

# Configurar la política de correlación en FMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configurar reglas de correlación](#)

[Configurar alertas](#)

[Configurar política de correlación](#)

---

## Introducción

Este documento describe el procedimiento para configurar una política de correlación para conectar eventos y detectar anomalías en su red.

## Prerequisites

### Requirements

Cisco recomienda que conozca estos productos:

- Centro de gestión de firewall seguro (FMC)
- Protección frente a amenazas de firewall (FTD)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Threat Defense para VMware versión 7.6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Las políticas de correlación se utilizan para identificar posibles amenazas de seguridad en la red

mediante la configuración de diferentes tipos de eventos, y se utilizan para la remediación, alertas condicionales y políticas de tráfico.

## Configurar

### Configurar reglas de correlación

Paso 1. Navegue hasta Políticas > Correlación y seleccione Administración de reglas.

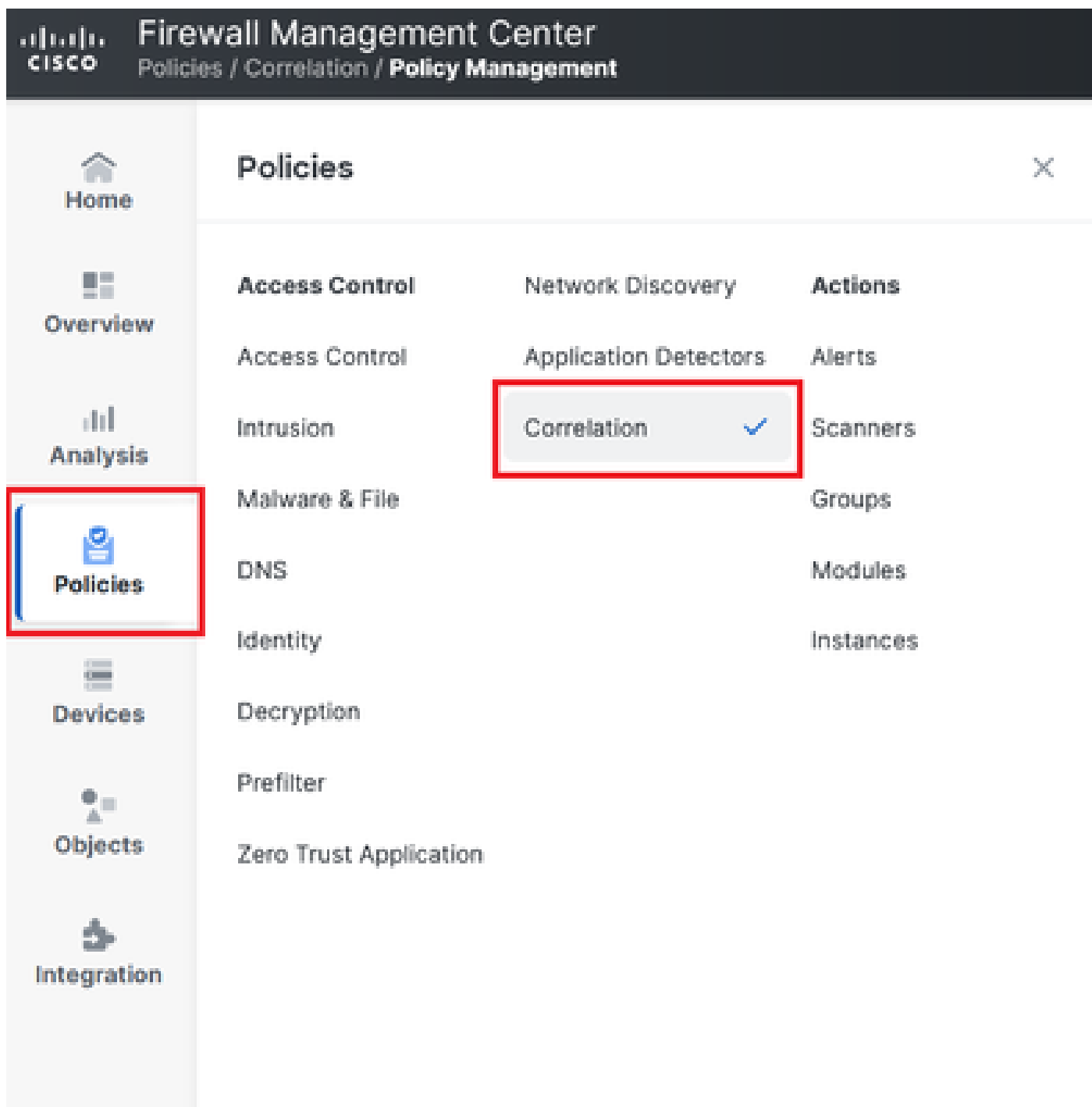


Imagen 1. Navegación al menú Política de correlación

Paso 2. Cree una nueva regla seleccionando Create Rule.

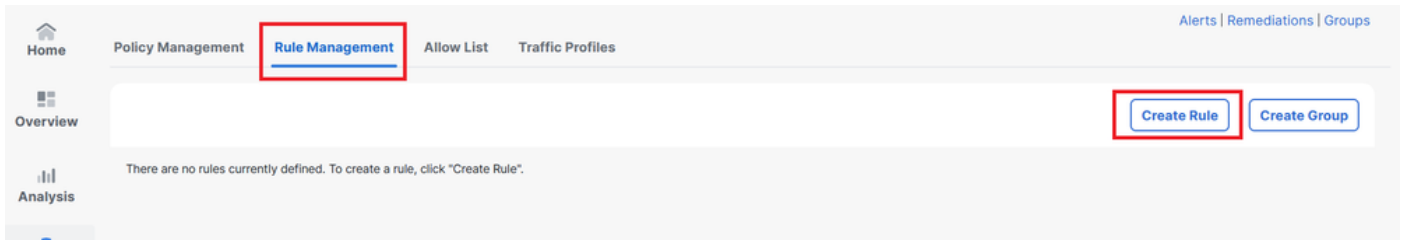


Imagen 2. Creación de reglas en el menú Administración de reglas

Paso 3. Seleccione un tipo de evento y las condiciones para que coincidan con la regla.

Cuando la regla contiene varias condiciones, debe vincularlas con AND o con un operador OR.

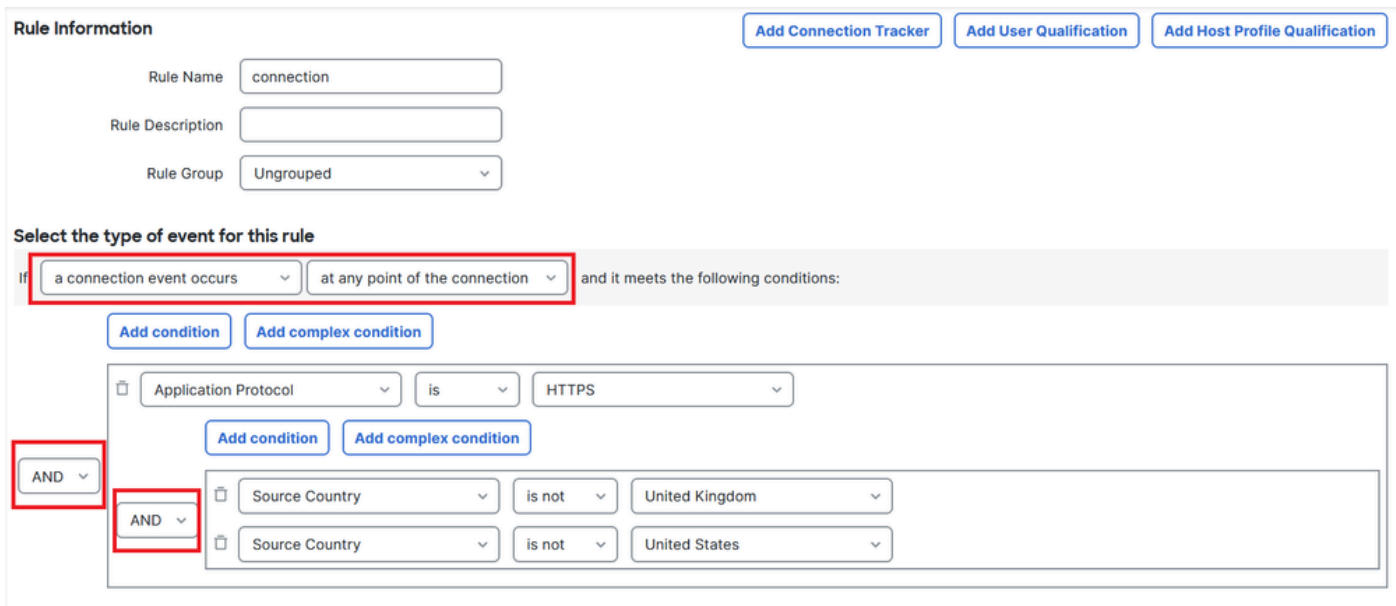



Imagen 3. Menú de creación de reglas

 Nota: Las reglas de correlación no deben ser genéricas. Si el tráfico normal activa constantemente la regla, esto puede consumir CPU adicional y afectar al rendimiento de FMC.

## Configurar alertas

Paso 1. Vaya a Políticas > Acciones > Alertas.

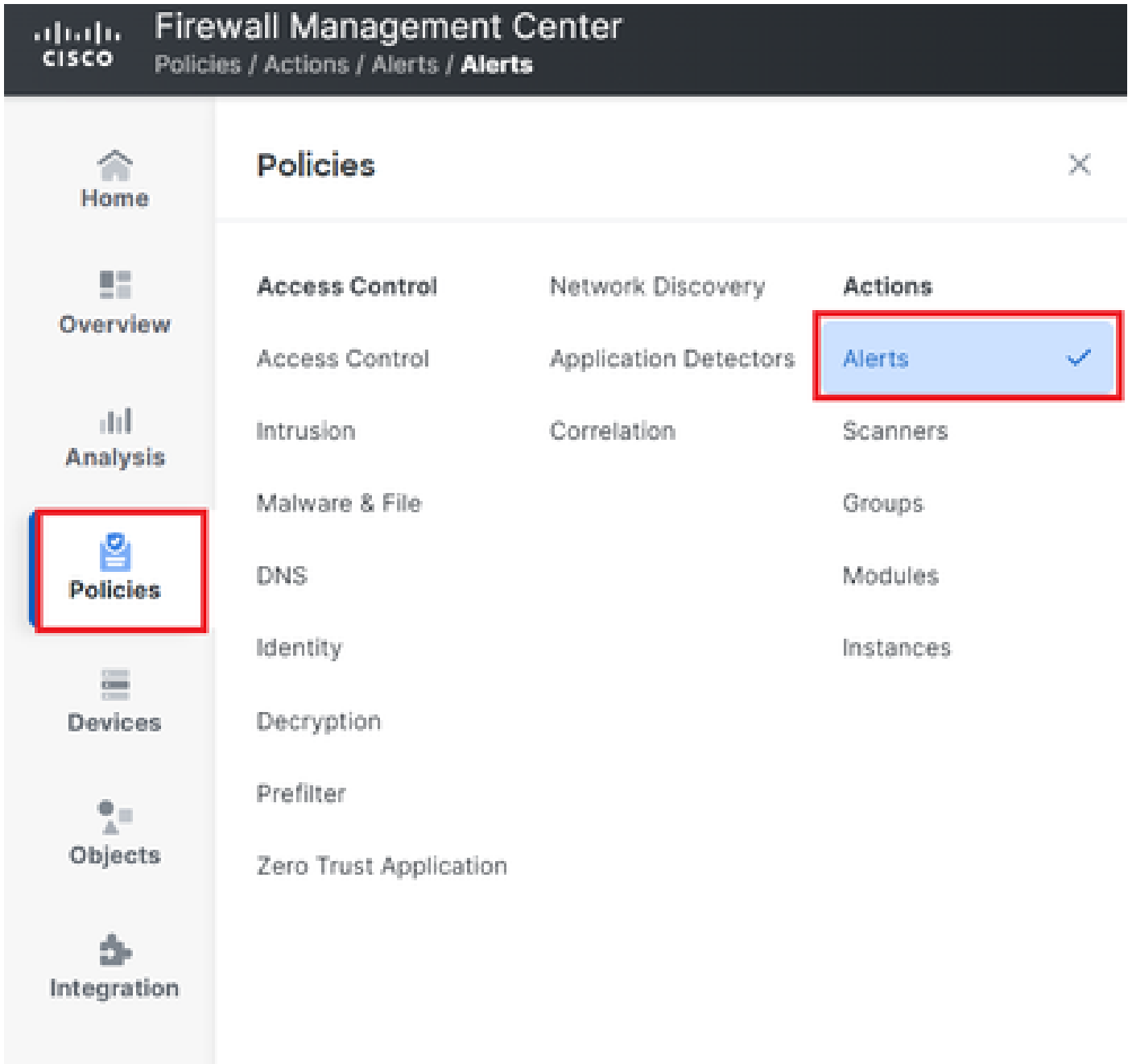


Imagen 4. Navegación al menú Alertas

Paso 2. Seleccione Create Alert y cree un Syslog, SNMP o alerta de correo electrónico.

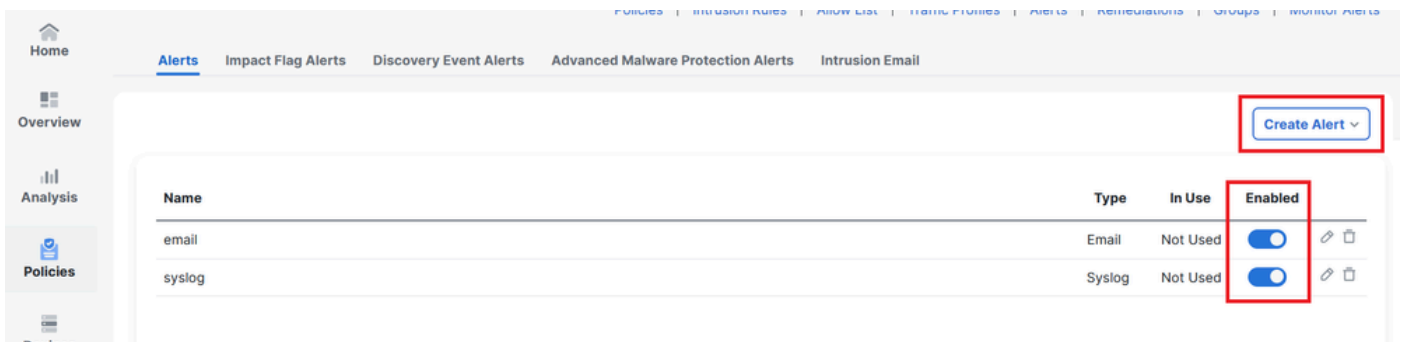
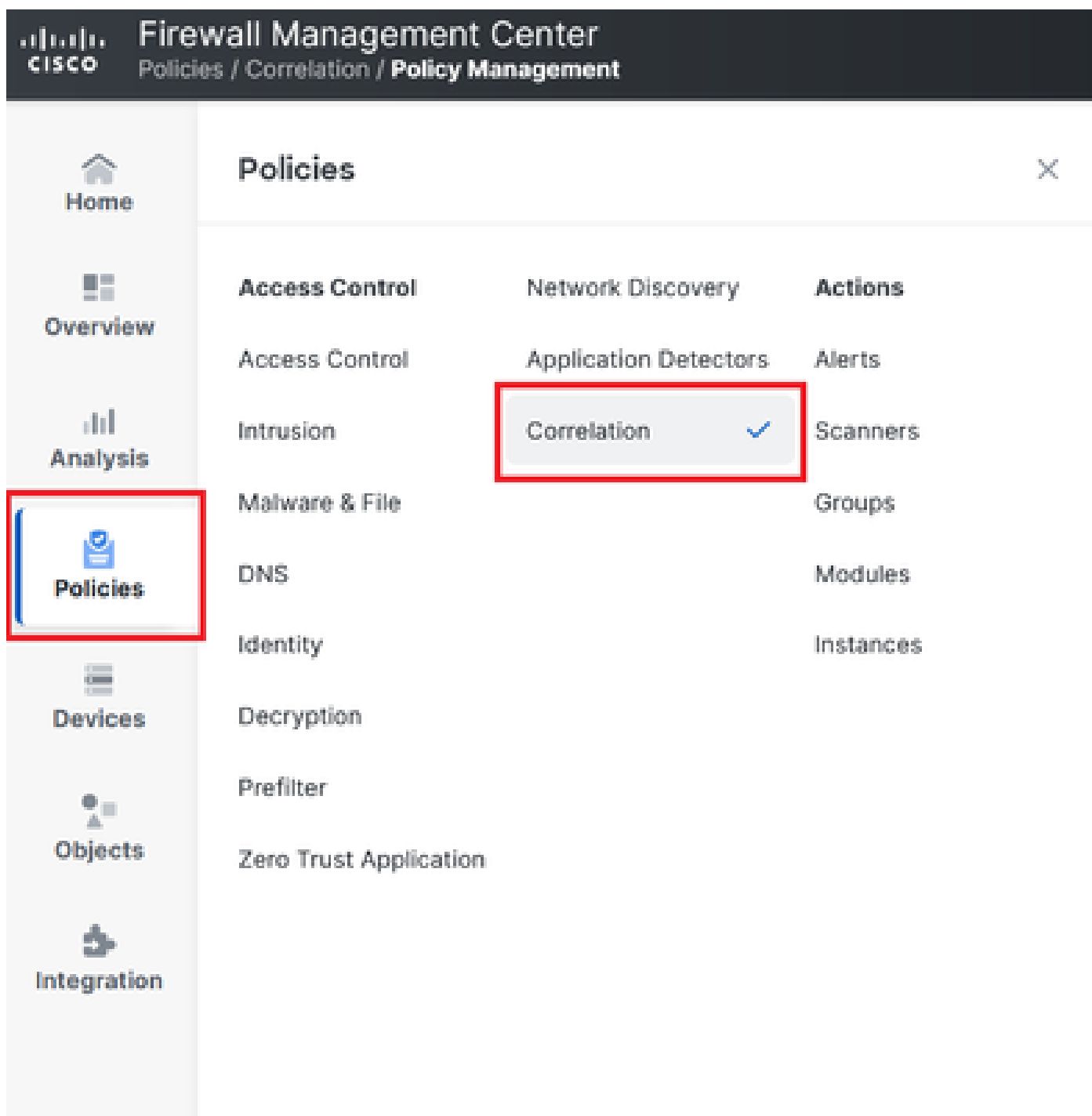


Imagen 5. Crear alerta

Paso 3. Verifique que la alerta esté habilitada.

## Configurar política de correlación

Paso 1. Vaya a Políticas > Correlación.



Navegación al menú Política de correlación

Imagen 6. Navegación al menú Política de correlación

Paso 2. Cree una nueva política de correlación. Seleccione la prioridad predeterminada. Utilice None para utilizar las prioridades de las reglas específicas.

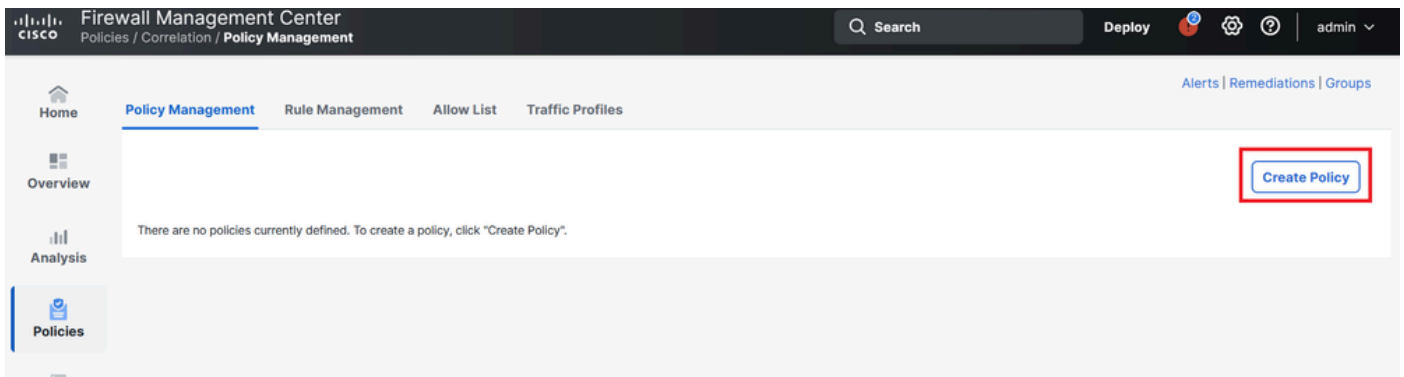


Imagen 7. Crear nueva política de correlación

Paso 3. Agregue reglas a la directiva seleccionando Add Rules.

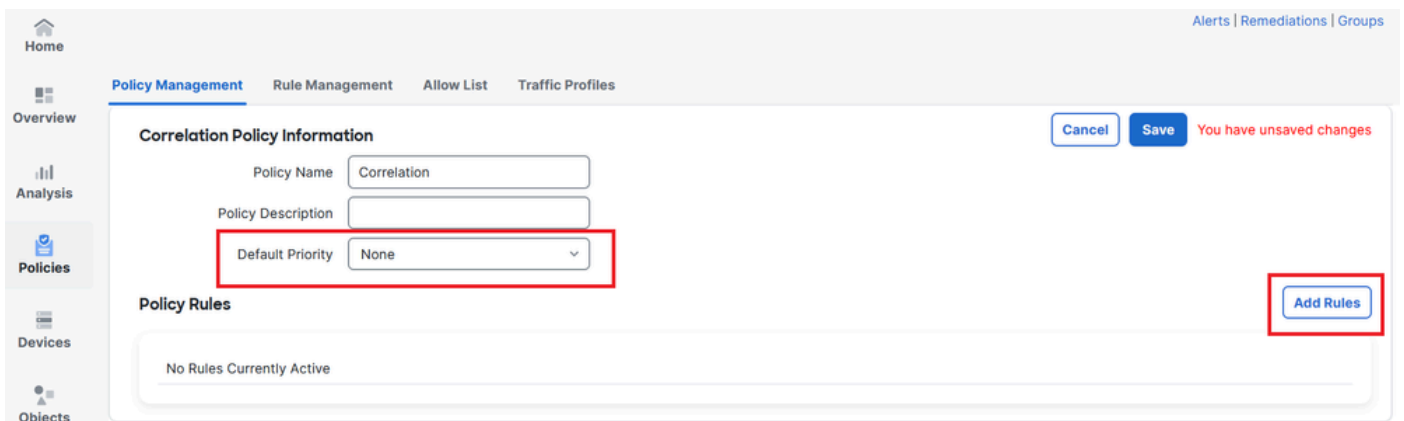


Imagen 8. Agregar reglas y seleccionar prioridad para la política de correlación

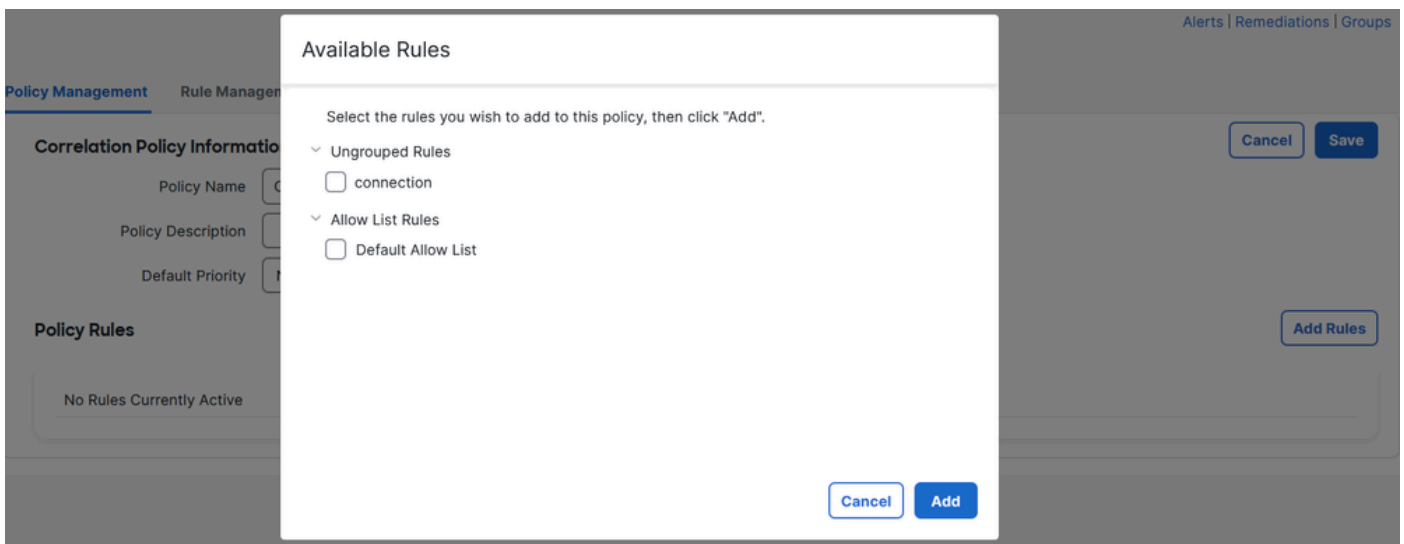


Imagen 9. Seleccionar reglas para agregar a la directiva de correlación

Paso 4. Asigne una respuesta a la regla desde las alertas que ha creado, de modo que siempre que se active, enviará el tipo de alerta seleccionado.

Cancel Save

Correlation Policy Information

Policy Name

Policy Description

Default Priority

Add Rules

Policy Rules

Rule	Responses	Priority
<a href="#">connection</a>	This rule does not have any responses.	Default <input type="text" value="Default"/>



Imagen 10. Botón Agregar respuestas

## Responses for connection

### Assigned Responses



### Unassigned Responses

email  
syslog

Cancel

Update

Imagen 1. Asignar respuestas a regla de correlación

Paso 5. Guarde y active la política de correlación.



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

Imagen 12. Respuesta agregada correctamente a la regla de correlación

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name

Sort by

Imagen 13. Habilitar política de correlación

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).