# 在FMC上配置关联策略

### 目录

<u>简</u> :	<u>ት</u>
<u>先</u> )	<u> </u>
	要求
	使用的组件
<u>背</u> :	<u>景信息</u>
配	
	<u>配置关联规则</u>
	配置警报
	配置关联策略

## 简介

本文档介绍配置关联策略以连接事件并检测网络上异常的过程。

## 先决条件

#### 要求

思科建议您了解以下产品:

- 安全防火墙管理中心(FMC)
- 安全防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本:

• 适用于VMware的Firepower威胁防御7.6.0版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 背景信息

关联策略通过配置不同类型的事件来识别网络上的潜在安全威胁,并用于补救、条件警报和流量策 略。

## 配置

#### 配置关联规则

步骤1:导航到策略>关联,然后选择规则管理。



图 1.导航至Correlation Policy菜单

第二步:通过选择Create Rule创建新规则。

Home	Policy 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".	

#### 图 2.Rule Management菜单上的规则创建

#### 第三步:选择事件类型和条件以匹配规则。

#### 当规则包含多个条件时,必须使用AND或OR运算符连接这些条件。

Rule Information	Add Connection Tracker         Add User Qualification         Add Host Profile Qualification						
Rule Name	connection						
Rule Description							
Rule Group	Ungrouped v						
Select the type of event for	this rule						
If a connection event occurs	at any point of the connection						
Add condition	Add complex condition						
Application	rotocol  v is  v HTTPS  v						
Add condition Add complex condition							
	Source Country						
	Source Country						

#### 图 3.规则创建菜单

✤ 注意:关联规则不能是通用的,如果规则经常由正常流量触发,这可能会占用额外的CPU并 影响FMC性能。

#### 配置警报

步骤1: 导航到策略>操作>警报。

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





#### 图 4.导航到"警报"菜单

#### 第二步:选择Create Alert,并创建Syslog、SNMP或email alert。

~			Policies   Indusion Rules	Allow List   Hame Fromes   Ale	ats   Kenieu	ations   on	Jups 1 Mo	Alerts
Home	Alerts Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
Overview							Create	Alert ~
III Analysis	Name				Туре	In Use	Enabled	
2	email				Email	Not Used		0 Ū
Policies	syslog				Syslog	Not Used		00

图 5.创建警报

#### 第三步:验证警报是否已启用。

#### 配置关联策略

步骤1:导航到策略>关联。



导航至Correlation Policy菜单

图 6.导航至Correlation Policy菜单

第二步: 创建新的关联策略。选择default priority。使用无以使用特定规则的优先级。

cisco Policie	vall Management Center s / Correlation / Policy Management		Q Search	Deploy 🧳 🛞 🕐 admin 🗸
Home	Policy Management Rule Management Allow List T	raffic Profiles		Alerts   Remediations   Groups
Overview				Create Policy
ili] Apalysis	There are no policies currently defined. To create a policy, click "Create P	olicy".		
Policies				

#### 图 7.创建新的关联策略

第三步: 通过选择Add Rules将规则添加到策略。

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		

#### 图 8.添加规则并选择关联策略的优先级

	Available Rules	Alerts   Remediations   Groups
Policy Management Rule Management Correlation Policy Informatio Policy Name C Policy Description	Select the rules you wish to add to this policy, then click "Add".  Vungrouped Rules  connection  V Allow List Rules	Cancel
Default Priority	Default Allow List	Add Rules
No Rules Currently Active	Cancel	

#### 图 9.选择要添加到关联策略的规则

第四步: 从您创建的风险通告中向规则分配响应,因此只要触发该响应,它就会发送所选的风险通 告类型。

orrelation Policy Informa	tion	Cancel
Policy Name	Correlation	
Policy Description		
Default Priority	None ~	
olicy Rules		A
Rule	Responses	Priority
connection	This rule does not have any responses.	Default

#### 图 10."添加响应"按钮

Responses for connection						
Assigned Responses						
Unassianed Responses						
email syslog						
Cancel Update						

图 11.将响应分配到关联规则

第五步:保存并启用关联策略。

Policy Management Rule Manag	gement Allow List Traffic Profiles	S		
Correlation Policy Information	tion		Cancel Save	You have unsaved changes
Policy Name	Correlation			
Policy Description				
Default Priority	None ~			
Policy Rules				Add Rules
Rule	Resp	ponses	Priority	
connection	emai	il (Email)	Default	~ D Ū

#### 图 12.响应已正确添加到关联规则

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					Ū ()

图 13.启用关联策略

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。