

FMCでの関連ポリシーの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[相関ルールの設定](#)

[アラートの設定](#)

[相関ポリシーの設定](#)

はじめに

このドキュメントでは、イベントを接続し、ネットワーク上の異常を検出するために相関ポリシーを設定する手順について説明します。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- セキュアファイアウォール脅威対策(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VMware向けFirepower Threat Defenseバージョン7.6.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

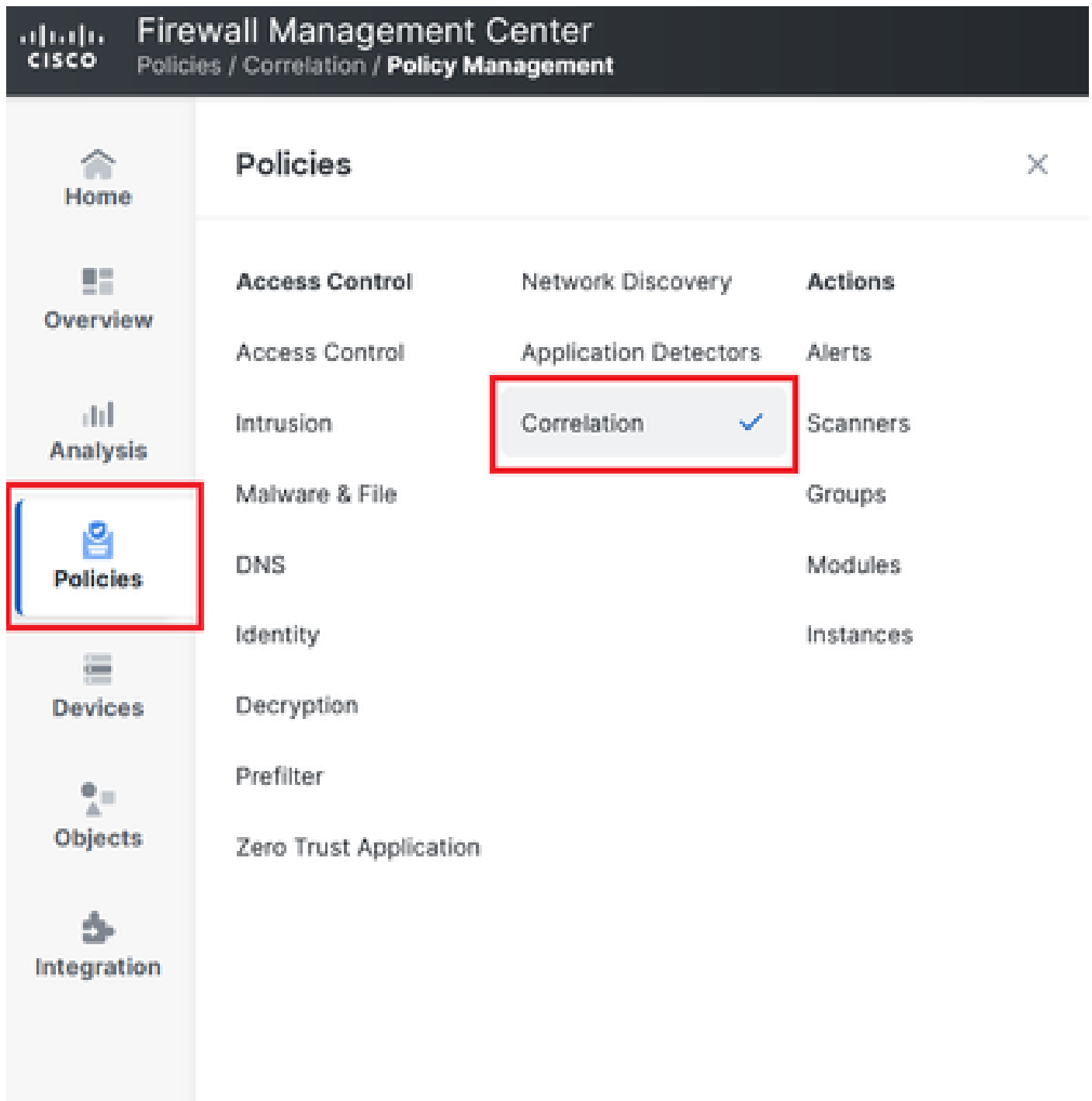
相関ポリシーは、さまざまなタイプのイベントを設定してネットワーク上の潜在的なセキュリティ脅威を特定するために使用され、修復、条件付きアラート、およびトラフィックポリシーに使

用されます。

設定

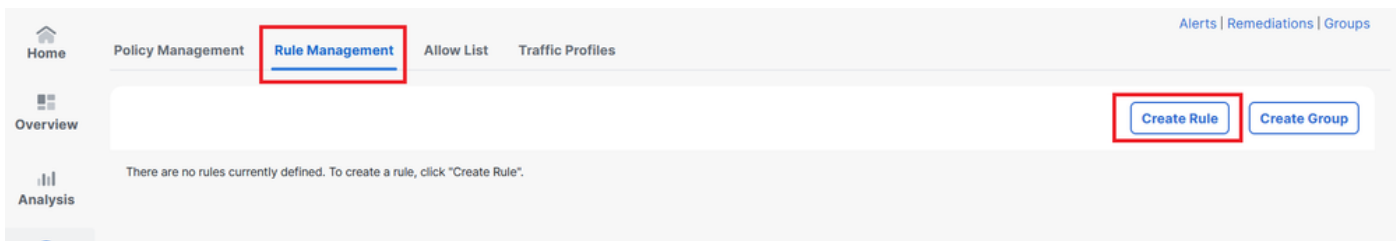
関連ルールの設定

ステップ 1 : Policies > Correlationに移動し、Rule Managementを選択します。



画像 1. 関連ポリシーメニューへのナビゲーション

ステップ 2 : Create Ruleを選択して、新しいルールを作成します。




画像 2.ルール管理メニューでのルールの作成

ステップ 3： ルールに一致するイベントタイプと条件を選択します。

ルールに複数の条件が含まれている場合は、それらの条件をAND演算子またはOR演算子でリンクする必要があります。

画像 3.ルール作成メニュー

 注： 相関ルールは汎用的なものにしないでください。ルールが常に通常のトラフィックによってトリガーされる場合、追加のCPUを消費し、FMCのパフォーマンスに影響を与える可能性があります。

アラートの設定

ステップ 1： [Policies] > [Actions] > [Alerts] の順に移動します。

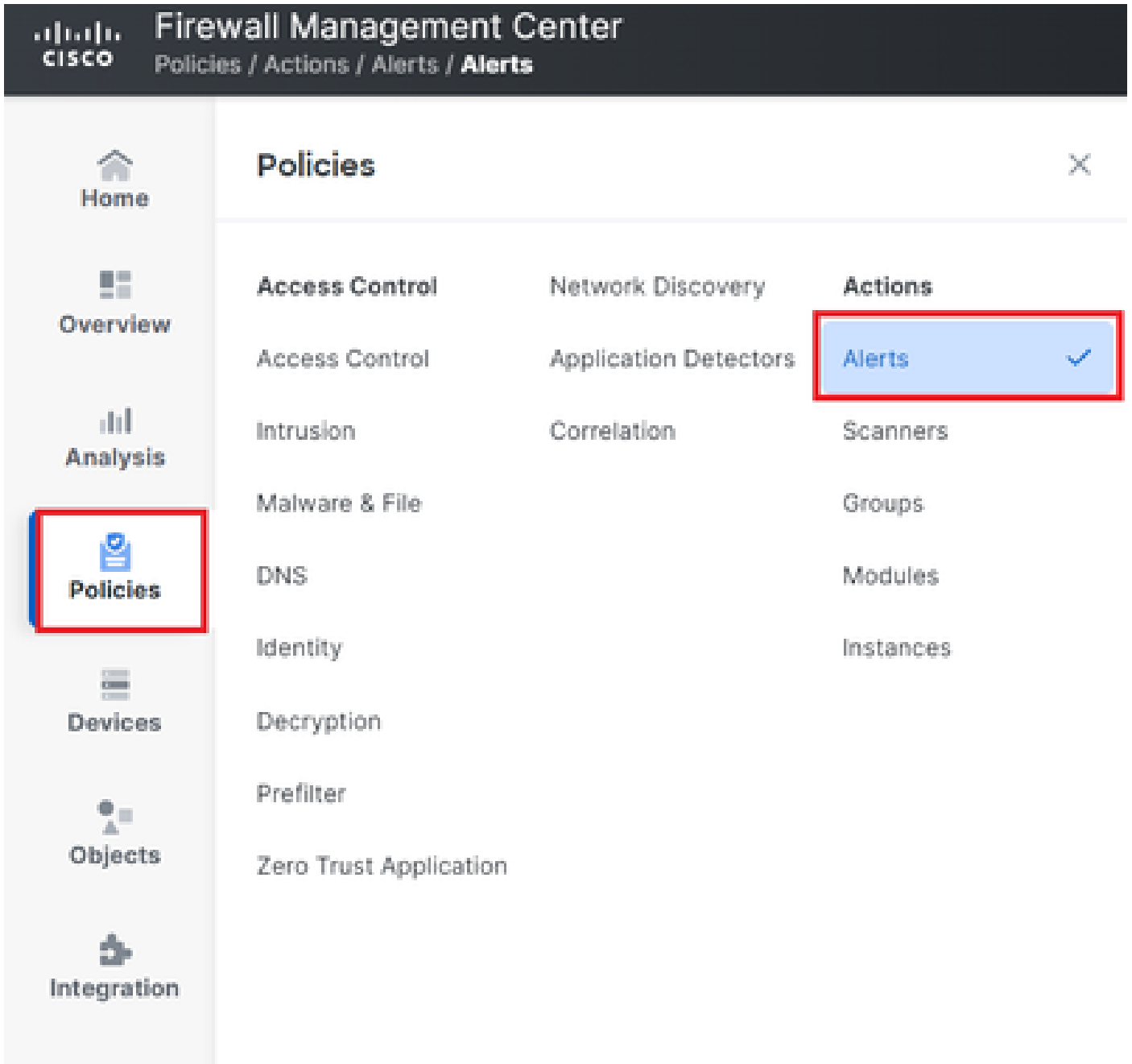


図 4.[Alerts]メニューへのナビゲーション

ステップ 2： Create Alertを選択し、Syslog、SNMP、または電子メールアラートのいずれかを作成します。

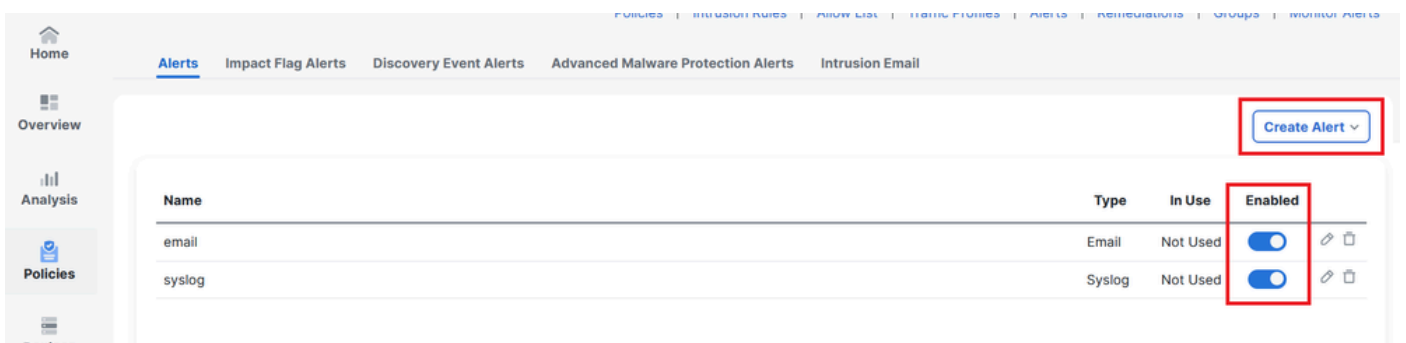
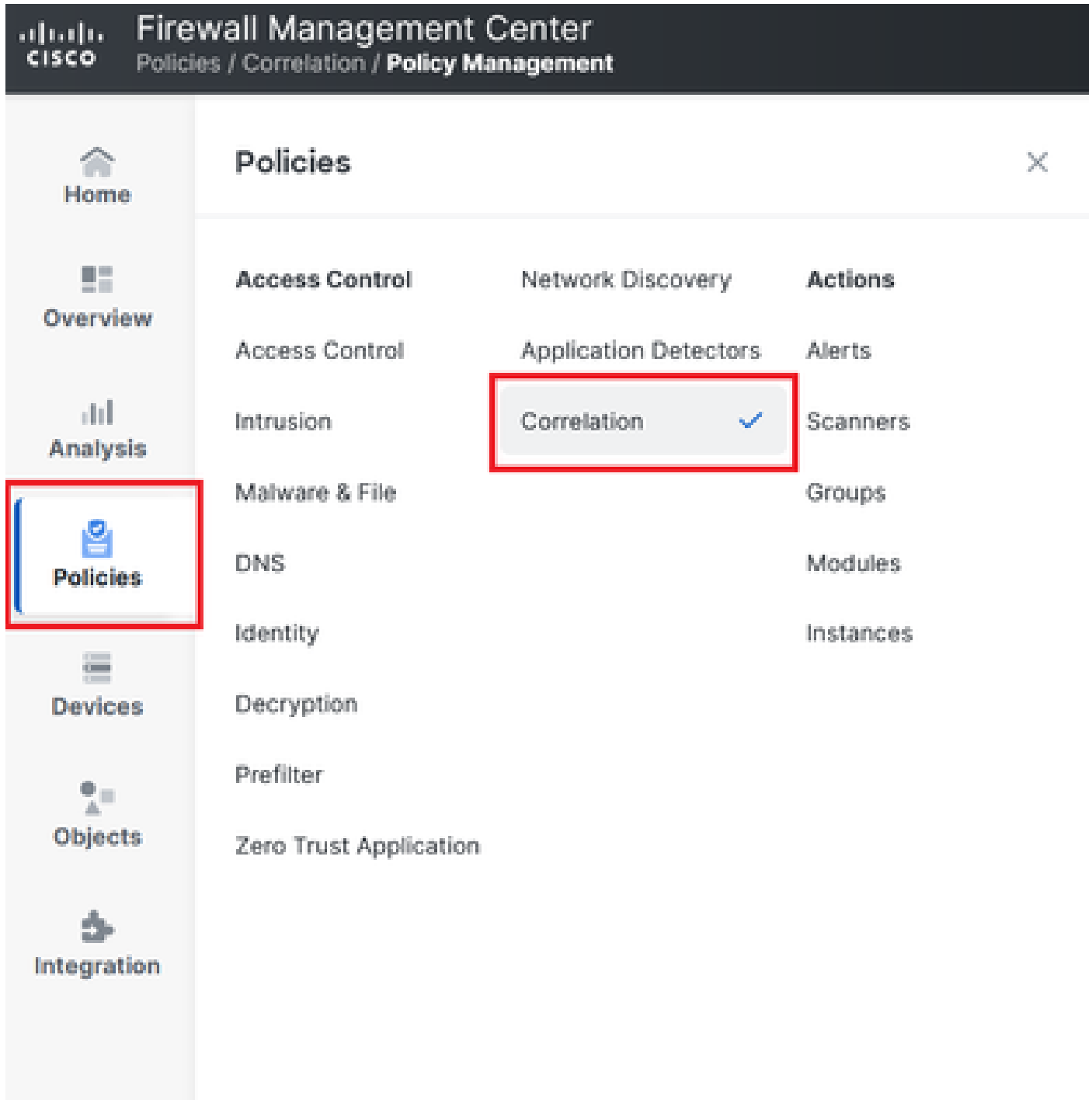


図 5.アラートの作成

ステップ 3： アラートが有効になっていることを確認します。

関連ポリシーの設定

ステップ 1： Policies > Correlationの順に移動します。



関連ポリシーメニューへのナビゲーション

図 6. 関連ポリシーメニューへのナビゲーション

ステップ 2： 新しい関連ポリシーを作成します。デフォルトの優先度を選択します。特定のルールの優先度を使用するには、Noneを使用します。

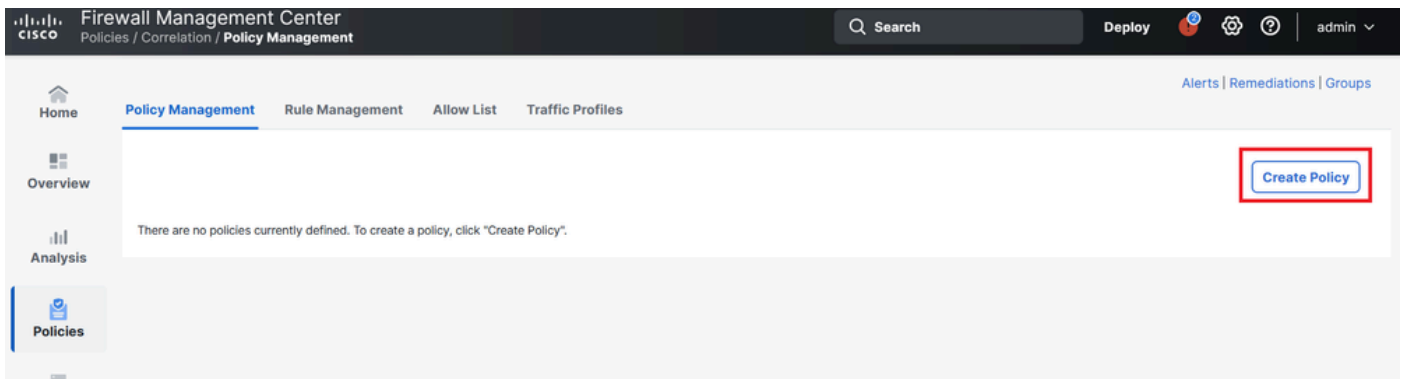


図 7.新しい相関ポリシーの作成

ステップ 3 : Add Rulesを選択して、ポリシーにルールを追加します。

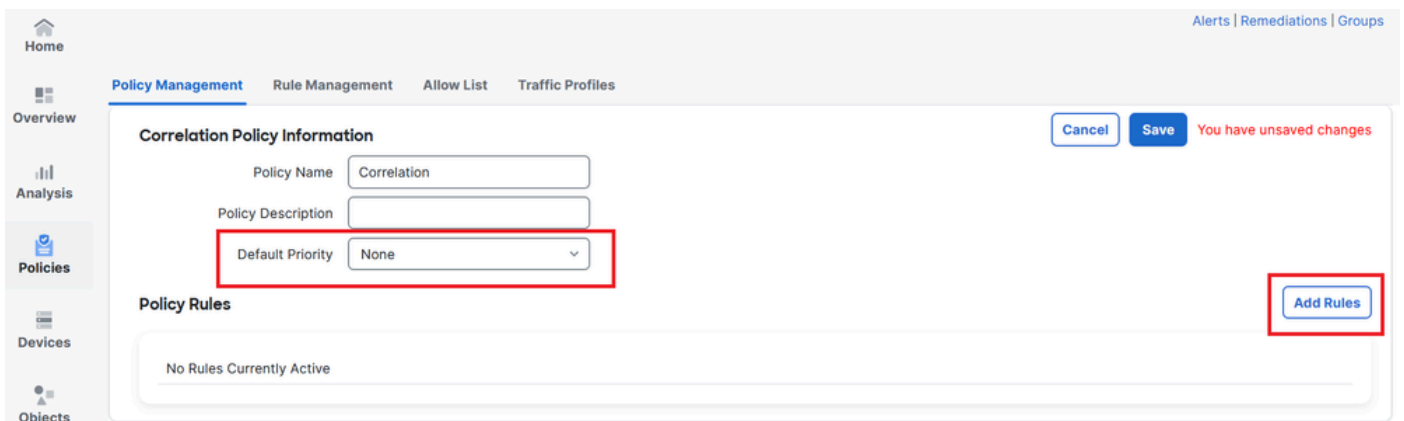


図 8.相関ポリシーのルールの追加と優先度の選択

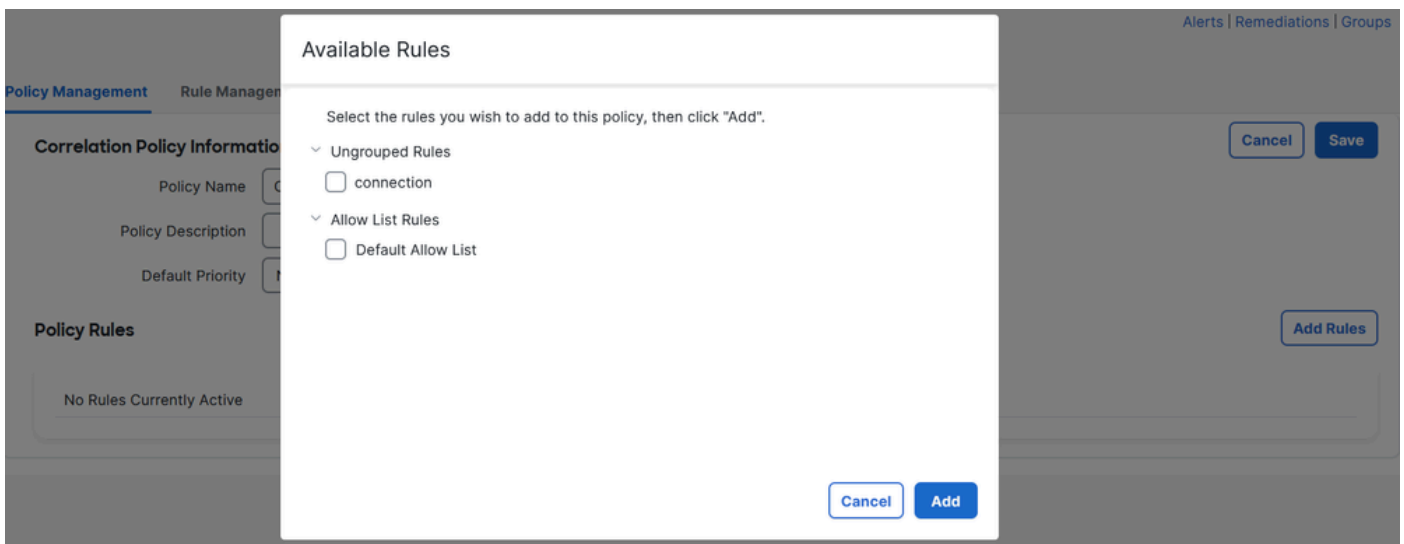


図 9.相関ポリシーに追加するルールの選択

ステップ 4 : 作成したアラートからルールに応答を割り当てると、トリガーされるたびに選択したアラートタイプが送信されます。

Policy Management Rule Management Allow List Traffic Profiles

Correlation Policy Information Cancel Save

Policy Name

Policy Description

Default Priority

Policy Rules Add Rules

Rule	Responses	Priority
connection	This rule does not have any responses.	Default <input type="text" value="Default"/> [Add]

図 10.[返信の追加]ボタン

Responses for connection

Assigned Responses



Unassigned Responses

email
syslog

Cancel

Update

図 11. 相関ルールへの応答の割り当て

ステップ 5: 相関ポリシーを保存して有効にします。

Policy Management Rule Management Allow List Traffic Profiles

Correlation Policy Information Cancel Save You have unsaved changes

Policy Name

Policy Description

Default Priority

Policy Rules Add Rules

Rule	Responses	Priority
connection	email (Email)	Default

図 12. 関連ルールに正しく追加された応答

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name Sort by

↗ ↖ 🗑️

図 13. 関連ポリシーの有効化

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。