Firepower管理中心:顯示訪問控制策略命中計數 器

目錄

<u>簡介</u> <u>必要條件</u> <u>要求用元件</u> <u>設 驗 難 開</u> 麗 調資訊

簡介



Firepower(FMC)(ACP)(

需求

本文件沒有特定需求。

- Firepower(FMC) 6.1.0.153
- Firepower(FTD)4150 6.1.0.153

附註:本文檔中描述的資訊不適用於Firepower裝置管理器(FDM)。

本文件也適用於以下硬體和軟體版本:

- Firepower(FMC) 6.0.x
- Firepower 6.1.x

1

要建立自定義工作流程,請導航到**分析>自定義>自定義工作流程>建立自定義工作流程:**

Overview Anal	ysis Policies	Devices Obj	ects A	MP			Deploy	System	Help 🔻	admin 🔻
Context Explorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities v	Correlation •	Custom +	Custom	Workflow
Create Custom V									Workflow	
Custom Workflow						Table				
Events by Impact, Summary of Critical	Priority, and Host Events to Destination	Intrusion Events with	Destination Critical	lity		200				

2

Custom WorkflowACPConnection Events												
Overview Anal	ysis Policies	Devices Ob	jects A	мр		Deploy	📀 S	ystem	Help 🔻	admin 🔻		
Context Explorer	Connections •	Intrusions v	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilit	ies 🔻	Correla	ation 🔻	Custom		
			C	Add Page	O Add Graph	🗿 Add S	Summary	Page	O Add T	Table View		
		Creati	ng Workf	ow								
		Name	ACP ru	le hit counters	5							
		Descript	ion									
		Table	Connec	tion Events								
				Sa	Cancel							

3

/					
Overview Analysis Policies D	evices Objects AMP	Deple	oy 🛛 📀	System Help 🔻	admin 🔻
Context Explorer Connections •	Intrusions • Files • Hosts •	Users • Vulner	abilities 🔻	Correlation v	Custom
				O Create Custom	Workflow
	Success Custom Workflow ACP rule hit count	x ers Saved			
Custom Workflow		Table			
ACP rule hit counters		Connection Events		(a <mark>0</mark> 0

4

CountInitiator IPResponder IP

Overview Anal	lysis Policies	Devices	Objects /	AMP			Deplo	y 😔	System	Help 🔻	admin
Context Explorer	Connections •	Intrusion	ns ▼ Files ▼	Hosts •	Users •	Vulnerabilitie	es 🔻	Correlatio	on v C	ustom 🕨	Custom
				(Add Page	O Add Graph	h) 📀 A	Add Summa	ary Page	O Add	Table View
			Editing W	/orkflow							
			Name	ACP rule hit	counters						
			Description								
			Table	Connection E	vents						
					Save	Cancel					

Overview /	Analysis	Policies	Devices	Objects	AMP				Deploy	🛛 😔 System	Help 🔻	admin 🔻
Context Explor	rer Con	nections 🔻	Intrusion	s 🔻 Files 🕯	 Hosts 	Users 🔻	Vulnerabilitie	es 🔻 Correla	tion • Custo	om > Custom \	Norkflows	Look
							🔕 Add F	Page 🔇 Add C	Graph 📀 Add S	Summary Page	🔇 Add Ta	able View
Editing Wo	orkflow											
Name	ACP rule hit	t counters										
Description												
Table	Connection	Events										
Page 1 Page Name Sort Type	Rule Hits Descendir	ng 🗘										×
Column 1			Column 2		Colu	mn 3		Column 4		Column 5		
Sort Priorit	y Field		Sort Priority	/ Field	Sort	Priority F	Field	Sort Priority	Field	Sort Priorit	y Field	
\$	Acces	s Control 🗘	\$	Access Co	ontrol 🗘 🛛 🗘) (Count \$	\$	Initiator IP	•	Respo	nder IP 🛟
											Save	Cancel

步驟5

Anal	ysis Policies	Devices Obje	ects AN	٩P				Deploy 🤤	System	Help 🔻	admin 🔻
plorer	Connections •	Intrusions •	Files v	Hosts 🔻	Users •	Vulnerabilities •	Correlation •	Custom	Custom	Workflows	Looki
						O Add Page	3 Add Graph	O Add Sum	mary Page	Add Ta	ble View

6

Table ViewSave

Overview A	nalysis Policies	Devices O	bjects AMP				Deploy	System	Help 🔻 admin 🔻
Context Explore	er Connections •	Intrusions •	Files V Ho	sts • Users •	Vulnerabilities	S ▼ Correlation	n • Custom	► Custom W	orkflows Looku
					💿 Add P	age 🚺 🔕 Add Gra	aph 📀 Add Su	mmary Page	O Add Table View
Editing Wo	orkflow								
Name	ACP rule hit counters								
Description									
Table	Connection Events								
Page 1									×
Page Name	Dula Hita								
Sort Type									
Column 1		Column 2		Column 3		Column 4		Column 5	
Sort Priorit	y Field	Sort Priority	Field	Sort Priority	Field	Sort Priority F	ield	Sort Priority	Field
1\$	Access Control \$	2 \$	Access Control \$	3 \$	Count \$	4 🗘	Initiator IP 🛟	5 \$	Responder IP
Page 2 is a	a Table View								×
Table views ar	re not configurable.								
									Save

7



Overview Anal	ysis Policies	Devices	Obje	
Context Explorer	Connections •	Intrusion	ns 🔻	
	Events			
	Security Intellig	gence Event	s	
Overview Ana	lysis Policies	Devices	Objects	AMP
Context Explorer	Connections	Events	Intrusions	s ▼ File
Connections with A Overview Ana	pplication Details	> <u>Table Viev</u> Devices	of Connection	AMP
Overview Ana	lysis Policies	Devices	Objects	AMP
Context Explorer	Connections	Events	Intrusions	s▼ File
Connection ACP rule hit counters Connection Events Connections by Appli	Events ×	> <u>Table Viev</u>	v of Connectio	on Events
АСРАС				
Overview Analysis Policies Device Context Explorer Connections > Event	ces Objects AMP ts Intrusions • Files • Hos	sts 🔻 Users 🕶 Vulne	erabilities Correlation	Deploy Solution The Custom The Cu
ACP rule hit counters (switch v Rule Hits > Table View of Connection Events No Search Constraints (Edit Search)	<u>vorkflow)</u>		Bookmark This Page R	teport Designer Dashbo

	★ Access Control Policy	Access Control Rule	Count	Initiator IP	Responder IP					
1	allow-all	lle pol	1	<u>10.10.10.122</u>	192.168.0.14					
K Page 1 of 1) Displaying row 1 of 1 rows										
View	Delete									
View A	All Delete All									



通過FTD CLISH(CLI SHELL)**show access-control-config**命令,可以獲得根據規則(全域性)確認所有流量的訪問控制規則命中計數器的方法,如下所示:

> show access-control-config

Default Policy : Balanced Security and Connectivity Logging Configuration DC : Disabled Beginning : Disabled End : Disabled Rule Hits : O 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)



使用firewall-engine-debug命令,可以確認是否根據正確的訪問控制規則評估流量:

> 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
```

logACP(CLI)GUICLIIPFMC GUI

相關資訊

- 自定義工作流程
- 訪問控制策略入門
- 技術支援與文件 Cisco Systems