Firepower 管理中心:显示访问控制策略点击计数 器

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用置</u> <u>验障排除</u> 相关信息

简介

先决条件

Firepower (FMC) Firepower (FMC) (ACP)

要求

本文档没有任何特定的要求。

- Firepower (FMC) 6.1.0.1 53
- Firepower (FTD) 4150 6.1.0.1 53

注意:本文档中所述信息不适用于 Firepower 设备管理器 (FDM)。

本文档也可用于以下硬件和软件版本:

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

1

要创建自定义工作流程,请依次导航至**分析 > 自定义 > 自定义工作流程 > 创建自定义工作流程:**

0	verview Anal	ysis Policies	Devices Obj	ects A	MP			Deploy	System	Help 🔻	admin 🔻
Co	ntext Explorer	Connections •	Intrusions 🔻	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities v	Correlation •	Custom •	Custom	Workflow
Create Custom W									Workflow		
c	ustom Workflow						Table				
Events by Impact, Priority, and Host Criticality Intrusion Events with Destination Summary of Critical Events to Destination Criticality Intrusion Events with Destination								Destination Critical	lity	C	200

2	
	~

AUF											
Overview An	alysis Policies	Devices	Objects	AM	IP		Deploy) 📀	System	Help 🔻	admin 🔻
Context Explorer	Connections •	Intrusio	ns 🔻 🛛 File	s 🕶	Hosts 🔻	Users 🔻	Vulnerabi	lities 🔻	Corre	lation 🔻	Custom
					Add Page	O Add Grap	oh 🔇 Add	Summa	ary Page	O Add	Table View
		Cr	eating Wo	orkflo	w						
		Na	me 🧧	CP rule	hit counters	5					
		De	scription								
		Tab	ble C	onnectio	on Events						
					Sa	ve Cance	21				

3

<u>/</u>					
Overview Analysis Policies D	Devices 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	× ters Saved			
Custom Workflow		Table			
ACP rule hit counters		Connection Events		(a <mark>0</mark> 0

4

IP IP											
Overview Anal	ysis Policies	Devices Ob	jects	AMP			Dep	oloy 😔	System	Help 🔻	admin
Context Explorer	Connections •	Intrusions v	Files	 Hosts 	Users 🔻	Vulnerabil	ities 🔻	Correlat	ion 🔹 🔇	Sustom •	Custom
				ĺ	📀 Add Page	O Add Gr	aph 📀	Add Sum	mary Page	🔕 Add	Table View
			Editing	Workflow							
			Name	ACP rule hit	counters						
			Descriptior	1							
			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

步骤 5

Anal	ysis Policies	Devices Obje	ects AN	1P				Deploy	System	Help 🔻	admin 🔻
plorer	Connections •	Intrusions •	Files v	Hosts 🔻	Users 🔻	Vulnerabilities v	Correlation •	Custom	Custom	Workflows	Looki
						O Add Page	O Add Graph	O Add Sum	imary Page	O Add Tal	ble View

6

Overview A	nalysis Policies	Devices O	bjects AMP				Deploy	🛛 System	Help 🔻 admin 🔻
Context Explore	er Connections •	Intrusions •	Files V Ho	sts 🔹 Users	 Vulnerabilities 	s • Correlat	ion • Custom	► Custom W	orkflows Looku
					🔕 Add P	Page 📀 Add G	Graph 📀 Add Su	mmary Page	O Add Table View
Editing Wo	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 Priority	y Field	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	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									

> ACP

Overview Ar	nalysis Policies	Devices	Obje	
Context Explore	Connections •	Intrusion	ns 🔻	
	Events			
	Security Intel	ligence Event	s	
Overview	Palicia Palicia	Dovicos	Objects	
Overview A	nalysis Policies	5 Devices	Objects	АМР
Context Explore	r Connections	Events	Intrusions	File
Connections wit	h Application Detail	s Devices	v of Connection Objects	Events
Context Explore	Connections	Evente	Intrusions	Eile
	connections	- Li ciita	110 0310113	- The
Connectio	on Events ×			
ACP rule hit count	ters	s > Table View	w of Connection	Events
Connection Eve	nts			
Connections by A	pplication			
ACP AC				
Overview Analysis Policies Context Explorer Connections	Devices Objects AMP Events Intrusions • Files • H	Hosts 🔹 Users 💌 Vuln	erabilities Correlation	Deploy 🗸
			Bookmark This Page Report	rt Designer Dashboa
Rule Hits > Table View of Connection Ev	<u>switch workflow)</u> <u>rents</u>			2017-03-30 15
No Search Constraints (Edit Search)				

	Jump to 🔻	to 🔻										
	★ Access Control Policy	Access Control Rule	Count	Initiator IP	Responder IP							
	I allow-all	lls 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											
ſ	View All Delete All											

验证

通过 FTD CLISH (CLI SHELL) show access-control-config 命令,可以根据规则确认所有流量(全局)的访问控制规则点击计数器,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,您可以确认是否根据正确的访问控制规则评估流量:

> 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
```

log all ACP (CLI) GUI CLI IP FMC GUI

相关信息

- 自定义工作流程
- 访问控制策略使用入门
- 技术支持和文档 Cisco Systems