# Korrelationsrichtlinie auf FMC konfigurieren

# Inhalt

inleitung
oraussetzungen
Anforderungen
Verwendete Komponenten
intergrundinformationen
onfigurieren
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.

Home	Policy Management Rule Management Allow List Traffic Profiles	Alerts   Remediations   Groups
Overview		Create Rule Create Group
III Analysis	There are no rules currently defined. To create a rule, click "Create Rule".	

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.

Rule Information	Add Connection Tracker         Add User Qualification         Add Host Profile Qualification
Rule Name	connection
Rule Description	
Rule Group	Ungrouped ~
Select the type of event fo	r this rule
If a connection event occurs	✓ at any point of the connection ✓ and it meets the following conditions:
Add condition	Add complex condition
Application	Protocol  v lis  v HTTPS  v
Ad	d condition Add complex condition
	Source Country v is not v United Kingdom v
Ē	Source Country v is not v United States v

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.

#### Firewall Management Center Policies / Actions / Alerts / Alerts



Image 4. Navigation zum Menü "Warnmeldungen"

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

Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email	Fromes   Alerts   Ke		ioups ( mo	Alerta
Overview								Create	Alert ~
III Analysis	Name					Тур	e In Use	Enabled	
8	email					Emai	Not Used		00
Policies	syslog					Syste	ng Not Used		00
-									

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.

Alerts	Remediations Groups
E Overview	Create Policy
III There are no policies currently defined. To create a policy, click "Create Policy". Analysis	
Policies	

Image 7. Neue Korrelationsrichtlinie erstellen

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

Home		Alerts   Remediations   Groups
	Policy Management Rule Management Allow List Traffic Profiles	
Overview	Correlation Policy Information	Cancel Save You have unsaved changes
⊣II Analysis	Policy Name Correlation	
	Policy Description	
Policies	Default Priority None ~	
	Policy Rules	Add Rules
Devices	No Rules Currently Active	
•=		
Objects		

Image 8. Regeln hinzufügen und Priorität für Korrelationsrichtlinie auswählen

	Available Rules	Alerts   Remediations   Groups
Correlation Policy Name C	Select the rules you wish to add to this policy, then click "Add". ~ Ungrouped Rules _ connection	Cancel
Policy Description	<ul> <li>Allow List Rules</li> <li>Default Allow List</li> </ul>	
Policy Rules No Rules Currently Active		Add Rules
	Cancel	Add

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.

orrelation Policy Inforr	nation	Cancel
Policy Nam	e Correlation	
Policy Description	n	
Default Priorit	y None ~	
olicy Rules		Add
Rule	Responses	Priority
connection	This rule does not have any responses	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 Manag	gement Allow List Traffic Profiles	
Correlation Policy Information	tion	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				Sort by State	~
Correlation					0 0 C

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.