Firepower Management Center: Exibir contadores de ocorrências de políticas do controle de acesso

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Verificar Troubleshoot Informações Relacionadas

Introduction

Prerequisites

Este documento descreve as instruções para criar Fluxos de trabalho personalizados no Firepower Management Center (FMC), permitindo que o sistema exiba os contadores de ocorrências da política de controle de acesso (ACPI) de forma global e por regra. Isso é útil para solucionar problemas, caso o fluxo de tráfego corresponda à regra correta. Também é útil obter informações sobre o uso geral das regras de controle de acesso, por exemplo, as regras de controle de acesso sem ocorrências por um período prolongado podem ser um indicação de que a regra não é mais necessária e pode ser removida com segurança do sistema.

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

- Virtual Firepower Management Center (FMC) versão do software 6.1.0.1 (compilação 53)
- Firepower Threat Defense (FTD) 4150 versão do software 6.1.0.1 (compilação 53)

Note: As informações descritas neste documento não são aplicáveis para o Firepower Device Manager (FDM).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Firepower Management Center (FMC) versão do software 6.0 e posterior
- Dispositivos gerenciados do Firepower versão do software 6.1.x e posterior

Configurar

Passo 1

Para criar um fluxo de trabalho personalizado, navegue por Analysis > Custom > Custom Workflows > Create Custom Workflow (Análise > Personalizar > Fluxos de trabalho personalizados > Criar fluxo de trabalho):

Overvie	w <mark>Anal</mark>	ysis Policies	Devices Obj	ects A	MP			Deploy 🤤	System	Help 🔻	admin 🔻
Context	Explorer	Connections •	Intrusions v	Files v	Hosts •	Users 🔻	Vulnerabilities v	Correlation •	Custom •	Custom	Workflow
									O Crea	ate Custom	Workflow
Custom	Workflow						Table				
Events Summar	by Impact,	Priority, and Host Events to Destination	c Criticality				Intrusion Events with	Destination Criticali	ty	(2 0

Passo 2

Defina o nome do Fluxo de trabalho, por exemplo contadores de ocorrências de regra de ACP e selecione Connection Events (Eventos de conexão) em um campo da tabela. Posteriormente, Salve seu novo fluxo de trabalho.

Overview Anal	ysis Policies	Devices Ob	jects AN	٩P	(Deploy	0	System	Help 🔻	admin 🔻
Context Explorer	Connections •	Intrusions 🔻	Files 🔻	Hosts •	Users •	Vulnerabilit	ties 🔻	Corre	lation 🔻	Custom
			\bigcirc	Add Page	🗿 Add Graph	O Add S	Summa	ary Page	O Add	Table View
		Creat	ng Workflo	w						
		Name	ACP rule	e hit counters]				
		Descrip	ion		·]				
		Table	Connect	tion Events						
				Save	e Cancel)				

Etapa 3

Personalize o fluxo de trabalho recém-criado com o botão Edit/Pencil (Editar/Lápis).

Overview Analysis Policies D	evices Objects AMP	Deploy 🤡	System Help 🔻 admin 🔻
Context Explorer Connections •	Intrusions • Files • Hosts •	Users • Vulnerabilities •	Correlation • Custom
	Success Custom Workflow ACP rule hit count	× ers Saved	Create Custom Workflow
Custom Workflow		Table	
ACP rule hit counters		Connection Events	E <mark>.</mark> 2

Passo 4

Adicione uma nova página para um fluxo de trabalho com a opção Add Page (Adicionar página), defina o nome e classifique os campos da coluna em Access Control Policy (Política de controle de acesso), Access Control Rule (Regra de controle de acesso) e nos campos Count (Contagem), Initiator IP (IP iniciador) e Responder IP (IP de resposta).

Overview	Analysis	Policies	Devices	Objects	AMP			Deploy	😔 Syst	em Help v	admin
Context Expl	orer Con	nections 🔻	Intrusio	ons 🔹 Files	 Hosts 	Users 🔻	Vulnerabilitie	es 🔹 Co	rrelation 🔻	Custom •	Custom
						O Add Page	O Add Graph	n 📀 Add	Summary Pa	ge 📀 Add	Table View
				Editing	Workflow						
				Name	ACP rule h	it counters					
				Descriptio	n						
				Table	Connection	n Events					
						Save	Cancel				
Overview	Analysis P	olicies De	vices Obj	jects AMP				Depl	oy 🥝 Sy	stem Help 🔻	admin 🔻
Context Explo	rer Connec	tions • I	ntrusions 🔻	Files • Ho	osts 🔹 Users	vulnerabili	ties • Correla	ation 🔹 🖸 C	ustom > Cust	om Workflov	vs Look
						O Add	l Page 📀 Add	Graph 📀 /	Add Summary P	age 📀 Add	Table View
Editing W	orkflow										
Name	ACP rule hit cou	unters									
Description											
Table	Connection Eve	nts									
Page 1											×
Page Name	Rule Hits										
Sort Type	Descending \$)									
Column 1		Colu	umn 2		Column 3		Column 4		Colum	ın 5	
Sort Priori	ty Field	Sort	t Priority F	Field	Sort Priority	Field	Sort Priority	Field	Sort P	riority Field	
\$	Access Co	ntrol 🗘 🧲)	Access Control \$	(Count \$)	Initiator IP	•	Res	ponder IP 💲
										Save	Cancel

Etapa 5

Adicione uma segunda página com a opção Add Table View (Adicionar visualização de tabela).

Ana	lysis Policies	Devices Obje	cts Al	٩P			C	Deploy	System	Help 🔻	admin 🔻
plorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Custo	m • Custom	Workflows	Looki
						O Add Page	O Add Graph	O Add S	ummary Page	O Add Ta	ble View

Etapa 6

Table View (Visualização de tabela) não é configurável, portanto, apenas continue com Save para salvar o fluxo de trabalho.

Overview	nalysis Policies	Devices O	bjects AMP				Deploy	System	Help 🔻 admin 🔻
Context Explor	er Connections •	Intrusions 🔻	Files V Ho	sts • Users	 Vulnerabilities 	s Correlation	Custom	Custom W	orkflows Looku
					O Add P	age 🔇 Add Gra	ph 📀 Add Sun	nmary Page	O Add Table View
Editing Wo	orkflow								
Name	ACP rule hit counters								
Description									
Table	Connection Events								
Page 1 Page Name Sort Type	Rule Hits Descending \$								×
Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priorit	y Field	Sort Priority	Field	Sort Priority	Field	Sort Priority Fi	eld	Sort Priority	Field
1\$	Access Control \$	2 \$	Access Control \$	3 \$	Count \$	4 🗘	Initiator IP 💠	5 \$	Responder IP 💲
Page 2 is a Table views a	a Table View re not configurable.								×
									Save Cancel

Etapa 7

Navegue até **Analysis > Connections Events** (Análise > Eventos de conexões) e selecione **Switch Workflow** (Fluxo de trabalho do switch), em seguida, escolha o fluxo de trabalho recém-criado chamado **contadores de ocorrências de regra de ACP e aguarde até a página recarregar.**

Overview Anal	ysis	Policies	Devices	Obje	
Context Explorer	Con	nections 🔻	nections 🔹 Intrusion		
	Eve	nts			
	Sec	urity Intellig	gence Event	s	
Overview Anal	ysis	Policies	Devices	Objects	AMP
Context Explorer	Cor	nections	• Events	Intrusions	s ▼ File
Connection	Eve pplica	ents <u>(swite</u> tion Details	ch workflow) > Table Viev	v of Connection	on Events
Overview Ana	lysis	Policies	Devices	Objects	
Context Explorer	Co	nnections	Events	Intrusions	s▼ File
Connection	Eve	nte «			
Connection	Eve		> Table Viev	w of Connecti	on Events
ACP rule nit counters				or connect	
Connections by Appli	cation				

Depois que a página for carregada, os contadores de ocorrências de regra por cada regra ACP são exibidos, apenas atualize essa exibição sempre que quiser obter os contadores de ocorrências recentes da regra de controle de acesso.

Overview Analysis Policies Devices	Objects AMP			Deploy 🤣 Sys	tem Help v admin v
Context Explorer Connections > Events	Intrusions • Files • Hosts •	Users • Vulnera	abilities • Correlation •	Custom • Looku	p 🔻 Search
			Bookmark This Page Report	rt Designer Dashboard V	iew Bookmarks Search 🔻
ACP rule hit counters (switch workflo Rule Hits > Table View of Connection Events No Search Constraints (Edit Search) Jump to	<u>w)</u>			1 <u>2017-03-30 15:58:2</u>	<u>2 - 2017-03-30 17:00:12</u> (Expanding
★ <u>Access Control Policy</u>	Access Control Rule	Count	Initiator IP	Respo	nder IP
I allow-all	log all	1	<u>10.10.10.122</u>	<u>192</u>	.168.0.14
<pre>I< < Page 1 of 1 >> Displaying row 1 of 1 rows</pre>	5				
View Delete					

Verificar

Uma forma de confirmar os contadores de ocorrências de regras de controle de acesso com base na regra para todo o tráfego (globalmente) pode ser obtida com o comando CLISH FTD (CLI SHELL) show access-control-config demonstrado abaixo:

> show access-control-config

```
Source Networks : 10.10.10.0/24
Destination Networks : 192.168.0.0/24
URLs
Logging Configuration
DC : Enabled
Beginning : Enabled
End : Enabled
Files : Disabled
Rule Hits : 3
Variable Set : Default-Set
```

... (output omitted)

Troubleshoot

> system support firewall-engine-debug

Please specify an IP protocol: **icmp** Please specify a client IP address: 10.10.10.122 Please specify a server IP address: 192.168.0.14 Monitoring firewall engine debug messages

10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 New session 10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, sgt tag: untagged, svc 3501, payload 0, client 2000003501, misc 0, user 9999997, icmpType 8, icmpCode 0 10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 no match rule order 1, id 2017150 dst network and GEO 10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 match rule order 3, 'log all', action Allow 10.10.10.122-8 > 192.168.0.14-0 1 AS 2 I 0 allow action

Ao comparar os contadores de ocorrências para a regra de ACP chamado **log all você observa que as saídas de linha de comando (CLI) e da interface de usuário não coincidem.** O motivo é que os contadores de ocorrências da CLI são removidos após cada implantação da Política de controle de acesso e se aplicam a todo o tráfego globalmente e não a endereços IP específicos. Por outro lado, a interface de usuário do FMC mantém os contadores no banco de dados, para que possa exibir os dados históricos com base em um período determinado.

Informações Relacionadas

- Fluxo de trabalho personalizados
- Introdução às políticas de controle de acesso
- Suporte Técnico e Documentação Cisco Systems