

# Configurer la politique de corrélation sur FMC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurer les règles de corrélation](#)

[Configurer les alertes](#)

[Configurer la politique de corrélation](#)

---

## Introduction

Ce document décrit la procédure de configuration d'une politique de corrélation pour connecter des événements et détecter des anomalies sur votre réseau.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- Centre de gestion du pare-feu sécurisé (FMC)
- Protection pare-feu contre les menaces (FTD)

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Threat Defense pour VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les politiques de corrélation permettent d'identifier les menaces de sécurité potentielles sur votre réseau en configurant différents types d'événements. Elles sont utilisées pour la correction, les

alertes conditionnelles et les politiques de trafic.

## Configurer

### Configurer les règles de corrélation

Étape 1. Accédez à Politiques > Corrélation et sélectionnez Gestion des règles.

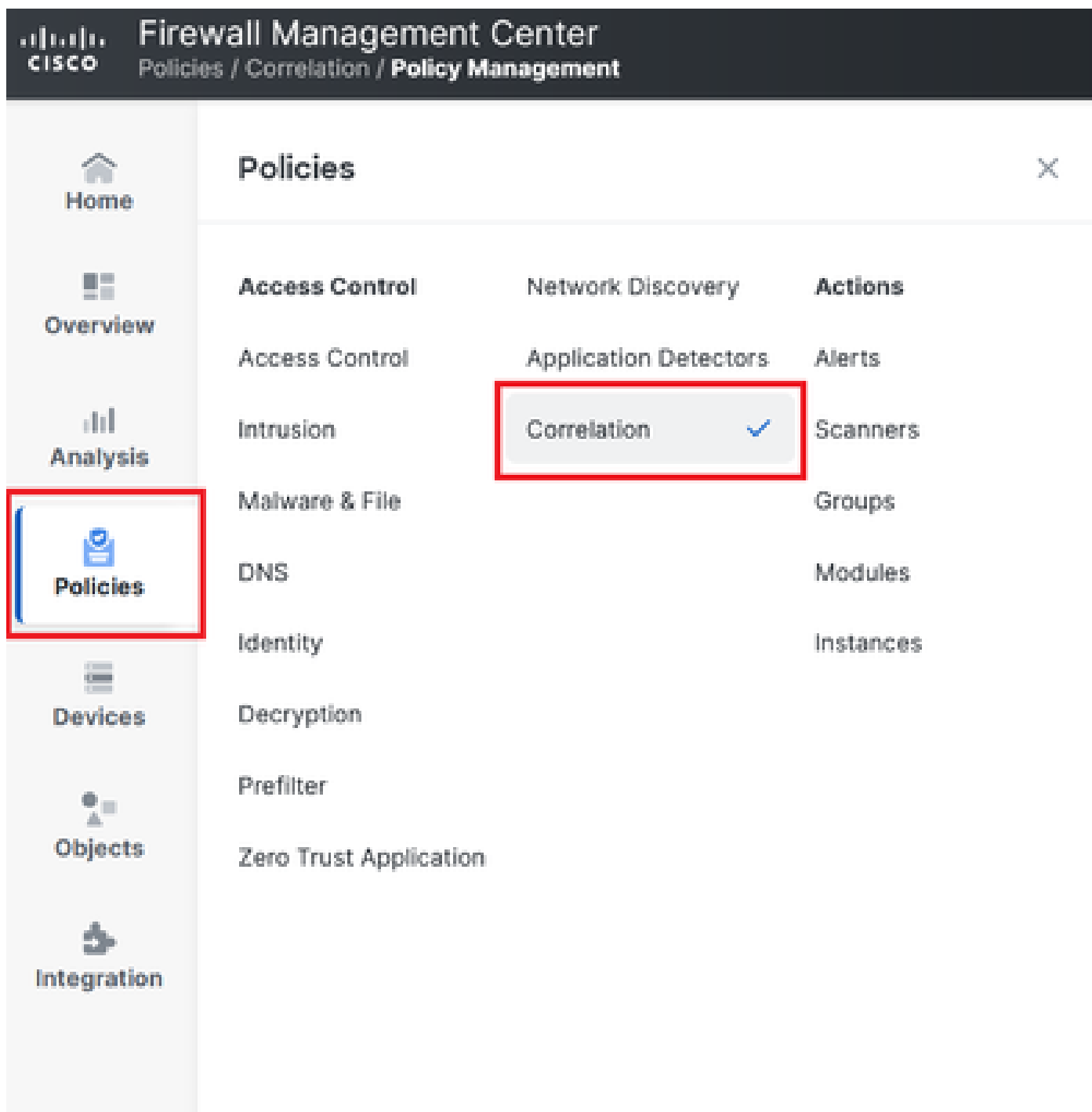


Image 1. Navigation jusqu'au menu Correlation Policy

Étape 2. Créez une nouvelle règle en sélectionnant Créer une règle.

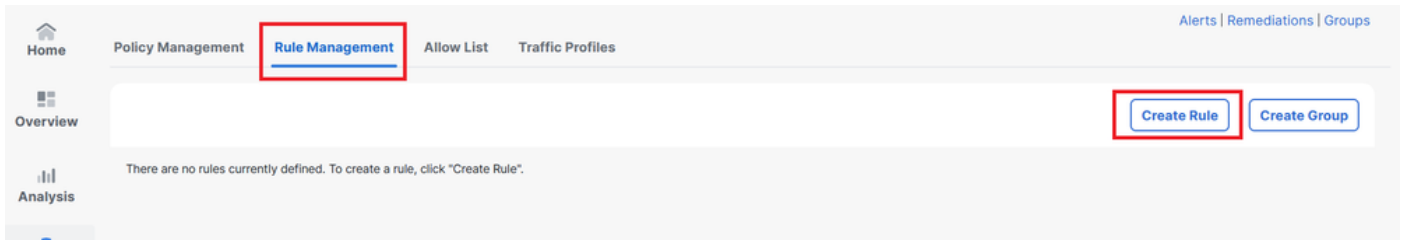


Image 2. Création de règle dans le menu Gestion des règles

Étape 3. Sélectionnez un type d'événement et les conditions qui correspondent à la règle.

Lorsque votre règle contient plusieurs conditions, vous devez les lier à l'opérateur AND ou OR.

**Rule Information** Add Connection Tracker Add User Qualification Add Host Profile Qualification

Rule Name:

Rule Description:

Rule Group:

Select the type of event for this rule

If   and it meets the following conditions:

Add condition Add complex condition


Application Protocol

Add condition Add complex condition

Source Country

Source Country

Image 3. Menu Création de règle

 Remarque : les règles de corrélation ne doivent pas être génériques. Si la règle est constamment déclenchée par le trafic normal, cela peut consommer davantage de CPU et affecter les performances FMC.

## Configurer les alertes

Étape 1. Accédez à Politiques > Actions > Alertes.

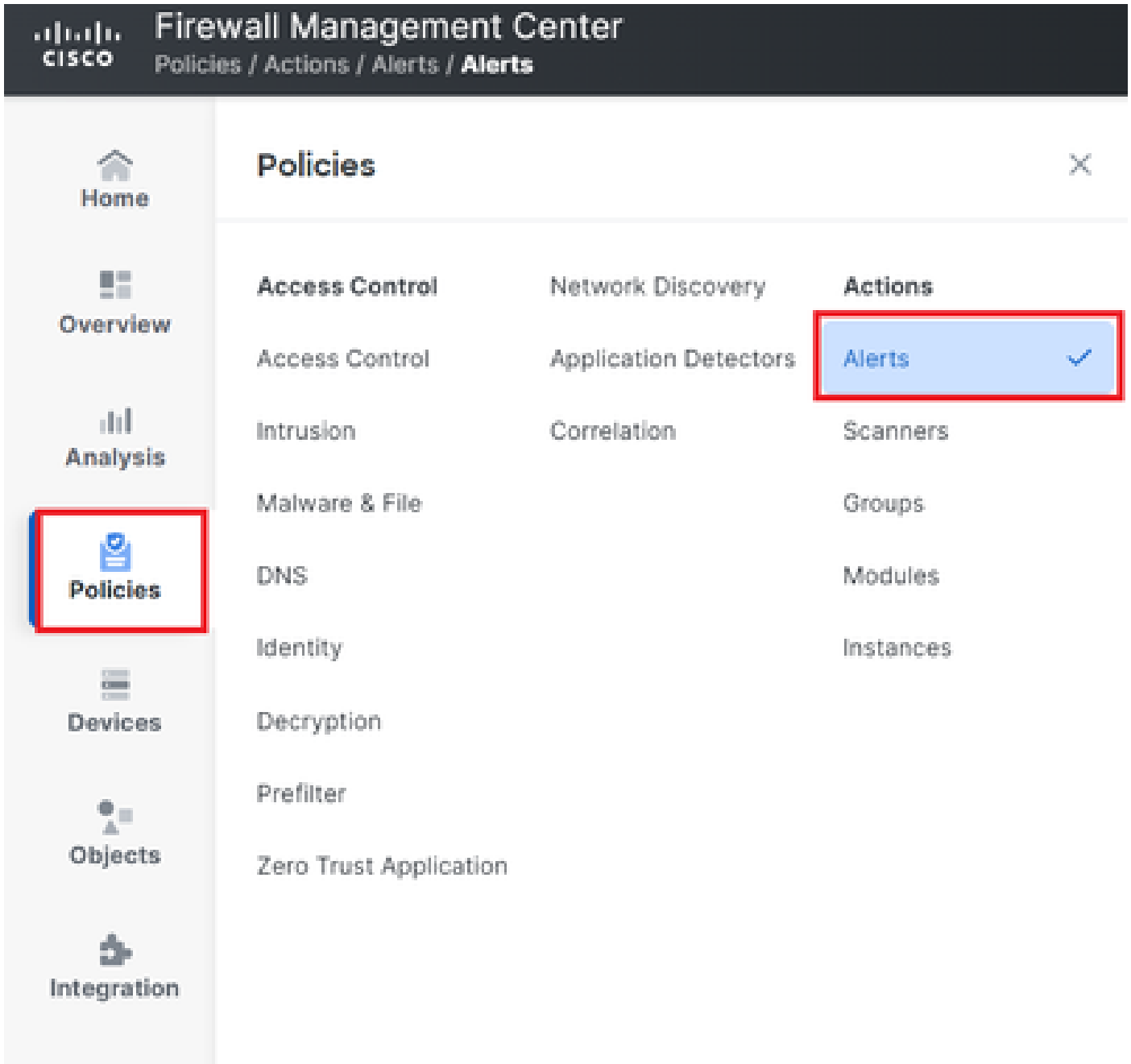


Image 4. Navigation vers le menu Alertes

Étape 2. Sélectionnez Create Alert et créez une alerte Syslog, SNMP ou une alerte par e-mail.

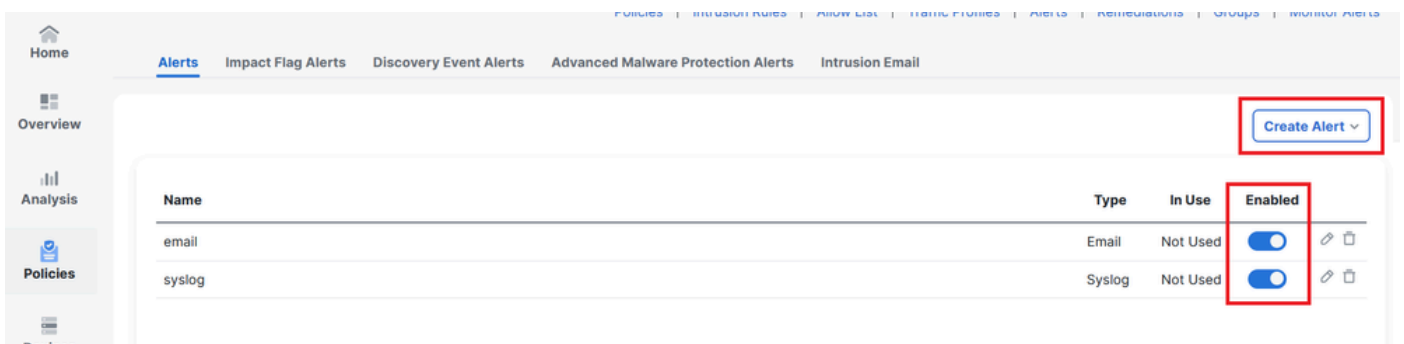
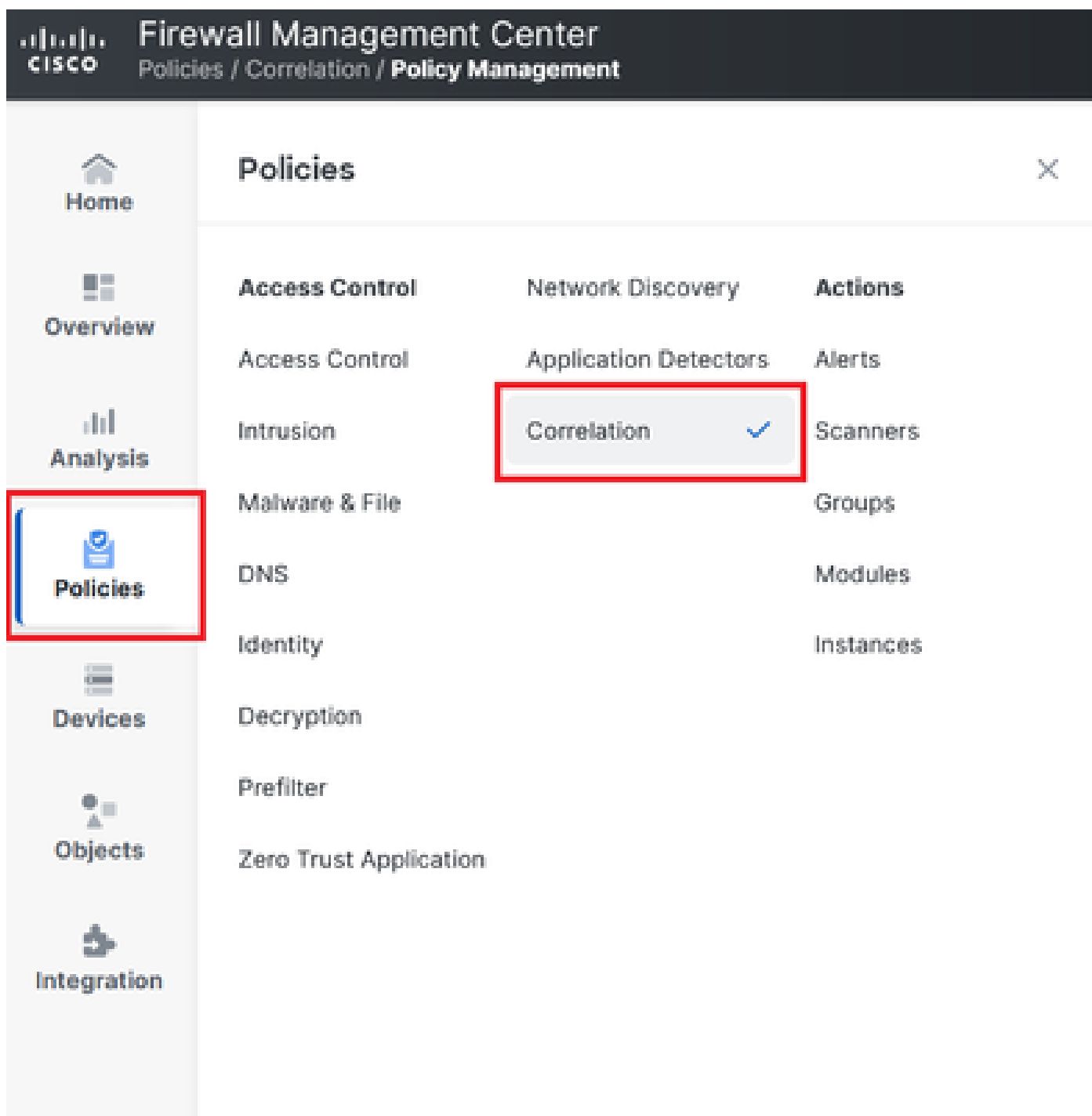


Image 5. Créer une alerte

Étape 3. Vérifiez que l'alerte est activée.

## Configurer la politique de corrélation

Étape 1. Accédez à Politiques > Corrélation.



Navigation jusqu'au menu Correlation Policy

Image 6. Navigation jusqu'au menu Correlation Policy

Étape 2. Créez une nouvelle politique de corrélation. Sélectionnez la priorité par défaut. Utilisez None pour utiliser les priorités des règles spécifiques.

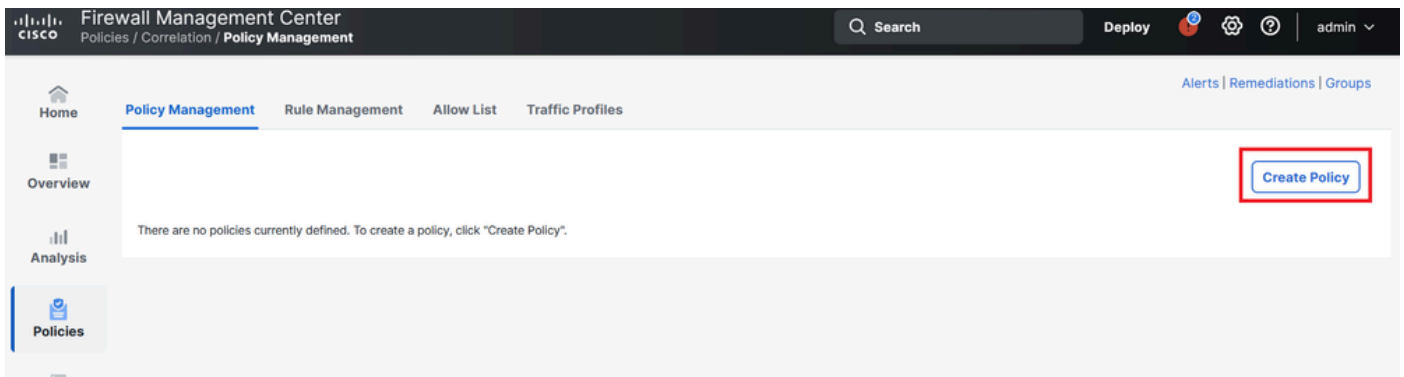


Image 7. Créer une nouvelle stratégie de corrélation

Étape 3. Ajoutez des règles à la stratégie en sélectionnant Ajouter des règles.

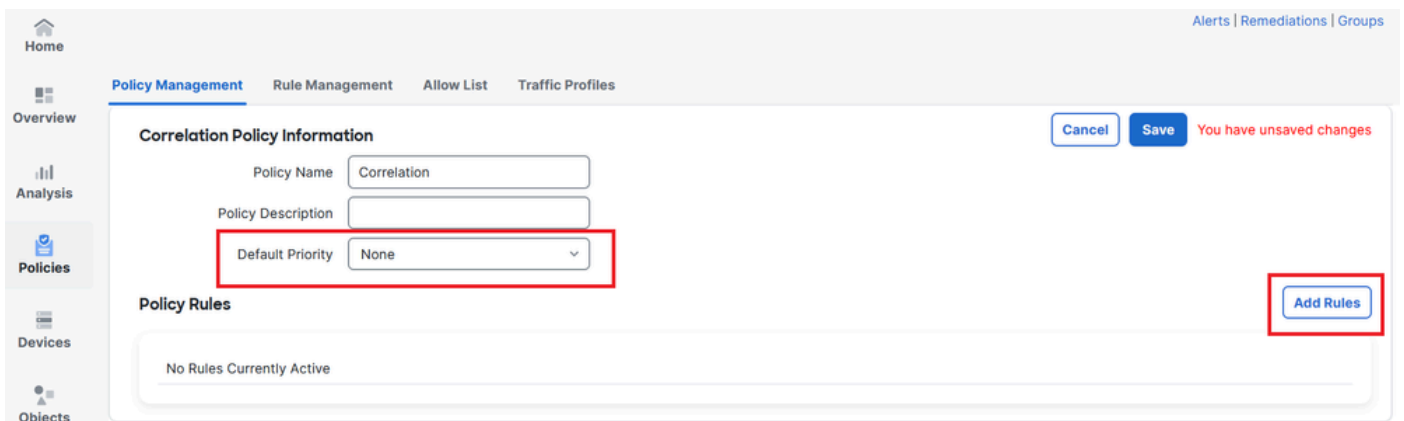


Image 8. Ajouter des règles et sélectionner la priorité pour la stratégie de corrélation

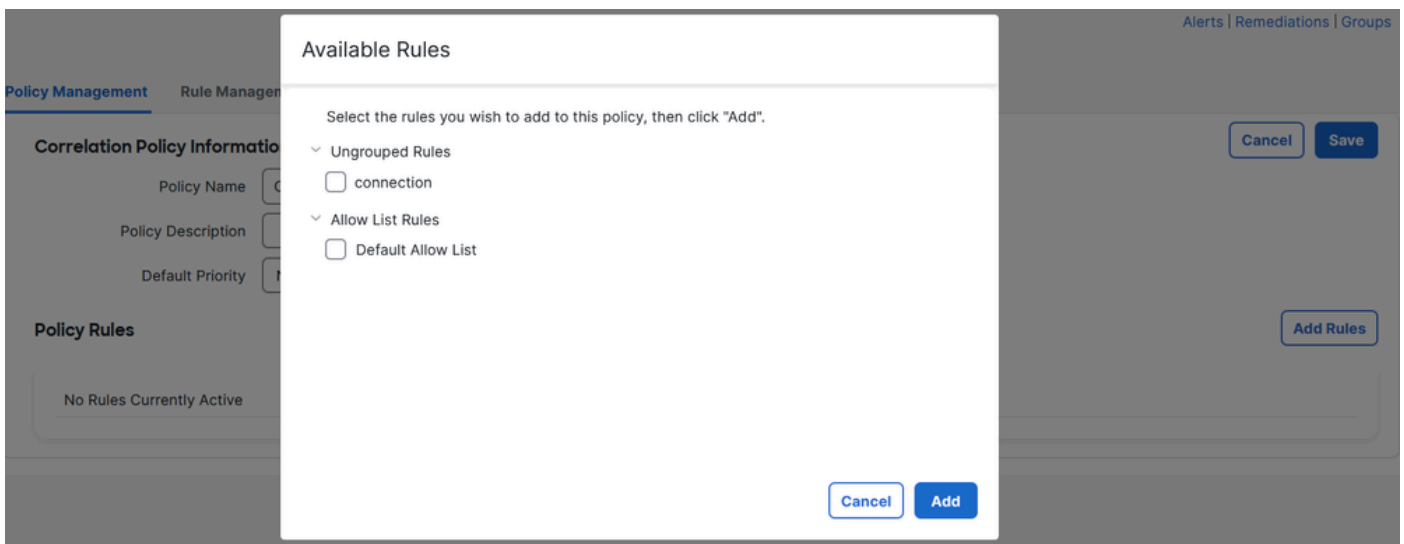


Image 9. Sélectionner les règles à ajouter à la politique de corrélation

Étape 4. Affectez une réponse à la règle à partir des alertes que vous avez créées, de sorte que chaque fois qu'elle est déclenchée, elle envoie le type d'alerte sélectionné.

**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
<a href="#">connection</a>	This rule does not have any responses.	Default <input type="text" value="Default"/> <span>+</span> <span>-</span>

Image 10. Bouton Ajouter des réponses

## Responses for connection

### Assigned Responses



### Unassigned Responses

email  
syslog

Cancel

Update

Image 11. Affecter des réponses à la règle de corrélation

Étape 5. Enregistrez et activez votre politique de corrélation.



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

Image 12. Réponse ajoutée correctement à la règle de corrélation

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name

Sort by

Image 13. Activer la stratégie de corrélation

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.