Configurer des règles de sniffage local personnalisées dans Snort2 sur FTD

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Diagramme du réseau
Configuration
Étape 1. Confirmer la version Snort
Étape 2. Créer une règle de détection locale personnalisée dans Snort 2
Étape 3. Confirmer la règle de détection locale personnalisée
Étape 4. Action Modifier la règle
Étape 5. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)
Étape 6. Déployer les modifications
Vérifier
La règle d'analyse locale personnalisée n'est pas déclenchée
Étape 1. Définition du contenu du fichier dans le serveur HTTP
Étape 2. Requête HTTP initiale
La règle d'analyse locale personnalisée est déclenchée
Étape 1. Définition du contenu du fichier dans le serveur HTTP
Étape 2. Requête HTTP initiale
Étape 3. ConfirmIntrusion, événement
<u>Dépannage</u>

Introduction

Ce document décrit la procédure pour configurer des règles de détection locale personnalisées dans Snort2 sur Firewall Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Protection contre les menaces par pare-feu

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La règle Snort locale personnalisée fait référence à une règle définie par l'utilisateur que vous pouvez créer et mettre en oeuvre dans le système de détection et de prévention des intrusions Snort intégré au FTD. Lorsque vous créez une règle Snort locale personnalisée dans Cisco FTD, vous définissez essentiellement un nouveau modèle ou un nouvel ensemble de conditions que le moteur Snort peut surveiller. Si le trafic réseau correspond aux conditions spécifiées dans votre règle personnalisée, Snort peut effectuer l'action définie dans la règle, comme la génération d'une alerte ou l'abandon du paquet. Les administrateurs utilisent des règles Snort locales personnalisées pour traiter des menaces spécifiques qui ne sont pas couvertes par les ensembles de règles générales.

Dans ce document, vous apprendrez à configurer et à vérifier une règle de détection locale personnalisée conçue pour détecter et supprimer les paquets de réponse HTTP contenant une chaîne spécifique (nom d'utilisateur).



Attention : la création de règles Snort locales personnalisées et leur prise en charge ne sont pas couvertes par le centre d'assistance technique. Par conséquent, ce document ne peut être utilisé qu'à titre de référence et vous demandez de créer et de gérer ces règles personnalisées à votre discrétion et sous votre responsabilité.

Configurer

Diagramme du réseau

Ce document présente la configuration et la vérification de la règle de sniffage local personnalisée dans Snort2 sur ce schéma.



Configuration

Il s'agit de la configuration de la règle de détection locale personnalisée pour détecter et supprimer les paquets de réponse HTTP contenant une chaîne spécifique (nom d'utilisateur).

Étape 1. Confirmer la version Snort

Accédez à Périphériques > Gestion des périphériques sur FMC, cliquez sur l'onglet Périphérique. Confirmation de la version Snort2.

Firewall Management C Devices / Secure Firewall Device S	Center Overview Analysis	Policies Devices Objects	Integration	Deploy	Q. ⊘ ☆ Ø admin ∨ tinde SECU
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	MP			
General	/ <u>+</u> +	License	1	System	8 G
Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	UNPOT LICEUE
Troubleshoot:	Logs CLI Download	Malware Defense:	Yes	Time:	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	Inventory	View
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:	0	Remote Host Address:	1.10%0.25

Version Snort

Étape 2. Créer une règle de détection locale personnalisée dans Snort 2

Accédez à Objets > Règles d'intrusion > Snort 2 All Rules sur FMC, cliquez sur le bouton Create Rule .

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Analysis Policies	Devices Objects Integration	Deploy Q 🥥 🄅 🕢 admin - 🖞
Snort 2 All Rules Snort 3 All Rules			
< Intrusion Policy			Search Delete Local Rules Import Rules Create Rule
Group Rules By Category (62655)			
Category			

Créer une règle personnalisée

Entrez les informations nécessaires pour la règle de sniffage local personnalisée.

- Intrusion : custom_http_sig
- Action : alerte
- Protocole : TCP
- flux : établi, au client
- content : username (Raw Data)

Objects / Intrusion Rules / Create Overview Analysis	Policies Devices Objects Integration	Deploy Q 🥝 🌣 🚱 admin - 🖓 🐯 SECURE
Snort 2 All Rules Snort 3 All Rules		Search Upload Update Intrusion
	Areace New Rule Message custom_http_sig Classification Utknown Traffic Area etre Protocol ter Direction Bidirectional Source BF any Direction Bidirectional Source BF any Direction Bidirectional Source BF any Direction Options any Content V Established To Client Not V Case Insensitive V Case Insensitive V HTTP New URE HTTP New URE HTTP New URE HTTP New URE HTTP New URE HTTP New URE HTTP Status Code Distance Use Fast Pattern Matcher Offset and Length Depti Use Fast Pattern Matcher Offset and Length Exer Val Pattern Content Case Internet Content Exer Val Pattern Matcher Offset and Length	

Informations requises pour la règle

Étape 3. Confirmer la règle de détection locale personnalisée

Accédez à Policies > Intrusion Policies sur FMC, cliquez sur le bouton Snort 2 Version.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Polic	Overview A	nalysis Policies	Devices	Objects	Integration	Deploy	Q	00	admin v	cisco SECURE
Intrusion Policies Network Analysis Policies										
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusion I	Policy, Description, or Base F	Policy			All IPS Rules	IPS Map	ping 📵	c	ompare Policies	Create Policy
Intrusion Policy Description		Base Policy		Usage Inf	formation					
snort_test → Snort 3 is in sync vith Snort 2, 2024-01-12		Balanced Security and	d Connectivity	1 Access No Zero 7 1 Device	Control Policy Trust Application Policy		Snort 2	2 Versio	n Snort 3 Versior	/807

Confirmer la règle personnalisée

Accédez à Rules > Category > local sur FMC, confirmez le détail de Custom Local Snort Rule.

Firewall Manageme Policies / Access Control / I	ent Center o	Overview Analysis	Policies	Devices	Objects	Integration	Deploy	Q 📀	° 0	admin ~ dudu S	ECURE
Intrusion Policies Network A	Analysis Policies										
Policy Information	Rules										< Back
Cisco Recommendations	Rule Configuration	Filter:									
> Advanced Settings	Category	Category:"local"									XØ
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation	 0 selected rules of 1 Rule State + Event F 	iltering 👻 Dyr	namic State	Alerting	Comments +			Policy		•
	indicator-scan	GID SID	Message 4						-+		
	malware-backdoor	1 1000001	custom_http_	sig					-+		
	malware-cnc										
	malware-other malware-tools netbios	Hide details	(0)						Κ <	1 of 1 >	X •
	os-mohile	 Dynamic State 	e (0)							Add	
	Classifications Microsoft Vulnerabilities	Alerts (0)								Add SNMP Alert	1
	Microsoft Worms Platform Specific	Comments (0)								Add	
	Preprocessors	 Documentatio 	n								
	Priority Rule Update		rule a	elert top any an	y <> any any (sic	:1000001; gid:1; flow:established.to_client; content:"username	e"; rawbytes; msg:"o	ustom_http_sk	r; classtype	:unknown; rev:1;)	-

Détail de la règle personnalisée

Étape 4. Action Modifier la règle

Cliquez sur le bouton State, définissez l'état sur Drop and Generate Events et cliquez sur le bouton OK.

Firewall Manageme Policies / Access Control / I	ent Center Intrusion / Edit Policy	Dverview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	• •	0	admin ~	cisco S	ECURE
Intrusion Policies Network A	Analysis Policies														
Policy Information	Rules														< Back
Cisco Recommendations	Rule Configuration	Filter:													
> Advanced Settings	Rule Content	Category	/:"local"												× Ø
	file-pdf	0 selected	rules of 1												~ ~
> Policy Layers	indicator-compromise	Dulo State	Event F	illering -	Dunamic State	 Alerting = 	Commente +					Policy			•
	indicator-obfuscation	Hune State	LVOIR P	ntennig *	Dynamic State	 Horning * 	Comments +								
	indicator-shellcode	GID	SID	Message -	k in the second s							->		Y () ()	
	local	0.1	1000001	custom bt	to sig										
	malware-backdoor				-0-3 -0-3										
	malware-other														
	malware-tools				Set rule s	tate for "cu	stom_http_sig" 🔞								
	netbios							-							
	os-linux os-mobile	-			State										
	<				Disabled		¥								
	Classifications				Generate Drop and	Events Generate Even	te								
	Microsoft Worms				Disabled	Generate Even									
	Platform Specific						Cancel OK								
	Preprocessors														

Action Modifier la règle

Cliquez sur le bouton Policy Information , cliquez sur Commit Changes pour enregistrer les modifications.

Firewall Managemen Policies / Access Control / In	nt Center Overview Analysis Policies Devices Objects Integration Deplo	ny (2 (0 0	6 0	admin \sim	cisco SEC	URE
Intrusion Policies Network Ar	nalysis Policies							
Policy Information Rules	Policy Information						< B	lack
Cisco Recommendations > Advanced Settings	Drop when Inline							
> Policy Layers	Base Policy Description of Changes @					🖌 Mana	ige Base Polic	y
	The base policy is up to date (Rule Update 2024-04-03-001-vr change rule action)							
	This policy has 9958 enabled rules					/	Manage Rule	s
	494 rules drop and generate events						 Viev 	v
	No recommendations have been generated. Click here to set up Cisco recommendations.							
	This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules							
				scard	Change	is Cor	nmit Changes	

Valider les modifications

Étape 5. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Accédez à Policies > Access Control sur FMC, associez Intrusion Policy à ACP.

1 🔶 Editing Ru	le ftd_acp												Mandatory 🛛 🗙
Name ftd_acp		ţ			Action 💿	Allow	l Y		ogging ON	r Time Ran	ge None		Rule Enabled
					Intrusion	Policy	snort_tes	t ×	 ✓ Defau 	llt-Set X	~ E,	File Policy None	
Q Zones (2)	Networks	Ports	Applicatio	ns 🛕 Use	ers UR	Ls	Dynamic	Attributes	VLAN	Tags			
Q Search Security Z	one Objects			Showing 2 out	of 2	s	elected S	ources: 1			Selected	Destinations and	Applications: 1
inside_zone (R	outed Security Zone)					c	Collapse A	I		Remove All	Collapse	All	Remove All
- 🚓 outside_zone (Routed Security Zone)					ZONE	1 Object	zone		ZONE	 1 Object dutside_zc 	one

Associer à la règle ACP

Étape 6. Déployer les modifications

Déployez les modifications sur FTD.

Firewall Management Center Policies / Access Control / Policy Editor	Overview Analysis	Policies	Devices	Objects	Integration		Deploy	९ 💿 🌣 🙆	admin ~ dis	SECURE
Return to Access Control Policy Management acp-rule ✓						۹	Advanced Deploy	▲ □ Ignore warnin	ngs Deploy All	Legacy UI Save
Packets → O Prefilter Rules → O Decryption	→ O Security Intelligence →	○ Identity →	😋 Access C	Control 0	More	FPR2120_FTD		Ready for D	eployment	1 device

Déployer les modifications

Vérifier

La règle d'analyse locale personnalisée n'est pas déclenchée

Étape 1. Définition du contenu du fichier dans le serveur HTTP

Définissez le contenu du fichier test.txt côté serveur HTTP sur utilisateur.

Étape 2. Requête HTTP initiale

Accédez au serveur HTTP (192.168.20.1/test.txt) à partir du navigateur du client (192.168.10.1) et vérifiez que la communication HTTP est autorisée.

6	3	192.1	168.20).1/te	est.txt	×	+	-	٥	×
÷		\rightarrow	C		A		192.168.20.1/test.txt	☆	θ	:
use	r									

Requête HTTP initiale

La règle d'analyse locale personnalisée est déclenchée

Étape 1. Définition du contenu du fichier dans le serveur HTTP

Définissez le contenu du fichier test.txt côté serveur HTTP sur username.

Étape 2. Requête HTTP initiale

Accédez au serveur HTTP (192.168.20.1/test.txt) à partir du navigateur du client (192.168.10.1) et vérifiez que la communication HTTP est bloquée.





Requête HTTP initiale

Étape 3. Confirmer l'incident

Accédez à Analysis > Intrusions > Events sur FMC, confirmez que l'événement d'intrusion est généré par la règle de détection locale personnalisée.

Firewall Manageme Analysis / Intrusions / Event	ent Center s	Overview	Analysis	Policies	Devices	Objects	Integration				Deplo	y Q	0 \$	t 🕜 ad	min v dia	SECURE
							В	ookmark This Pa	ige Reporting	Dashboard	d View Bo	ookmark	Search	Predefin	ed Searches	٣
Events By Priority and	d Classifica	ion (switch war	kflow)									п	2024-04	-06 09:41:20) - 2024-04-(06 11:06:04
Search Constraints (Edit Search)	h Save Search)															Expanding
Drilldown of Event, Priority, and	Classification T	able View of Ev	ents Pac	kets												
Jump to																
□ ↓ Time ×	Priority X Impact 3	Result ×	Reason X	Source IP X	Source x	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	ULAN X	Messa	20 X		Classification	on X General
▼ 2024-04-06 11:05:13	low 0 Unkr	own Dropped		192.168.20.1		192.168.10.	1	80 (http) / tcp	50057 / tcp			custon	http_sig	(1:1000001:1) Unknown T	raffic Standa

Événement D'Intrusion

Cliquez sur l'onglet Packets, confirmez le détail de l'événement Intrusion.

Firewall Management Center Overview Analysis / Intrusions / Events Devices Objects Integration Deploy Q 📀 🌣 😡 admin 🗸 the Secure
Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches *
Events By Priority and Classification Institute According
11 2024-04-00 056.120 - 2024-04-06 1107.15
Search Constraints (Edit Search Save Search)
Drilldown of Event, Priority, and Classification Table View of Events Packets
Event Information
Message custom_http_sig (1:100001:1)
Into 2024/04/00 FL/06.544
Priority law
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 ftd_acp
Rule alert top any any ⇔ any any (sid:1000001; gid:1; flow:established.to_client; content:"username"; rambytes; msg:"custom_http_sig"; classtyme:umknown; rev:1;)
⋆ Actions

Détail de l'incident

Dépannage

Exécutez system support trace la commande pour confirmer le comportement sur FTD. Dans cet exemple, le trafic HTTP est bloqué par la règle 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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.