透過FDM設定和測試AMP檔案原則

目錄

<u>簡介</u>		
<u>必要條件</u>		
<u>需求</u>		
採用元件		
<u>說明</u>		
<u>授權</u>		
<u>組態</u>		
<u>測試</u>		
<u>疑難排解</u>		

簡介

本文檔介紹如何透過Firepower裝置管理器(FDM)配置和測試高級惡意軟體防護(AMP)檔案策略。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower裝置管理器(FDM)
- Firepower Threat Defense (FTD)

採用元件

- 透過FDM管理的Cisco虛擬FTD 7.0版
- 評估許可證(評估許可證用於演示目的。思科建議獲取並使用有效的許可證)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

說明

授權

1. 要啟用惡意軟體許可證,請導航到FDM GUI上的DEVICE頁。

CISCO., Firepower Device Manager MONITORING POLICIES OBJECTS DEVICE: FTD

2. 找到標籤為Smart License的框,然後按一下View Configuration。

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

FDM裝置頁面

3. 啟用標籤為Malware的許可證。



組態

1. 導覽至FDM上的POLICIES頁面。



FDM原則標籤

2. 在安全策略下, 導航到訪問控制部分。

Manager MONITORING POLICIES OBJECTS DEVICE: FTD	admin Administrator
$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \bigcirc$ Identity $\rightarrow \oslash$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \oslash$ Access Control \rightarrow Intrusion	
5 rules Q Search	<u></u>

FDM存取控制標籤

3. 查詢或建立訪問規則以配置檔案策略。點選訪問規則編輯器。有關如何建立訪問規則的說明,請 參閱此<u>連結。</u>

Manage	r MON	IITORING	POLICIES	OBJECTS	DEVICE: FTD				⊙ (3 🔊 (admin Admin	n nistrator	② ~
ø S	Security Pol	icies											
P	$1 \rightarrow \bigcirc SSL$	Decryptior	$n \rightarrow \bigcirc$ Ident	ity $ ightarrow$ 📀 Se	curity Intelligence	ightarrow NAT	→ 🖌 Access	Control $ ightarrow$	Intrusion				
5 rules	5 rules Q Search Q in +												
			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	🗞 C.,	00
		Allow											Edit

FDM存取控制規則

4. 按一下訪問規則上的檔案策略部分,然後從下拉選單中選擇首選的檔案策略選項。按一下OK以儲 存對規則的更改。

Edit Access Rule				8	×
Order Title 1 Inside_Outside_Rule Source/Destination Applications URLs	Action Allow	File policy 0	Logging		
Evaluation Period This feature needs a license to be purchased. For more details, go to Sm 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	art License.	CONTROLLING FI Use file policies to or Malware Protection policies to perform regardless of wheth	ILES AND MALWARE detect malicious software, or malware, using Adva for Firepower (AMP for Firepower.) You can also u file control, which allows control over all files of a s her the files contain malware	nced ise file specific t	уре

ОК

5. 透過檢查檔案策略圖示是否已啟用,確認已將檔案策略應用於訪問規則。

檔案



件策略圖示已啟用

6.儲存並部署更改到受管裝置。

測試

要驗證用於惡意軟體防護的配置檔案策略是否有效,請使用以下測試方案嘗試從終端主機的Web瀏 覽器下載惡意軟體測試檔案。

如螢幕截圖所示,嘗試從Web瀏覽器下載惡意軟體測試檔案失敗。



從FTD CLI中,系統支援追蹤顯示檔案下載被檔案程式封鎖。有關如何透過FTD CLI運行系統支援跟 蹤的說明,請參閱此<u>連結</u>。

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 FTFE Process: drop /e1car/e1car_com.21p
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 O Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 85 1 1 0 deleting firmall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Smort 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
Verdict reason is sent to DAQ

系統支援追蹤測試

這確認檔案策略配置成功阻止了惡意軟體。

疑難排解

如果在使用以前的配置時惡意軟體未被成功阻止,請參閱以下故障排除建議:

1. 驗證惡意軟體許可證未過期。

2. 確認訪問控制規則的目標流量是否正確。

3. 確認選定的檔案策略選項對於目標流量和所需惡意軟體防護是正確的。

如果問題仍無法解決,請與Cisco TAC聯絡以獲取其他支援。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。