Configuración de reglas de Snort locales personalizadas en Snort2 en FTD

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Configuración
Paso 1. Confirmar versión de Snort
Paso 2. Crear una regla de Snort local personalizada en Snort 2
Paso 3. Confirmar regla de Snort local personalizada
Paso 4. Cambiar acción de regla
Paso 5. Asociar política de intrusión a la regla de política de control de acceso (ACP)
Paso 6. Implementar cambios
Verificación
La regla de Snort local personalizada no se activa
Paso 1. Establecer el contenido del archivo en el servidor HTTP
Paso 2. Solicitud HTTP inicial
Se Activa la Regla de Snort Local Personalizada
Paso 1. Establecer el contenido del archivo en el servidor HTTP
Paso 2. Solicitud HTTP inicial
Paso 3. Evento ConfirmIntrusion
Troubleshoot

Introducción

Este documento describe el procedimiento para configurar las reglas de Snort local personalizado en Snort2 en Firewall Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La regla de Snort local personalizada hace referencia a una regla definida por el usuario que se puede crear e implementar dentro del sistema de detección y prevención de intrusiones de Snort integrado en el FTD. Cuando se crea una regla Snort local personalizada en Cisco FTD, básicamente se define un nuevo patrón o conjunto de condiciones que el motor Snort puede observar. Si el tráfico de red coincide con las condiciones especificadas en la regla personalizada, Snort puede realizar la acción definida en la regla, como generar una alerta o descartar el paquete. Los administradores utilizan reglas Snort locales personalizadas para hacer frente a amenazas específicas que no están cubiertas por los conjuntos de reglas generales.

En este documento, se explica cómo configurar y verificar una regla de Snort local personalizada diseñada para detectar y descartar paquetes de respuesta HTTP que contengan una cadena específica (nombre de usuario).



Precaución: la creación de reglas de Snort locales personalizadas y la prestación de asistencia para ellas quedan fuera de la cobertura de asistencia del TAC. Por lo tanto, este documento sólo se puede utilizar como referencia y solicite que cree y administre estas reglas personalizadas según su propio criterio y responsabilidad.

Configurar

Diagrama de la red

Este documento presenta la configuración y verificación de la regla de Snort local personalizado en Snort2 en este diagrama.



Configuración

Esta es la configuración de la regla de snort local personalizada para detectar y descartar paquetes de respuesta HTTP que contienen una cadena específica (nombre de usuario).

Paso 1. Confirmar versión de Snort

Vaya a Dispositivos > Administración de dispositivos en FMC, haga clic en la pestaña Dispositivo. Confirmación de que la versión del snort es Snort2.

FPER120_ETPE Joo Frepower 2120 Treat Defense Device Nume: PR2120_FTD Name: FPR2120_FTD Name: FPR2120_FTD Name: FPR2120_FTD Transfer Packets: Yes Toubleshoot: FPR2120_FTD Nade: Routed Mode: Routed Mode: Routed Tis Crypto Acceleration: Registration Key Device Configuration: Registration Key Inspection Engine: Source Clent VPN Only:	Firewall Management C Devices / Secure Firewall Device S	Senter Overview Analysis	Policies Devices Objects	Integration	Deploy	Q 📀 🌣 🚱 admin ~ diada SEC
General Image: Constraint of the section of the sectin of the section of the	FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	MP			
Name:FPR2120_FDEssentials:YesTransfer Packets:YesKodel:Cisco Firepower 2120 Threat DefenseTroubleshoot:Cong CL DoernsorMalware Defense:YesModel:RoutedIPS:YesCompliance Model:NoneCarrier:NoTLS Crypto Acceleration:EnabledURL:NoDevice Configuration:Eregistration KeySecure Client Premier:NoInspection Engine:Snot 2HeatthStatus:Inspection Engine:Snot 2Status:Malagement	General	/±+	License	1	System	© G
Transfer Packets: Yes Troubleshoot: Logi CL Doerstaar Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Enabled Device Configuration: Emort Controlled Fremier: No Device Configuration: Registration Key Inspection Engine: Secure Client VPN Only: No Inspection Engine: Snot 2	Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense
Troubleshoot: Logi CL Downsolf Malware Defense: Yes Time: 2024-04-06 01:26:12 Mode: Routed IPS: Yes Time: 2024-04-06 01:26:12 Compliance Mode: None Carrier: No Time: 2024-04-06 01:26:12 T.S. Crypto Acceleration: Enabled URL: No Version: 7.4.1 Device Configuration: Emore Teport Downsolf Secure Client Premier: No No Time Zone setting for Time Dut C (UTC+0:00) Secure Client Premier: No Secure Client Advantage: No No Inventory: View Inspection Engine Snot 2 Status: Status: Status: Management Renote Host Address: 1.1010.0.20	Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	JUNPOT TOFUE
Mode:RoutedIPS:YesTime Zone:UTC (UTC+0:00)Compliance Mode:NoneCarrier:NoVersion:7.4.1TLS Crypto Acceleration:EnabledURL:NoTime Zone setting for Time based Rules:UTC (UTC+0:00)Device Configuration:Imort Tiport CommonderSecure Client Premier:NoInventory:Version:Secure Client Advantage:NoSecure Client Advantage:NoInventory:ViewInspection EngineSnot 2Status:Status:ManagementRenote Host Address:1.1010.0.20	Troubleshoot:	Logs CLI Download	Malware Defense:	Yes	Time:	2024-04-06 01:26:12
Compliance Mode: None Carrier: No Version: 7.4.1 TLS Crypto Acceleration: Enabled URL: No Time Zone setting for Time based Rules: UTC (UTC+0:00) Device Configuration: Import Icport Commonset No Secure Client Premier: No OnBoarding Method: Registration Key Registration Key No Ne Ne Inspection Engine: Snot 2 Status: Status: Management Remote Host Address: 1.1010.0.00	Mode:	Routed	IPS:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration: Enabled URL: No Time Zone setting for Time based Rules: UTC (UTC+0:00) Device Configuration: Import Icport Commonse No Secure Client Premier: No Inventory: View OnBoarding Method: Registration Key Registration Key No No Management View Inspection Engine: Snot 2 Status: Status: Status: Management Remote Host Address: 1,101,012	Compliance Mode:	None	Carrier:	No	Version:	7.4.1
Device Configuration: Import Configuration: Secure Client Premier: No Inventory: View OnBoarding Method: Registration Key Secure Client VPN Only: No Inventory: View Inspection Engine: Snot 2 Status: Status: Status: Remote Host Address: 1.101.0.22	TLS Crypto Acceleration:	Enabled	URL:	No	Time Zone setting for Time	UTC (UTC+0:00)
Device Configuration: Import Toport Configuration OnBoarding Method: Registration Key Inspection Engine Notation Inspection Engine: Snort 2			Secure Client Premier:	No	leventer.	Monu
OnBoarding Method: Registration Key Secure Client VPN Only: No Inspection Engine Health Management Inspection Engine: Snort 2 Status: Ø	Device Configuration:	Import Export Download	Secure Client Advantage:	No	inventory.	view
Inspection Engine Health Management Imagement Inspection Engine: Snort 2 Status: Imagement	OnBoarding Method:	Registration Key	Secure Client VPN Only:	No		
Inspection Engine Health Management Imagement Inspection Engine: Snort 2 Status: Imagement Remote Host Address: 1.1010.020						
Inspection Engine: Short 2 Status: Status: Remote Host Address: 1.101.0.20	Inspection Engine		Health		Management	/ 🔍
	Inspection Engine:	Snort 2	Status:	0	Remote Host Address:	1.10%0.25

Versión de Snort

Paso 2. Crear una regla de Snort local personalizada en Snort 2

Navegue hasta Objetos > Reglas de intrusión > Snort 2 All Rules en FMC, haga clic en el botón Create Rule.

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			

Crear regla personalizada

Introduzca la información necesaria para la regla de snort local personalizado.

- Intrusión: custom_http_sig
- Acción: alerta
- Protocolo: tcp
- flujo: establecido, al cliente
- content: username (Raw Data)

Firewall Management Center Overview Analys Objects / Intrusion Rules / Create	is Policies Devices Objects Integration	Deploy Q 🥥 🌣 🚱 admin 🗸 👶 SECURE
Snort 2 All Rules Snort 3 All Rules		Search Upload Update Intrusion
	Create New Rule Message custom_http_sig Classification Unknown Traffic Concentence Image: Custom Concentence Action alert Protocol top Direction Bidirectonal Source Bs any Destination Bs any Destination Bs any Destination Bs To Client For To Client Established To Client Not Image: Case Insensitive With Concentence Image: Case Insensitive With Concentence Image: Case Insensitive With Concentence Image: Case Insensitive Image: Case Insensitive Image: Case Insensitive <td< th=""><th></th></td<>	

Introduzca la información necesaria para la regla

Paso 3. Confirmar regla de Snort local personalizada

Navegue hasta Políticas > Políticas de intrusión en FMC, haga clic en el botón Versión Snort 2.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	Overview Analysis Policies Devices	Objects Integration Dep	oloy Q 🥝 🌣 🍘 admin 🗸 🔥 SECURE
Intrusion Policies Network Analysis Policies			
Hide Snort 3 Sync status 🜒 🔍 Search by Intrusion Policy, Des	cription, or Base Policy	All IPS Rules IPS	S Mapping Compare Policies Create Policy
Intrusion Policy Description	Base Policy	Usage Information	
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12	Balanced Security and Connectivity	1 Access Control Policy No Zero Trust Application Policy 1 Device	Snort 2 Version Snort 3 Version 🖌 🗟 🖻

Confirmar regla personalizada

Navegue hasta Reglas > Categoría > local en FMC, confirme los detalles de la Regla de Snort Local Personalizada.

Firewall Management Policies / Access Control / Intrus	Center Overview	Analysis Policies	Devices Of	bjects Integration		Deploy Q 🕝 🐇	> @ ≥	dmin v dudu S	ECURE
Intrusion Policies Network Analy	sis Policies								
Policy Information Rules Cisco Recommendations	Rules								< Back
> Advanced Settings	Rule Content Category Cate	gory:"local"							XØ
> Policy Layers	hle-pdf indicator-compromise indicator-obfuscation Rule S	ted rules of 1 tate	Dynamic State 🕶	Alerting - Comments -			Policy		•
_	indicator-scan	ID SID Message 4					-	• • • •	
L	malware-backdoor		tp_sig				-+		
I	malware-onc malware-other malware-tools netbios os-linux os-mohile	details Suppressions (0) Dynamic State (0)					K <	1 of 1 > Add Add	>
	Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific	Alerts (0) Comments (0)					I	Add SNMP Alert Add	Ц.
	Preprocessors Priority Rule Update	Documentation	alert tcp any any <> a	any any (sid:1000001; gid:1; flow:establ	ished,to_client; content:"username"; rawbytr	es; msg:"custom_http_sig"	; classtype:unk	nown; rev:1;)	

Detalle de la regla personalizada

Paso 4. Cambiar acción de regla

Haga clic en el botón State, establezca el State en Drop and Generate Events y haga clic en el botón OK.

Firewall Management Center Policies / Access Control / Intrusion / Edit Policy	Ov	erview	Analysis	Policies	Devices	Objects	Integration	Dep	loy Q	0	° 0	admin	cisco	SECU	IRE
Intrusion Policies Network Analysis Policies															
Policy Information Rules														< Ba	ick
Cisco Recommendations Rule Configuration		Filter:													
> Advanced Settings Category		Category:	"local"											×	0
file-pdf		0 selected r	ules of 1												
> Policy Layers indicator-compromise		Rule State	Fvent F	iltering v	Dynamic State	 Alerting w 	Comments +				Policy				-
indicator-obruscation indicator-scan					bynamie entre	, poorting .									
indicator-shellcode		GID	SID	Message -	÷						-)	•	Y ()	0 =	
local .	8	1	1000001	custom_ht	ttp_sig										
malware-backdoor malware-cnc												_			
malware-other															
malware-tools					Set rule s	ate for cu	stom_nttp_sig*								
os-linux															
os-mobile	*				State										
Classifications					Generate	vents	•								
Microsoft Vulnerabilitie	s				Drop and	Generate Even	ts								
Microsoft Worms					Disabled		Cancel OK								
Platform Specific															

Cambiar la acción de regla

Haga clic en el botón Información de política, haga clic en el botón Registrar cambios para guardar los cambios.



Registrar cambios

Paso 5. Asociar política de intrusiones con regla de política de control de acceso (ACP)

Vaya a Políticas > Control de Acceso en FMC, asocie la Política de Intrusión con ACP.

¹ \bigcirc Editing Rule ftd_acp	Mandatory 🛛 🗙
Name [ftd_acp 1 Action C Allo	w V BLogging ON Time Range None V Rule Enabled
Intrusion Pol	cy snort_test $X \vee$ Default-Set $X \vee$ E File Policy None $ \vee$
Q Zones (2) Networks Ports Applications 🛕 Users URLs	Dynamic Attributes VLAN Tags
Q Search Security Zone Objects Showing 2 out of 2	Selected Sources: 1 Selected Destinations and Applications: 1
inside_zone (Routed Security Zone)	Collapse All Remove All Collapse All Remove All
dutside_zone (Routed Security Zone)	ZONE • 1 Object ZONE • 1 Object
Asociar con Regla ACP	

Paso 6. Implementar cambios

Implemente los cambios en FTD.

Firewall Management Center Policies / Access Control / Policy Editor	Overview Analy	lysis Policies	Devices	Objects	Integration		Deploy	९ 💿 🌣 🙆	admin v 🚽	SECURE
the second						٩	Advanced Deploy	▲ □ Ignore warnin	gs Deploy All	Legacy UI Save
Packets → Prefilter Rules → O Decryption	→ Security Intelligence	ce → ◯ Identity →	O Access C	Control	More	FPR2120_FTD		Ready for De	ployment	1 device

Implementar cambios

Verificación

La regla de Snort local personalizada no se activa

Paso 1. Establecer el contenido del archivo en el servidor HTTP

Establezca el contenido del archivo test.txt en el lado del servidor HTTP como usuario.

Paso 2. Solicitud HTTP inicial

Acceda al servidor HTTP (192.168.20.1/test.txt) desde el explorador del cliente (192.168.10.1) y confirme que la comunicación HTTP está permitida.

0	192.1	168.20.1	1/test.tx	t	×	+	-	٥	×
←	\rightarrow	G	▲			192.168.20.1/test.txt	☆	Θ	:
user									

Solicitud HTTP inicial

Se Activa la Regla de Snort Local Personalizada

Paso 1. Establecer el contenido del archivo en el servidor HTTP

Establezca el contenido del archivo test.txt en el lado del servidor HTTP en username.

Paso 2. Solicitud HTTP inicial

Acceda al servidor HTTP (192.168.20.1/test.txt) desde el explorador del cliente (192.168.10.1) y confirme que la comunicación HTTP está bloqueada.





Solicitud HTTP inicial

Paso 3. Confirmar evento de intrusión

Navegue hasta Análisis > Intrusiones > Eventos en FMC, confirme que el Evento de Intrusión es generado por la Regla de Snort Local Personalizada.

Firewall Managemen Analysis / Intrusions / Events	nt Center	Overview	Analysis	Policies	Devices	Objects	integration				Deplo	, Q	⊘ <	≯ Ø ad	min v ettat	SECURE
							В	ookmark This Pa	ige Reporting	Dashboar	d View Bo	okmarkr	s Search	Predefin	ed Searches	Ŧ
Events By Priority and	d Classificati	on (switch wor	kflow)										2024-04	4-06 09:41:2	0 - 2024-04-1	06 11:06:04
Search Constraints (Edit Search)	Save Search)															Expanding
Drilldown of Event, Priority, and C	lassification Tal	le View of Ev	ents Pac	kets												
Jump to																
□ ↓ Time × F	Priority X Impact X	Inline Result ×	Reason X	Source IP X	Source x	Destination IP X	Destination x	Source Port/ICMP X Type	Destination Port / ICMP X Code	SSL Status ×	VLAN x	Messa	pe ×		Classificati	on × Generat
· 2024-04-06 11:05:13	ow O Unkno	wn Dropped		192.168.20.	1	9 192.168.10.	1	80 (http) / tcp	50057 / tcp			custom	h_http_sig	(1:1000001:1) Unknown T	raffic Standar

Evento de intrusión

Haga clic en la pestaña Paquetes, confirme los detalles del evento de intrusión.

Firewall Manage Analysis / Intrusions / E	ment Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin v viewe SECURE
	Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches •
Events By Priority	and Classification (automotion)
	II 2024-04-06 09.41.20 - 2024-04-06 11.07.15 Expanding
Search Constraints (Edit S	arch Save Search)
Drilldown of Event, Priority,	Ind Classification Table View of Events Packets
- Event Information	
Message	eustem.http:sig(1:1000001:1)
Classification	2024/94-00 11:00:04
Priority	Vender Hand
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	Restba
Intrusion Policy	snort_test
Access Control Policy	acp-rule
Access Control Rule	ftd_acp
Rule	alert tos any any \diamond any any (sid:1000001; gid:1; flow:established_to_client; content:"username"; rambytes; msg:"custom_http_sig"; classtype:unknown; rev:1;)
 Actions 	

Detalle del evento de intrusión

Troubleshoot

Ejecute system support trace el comando para confirmar el comportamiento en FTD. En este ejemplo, la regla IPS bloquea el tráfico HTTP (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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).