FDMによるAMPファイルポリシーの設定および テスト

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>		
<u>手順</u>		
ライセンス		
<u>コンフィギュレーション</u>		
<u>テスト</u>		
<u>トラブルシューティング</u>		

はじめに

このドキュメントでは、Firepower Device Manager(FDM)を使用して高度なマルウェア防御 (AMP)ファイルポリシーを設定およびテストする方法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。

- Firepower Device Manager (FDM)
- Firepower Threat Defense (FTD)

使用するコンポーネント

- FDMで管理されるCisco仮想FTDバージョン7.0
- 評価ライセンス(評価ライセンスはデモ目的で使用されます。有効なライセンスを取得して 使用することを推奨します)

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。

手順

1. マルウェアライセンスを有効にするには、FDM GUIのDEVICEページに移動します。

uluilu cisco.	Firepower Device Manager	MONITORING	POLICIES	OBJECTS	DEVICE: FTD	0	(0?	0	admin Administrator	@ ~

FDMデバイス・タブ

o

2. Smart Licenseというラベルの付いたボックスを見つけ、View Configurationをクリックします

Site to Site VPN There are no connections yet		Remote Access VPN Requires RA VPN license No connections 1 Group Policy		Advanced Configuration Includes: FlexConfig, Smart CLI		Device Administration Audit Events, Deployment History, Download Configuration	
View Configuration	>	View Configuration	>	REQUEST FILE TO BE CREATED		Traffic Settings URL Filtering Preferences	
Smart License Evaluation expires in 89 days	89 DATS	Backup and Restore		Troubleshoot No files created yet		Management Interface Hostname NTP Cloud Services	
7 Enabled	>	View Configuration	>	Security Intelligence Feeds View Configuration	>	Logging Settings DHCP Server DNS Server	
Interface	7 9	Routing 1 route		Updates Geolocation, Rule, VDB, System Upgrad	de,	System Settings Management Access	

FDMデバイス・ページ

3. Malwareというラベルの付いたライセンスを有効にします。

R Enabled				
Chabied				
This License allows	you to perform Cisco Ad	vanced Malware Pro	tection (AMP) v	ith AMP for
Firepower and AMP	Threat Grid. You must ha	we this license to ap	ply file policies	that detect
and block malware in	1 files transmitted over y	our network.		
Includes: Co File De	lieu			
includes: 📲 File Po	ncy			

コンフィギュレーション

1. FDMで「ポリシー」ページにナビゲートします。

،۱۱،۱۱،۱ cisco	Firepower Device Manager	MONITORING	POLICIES	OBJECTS	DEVICE: FTD

FDMポリシー・タブ

2. セキュリティポリシーで、アクセスコントロールセクションに移動します。

Manager	MONITORING	POLICIES	OBJECTS	DEVICE: FTD		6) 🖨	0	?	admin Administrator	2)~
🛷 Securi	ty Policies											
$\square \ \rightarrow$	SSL Decryption	\rightarrow O Identity	🗸 $ ightarrow$ Secu	urity Intelligence $ ightarrow$	NAT \rightarrow Access Control	ightarrow Intrus	on					
5 rules					Q s	earch					<u>)</u>	+

FDMの「アクセス制御」タブ

3. ファイルポリシーを設定するアクセスルールを検索または作成します。Access Ruleエディタ をクリックします。アクセスルールの作成方法については、この<u>リンク</u>を参照してください<u>。</u>

Man	ager	MON	ITORING	POLICIES	OBJECTS	DEVICE: FTD				0	2	adm Adm	n in ninistrator	② ~
¢	d S	ecurity Pol	icies											
	민	\rightarrow () SSL	Decryptior	ightarrow $ ightarrow$ Ident	ity $ ightarrow$ 🕑 Se	curity Intelligence	ightarrow NAT	→ 🖌 Access	Control $ ightarrow$	Intrusion				
5	rules								Q Search				0	+
1				SOURCE			DESTINATION							
	н	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
	> 1	Inside_Outside	€	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	🗣 D_	00
			Allow											Edit

FDMアクセス制御規則

4. Access RuleにあるFile Policyセクションをクリックして、ドロップダウンから必要なFile Policyオプションを選択します。OKをクリックして、ルールの変更を保存します。

Edit Access Rule	0 ×
Order Title Acting Inside_Outside_Rule Source/Destination Applications URLs Users Internation	Allow File policy Logging
Evaluation Period This feature needs a license to be purchased. For more details, go to Smart Like SELECT THE FILE POLICY Block Malware All None Block Malware All Cloud Lookup All Block Office Document and PDF Upload, Block Malware Others Block Office Documents Upload, Block Malware Others	Icense. Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware
Show Diagram	CANCEL

FDMの「アクセス制御規則ファイル・ポリシー」タブ

5. ファイルポリシーアイコンが有効になっているかどうかをチェックして、ファイルポリシーが アクセスルールに適用されていることを確認します。

ファイル

	> 1	Inside_Outside	€	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	§ 🗣 🖉 🔁
ファ			Allow										Block Malware All
イル	ポリ	シーアイコ	コンが	「有効									

6.変更内容を保存して管理対象デバイスに展開します。

テスト

マルウェア防御のために設定されたファイルポリシーが機能していることを確認するには、次の テストシナリオを使用して、エンドホストのWebブラウザからマルウェアテストファイルをダウ ンロードします。

次のスクリーンショットに示されているように、Webブラウザからマルウェアテストファイルを ダウンロードしようとしても失敗します。

6			Problem loading page — Mozilla Firefox			~	-	• ×
	Problem loading	g page 🛛 🗙	+					\sim
~	→ C	① 10.122	149.2:8080/eicar/eicar_com.zip	\$	0	\pm	Û	=
•								
	The	connec	tion was reset					
	The co	nnection t	o the server was reset while the page was lo	ading.				
	• The	site could b	e temporarily unavailable or too busy. Try again in	a few moments.				
	- If yo	ou are unab	e to load any pages, check your computer's networ	rk connection.	in a state			
	• If you to a	ccess the w	r or network is protected by a firewall or proxy, mai eb.	ke sure that Firefox is perm	tted			
					in .			
				Try Aga	un _			

ブラウザのダウンロードテスト

FTD CLIのシステムサポートトレースに、ファイルのダウンロードがファイルプロセスによって ブロックされたことが示されます。FTD CLIを使用してシステムサポートトレースを実行する方 法については、この<u>リンク</u>を参照してください。

192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ===> Blocked by File Process
vardict reason is sent to DAD

システムサポートトレーステスト

これにより、ファイルポリシー設定がマルウェアのブロックに成功したことが確認されます。

トラブルシューティング

上記の設定を使用したときにマルウェアが正常にブロックされない場合は、次のトラブルシュー ティングの提案を参照してください。

1. マルウェアライセンスが期限切れでないことを確認します。

2. アクセスコントロールルールが正しいトラフィックを対象としていることを確認します。

3. 選択したファイルポリシーオプションがターゲットトラフィックに対して正しいこと、および マルウェア防御を希望していることを確認します。

それでも問題を解決できない場合は、Cisco TACにサポートを依頼してください。

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。