# Configura regole personalizzate di snort locale in Snort2 su FTD

# Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Esempio di rete
Configurazione
Passaggio 1. Conferma versione snort
Passaggio 2. Creare una regola personalizzata per l'orientamento locale nell'angolo 2
Passaggio 3. Conferma regola snort locale personalizzata
Passaggio 4. Azione regola di modifica
Passaggio 5. Associa criterio di intrusione alla regola dei criteri di controllo di accesso (ACP)
Passaggio 6. Distribuisci modifiche
Verifica
Regola snort locale personalizzata non attivata
Passaggio 1. Imposta contenuto del file nel server HTTP
Passaggio 2. Richiesta HTTP iniziale
Regola snort locale personalizzata attivata
Passaggio 1. Imposta contenuto del file nel server HTTP
Passaggio 2. Richiesta HTTP iniziale
Passaggio 3. ConfirmIntrusion, evento
Risoluzione dei problemi

# Introduzione

In questo documento viene descritta la procedura per configurare le regole di snort locali personalizzate in Snort2 on Firewall Threat Defense (FTD).

# Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD)

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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.

# Premesse

Custom Local Snort Rule si riferisce a una regola definita dall'utente che è possibile creare e implementare all'interno del sistema di rilevamento e prevenzione delle intrusioni Snort integrato nel FTD. Quando si crea una regola Snort locale personalizzata in Cisco FTD, si definisce essenzialmente un nuovo pattern o set di condizioni che il motore Snort è in grado di osservare. Se il traffico di rete soddisfa le condizioni specificate nella regola personalizzata, Snort può eseguire l'azione definita nella regola, ad esempio generare un avviso o eliminare il pacchetto. Gli amministratori utilizzano regole di tipo Snort locali personalizzate per gestire minacce specifiche non coperte dai set di regole generali.

In questo documento viene illustrato come configurare e verificare una regola di snort locale personalizzata progettata per rilevare ed eliminare pacchetti di risposta HTTP contenenti una stringa specifica (nome utente).



Attenzione: la creazione di regole personalizzate per lo snort locale e il relativo supporto esulano dalla copertura del supporto TAC. Pertanto, questo documento può essere utilizzato solo come riferimento e richiede la creazione e la gestione di queste regole personalizzate a propria discrezione e responsabilità.

# Configurazione

#### Esempio di rete

In questo documento viene illustrata la configurazione e la verifica della Regola snort locale personalizzata in Snort2 nel diagramma.



#### Configurazione

Questa è la configurazione di Custom Local Snort Rule per rilevare ed eliminare i pacchetti di risposta HTTP contenenti una stringa specifica (nome utente).

Passaggio 1. Conferma versione snort

Selezionare Dispositivi > Gestione dispositivi in FMC, quindi fare clic su scheda Dispositivo. Confermare la versione snort è Snort2.

Firewall Management Center Devices / Secure Firewall Device Summary Overview Analysi	s Policies Devices Objects Integration	c	beploy Q 🥝 🌣 🕢 admin 🗸 🔐 SECU
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces Inline Sets DHCP VTEP	SNMP		
General 🖉 🛓 🛉	License	✓ System	<b>Ø</b> G
Name: FPR2120_FTD	Essentials:	Yes Model:	Cisco Firepower 2120 Threat Defense
Transfer Packets: Yes	Export-Controlled Features:	Yes Serial:	U.VPOTITCEUE
Troubleshoot: Logs CLI Download	Logs CLI Download Malware Defense:		2024-04-06 01:26:12
Mode: Routed	IPS:	Yes Time Zone:	UTC (UTC+0:00)
Compliance Mode: None	Carrier:	No Version:	7.4.1
TLS Crypto Acceleration: Enabled	URL:	No Time Zone setting for	Time UTC (UTC+0:00)
	Secure Client Premier:	No based Rules:	
Device Configuration: Import Export Download	Secure Client Advantage:	No Inventory:	view
OnBoarding Method: Registration Key	Secure Client VPN Only:	No	
·			
Inspection Engine	Health	Management	/ 🔍
Inspection Engine: Snort 2	Status:	Remote Host Address	1.105.0.25

Versione snort

Passaggio 2. Creare una regola personalizzata per l'orientamento locale nell'angolo 2

Selezionare Oggetti > Regole intrusione > Ordina 2 tutte le regole in FMC, quindi fare clic sul pulsante Crea regola.

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Analysis Policies	Devices Objects Integration	Deploy Q 🤣 🏠 🕢 admin 🗸 👘 SECURE
Snort 2 All Rules Snort 3 All Rules			
< Intrusion Policy			Search Delete Local Rules Import Rules Create Rule
Group Rules By   Category (62655)  Category (626			
Category			

Crea regola personalizzata

Immettere le informazioni necessarie per la Regola snort locale personalizzata.

- Intrusione : custom\_http\_sig
- Azione : avviso
- Protocollo : tcp
- flusso : stabilito, al client
- content : nomeutente (dati non elaborati)

Cipiects / Intrusion Rules / Create Overview Analy	sis Policies Devices Objects Integration	Deploy Q 🙆 🌣 🕢 admin 🖓 🚮 SECURE
Snort 2 All Rules Snort 3 All Rules		Search   Upload Update   Intrusion
	Create New Rule	

Inserisci le informazioni necessarie per la regola

#### Passaggio 3. Conferma regola snort locale personalizzata

Selezionare Policies > Intrusion Policies on FMC (Policy > Intrusion Policies su FMC), quindi fare clic sul pulsante Snort 2 Version (Avvia versione).

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	Overview Analysis Policies	Devices Objects Integration	Deploy Q 📀 🔅	admin v diale SECURE
Intrusion Policies Network Analysis Policies				
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusion F	olicy, Description, or Base Policy	All I	IPS Rules IPS Mapping () Con	npare Policies Create Policy
Intrusion Policy Description	Base Policy	Usage Information		
snort_test	Balanced Security and Co	1 Access Control Policy xnnectivity No Zero Trust Application Pol 1 Device	Snort 2 Version	Snort 3 Version 📝 🖻 🖆 🖥

Conferma regola personalizzata

# Passare a Regole > Categoria > locale in FMC, confermare i dettagli di Regola snort locale personalizzata.

Firewall Management Center Policies / Access Control / Intrusion / Edit Policy	Overview Analysis	Policies Devices	Objects Integration	Deploy Q 🥝	Contraction of the second seco
Intrusion Policies Network Analysis Policies					
Policy Information Rules					< Back
Cisco Recommendations Rule Configurat	Filter:				
Advanced Settings     Category	Category:"local"				× 0
Policy Layers     Indicator-compresent     indicator-obfuse	mise tion 0 selected rules of 1 Rule State • Even	Filtering - Dynamic Sta	te • Alerting • Comments •		Policy
indicator-scan indicator-shelloo	de GID SID	Message 4			→ ©▼⊙ <b>9</b> ₽
local malware-backd	or 1 100000	1 custom_http_sig			
malware-cnc malware-other					
malware-tools	Hide details				< < 1 of 1 > >
netbios os-linux	> Suppression	s (0)			Add
<	Dynamic Sta	te (0)			Add
Classifications Microsoft Vulne	Alerts (0)				Add SNMP Alert
Microsoft Worm Platform Specif	Comments (	0)			Add
Preprocessors	<ul> <li>Documentat</li> </ul>	on			
Priority Rule Locate		ndo			
Rue opdate		rule alert top any	any <> any any (sid:1000001; gid:1; flow:establis	sneo,to_cxent; content:"username"; rawbytes; msg:"custom_http_sig	<ul> <li>classtype:Unknown; rev:1; )</li> </ul>

Dettaglio regola personalizzata

#### Passaggio 4. Azione regola di modifica

Fare clic su pulsante Stato, impostare lo stato su Elimina e genera eventi e fare clic su OK pulsante.

Firewall Manageme Policies / Access Control / In	nt Center htrusion / Edit Policy	Overview	Analysis	Policies	Devices	Objects	Integration	De	ploy Q	•	2 O (	admin $\sim$	cisco SE	CURE
Intrusion Policies Network A	nalysis Policies													
Policy Information Rules	Rules												<	Back
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Filter: Cate	gory:"local"										>	x 0
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation	<ul> <li>0 select</li> <li>Rule S</li> </ul>	ted rules of 1 tate + Event I	Filtering 👻	Dynamic State	• Alerting •	Comments +				Policy			•
	indicator-scan indicator-shellcode		ID SID	Message	÷						-		T © 0	-
	malware-backdoor		1000001	custom_ht	ttp_sig									
	malware-other malware-tools netbios os-linux	Ţ			Set rule st	ate for "cu	stom_http_sig" 🛛							
	Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific				Disabled Generate Drop and Disabled	Events Generate Even	ts Cancel OK							
	Preprocessors													

Fare clic su Informazioni criterio pulsante, fare clic su Conferma modifiche pulsante per salvare le modifiche.



Commit modifiche

Passaggio 5. Associa criterio di intrusione alla regola dei criteri di controllo di accesso (ACP)

Selezionare Policies > Access Control on FMC (Policy > Controllo di accesso su FMC), quindi Associare Intrusion Policy (Policy di intrusione) a ACP.

Editing Rule <b>ftd_acp</b>			Mandatory 🛛 🖉 🗙
Name ftd_acp	Action 💿 Allow	r V Logging ON Lo Ti	me Range None V Rule Enabled
	Intrusion Polic	y snort_test X V Default-Set	X V File Policy None V
Q Zones (2) Networks Ports Applicati	ons 🛕 Users URLs	Dynamic Attributes VLAN Tags	
Q Search Security Zone Objects	Showing 2 out of 2	Selected Sources: 1	Selected Destinations and Applications: 1
A inside_zone (Routed Security Zone)		Collapse All Remo	ve All Collapse All Remove All
determine (Routed Security Zone)		ZONE V 1 Object	ZONE V 1 Object
Associa a regola ACP			

Passaggio 6. Distribuisci modifiche

Distribuire le modifiche in FTD.

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 🤌 🏟 admin 🗸 dede	SECURE
The Return to Access Control Policy Management Control Policy Managem	۹	Advanced Deploy All	Legacy UI Savo
Deckets → OPenfilter Rules → ODecryption → OSecurity Intelligence → Oldentity → OAccess Control     OMore     Access Control     OMore	FPR2120_FTD	Ready for Deployment	1 device

Distribuisci modifiche

# Verifica

#### Regola snort locale personalizzata non attivata

Passaggio 1. Imposta contenuto del file in HTTP Server

Impostare il contenuto del file test.txt sul lato server HTTP su user.

Passaggio 2. Richiesta HTTP iniziale

Accedere al server HTTP (192.168.20.1/test.txt) dal browser del client (192.168.10.1) e confermare che la comunicazione HTTP è consentita.

0	192.168.20.1	/test.txt	×	+	-	٥	×
←	$\rightarrow$ G	A		192.168.20.1/test.txt	☆	Θ	:
user							

Richiesta HTTP iniziale

#### Regola snort locale personalizzata attivata

Passaggio 1. Imposta contenuto del file in HTTP Server

Impostare il contenuto del file test.txt sul lato server HTTP su username.

Passaggio 2. Richiesta HTTP iniziale

Accedere al server HTTP (192.168.20.1/test.txt) dal browser del client (192.168.10.1) e confermare che la comunicazione HTTP è bloccata.



Richiesta HTTP iniziale

Passaggio 3. Conferma evento di intrusione

Passare ad Analisi > Intrusioni > Eventi in FMC, verificare che l'evento Intrusione sia generato dalla regola personalizzata di snort locale.

Firewall Management C Analysis / Intrusions / Events	enter <sub>Over</sub>	rview Anal	vsis Policies	Devices	Objects I	integration				Deplo	, Q	<b>0</b> ¢	e 🕜 adr	nin v eisce SI	ECURE
						В	ookmark This Pa	ige   Reporting	Dashboard	d   View Bo	okmark	s   Search	Predefine	d Searches	¥
Events By Priority and C	assification	(switch workflow)										2024-04	-06 09:41:20	- 2024-04-06 1	1:06:04
Search Constraints (Edit Search Sav	Search)													Exp	panding
Drilldown of Event, Priority, and Classi	ication Table Vi	ew of Events	Packets												
Jump to															
Time X Priori	y X Impact X	Inline Result × Reaso	n X Source IP X	Source Country ×	Destination IP X	Destination x	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	VLAN x	Messa	ge X		Classification X	Generat
▼ 2024-04-06 11:05:13 low	Unknown	Dropped	9192.168.20	.1	- 192.168.10.	1	80 (http) / tcp	50057 / tcp			custor	m_http_sig	(1:1000001:1)	Unknown Traffic	Standan

Evento Intrusion

#### Fare clic sulla scheda Packets, quindi confermare i dettagli di Intrusion Event.

Firewall Manage Analysis / Intrusions / Ev	vents Overview Analysis Policies Devices Objects Integration Deploy Q 🤣 🏟 admin - 🖓 🖏 SECURE
	Bookmark: This Page   Reporting   Dashboard   View Bookmarks   Search Predefined Searches V
Events By Priority	and Classification (senter monthead
	II 2024-04-06 09:41:20 - 2022-04-06 11:07:15 Expanding
Search Constraints (Edit Search Constraints)	earch Save Search)
Drilldown of Event, Priority, a	and Classification Table View of Events Packets
- Event Information	
Message	custom_http_sig (1:1000001:1)
Classification	
Priority	
Ingress Security Zone	outside zone
Egress Security Zone	inside_zone
Device	FPR2120_FTD
Ingress Interface	outside
Egress Interface	inside
Source IP	192.168.20.1
Source Port / ICMP Type	80 (http) / tcp
Destination IP	192.168.10.1
Destination Port / ICMP Code	50061 / tcp
HTTP Hostname	192.168.20.1
HTTP URI	/test.txt
Intrusion Policy	snort_test
Access Control Policy	acp-rule
Access Control Rule	fid_acp
Rule	alert top any any ⇔ any sid:1000001; gid:1; flor:established.to_client; content:"username"; rambytes; msg:"custom_http_sig"; classtyme:unknown; rev:1; )
<ul> <li>Actions</li> </ul>	

Dettaglio dell'evento Intrusion

# Risoluzione dei problemi

**Eseguire il comando**system support trace per confermare il comportamento su FTD. Nell'esempio, il traffico HTTP è bloccato dalla regola IPS (gid 1, sid 1000001).

#### <#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:
```

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '

ftd\_acp

', allow 192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW 192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).