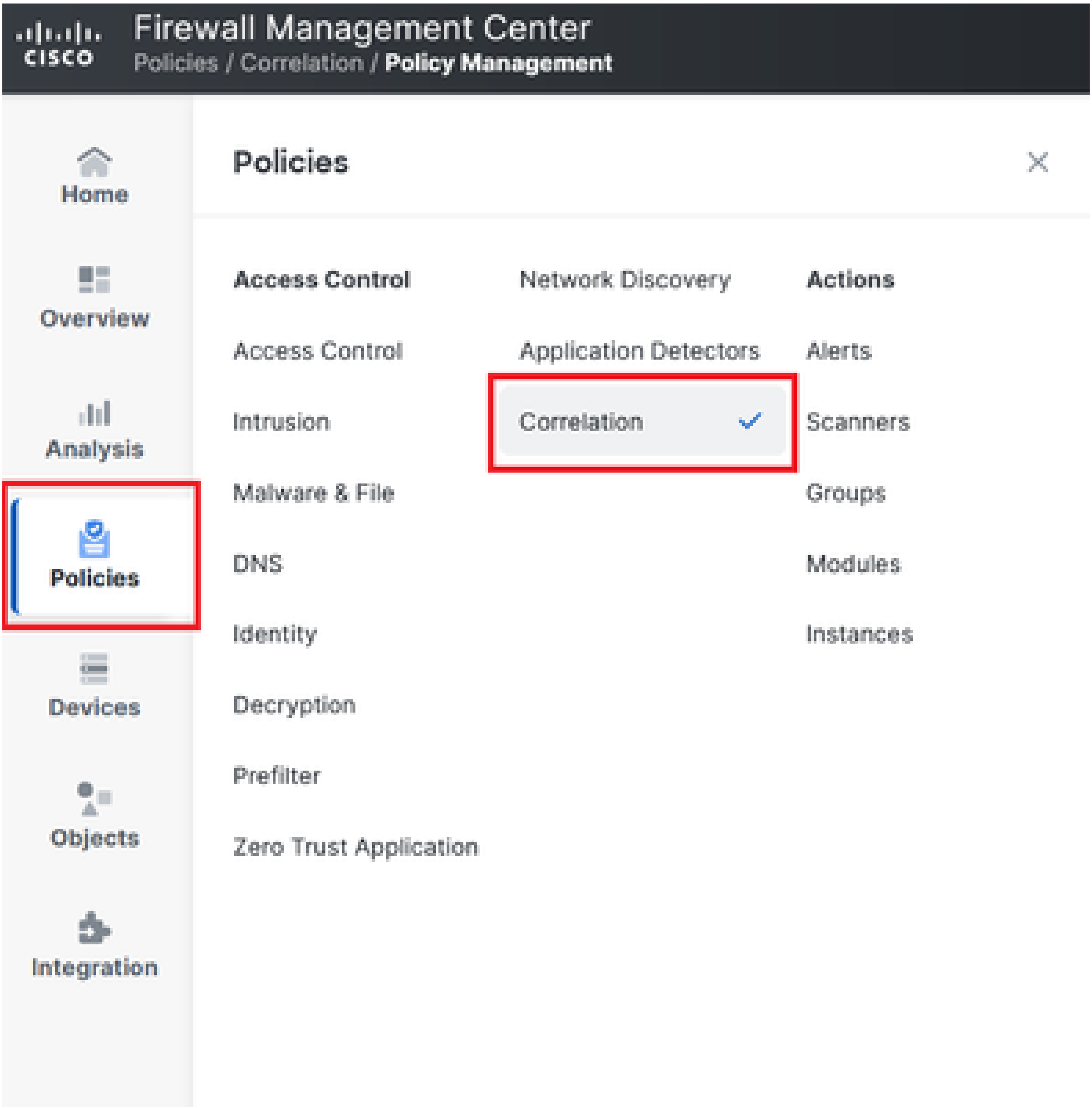
Name	Type	In Use	Enabled
email	Email	Not Used	●
syslog	Syslog	Not Used	●

圖5.建立警示

步驟 3. 驗證警報是否已啟用。

配置關聯策略

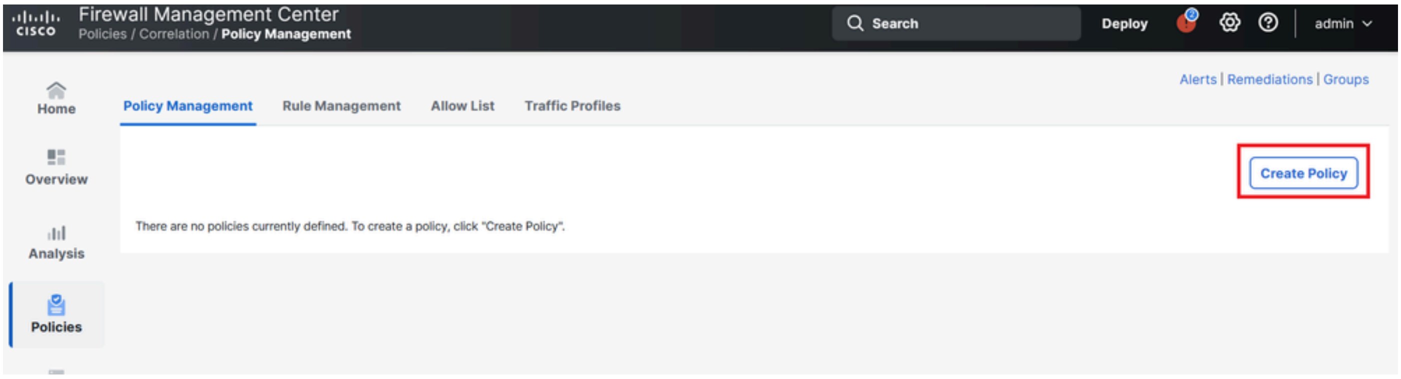
步驟 1.導航到策略>關聯。



導航到關聯策略選單

圖6.導航到關聯策略選單

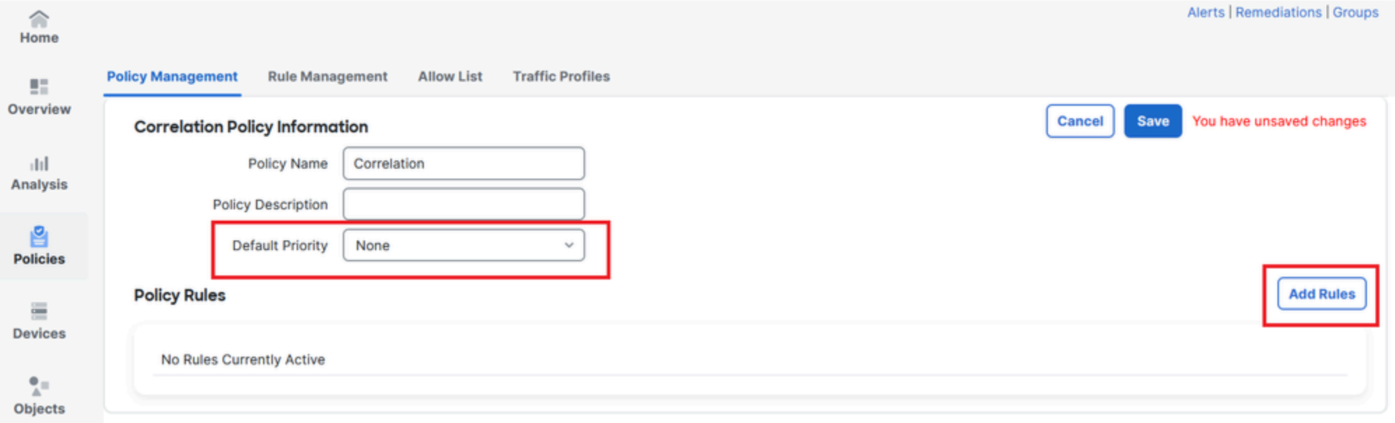
步驟 2. 建立新的關聯策略。選擇預設優先順序。使用None可使用特定規則的優先順序。



There are no policies currently defined. To create a policy, click "Create Policy".

圖7.建立新的關聯策略

步驟 3. 透過選擇Add Rules將規則增加到策略。



You have unsaved changes

Correlation Policy Information

Policy Name: Correlation

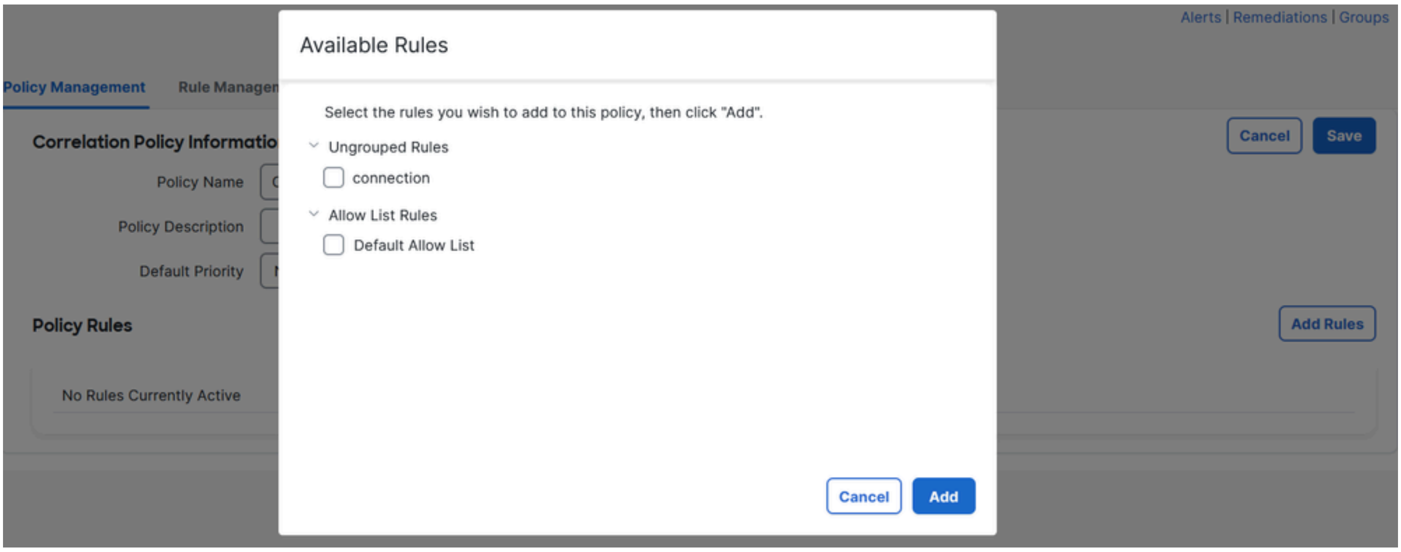
Policy Description:

Default Priority: None

Policy Rules

No Rules Currently Active

圖8.增加規則並選擇關聯策略的優先順序



Available Rules

Select the rules you wish to add to this policy, then click "Add".

- Ungrouped Rules
  - □ connection
- Allow List Rules
  - □ Default Allow List

Correlation Policy Informatio

Policy Name

Policy Description

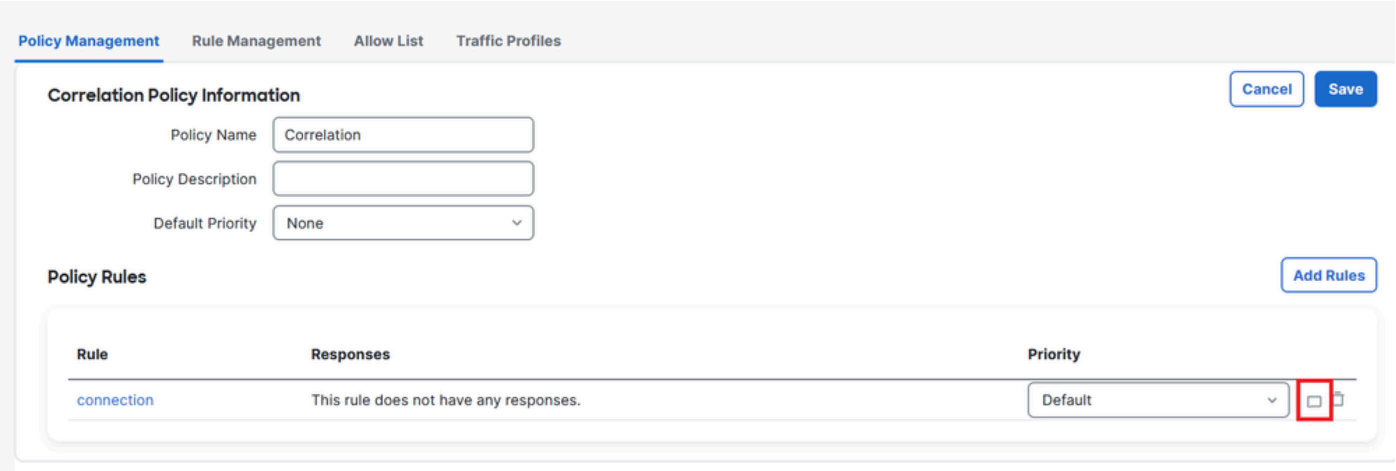
Default Priority

Policy Rules

No Rules Currently Active

圖9.選擇要增加到關聯策略的規則

步驟 4. 從您建立的風險通告為規則分配響應，因此每當觸發該響應時，它都會傳送所選風險通告型別。



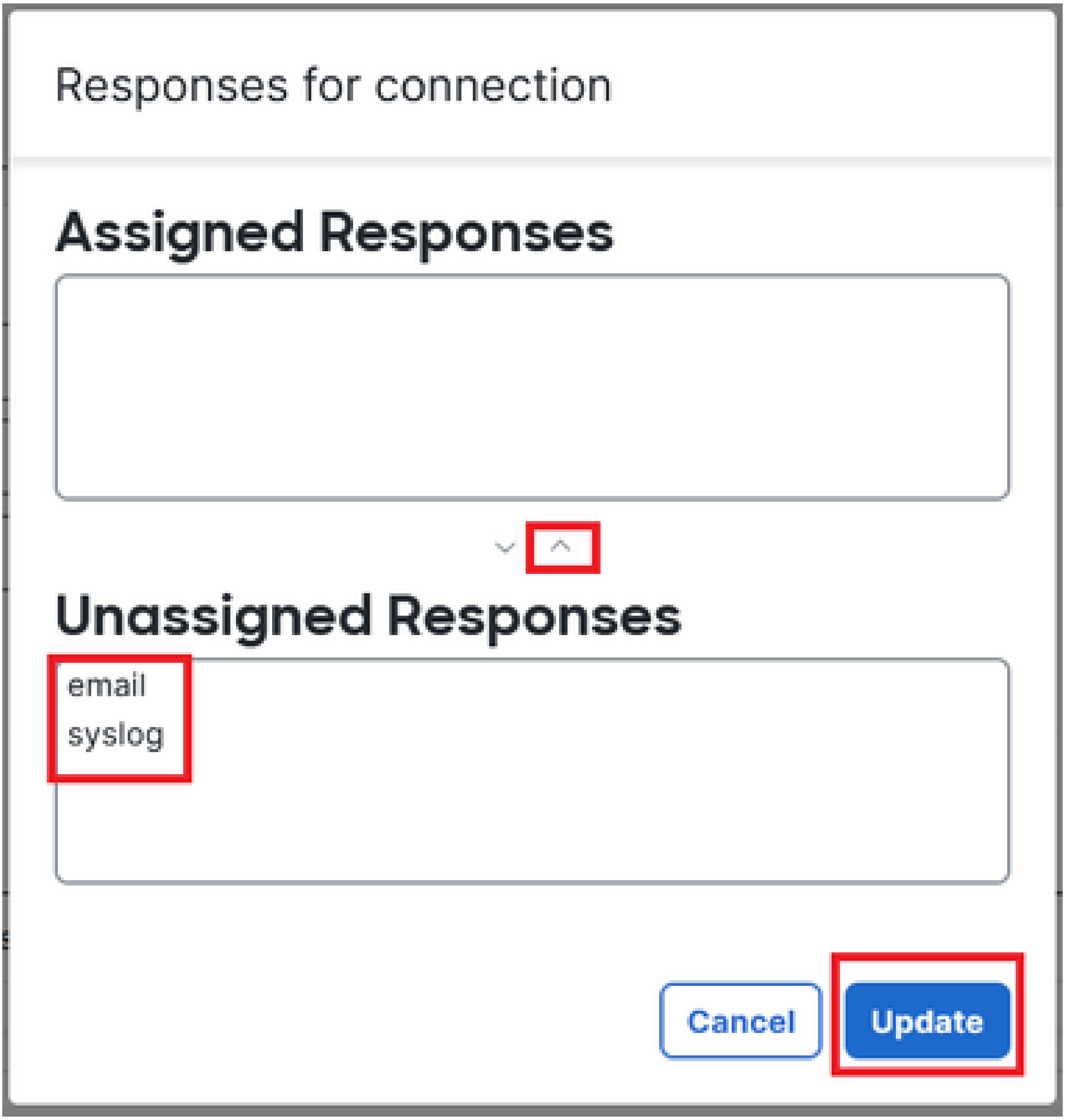
Correlation Policy Information

Policy Name	Correlation
Policy Description	
Default Priority	None

Policy Rules

Rule	Responses	Priority
connection	This rule does not have any responses.	Default

圖10.「增加響應」按鈕



Responses for connection

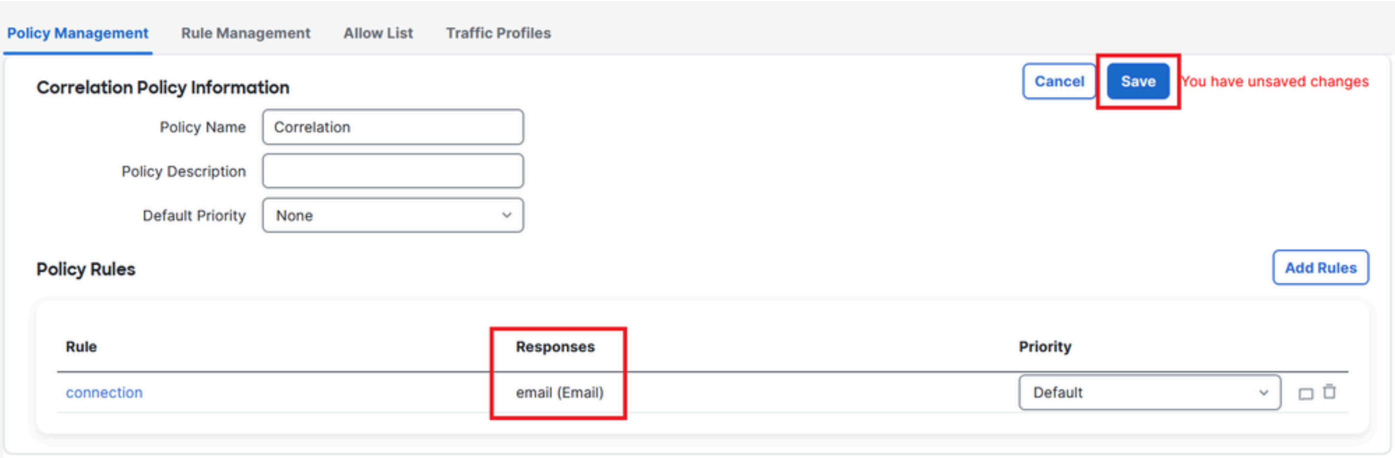
Assigned Responses

Unassigned Responses

email
syslog

圖11.將響應分配到關聯規則

步驟 5. 儲存並啟用您的關聯策略。



Policy Management Rule Management Allow List Traffic Profiles

Correlation Policy Information

Cancel Save You have unsaved changes

Policy Name: Correlation

Policy Description:

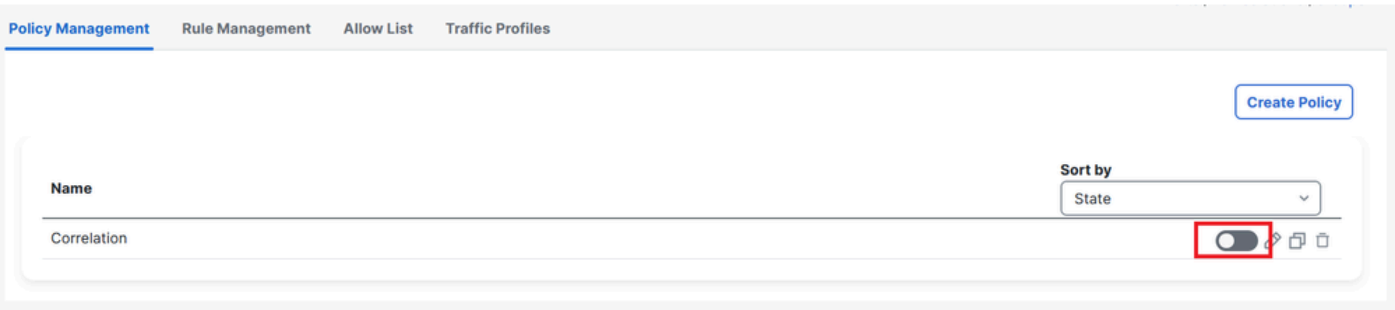
Default Priority: None

Policy Rules

Add Rules

Rule	Responses	Priority
connection	email (Email)	Default

圖12.響應已正確增加到關聯規則



Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name	Sort by State
Correlation	

圖13.啟用關聯策略