# Centro gestione Firepower: Visualizza contatori visite criteri di controllo di accesso

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Verifica Risoluzione dei problemi Informazioni correlate

## Introduzione

# Prerequisiti

In questo documento vengono descritte le istruzioni per creare **flussi di lavoro personalizzati** in un centro di gestione di Firepower (FMC) che consente al sistema di visualizzare i contatori di accesso ai criteri di controllo di accesso (ACP) in base a regole e a livello globale. Questa opzione consente di risolvere i problemi relativi alla corrispondenza del flusso di traffico con la regola corretta. È inoltre utile ottenere informazioni sull'utilizzo generale delle regole di controllo di accesso, ad esempio le regole di controllo di accesso senza accessi per un periodo di tempo prolungato potrebbero essere indica che la regola non è più necessaria e potrebbe essere potenzialmente rimossa dal sistema in modo sicuro.

## Requisiti

Nessun requisito specifico previsto per questo documento.

#### Componenti usati

- Virtual Firepower Management Center (FMC) versione software 6.1.0.1 (build 53)
- Firepower Threat Defense (FTD) 4150 versione software 6.1.0.1 (Build 53)

**Nota:** Le informazioni descritte in questo documento non sono applicabili a Firepower Device Manager (FDM).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Firepower Management Center (FMC) software versione 6.0.x e successive
- Appliance gestite con Firepower versione software 6.1.x e superiore

# Configurazione

#### Passaggio 1

Per creare un flusso di lavoro personalizzato, selezionare **Analisi > Personalizzato > Flussi di lavoro personalizzati > Crea flusso di lavoro personalizzato:** 

Overview Anal	lysis Policies	Devices Obje	ects   A	МР			Deploy	System	Help 🔻	admin 🔻
Context Explorer	Connections •	Intrusions 🔻	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities <b>v</b>	Correlation •	Custom •	Custom	Workflow
								Crea	ate Custom	Workflow
Custom Workflow						Table				
Events by Impact, Summary of Critical	Priority, and Host	Criticality				Intrusion Events with	Destination Critical	ity	(	2

#### Passaggio 2

Definire il nome del **flusso di lavoro personalizzato**, ad esempio **i contatori visite regola ACP** e selezionare **Eventi connessione** in un campo tabella. In seguito, **salvare** il nuovo workflow.

Overview An	alysis	Policies	Devices	Objects	A	MP		Deploy	) 📀	System	Help 🔻	admin 🔻
Context Explorer	Con	nections 🔻	Intrusio	ns 🔻 🛛 File	es 🔻	Hosts 🔻	Users 🔻	Vulnerabil	ities 🔻	Corre	lation 🔻	Custom
						Add Page	O Add Grap	h 📀 Add	Summ	ary Page	O Add	Table View
			Cr	eating W	orkfl	low						
			Na	me 🛃	CP ru	le hit counters	s					
			De	scription								
			Tal	ble C	onneo	ction Events						
						Sa	ve Cance	I				

#### Passaggio 3

Personalizzare il workflow appena creato utilizzando il pulsante Modifica/Matita.

Overview Analysis Policies De	evices Objects AMP	Deploy	) 📀 🤋	System Help 🔻	admin 🔫
Context Explorer Connections •	Intrusions • Files • Hosts •	Users • Vulnerab	ilities 🔻	Correlation •	Custom
	Success Custom Workflow ACP rule hit count	ers Saved		Create Custon	n Workflow
Custom Workflow		Table			
ACP rule hit counters		Connection Events			2 C

#### Passaggio 4

Aggiungere una nuova pagina per un flusso di lavoro utilizzando l'opzione Aggiungi pagina, definirne il nome e ordinare i campi della colonna in base a Criteri di controllo di accesso, Regola di controllo di accesso e in base ai campi **Conteggio**, **IP iniziatore** e **IP risponditore**.

Overview	Analysis	Policies	Devices	Objects	AMP			Deploy	🔗 Sys	tem Help 🖥	admin
Context Expl	orer Conn	ections 🔻	Intrusi	ons 🔻 🛛 Files	<ul> <li>Hosts</li> </ul>	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 <del>v</del>
Context Explo	rer Connect	ions 🔹 🛛 Ir	ntrusions 🔻	Files • He	osts 🔹 Users	vulnerabili	ties • Correla	ation 🔻 🛛 🕻	ustom <b>&gt;</b> 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 \$	<b>(</b>	Count \$	) ( \$	Initiator I		Res	ponder IP 💠
										Save	Cancel

### Passaggio 5

Aggiungere una seconda pagina con l'opzione Aggiungi vista tabella.

Ana	ysis Policies	Devices Obje	ects AN	MP			C	Deploy	Systen 📀	n Help 🔻	admin 🔻
plorer	Connections •	Intrusions 🔻	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Custo	m <b>&gt;</b> Custom	Workflows	Looki
						O Add Page	O Add Graph	O Add S	ummary Page	Add Ta	able View

#### Passaggio 6

La vista tabella non è configurabile, quindi è sufficiente procedere al salvataggio del flusso di lavoro.

Overview	Analysis Policies	Devices O	bjects AM	Ρ			Deploy	System	Help 🔻 admin	• •
Context Explor	er Connections •	Intrusions	Files •	Hosts • Users	s ▼ Vulnerabilitie	s     Correlation	Custom	Custom W	orkflows Lo	oku
					O Add F	Page 📀 Add Graph	h 🕜 Add Sum	mary Page	Add Table View	w
Editing W	orkflow									
Name	ACP rule hit counters									
Description										
Table	Connection Events									
Page 1	Rule Hits									×
Sort Type	Descending \$									
Column 1		Column 2		Column 3		Column 4		Column 5		
Sort Priori	ty Field	Sort Priority	Field	Sort Priority	Field	Sort Priority Fie	Id	Sort Priority	Field	
1 🛊	Access Control 🖨	2 \$	Access Contro	3 \$	Count 🗘	4 <b>\$</b>	nitiator IP 🛟	5 \$	Responder IP	\$
Page 2 is Table views a	a Table View re not configurable.									×
									Save	cel

#### Passaggio 7

Passare a **Analisi > Eventi di connessione** e selezionare **Cambia flusso di lavoro**, quindi scegliere il nuovo flusso di lavoro creato denominato **Contatori visite regola ACP** e attendere il ricaricamento della pagina.



Una volta caricata la pagina, vengono visualizzati i contatori delle visite alle regole per ogni regola ACP. È sufficiente

aggiornare questa visualizzazione ogni volta che si desidera ottenere i contatori delle visite alle regole CA recenti.

Overview Analysis Policies Device	es Objects A	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 Bo	ookmarks	Search 🔻
ACP rule hit counters (switch wo Rule Hits > Table View of Connection Events No Search Constraints (Edit Search) Jump to	rkflow)						<u>2017-03-30</u>	0 15:58:22 - 20	0 <u>17-03-30</u> E	17:00:12 xpanding
Access Control Policy	Acc	cess Control F	Rule		Count	Initiator IP		Responder	IP	
I allow-all	log a	all			1	<u>10.10.10.122</u>		<u>192.168.</u>	0.14	
Image 1     of 1     Image 2       Image 1     of 1     Image 2	rows									
View Delete All										

## Verifica

Il comando show access-control-config di FTD CLISH (CLI SHELL), illustrato di seguito, consente di confermare i contatori di accesso alle regole in base alle regole per tutto il traffico (a livello globale):

#### > show access-control-config

```
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)

## Risoluzione dei problemi

Il comando firewall-engine-debug consente di confermare se il flusso di traffico viene valutato in base alla regola di controllo dell'accesso appropriata:

#### > 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

Quando si confrontano i contatori delle corrispondenze per la regola del provider di servizi di audioconferenza denominata **log, si** nota che gli output della riga di comando (CLI) e dell'interfaccia utente non corrispondono. Il motivo è che i contatori di accesso CLI vengono cancellati dopo ogni distribuzione dei criteri di controllo dell'accesso e si applicano a tutto il traffico a livello globale e non a uno specifico indirizzo IP. L'interfaccia utente di FMC mantiene invece i contatori nel database, in modo da poter visualizzare i dati cronologici in base a un intervallo di tempo selezionato.

## Informazioni correlate

- Workflow personalizzati
- Introduzione ai criteri di controllo di accesso
- Documentazione e supporto tecnico Cisco Systems