# Correlatiebeleid voor VCC instellen

# Inhoud

nleiding
/oorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Configureren
Correlatieregels instellen
Waarschuwingen configureren
Correlatiebeleid configureren

# Inleiding

Dit document beschrijft de procedure om een Correlatiebeleid te configureren voor het verbinden van gebeurtenissen en het detecteren van anomalieën in uw netwerk.

### Voorwaarden

#### Vereisten

Cisco raadt u aan kennis te hebben van deze producten:

- Secure Firewall Management Center (FMC)
- Secure Firewall Threat Defence (FTD)

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

• Firepower Threat Defence voor VMware versie 7.6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

Correlatiebeleid wordt gebruikt om potentiële beveiligingsbedreigingen op uw netwerk te identificeren door verschillende soorten gebeurtenissen te configureren en wordt gebruikt voor herstel, voorwaardelijke waarschuwingen en verkeersbeleid.

# Configureren

Correlatieregels instellen

Stap 1. Blader naar Beleid > Correlatie en selecteer Regelbeheer.



Afbeelding 1. Navigatie naar het menu van het correlatiebeleid

Stap 2. Maak een nieuwe regel door Regel maken te selecteren.

Home	Policy Management	Rule Management	Allow List	Traffic Profiles		Alerts   Remediations   Groups
Overview						Create Rule Create Group
III Analysis	There are no rules currer	ntly defined. To create a rul	e, click "Create Ru	ıle".		
-						

Afbeelding 2. Regelaanmaak op het menu Regelbeheer

Stap 3. Selecteer een type gebeurtenis en de voorwaarden om aan de regel te voldoen.

Wanneer uw regel meerdere voorwaarden bevat, moet u deze koppelen aan EN of een ORoperator.

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 for	r this rule			
If a connection event occurs	v at any point of the connection v and it meets the followin	ig conditions:		
Add condition	Add complex condition			
Application I	Protocol v is v HTTPS	Ÿ		
Ad	d condition Add complex condition			
	Source Country ~ is not ~ United Kingdor	m v		
	Source Country	~		

Afbeelding 3. Menu Regelaanmaak

Opmerking: Correlatieregels mogen niet generiek zijn, als de regel constant wordt geactiveerd door normaal verkeer, kan dit extra CPU verbruiken en de prestaties van FMC beïnvloeden.

Waarschuwingen configureren

Stap 1. Ga naar Beleid > Acties > Waarschuwingen.

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



Afbeelding 4. Navigatie naar het menu Waarschuwingen

Stap 2. Selecteer Waarschuwing maken en maak een Syslog-, SNMP- of e-mailwaarschuwing.

Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
Overview								Create	Alert ~
III Analysis	Name					Туре	In Use	Enabled	
8	email					Email	Not Used		00
Policies	syslog					Syslog	Not Used		00

Afbeelding 5. Waarschuwing maken

Stap 3. Controleer of de waarschuwing is ingeschakeld.

Correlatiebeleid configureren

Stap 1. Ga naar Beleid > Correlatie.



Navigatie naar het menu van het correlatiebeleid

Afbeelding 6. Navigatie naar het menu van het correlatiebeleid

Stap 2. Creëer een nieuw correlatiebeleid. Selecteer de standaardprioriteit. Gebruik Geen om de prioriteiten van de specifieke regels te gebruiken.

cisco Policie	wall Management Center es / Correlation / Policy Management		Q Search	Deploy	<b>@</b>	0	admin 🗸
Home	Policy Management Rule Management Allow List	Traffic Profiles			Alerts   Re	mediation	ns   Groups
Overview						Create	e Policy
ili] Apalysis	There are no policies currently defined. To create a policy, click "Create	e Policy".					
.e.							
Policies							

#### Afbeelding 7. Nieuw correlatiebeleid maken

Stap 3. Voeg regels toe aan het beleid door Regels toevoegen te selecteren.

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

Afbeelding 8. Regels toevoegen en prioriteit voor correlatiebeleid selecteren

	Available Rules		Alerts   Remediations   Groups
Correlation Policy Informatio Policy Name	Select the rules you wish to add to this policy, then click "Add". ~ Ungrouped Rules _ connection		Cancel
Policy Description	✓ Allow List Rules □ Default Allow List		Add Rules
No Rules Currently Active			
		Cancel Add	

Afbeelding 9. Selecteer Regels om aan het correlatiebeleid toe te voegen

Stap 4. Wijs een reactie op de regel toe uit de waarschuwingen die u hebt aangemaakt, dus wanneer deze wordt geactiveerd, wordt het geselecteerde waarschuwingstype verzonden.

orrelation Policy Infor	mation	Cancel
Policy Nan	Correlation	
Policy Description	nc	
Default Priori	ty None ~	
olicy Rules		Add
Rule	Responses	Priority
connection	This rule does not have any responses.	Default

### Afbeelding 10. Knop Antwoorden toevoegen

Responses for connection
Assigned Responses
َ اللَّهُ اللَّهُ Unassigned Responses
email syslog
Cancel Update

Afbeelding 11. Antwoorden toewijzen aan correlatieregel

Stap 5. Sla uw correlatiebeleid op en schakel dit in.

Policy Management Rule Manag	gement Allow List Traffic Pro	ofiles		
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	~ D Ū

### Afbeelding 12. Correcte toevoeging aan de correlatieregel

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					<b>O</b> ()

Afbeelding 13. Correlatiebeleid inschakelen

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.