

Korrelationsrichtlinie auf FMC konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Korrelationsregeln konfigurieren](#)

[Warnmeldungen konfigurieren](#)

[Korrelationsrichtlinie konfigurieren](#)

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration einer Korrelationsrichtlinie beschrieben, um Ereignisse zu verbinden und Anomalien in Ihrem Netzwerk zu erkennen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

- Secure Firewall Management Center (FMC)
- Sichere Firewall-Bedrohungsabwehr (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firepower Threat Defense für VMware Version 7.6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Korrelationsrichtlinien werden verwendet, um potenzielle Sicherheitsbedrohungen in Ihrem

Netzwerk zu identifizieren, indem verschiedene Ereignistypen konfiguriert werden. Sie werden für die Behebung, für bedingte Warnungen und für Datenverkehrsrichtlinien verwendet.

Konfigurieren

Korrelationsregeln konfigurieren

Schritt 1: Navigieren Sie zu Policies > Correlation (Richtlinien > Korrelation), und wählen Sie Rule Management (Regelverwaltung).

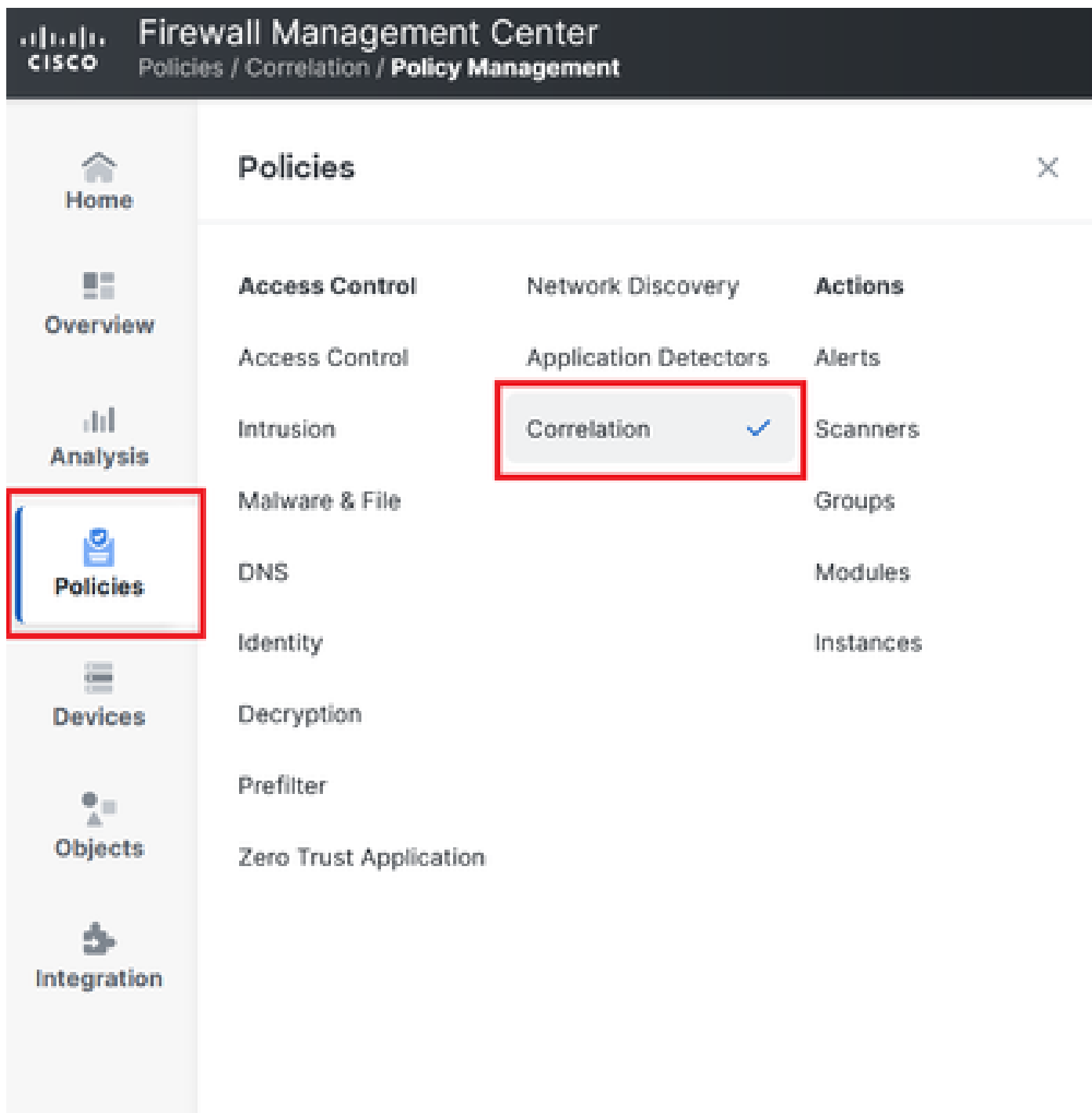


Image 1. Navigation zum Menü "Korrelationsrichtlinie"

Schritt 2: Erstellen Sie eine neue Regel, indem Sie Regel erstellen auswählen.

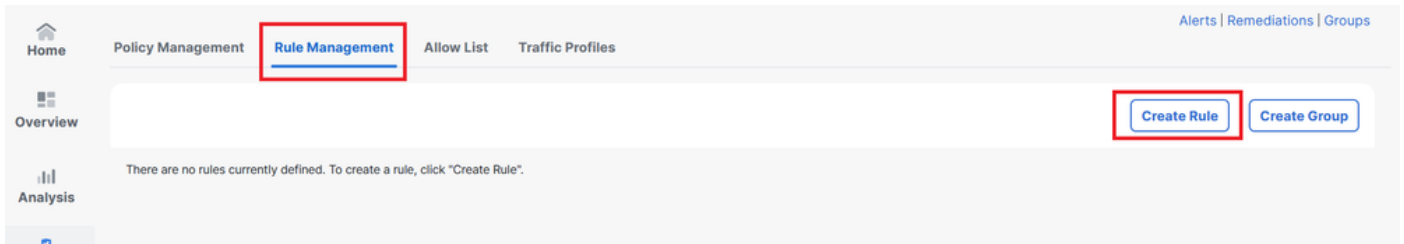


Image 2. Regelerstellung im Menü "Regelverwaltung"

Schritt 3: Wählen Sie einen Ereignistyp und die Bedingungen aus, die der Regel entsprechen sollen.

Wenn die Regel mehrere Bedingungen enthält, müssen Sie diese mit AND oder einem OR-Operator verknüpfen.

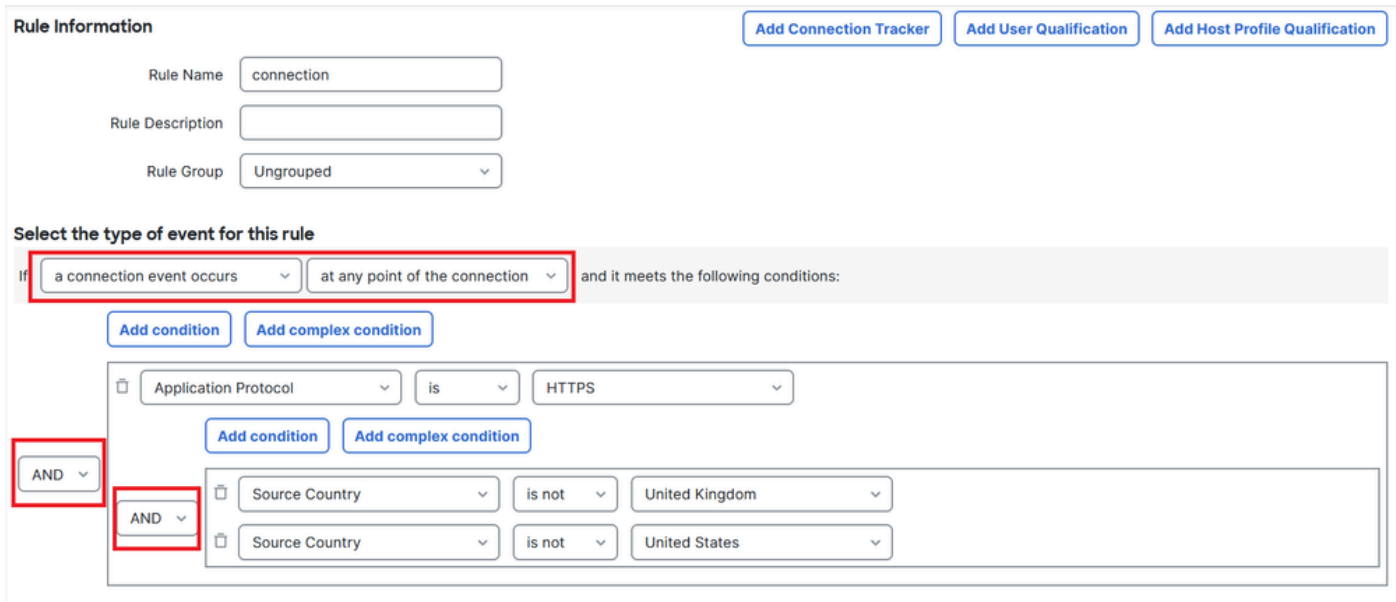



Image 3. Menü "Regelerstellung"

 Hinweis: Korrelationsregeln dürfen nicht allgemein gehalten werden. Wenn die Regel ständig durch normalen Datenverkehr ausgelöst wird, kann dies zusätzliche CPU-Ressourcen verbrauchen und die FMC-Leistung beeinträchtigen.

Warnmeldungen konfigurieren

Schritt 1: Navigieren Sie zu Richtlinien > Aktionen > Warnmeldungen.

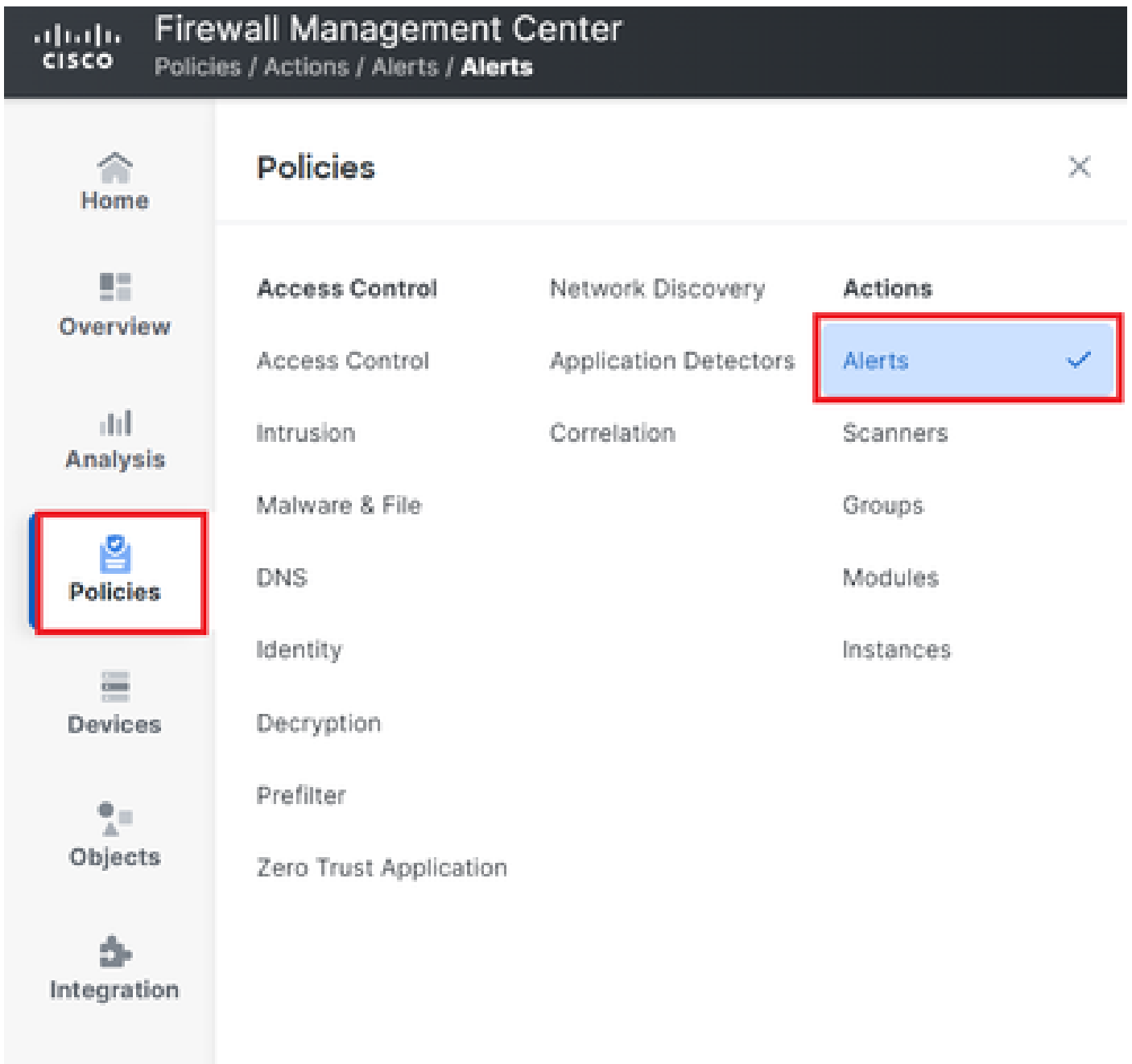


Image 4. Navigation zum Menü "Warnmeldungen"

Schritt 2: Wählen Sie Warnmeldung erstellen und erstellen Sie entweder ein Syslog, SNMP oder eine E-Mail-Warnmeldung.

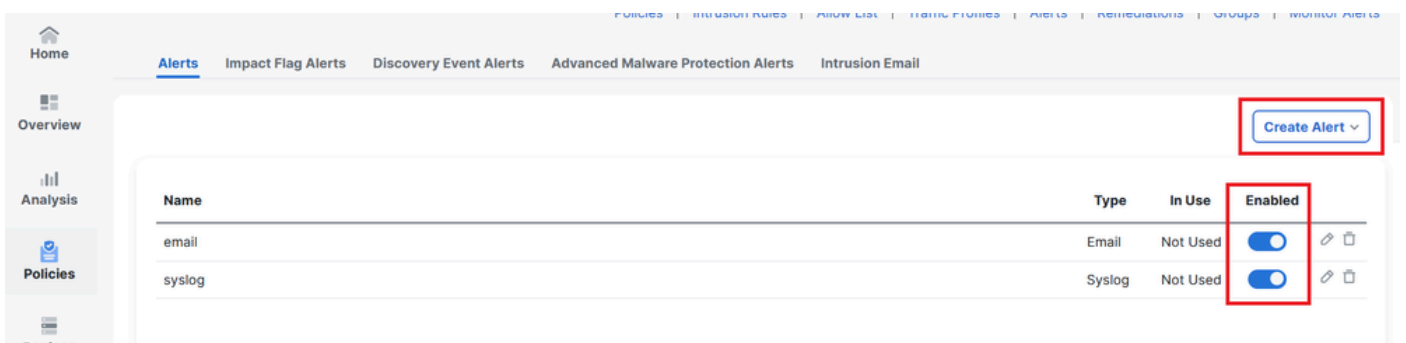
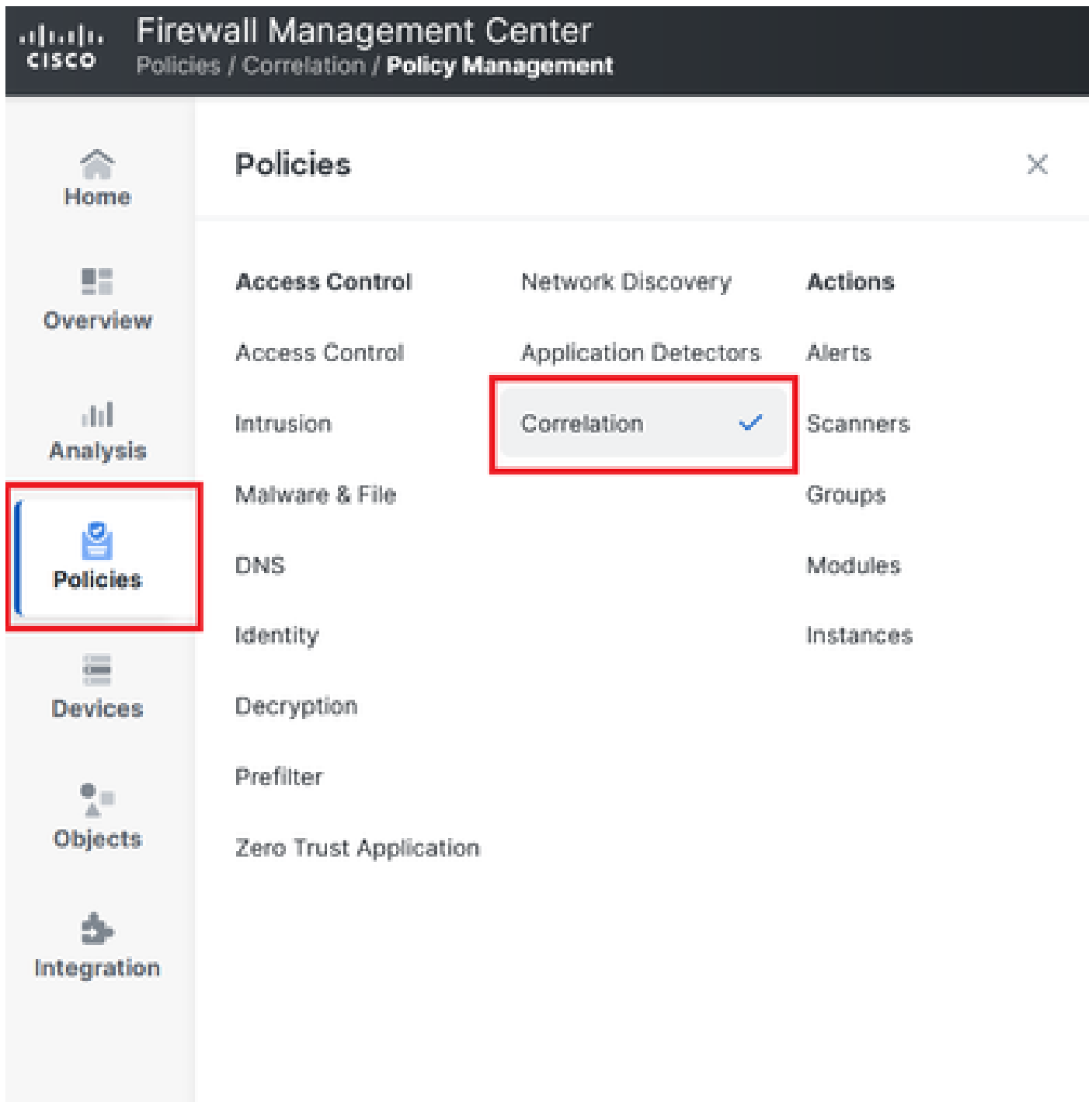


Image 5. Warnung erstellen

Schritt 3: Überprüfen Sie, ob die Warnmeldung aktiviert ist.

Korrelationsrichtlinie konfigurieren

Schritt 1: Navigieren Sie zu Policys > Korrelation.



Navigation zum Menü "Korrelationsrichtlinie"

Image 6. Navigation zum Menü "Korrelationsrichtlinie"

Schritt 2: Erstellen Sie eine neue Korrelationsrichtlinie. Wählen Sie die Standardpriorität aus. Verwenden Sie None, um die Prioritäten der spezifischen Regeln zu verwenden.

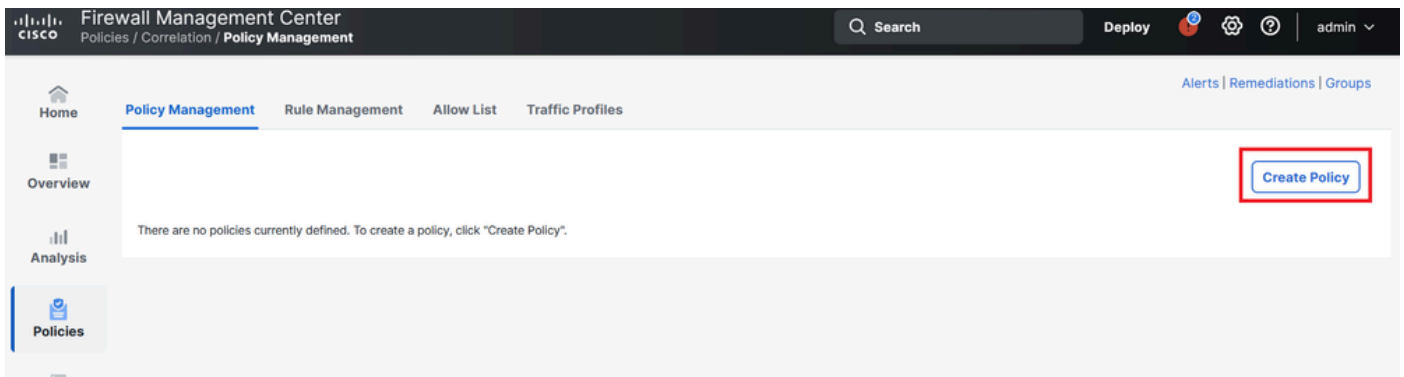


Image 7. Neue Korrelationsrichtlinie erstellen

Schritt 3: Fügen Sie der Richtlinie Regeln hinzu, indem Sie Regeln hinzufügen auswählen.

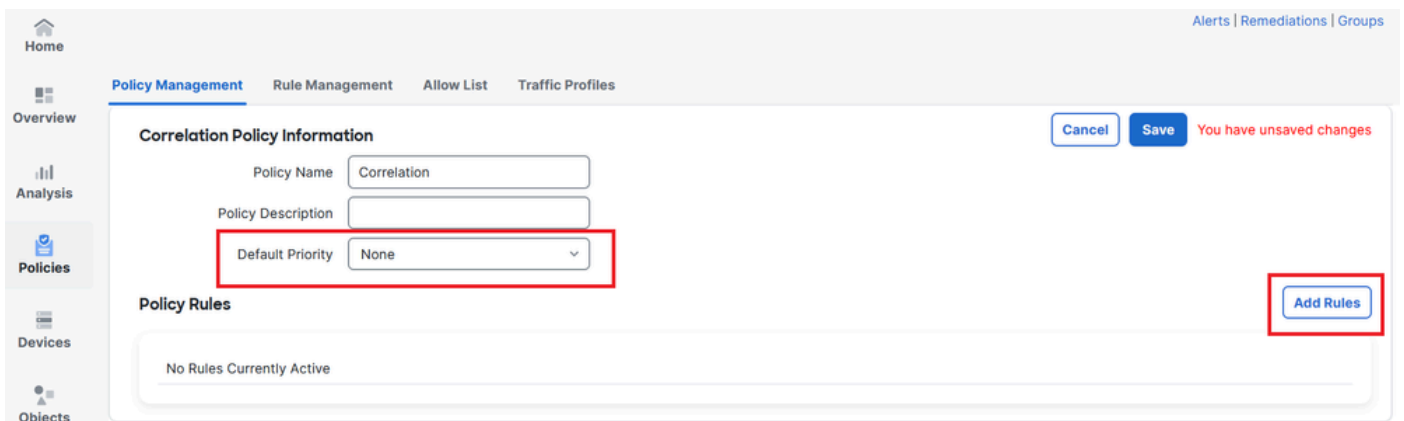


Image 8. Regeln hinzufügen und Priorität für Korrelationsrichtlinie auswählen

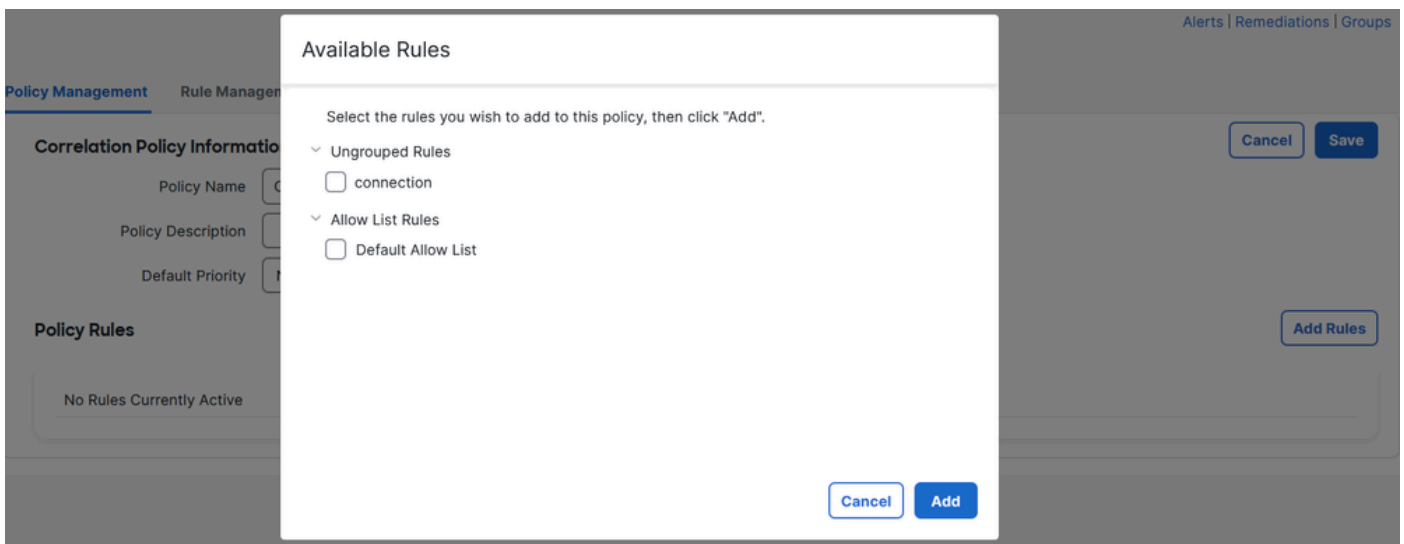


Image 9. Wählen Sie die Regeln aus, die der Korrelationsrichtlinie hinzugefügt werden sollen.

Schritt 4: Weisen Sie der Regel eine Antwort aus den von Ihnen erstellten Warnungen zu, sodass bei jeder Auslösung der ausgewählte Warnentyp gesendet wird.

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"/> + -

Image 10. Schaltfläche Antworten hinzufügen

Responses for connection

Assigned Responses



Unassigned Responses

email
syslog

Cancel

Update

Image 11. Antworten der Korrelationsregel zuweisen

Schritt 5: Speichern und aktivieren Sie Ihre Korrelationsrichtlinie.

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

Image 12. Die Antwort wurde der Korrelationsregel richtig hinzugefügt.

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name Correlation Sort by State

Image 13. Korrelationsrichtlinie aktivieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.