Configureer aangepaste lokale snortregels in Snort2 op FTD

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram **Configuratie** Stap 1. Snelversie bevestigen Stap 2. Een aangepaste lokale-snortregel maken in kleur 2 Stap 3. Aangepaste lokale snelregel bevestigen Stap 4. Handeling regels wijzigen Stap 5. Associate Inbraakbeleid met Access Control Policy (ACS)-regel Stap 6. Wijzigingen implementeren Verifiëren Aangepaste lokale snortregel wordt niet geactiveerd Stap 1. Inhoud van bestand in HTTP-server instellen Stap 2. Eerste HTTP-aanvraag Aangepaste lokale snortregel wordt geactiveerd Stap 1. Inhoud van bestand in HTTP-server instellen Stap 2. Eerste HTTP-aanvraag Stap 3. Inbraakgebeurtenis bevestigen Problemen oplossen

Inleiding

In dit document wordt de procedure beschreven om Aangepaste lokale snelregels te configureren in Snort2 op Firewall Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower Management Center voor VMware 7.4.1
- Cisco FirePOWER-applicatie 2120 7.4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Custom Local Snort Rule verwijst naar een door de gebruiker gedefinieerde regel die u kunt maken en implementeren binnen het snort inbraakdetectie- en preventiesysteem dat is geïntegreerd in de FTD. Wanneer u een aangepaste lokale snortregel in Cisco FTD maakt, definieert u in wezen een nieuw patroon of een nieuwe reeks voorwaarden waarop de snortengine kan letten. Als het netwerkverkeer voldoet aan de voorwaarden die in uw aangepaste regel zijn gespecificeerd, kunt u de actie uitvoeren die in de regel is gedefinieerd, zoals een waarschuwing genereren of het pakket laten vallen. Beheerders gebruiken aangepaste lokale Snortregels om specifieke bedreigingen aan te pakken die niet worden gedekt door de algemene regelsets.

In dit document, wordt u geïntroduceerd hoe te om een Douane Lokale Snelregel te vormen en te verifiëren die wordt ontworpen om HTTP- reactiepakketten te ontdekken en te laten vallen die een specifiek koord (gebruikersbenaming) bevatten.



Waarschuwing: het maken van aangepaste lokale snelregels en het bieden van ondersteuning ervoor valt buiten de TAC ondersteuning dekking. Daarom kan dit document alleen als referentie worden gebruikt en u vragen deze aangepaste regels naar eigen goeddunken en op eigen verantwoordelijkheid te maken en te beheren.

Configureren

Netwerkdiagram

Dit document introduceert de configuratie en verificatie voor Aangepaste lokale snortregel in Snort2 in dit diagram.



Configuratie

Dit is de configuratie van Aangepaste lokale snortregel om HTTP-reactiepakketten met een specifieke string (gebruikersnaam) te detecteren en te laten vallen.

Stap 1. Snelversie bevestigen

Navigeren naar Apparaten > Apparaatbeheer op FMC, klik op Apparaat tabblad. De snortversie bevestigen is Snort2.

Firewall Management C Devices / Secure Firewall Devices	Center Overview Analysis	Policies Devices Objects	Integration	Deploy	Q 📀 🌣 🚱 admin 🗸 divide SECU				
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SA	MP							
General	/ <u>+</u> +	License	1	System	G G				
Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense				
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial: J.VPT17CFUI					
Troubleshoot:	Logs CLI Download	Malware Defense:	Yes	Time:	2024-04-06 01:26:12				
Mode:	Routed	IPS:	Yes	Time Zone: UTC (UTC /					
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:	0	Remote Host Address:	1.10%0.25				

Snelversie

Stap 2. Een aangepaste lokale-snortregel maken in kleur 2

Navigeer naar objecten > Inbraakregels > Sneltoets 2 Alle regels op FMC, klik op Regel maken knop.

Copiects / Intrusion Rules / Snort 2 All Rules Overview	Analysis Policies	Devices Objects Integration	Deploy Q 📀 🌣 🕢 admin – 🖞 the SECURE
Snort 2 All Rules Snort 3 All Rules			
< Intrusion Policy			Search Delete Local Rules Import Rules Create Rule
Group Rules By Category (62655) A structure (162)			
Category			

Aangepaste regel maken

Voer de benodigde informatie in voor Aangepaste lokale snelregel.

- Inbraak : custom_http_sig
- Actie : waarschuwing
- Protocol: TCP
- stroom : vastgesteld, naar de klant
- inhoud: gebruikersnaam (ruwe gegevens)

Firewall Management Center Objects / Intrucion Rules / Create Overview Analysis Policies Devices Objects Integration	Deploy Q 🥥 🔅 🚱 admin 🗸 🔥 SECURE
	Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules	
Sont 2 AD Rows Vint 2	Port any
Use Fast Pattern Matcher	
Fast Pattern Matcher Offset and Length	
content Add Option	Save As New

Voer de benodigde informatie voor deze regel in

Stap 3. Aangepaste lokale snelregel bevestigen

Navigeren naar Beleid > Inbraakbeleid op FMC, klik op Sneltoets 2 Versie knop.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	licies Overview Analysis Po	licies Devices Objects	Integration Deploy	० 📀 🌣	admin v dodu SECURE
Intrusion Policies Network Analysis Policies					
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusio	n Policy, Description, or Base Policy		All IPS Rules IPS Ma	apping 🚺 Com	pare Policies Create Policy
Intrusion Policy Description	Base Policy	Usage	e Information		
snort_test → Snort 3 is in sync with Snort 2, 2024-01-12	Balanced Sec	urity and Connectivity No Ze 1 Devi	ess Control Policy ro Trust Application Policy ice	Snort 2 Version	Snort 3 Version 🛛 🖊 🖥 🔃 🗑

Aangepaste regel bevestigen

Ga naar Regels > Categorie > Lokaal op VCC, bevestig de details van de Aangepaste Lokale Snortregel.

Firewall Management Center Policies / Access Control / Intrusion / Edit Policy	Overview Analysis	Policies Devices	Objects Integration	Deploy Q 🥝	🔅 😰 admin ~ 🖞
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			→ @▼⊙ ₽
local malware-backdo	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	 Documentat 	on			
Priority Rule Locate		ndo			
Rue opdate		rule alert top any	any <> any any (sid:1000001; gid:1; flow:establis	<pre>sned,to_cirers; content:"username"; rawbytes; msg:"custom_http_s</pre>	.gr; classtype:unknown; rev:1;)

Detail van aangepaste regel

Stap 4. Handeling regels wijzigen

Klik op de knop Status, stel de status in om gebeurtenissen te laten vallen en te genereren en klik op de knop OK.

Firewall Managemen Policies / Access Control / Int	nt Center trusion / Edit Policy	Overv	view A	unalysis	Policies	Devices	Objects	Integration		Deploy	۹	• •	0	admin v	cisco	SECUR	ε
Intrusion Policies Network An	nalysis Policies																
Policy Information	Rules															< Bac	k
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Fil	lter: Category:"k	ocal"												X	0
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation indicator-scan	* 0 R	selected rul tule State ¥	les of 1 Event F	iltering 👻	Dynamic State	 Alerting 	Comments *					Policy				2
	indicator-shellcode		GID	SID 1000001	Message -	↓ Itp_sig								•	▼ ⊙ (9 🗰	
	malware-onc malware-other malware-tools netbios					Set rule st	tate for "cu	stom_http_sig" 🕑									
	os-linux os-mobile	•				State Disabled		Ŧ									
	Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific					Generate B Drop and O Disabled	Events Generate Ever	Cancel OK									

Verander de actie van de regel

Klik op de knop Beleidsinformatie en klik op de knop Wijzigingen vastleggen om de wijzigingen op te slaan.



Wijzigingen vastleggen

Stap 5. Associate Inbraakbeleid met Access Control Policy (ACS)-regel

Ga naar Beleid > Toegangsbeheer bij VCC, associeer Inbraakbeleid met ACS.

Leiting Rule ftd_acp			Mandatory @ 🗙
Name ftd_acp	Action 🕒 Allow	U Logging ON Time Rar	nge None V Rule Enabled
	Intrusion Policy	y snort_test x ↓ Default-Set x ↓	V File Policy None V
Q. Zones (2) Networks Ports Ap	pplications 🛕 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 Remove All	Collapse All Remove All
detaile_zone (Routed Security Zone)		ZONE v 1 Object	ZONE V 1 Object

Associatie met de ACS-regeling

Stap 6. Wijzigingen implementeren

Breng de wijzigingen in FTD aan.

Firewall Management Center Policies / Access Control / Policy Editor	Overview Analysis	Policies	Devices	Objects	Integration		Deploy Q Ø 🔅 Ø admin V deale SECUR	ŧE
Return to Access Control Policy Management						۹	Advanced Deploy All Ignore warnings Deploy All Legacy	UI
Packets Prefilter Rules O Decryption	→ 🤣 Security Intelligence →	⊖ Identity →	📀 Access C	ontrol	More	FPR2120_FTD	Ready for Deployment 1 device	e .

Wijzigingen implementeren

Verifiëren

Aangepaste lokale snortregel wordt niet geactiveerd

Stap 1. Inhoud van bestand in HTTP-server instellen

Stel de inhoud van het test.txt bestand op de HTTP server kant in op gebruiker.

Stap 2. Eerste HTTP-aanvraag

Open de HTTP Server (192.168.20.1/test.txt) vanuit de browser van de client (192.168.10.1) en bevestig dat de HTTP-communicatie is toegestaan.

192.168.20.1/test.txt	× +	- 0 ×
\leftrightarrow \rightarrow C \blacksquare	192.168.20.1/test.txt	☆ 🔒 :
user		

Eerste HTTP-aanvraag

Aangepaste lokale snortregel wordt geactiveerd

Stap 1. Inhoud van bestand in HTTP-server instellen

Stel de inhoud van het test.txt bestand op HTTP server kant in op gebruikersnaam.

Stap 2. Eerste HTTP-aanvraag

Open de HTTP Server (192.168.20.1/test.txt) vanuit de browser van de client (192.168.10.1) en bevestig dat de HTTP-communicatie is geblokkeerd.





Eerste HTTP-aanvraag

Stap 3. Inbraakgebeurtenis bevestigen

Navigeren naar Analyse > Inbraakacties > Evenementen op FMC, bevestigen dat de Inbraakgebeurtenis wordt gegenereerd door de Aangepaste lokale Snortregel.

Firewall Management Cen Analysis / Intrusions / Events	ter Overview	Analysis	Policies	Devices	Objects I	integration				Deplo	, Q	0 ¢	Ø adr	nin v ensce SI	CURE
						В	ookmark This Pa	ge Reporting	Dashboard	d View Bo	okmarks	Search	Predefine	d Searches	٣
Events By Priority and Clas	sification (antich w	arkflow)										2024-04-	06 09:41:20	- 2024-04-06 1	1:06:04
Search Constraints (Edit Search Save Se	arch)													Exp	anding
Drilldown of Event, Priority, and Classificat	ion Table View of E	vents Pack	tets												
Jump to															
□ ↓ Time × Priority ×	Impact × Inline Result ×	Reason X	Source IP X	Source x	Destination IP ×	Destination x	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	ULAN x	Messag	pe X		Classification X	Generat
▼ 2024-04-06 11:05:13 low	Unknown Droppe	d	192.168.20.1		192.168.10.	1	80 (http) / tcp	50057 / tcp			custom	_http_sig ((1:1000001:1)	Unknown Traffic	Standan

Inbraakgebeurtenis

Klik op het tabblad Pakketten en bevestig de details van Inbraakgebeurtenis.

Firewall Manage Analysis / Intrusions / E	ement Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin - "the SECURE
	Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches v
Events By Priority	and Classification (antic) montion
	II 2024-04-06 09:41:20 - 2024-04-06 11:07:15 Expanding
Search Constraints (Edit S	Search Save Search)
Drilldown of Event, Priority,	and Classification Table View of Events Packets
 Event Information 	
Message	custom_http_sig (1:100001:1)
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	9 192.168.10.1
Destination Port / ICMP Code	50061 / tcp
HTTP Hostname	192.168.20.1
HTTP URI	/test.txt
Intrusion Policy	r snort_test
Access Control Policy	r acp-rule
Access Control Rule	ftd_acp
Rule	: alert top any 🗛 any any (sid:1000001; gid:1; flow:established.to_client: content:"username"; rambytes; msg:"custom_http_sig"; classtype:unknown; rev:1;)
 Actions 	

Detail van inbraakgebeurtenis

Problemen oplossen

Start de opdrachtsystem support trace om het gedrag op FTD te bevestigen. In dit voorbeeld wordt het HTTP-verkeer geblokkeerd door de IPS-regel (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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.