Firepower Management Center:アクセスコン トロール ポリシー ヒット カウンタの表示

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>設定</u> <u>確認</u> トラブルシュート</u> 関連情報



前提条件

ACP Firepower Management CenterFMC

要件

このドキュメントに特有の要件はありません。

- Firepower Management CenterFMC- 6.1.0.1 53
- Firepower Threat DefenseFTD4150 6.1.0.1 53

注:このドキュメントで説明する情報は、Firepower Device Manager(FDM)には当ては まりません。

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

• Firepower - 6.1.x

[•] Firepower Management CenterFMC- 6.0.x

1

カスタム ワークフローを作成するには、[分析(Analysis)] > **[カスタム(Custom)] > [カスタム** ワークフロー(Custom Workflows)] > **[カスタムワークフローの作成(Create Custom** Workflow)] の順に移動します。

Overview	Analysis Policies	Devices Obj	ects A	мр			Deploy	System	Help 🔻	admin 🔻
Context Explo	orer Connections	Intrusions •	Files 🔻	Hosts 🔻	Users •	Vulnerabilities •	Correlation •	Custom >	Custom	Workflow
								Crea	te Custom	Workflow
Custom Wor	rkflow					Table				
Events by In Summary of	mpact, Priority, and Ho Critical Events to Destina	st Criticality				Intrusion Events with	Destination Critica	lity	6	20

2

ACP rule hit counters[Table] [Connection Events] [Save]

Overview 🖊	Analysis	Policies	Devices	Objects	AMP		Deploy) 📀	System	Help 🔻	admin 🔻
Context Explor	rer Con	nections 🔻	Intrusio	ns 🔻 Files	s 🔹 Hosts 🔻	Users 🔻	Vulnerabil	ities 🔻	Corre	ation 🔻	Custom
					O Add Page	O Add Gra	ph 📀 Add	Summa	ary Page	O Add	Table View
			Cr	eating Wo	rkflow						
			Na	me Ad	CP rule hit counter	s					
			De	scription							
			Tab	ble Co	nnection Events						
					Sa	ave Canc	el				

3

<u>/</u>				
Overview Analysis Policies D	evices Objects AMP	Deploy 🤗 🤮	System Help 🔻	admin 🔻
Context Explorer Connections •	Intrusions ▼ Files ▼ Hosts ▼ Users ▼	Vulnerabilities •	Correlation •	Custom
			O Create Custom	Workflow
	Success Custom Workflow ACP rule hit counters Saved	×		
Custom Workflow	Table			_
ACP rule hit counters	Connection E	vents	6	è 🖉 🖯

4

[Add Page] [Access Control Policy] [Access Control Rule] [Count][IPInitiator IP][IPResponder IP]

Overview	Analysis	Policies	Devices	Objects	AMP			Deploy	🛛 🕹 Sys	tem Help 🖥	admin
Context Expl	orer Conn	ections 🔻	Intrusi	ons 🔻 🛛 Files	 Hosts 	Users 🔻	Vulnerabilitie	es 🔹 Co	rrelation 🔻	Custom	Custom
						Add Page	O Add Graph	h 🔇 Add	Summary Pa	age 📀 Ado	Table View
				Editing Name	Workflow ACP rule h	nit counters					
				Table	Connection	n Events					
						Save	Cancel				
Overview	Analysis Po	licies De	vices Ob	jects AMP				Depl	loy 🥝 Sy	ystem Help v	√ admin v
Context Explo	rer Connect	ions 🔹 🛛 Ir	ntrusions 🔻	Files • He	osts 🔹 Users	vulnerabili	ties • Correla	ation 🔻 🛛 🕻	ustom > Cus	tom Workflo	ws Look
						O Ado	d Page 🚫 Add	Graph	Add Summary	Page 📀 Add	Table View
Editing W	orkflow										
Name	ACP rule hit cour	nters									
Description											
Table	Connection Even	ts									
Page 1											×
Page Name	Rule Hits										
Sort Type	Descending \$										
Column 1		Colu	ımn 2		Column 3		Column 4		Colu	mn 5	
Sort Priori	ty Field	Sort	Priority F	Field	Sort Priority	Field	Sort Priority	Field	Sort	Priority Field	
(\$)	Access Con	trol 🗘 🤇 🗘		Access Control \$	(Count \$) (\$	Initiator I		Res	ponder IP 💠
										Save	Cancel

手順 5

[Add Table View] 2

Anal	Analysis Policies Devices Objects AMP								System	n 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

6

[Table View] [Save]

Overview 🖊	nalysis Policies	Devices Of	ojects AMP				Deploy 🤇	System	Help 🔻	admin 🔻
Context Explor	er Connections •	Intrusions •	Files • H	osts 🔹 Users	 Vulnerabilities 	Correlation	Custom	Custom W	orkflows/	Looku
					O Add P	age 📀 Add Grapt	Add Sum	imary Page	O Add Ta	ble View
Editing W	orkflow									
Name	ACP rule hit counters									
Description										
Table	Connection Events									
Page 1										×
Page Name	Rule Hits									
Sort Type	Descending \$									
Column 1		Column 2		Column 3		Column 4		Column 5		
Sort Priorit	y Field	Sort Priority	Field	Sort Priority	Field	Sort Priority Fiel	d	Sort Priorit	y Field	
1 🛊	Access Control \$	2 \$	Access Control \$	3 \$	Count 🗘	4 \$	itiator IP 🛟	5 \$	Respor	nder IP 🛊
Page 2 is Table views a	a Table View re not configurable.									×
									Save	Cancel

7

[Analysis] > [Connections] > [Events] [switch workflow] [ACPACP rule hit counters]

Overview Anal	ysis	Policies	Devices	Obje	
Context Explorer	Con	nections 🔻	Intrusion	ns 🔻	
	Ever	nts			
	Secu	urity Intellig	ence Event	s	
Overview Anal	lysis	Policies	Devices	Objects	AMP
Context Explorer	Con	nections	Events	Intrusion	s ▼ File
Connection	Eve	nts (switc tion Details	h workflow) > <u>Table Viev</u>	v of Connecti	on Events
Overview Ana	lysis	Policies	Devices	Objects	
Context Explorer	Cor	nections	• Events	Intrusion	s ▼ File
Connection	Eve	nts ×			
ACP rule hit counters		5	> Table Viev	w of Connecti	on Events
Connection Events					
Connections by Appli	cation				

Overview Analysis Policies Devices	Objects AMP				Deploy	System	Help 🔻	admin 1
Context Explorer Connections > Events	Intrusions • Files •	Hosts • Users •	Vulnerabilities •	Correlation •	Custom •	Lookup 🔻	Search	
			Bookmar	k This Page Report	Designer Dash	board View B	ookmarks	Search 🔻
ACP rule hit counters (switch workf Rule Hits > Table View of Connection Events No Search Constraints (Edit Search)	low)				2017-03-30 <u>2017</u> -03-30	0 15:58:22 - 20	0 <u>17-03-30 1</u> E:	. <u>7:00:12</u> xpanding
Jump to 🔻								
Access Control Policy	Access Control	l Rule	Count	Initiator IP		Responder	IP	
I allow-all	log all		1	10.10.10.122		<u>192.168.</u>	0.14	
$ \langle$ < Page 1 of 1 \rangle > Displaying row 1 of 1 ro	ws							
View Delete Delete All								

確認

全トラフィックのアクセス コントロール ルール ヒット カウンタをルール ベースで(グローバルに)確認するには、FTD CLISH(CLI SHELL)の **show** access-control-config コマンドを使用します。その例を以下に示します。

> show access-control-config

```
==========[ allow-all ]=============
Description :
Default Action : Allow
Default Policy : Balanced Security and Connectivity
Logging Configuration
DC : Disabled
Beginning : Disabled
End : Disabled
Rule Hits : 0
Variable Set : Default-Set
...(output omitted)
-----[ Rule: log all ]-----
Action : Allow
Intrusion Policy : Balanced Security and Connectivity
ISE Metadata :
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)
```

トラブルシュート

firewall-engine-debug コマンドを使用すると、トラフィック フローが適切なアクセス コントロール ルールに照らし合わせて評価されているかどうかを確認 することができます。

> 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
Iog all ACP CLIGUICLI IP FMC GUI

関連情報

- カスタム ワークフロー
- アクセスコントロールポリシー入門
- <u>テクニカル サポートとドキュメント Cisco Systems</u>