Configurar política de correlação no FMC

Contents

Introdução

Este documento descreve o procedimento para configurar uma política de correlação para conectar eventos e detectar anomalias em sua rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- Centro de gerenciamento seguro de firewall (FMC)
- Defesa contra ameaças de firewall (FTD) segura

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Threat Defense para VMware versão 7.6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As políticas de correlação são usadas para identificar possíveis ameaças à segurança na rede, configurando diferentes tipos de eventos, e são usadas para correção, alertas condicionais e

políticas de tráfego.

Configurar

Configurar regras de correlação

Etapa 1. Navegue até Policies > Correlation e selecione Rule Management.

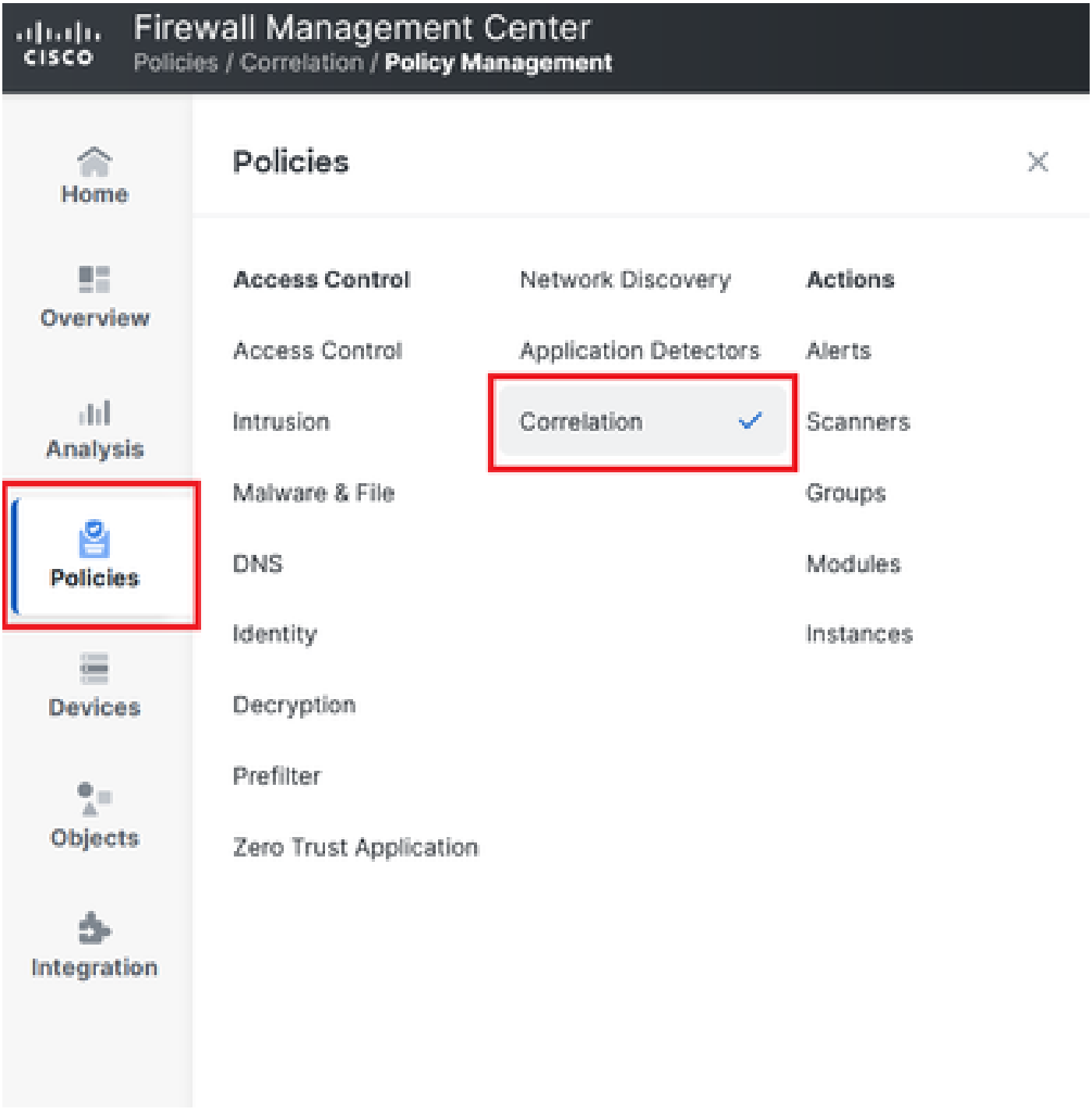


Imagem 1. Navegação para o menu Política de correlação

Etapa 2. Crie uma nova regra selecionando Criar regra.

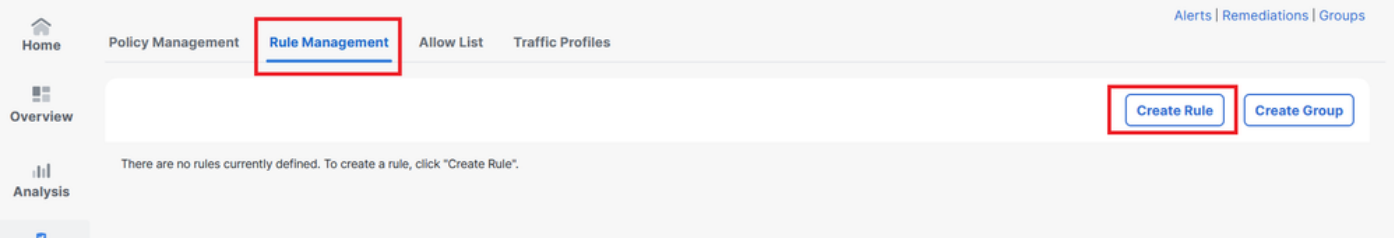


Imagem 2. Criação de Regras no Menu Gerenciamento de Regras

Etapa 3. Selecione um tipo de evento e as condições para corresponder à regra.

Quando a regra contiver várias condições, você deverá vinculá-las a um operador AND ou OR.

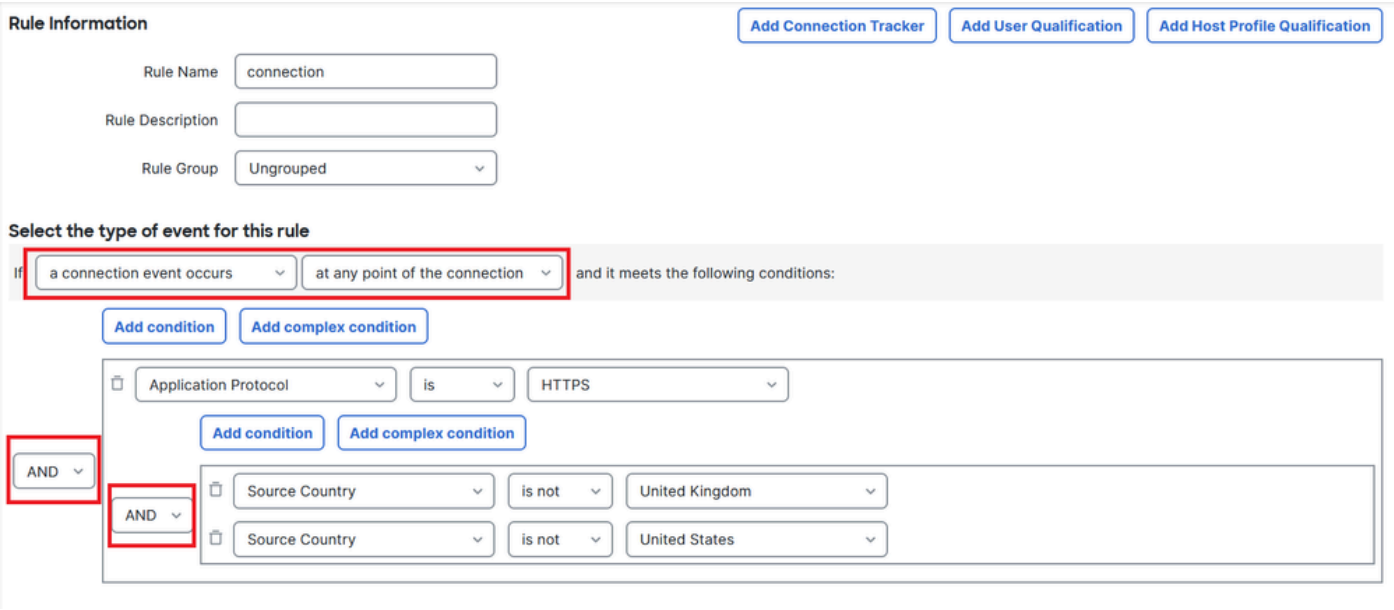


Imagem 3. Menu de Criação de Regra

Observação: as regras de correlação não devem ser genéricas; se a regra for acionada constantemente pelo tráfego normal, isso poderá consumir CPU adicional e afetar o desempenho do FMC.

Configurar alertas

Etapa 1. Navegue até Policies > Actions > Alerts.

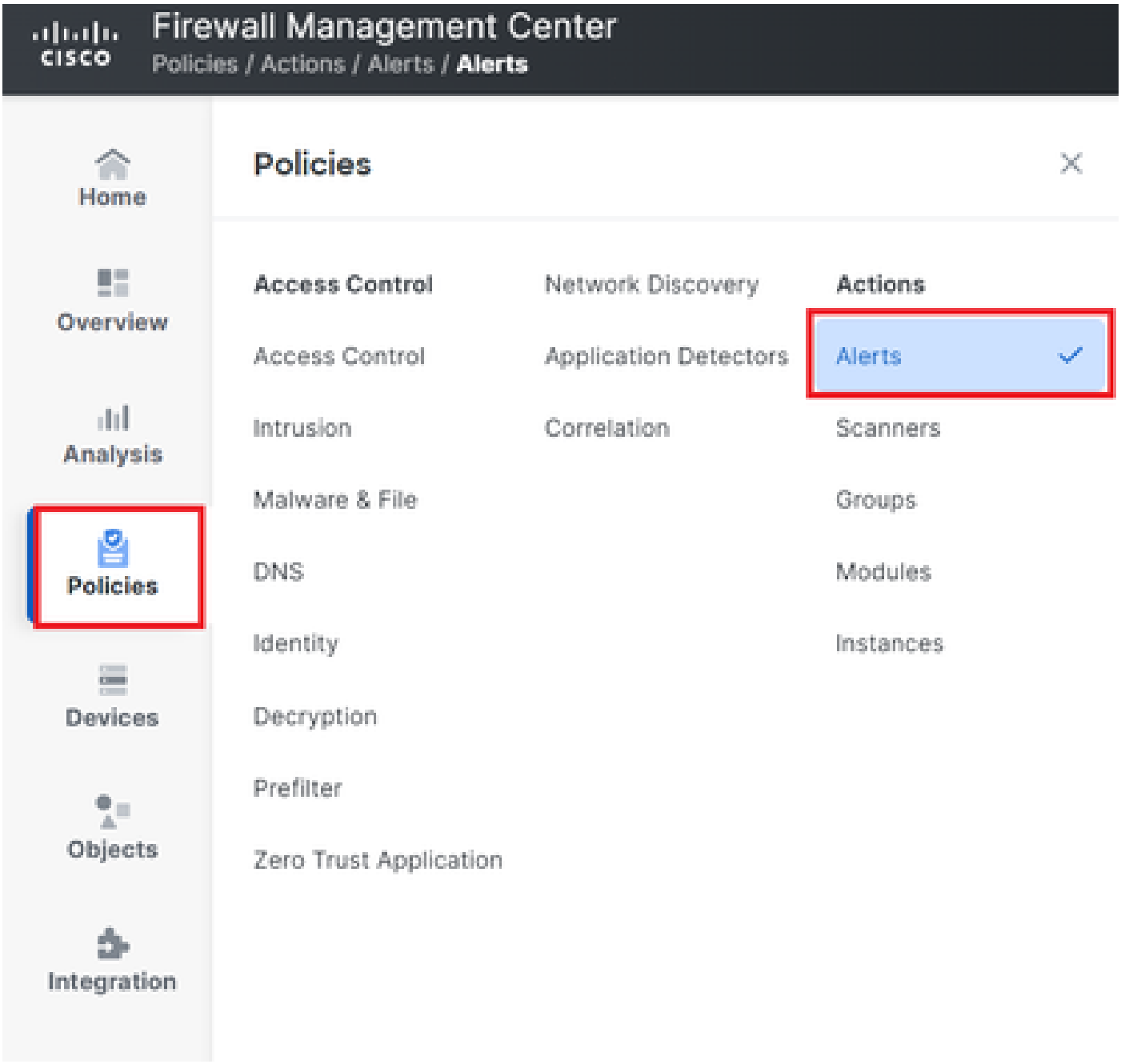


Imagem 4. Navegação para o menu Alertas

Etapa 2. Selecione Create Alert e crie um Syslog, SNMP ou alerta por e-mail.

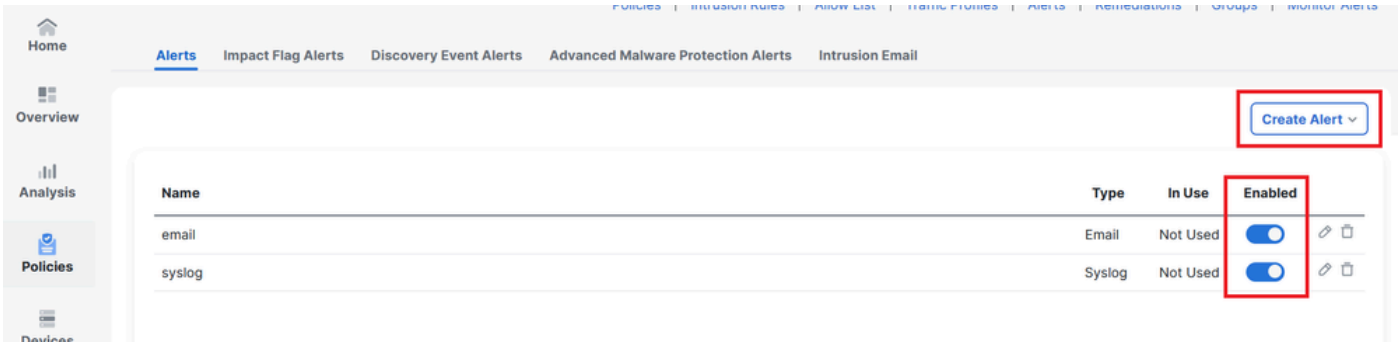
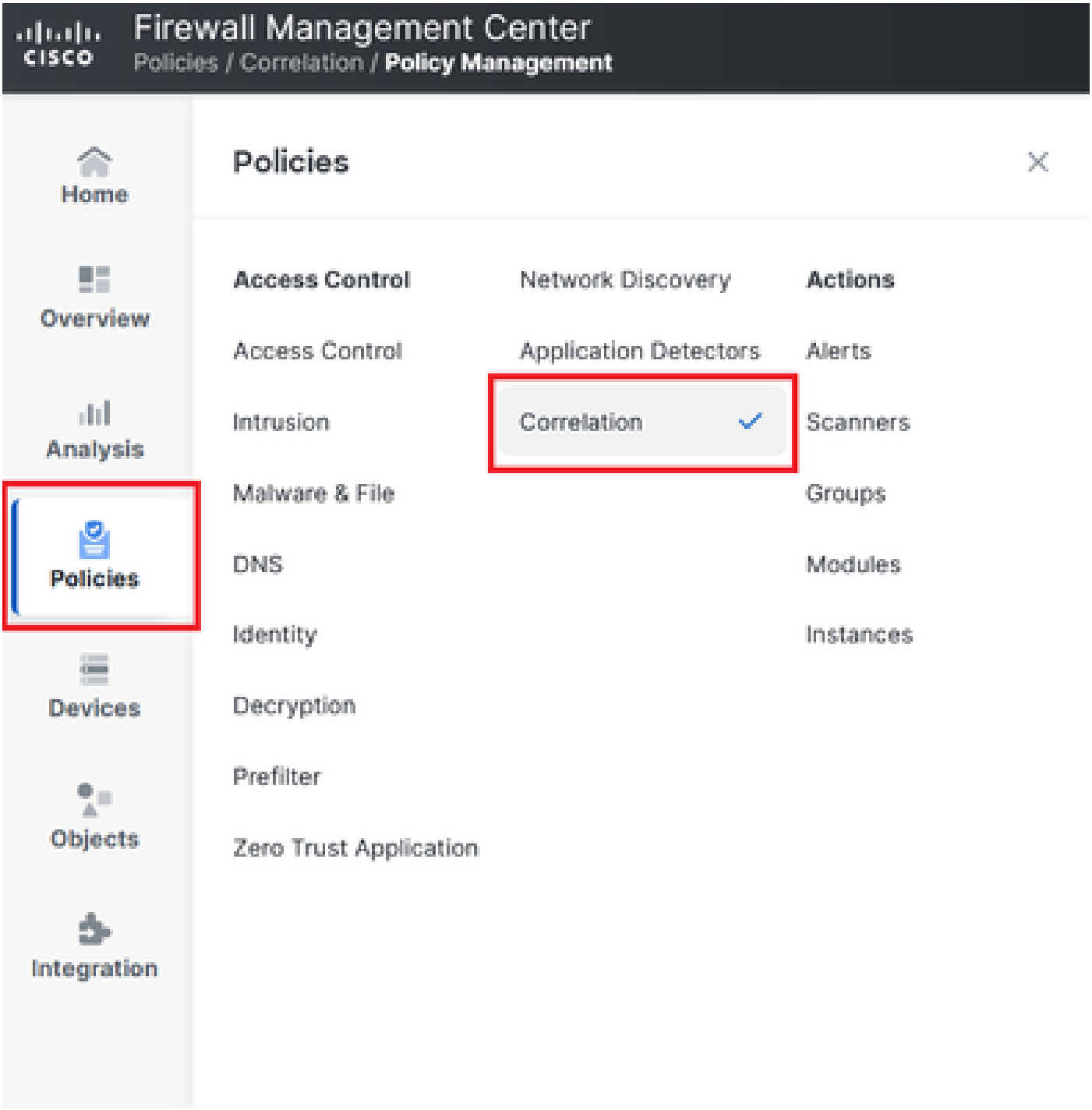


Imagem 5. Criar Alerta

Etapa 3. Verifique se o alerta está ativado.

Configurar política de correlação

Etapa 1. Navegue até Policies > Correlation.



Navegação para o menu Política de correlação

Imagem 6. Navegação para o menu Política de correlação

Etapa 2. Crie uma nova Política de Correlação. Selecione a prioridade padrão. Use Nenhum para usar as prioridades das regras específicas.

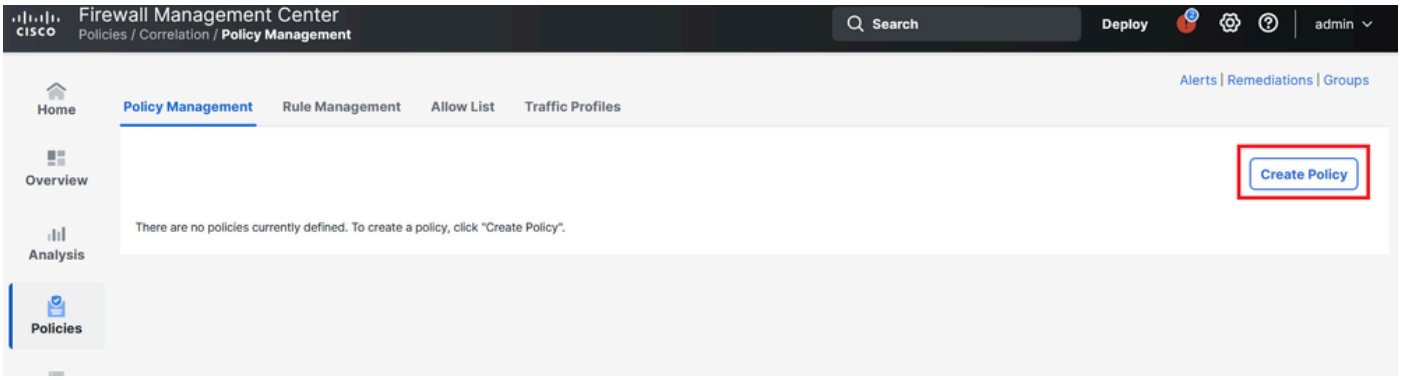


Imagem 7. Criar nova política de correlação

Etapa 3. Adicione regras à política selecionando Add Rules.

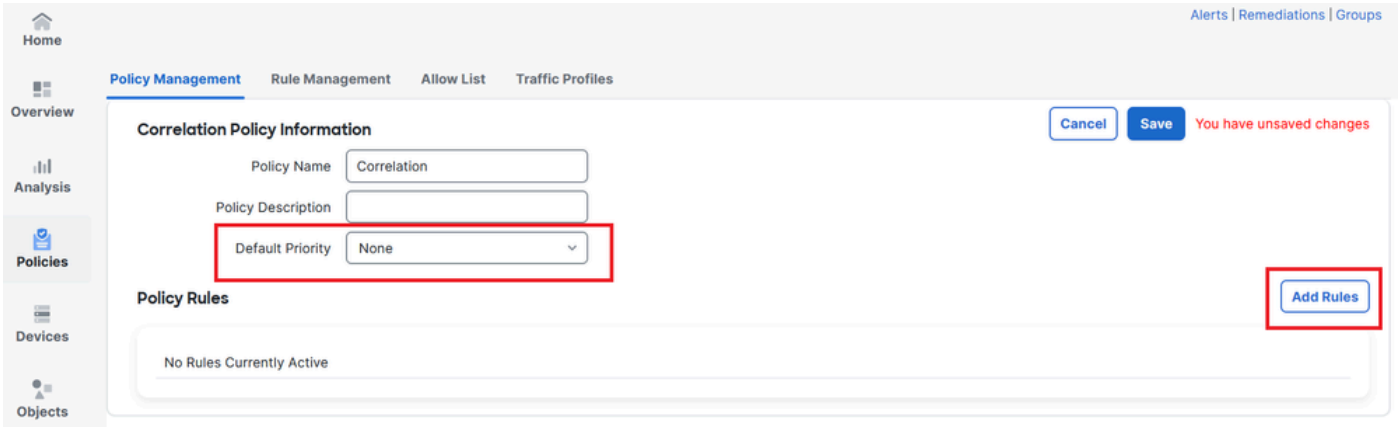


Imagem 8. Adicionar regras e selecionar prioridade para política de correlação

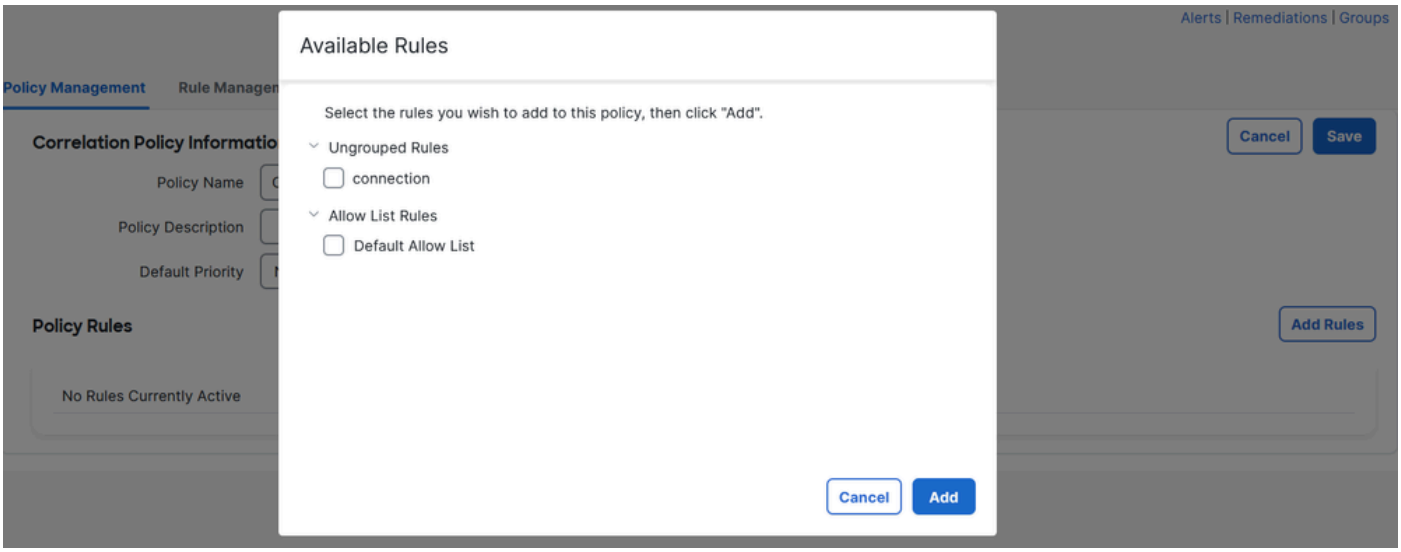


Imagem 9. Selecionar regras para adicionar à política de correlação

Etapa 4. Atribua uma resposta à regra a partir dos alertas criados, de modo que, sempre que ela for disparada, o tipo de alerta selecionado seja enviado.

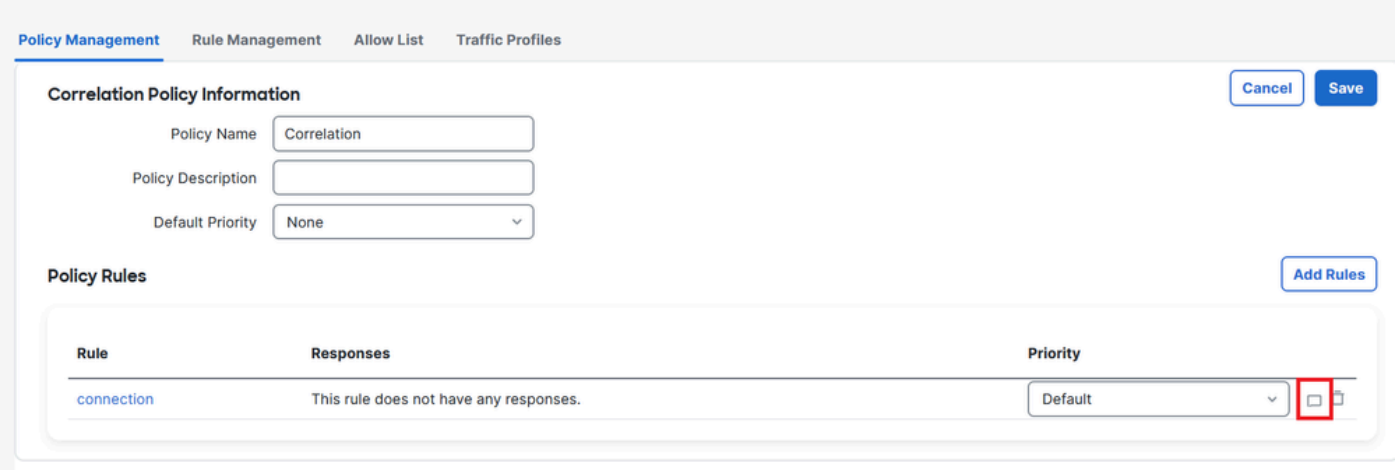


Imagem 10. Botão Adicionar respostas

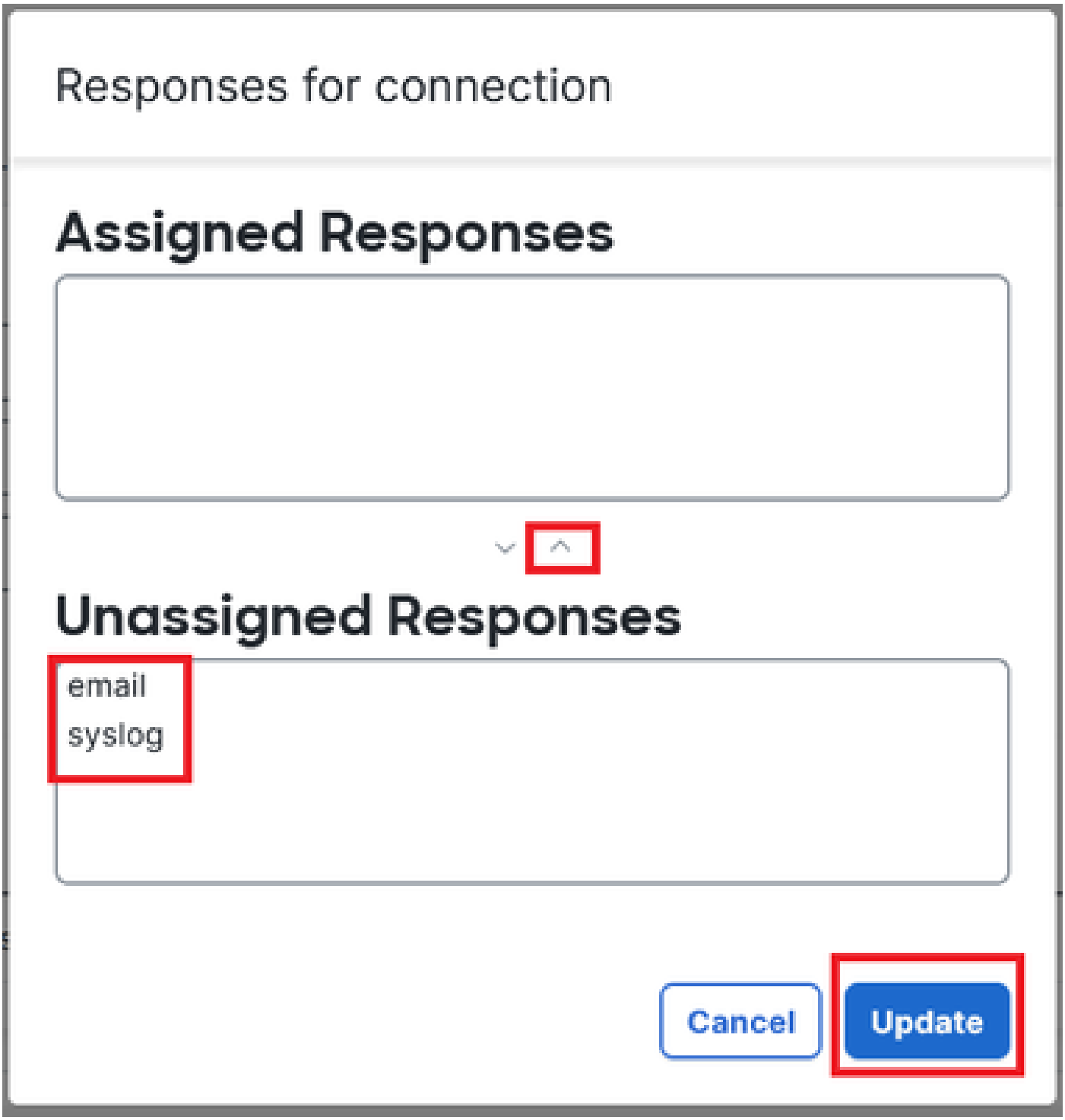


Imagem 11. Atribuir respostas à regra de correlação

Etapa 5. Salve e habilite sua Política de correlação.

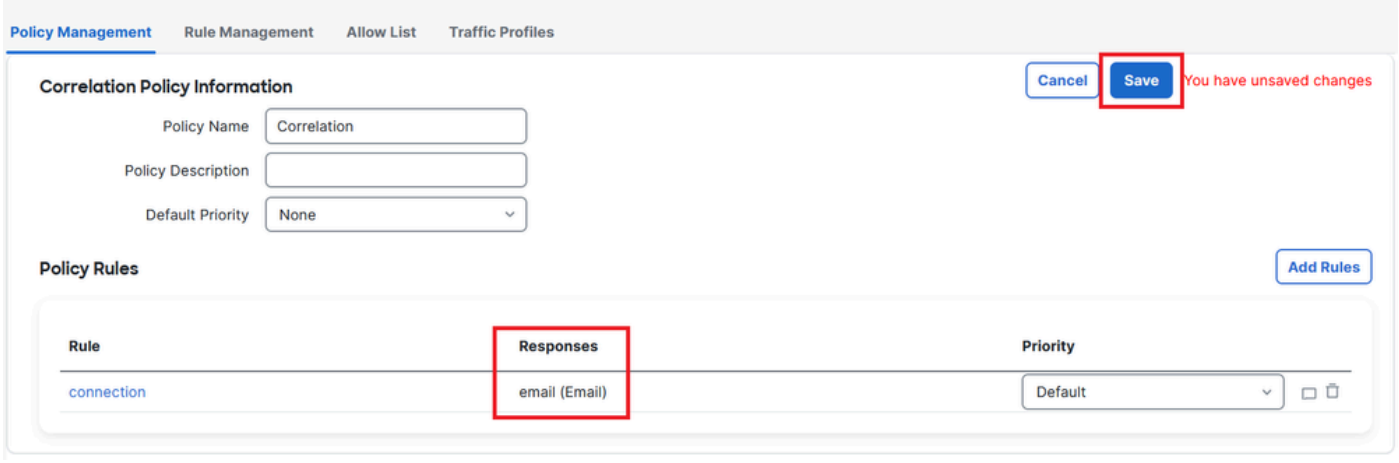


Imagem 12. Resposta Adicionada Corretamente à Regra de Correlação

Imagem 13. Habilitar Política de Correlação

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.