FTDでSnort2のカスタムローカルSnortルールを 設定する

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
背景説明
ネットワーク図
コンフィギュレーション
<u>ニー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</u>
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
<u>ステップ4:ルールの変更アクション</u>
<u>ステップ 5:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け</u>
<u>手順 6 : 変更の展開</u>
<u>確認</u>
<u>カスタムローカルSnortルールがトリガーされない</u>
<u>ステップ1:HTTPサーバーでのファイルの内容の設定</u>
<u>ステップ 2:初期HTTP要求</u>
<u>カスタムローカルSnortルールがトリガーされる</u>
<u>ステップ1:HTTPサーバーでのファイルの内容の設定</u>
<u>ステップ 2:初期HTTP要求</u>
<u>ステップ3:ConfirmIntrusionイベント</u>
トラブルシュート

はじめに

このドキュメントでは、ファイアウォール脅威対策(FTD)のSnort2でカスタムローカルSnortルールを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center (FMC)
- ファイアウォール脅威対策(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

カスタムローカルSnortルールとは、FTDに統合されているSnort侵入検知および防御システム内 で作成および実装できるユーザ定義ルールを指します。Cisco FTDでカスタムローカルSnortルー ルを作成すると、基本的にSnortエンジンが監視できる新しいパターンまたは一連の条件を定義す ることになります。ネットワークトラフィックがカスタムルールで指定した条件に一致する場合 、Snortはアラートの生成やパケットのドロップなど、ルールで定義されたアクションを実行でき ます。 管理者は、カスタムローカルSnortルールを使用して、一般的なルールセットの対象外で ある特定の脅威に対処します。

このドキュメントでは、特定の文字列(ユーザ名)を含むHTTP応答パケットを検出してドロッ プするように設計されたカスタムローカルSnortルールを設定し、確認する方法を紹介します。



注意:カスタムのローカルSnortルールを作成してサポートすることは、TACのサポート 対象外です。したがって、このドキュメントは参考資料としてのみ使用でき、これらの カスタムルールは独自の裁量と責任で作成および管理してください。

設定

ネットワーク図

このドキュメントでは、この図のSnort2のカスタムローカルSnortルールの設定および検証につい て説明します。



コンフィギュレーション

これは、特定の文字列(ユーザ名)を含むHTTP応答パケットを検出してドロップするカスタム ローカルSnortルールの設定です。

ステップ1:Snortバージョンの確認

FMCでDevices > Device Managementの順に移動し、Deviceタブをクリックします。Snortのバー ジョンがSnort2であることを確認します。

Firewall Management C Devices / Secure Firewall Device	Center Overview Analysis Summary	Policies Devices Objects	Integration	Deploy	Q 📀 ✿ Ø admin ∽ stadius	ECU
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	MP				
General	/±∓	License	1	System	8 G	
Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense	
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	J.VPht 1707U2	
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	based Rules.	Manu	
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%6.25	

Snortバージョン

ステップ2: Snort 2でのカスタムローカルSnortルールの作成

FMCで、Objects > Intrusion Rules > Snort 2 All Rulesの順に移動し、Create Rule ボタンをクリックします。

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Analysis Poli	cies 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				

カスタムルールの作成

カスタムローカルSnortルールに必要な情報を入力します。

- 侵入:custom_http_sig
- アクション:アラート
- ・プロトコル:tcp
- フロー:確立、クライアントへ
- コンテンツ:ユーザ名(未加エデータ)

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🥝 🌣 🚱 admin 🗸 🖏 SECURE
	Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules	
Stot 2 A IR Max Contain Name, Single, Sing	
content Add Option Save As New	

ルールに必要な情報の入力

ステップ3:カスタムローカルSnortルールの確認

FMCでPolicies >Intrusion Policiesの順に移動し、Snort 2 Versionボタンをクリックします。

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	Overview Analysis Policies Devices	Objects Integration Depk	oy Q 🥝 🔅 🖉 admin ~ 付
Intrusion Policies Network Analysis Policies			
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusion Policy, Des	cription, or Base Policy	All IPS Rules IPS	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 🖌 🖬 🔃 🗑

カスタムルールの確認

FMCでRules > Category > localの順に移動し、Custom Local Snort Ruleの詳細を確認します。

Firewall Management Center Policies / Access Control / Intrusion / Edit Polic	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	o 0	0	admin \sim	cisco S	SECURE
Intrusion Policies Network Analysis Policies														
Policy Information Rules														< Back
Cisco Recommendations > Advanced Settings Rule Configura Rule Configura Category	on Filter: Categ	ory:"local"												× 0
Policy Layers Indicator-comp Indicator-comp Indicator-comp Indicator-comp Indicator-comp	ation 0 select	ed rules of 1 ate v Event Fi	Itering 👻 🛛	Dynamic State	 Alerting 	Comments +					Policy			¥
indicator-shello indicator-shello iccall maharate.harket		D SID 1000001	Message 4	p_sig							→	• •	00	-
malware-cnc malware-chois malware-tools netbios	Hide	details									I< <	1] of 1 >	X
os-linux <	> = •	Suppressions (Dynamic State	(0) (0)										Add	
Classifications Microsoft Vuln Microsoft Worn Platform Speci	rabilities > 0 s > 0 c	Alerts (0) Comments (0)										Add S	NMP Alert Add	ų.
Preprocessors Priority Rule Update	~	Documentation	rule	alert top any an	ıy <> any any (sk	:1000001; gid:1; flow:estat	blished,to_client; content:"us	sername"; rawbytes; msg	"custom_	http_sig*;	classtype	unknown; re	v:1;)	

カスタム規則の詳細

ステップ4:ルールの変更アクション

Stateボタンをクリックし、StateをDrop and Generate Eventsに設定して、OKボタンをクリック します。

Firewall Managemen Policies / Access Control / In	nt Center htrusion / Edit Policy	Overview	Analysis	Policies	Devices	Objects	Integration	t.	Deploy C	03	* 0	admin \sim	cisco SE	CURE
Intrusion Policies Network Ar	nalysis Policies													
Policy Information Rules	Rules												<	Back
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Filter: Categ	jory:"local"										>	< 0
> Policy Layers	indicator-compromise indicator-obfuscation indicator-scan indicator-scan	O selec Rule S	ted rules of 1 tate + Event	Filtering v Message	Dynamic State	 Alerting 	Comments +				Policy		T © O	• •
	malware-backdoor malware-cnc		1000001	custom_h	ttp_sig									
	malware-other malware-tools netbios				Set rule s	tate for "cu	stom_http_sig" 🛛							
	os-linux os-mobile Classifications	•			State Disabled	Fuonts	•							
	Microsoft Vulnerabilities Microsoft Worms Platform Specific Promocessors				Drop and Disabled	Generate Even	Cancel OK							

ルールアクションの変更

Policy Informationボタンをクリックし、Commit Changesボタンをクリックして変更を保存します。

Firewall Managemen Policies / Access Control / In	nt Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 💿 🗱 🜒 admin ~ divide SECURE
Intrusion Policies Network Ar	alysis Policies		
Policy Information A Rules	Policy Information		< Back
Cisco Recommendations > Advanced Settings	Drop when Inline		
> Policy Layors	Base Policy Balanced Security and Connectivity The base policy is up to date (Rule Update 2024-04-03-001-v This policy has 9958 enabled rules This policy has exercise exercise	Description of Changes	✓ Manage Base Policy ✓ Manage Rules
	Nor recommendations have been generated. Click here to set up Click	isco recommendations.	◆ View
	This policy contains enabled preprocessor rules. Please read the r	ule documentation to ensure the preprocessors h	ave the correct settings for these rules
			Discard Changes Commit Changes

変更の確定

ステップ 5:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け

FMCでPolicies >Access Controlの順に移動し、侵入ポリシーをACPに関連付けます。

¹ Cditing Rule ftd_acp			Mandatory 🛛 🖉 🗙
Name ftd_acp	Action 🔤 Allow	r 🗸 🖌 Logging ON 🖥 Time F	tange None V Rule Enabled
	Intrusion Polic	y snort_test X V Default-Set X	V File Policy None V
Q Zones (2) Networks Ports Applicat	ions 🛕 Users URLs	Dynamic Attributes VLAN Tags	
Q Bearch Security Zone Objects	Showing 2 out of 2	Selected Sources: 1	Selected Destinations and Applications: 1
inside_zone (Routed Security Zone)		Collapse All Remove A	II Collapse All Remove All
dutside_zone (Routed Security Zone)		ZONE V 1 Object	ZONE V 1 Object
ACPルールとの関連付け			

手順6:変更の展開

変更をFTDに展開します。

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 🔗 🌣 🕢 admin v 🖏	SECURE
Seturn to Access Control Policy Management acp-rule ✓	٩	Advanced Deploy All Genore warnings Deploy All	Legacy UI Save
Packets O Prefitter Rules O Decryption O Security Intelligence O Identity O Access Control O More	FPR2120_FTD	Ready for Deployment	1 device

変更の展開

確認

カスタムローカルSnortルールがトリガーされない

ステップ1:HTTPサーバでのファイル内容の設定

HTTPサーバ側のtest.txtファイルの内容をuserに設定します。

ステップ2:初期HTTP要求

クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、 HTTP通信が許可されていることを確認します。

0	192.168.20.1,	/test.txt	×	+	-	٥	×
÷	\rightarrow G			192.168.20.1/test.txt	☆	Θ	:

user

初期HTTP要求

カスタムローカルSnortルールがトリガーされる

ステップ1:HTTPサーバでのファイル内容の設定

HTTPサーバ側のtest.txtファイルの内容をusernameに設定します。

ステップ2:初期HTTP要求

クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、 HTTP通信がブロックされていることを確認します。

) 192.168.20.1	×	+	-	٥	×
$\leftrightarrow \rightarrow \times$	(i) 192.168.20.1/test	.txt	*	Θ	:



初期HTTP要求

ステップ3:侵入イベントの確認

FMCでAnalysis > Intrusions > Eventsの順に移動し、侵入イベントがカスタムローカルSnortルールによって生成されていることを確認します。

Firewall Manageme Analysis / Intrusions / Even	ent Center	Overview	Analysis	Policies	Devices	Objects Ir	ntegration				Deploy	/ Q	o ¢ (adm adm	in ~ cisco SE	CURE
							В	ookmark This Pa	ge Reporting	Dashboard	d View Bo	okmarks	Search	Predefined	d Searches	¥
Events By Priority an	d Classifie	cation (switch wor	kflow)									п	2024-04-06	6 09:41:20 ·	- 2024-04-06_11	:06:04
Search Constraints (Edit Search)	ch Save Search)														Exp	anding
Drilldown of Event, Priority, and	Classification	Table View of Ev	ents Paci	kets												
Jump to																
Time ×	Priority X Imp	act × Inline Result ×	Reason X	Source IP X	Source x	Destination IP ×	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status ×	ID XLAN x	Messag	10 X		Classification X	Generat
 2024-04-06 11:05:13 	low 0	Unknown Dropped		9 192.168.20.1		9192.168.10.1		80 (http) / tcp	50057 / tcp			custom	_http_sig (1:1	1000001:1)	Unknown Traffic	Standar

侵入イベント

Packetsタブをクリックし、侵入イベントの詳細を確認します。

Firewall Manage Analysis / Intrusions / B	ement Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin v 就 SECURE
	Bookmark This Page Reporting Dashboard View Bookmarks Search Predefined Searches •
Events By Priority	and Classification institution
	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)
Time	2024-04-06 11:06:34
Classification	Unknown Traffic
Priority	r low
Ingress Security Zone	outside_zone
Egress Security Zone	n inside_zone
Device	FPR2120_FTD
Ingress Interface	outside
Egress Interface	n inside
Source IP	9 192.168.20.1
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	/ snort_test
Access Control Policy	r acp-rule
Access Control Rule	ftd_acp
Rule	alert top any any ⇔ any sur (sid:11000001; gid:1; flor:established.to_client; content:"username"; rambytes; mgg:"custom_http_sig"; classtyme:unknown; rev:1;)
 Actions 	

侵入イベントの詳細

トラブルシュート

system support traceコマンドを実行して、FTDの動作を確認します。この例では、HTTPトラフィックはIPSルール(gid 1、sid 1000001)によってブロックされています。

<#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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。