使用ASDM配置FirePOWER模組用於網路AMP或 檔案控制。

目錄

 簡介

 必要條件

 需求

 採用元件

 背景資訊

 為檔案控制/網路AMP配置檔案策略

 配置檔案訪問控制

 配置網路惡意軟體防護(網路AMP)

 為檔案策略配置訪問控制策略

 部署訪問控制策略

 監視檔案策略事件的連線

 驗證

 疑難排解

 相關資訊

簡介

本檔案介紹FirePOWER模組的網路進階惡意軟體防護(AMP)/檔案存取控制功能,以及使用調適型 安全裝置管理員(ASDM)設定這些功能的方法。

必要條件

需求

思科建議您瞭解以下主題:

- 自適應安全裝置(ASA)防火牆和ASDM知識。
- FirePOWER裝置知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 運行軟體版本5.4.1及更高版本的ASA Firepower模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。
- 運行軟體版本6.0.0及更高版本的ASA Firepower模組(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。
- ASDM 7.5.1及更高版本。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

惡意軟體/惡意軟體可以通過多種方式進入組織的網路。為了識別並緩解此惡意軟體和惡意軟體的影 響,FirePOWER的AMP功能可用於檢測並阻止惡意軟體和惡意軟體在網路中的傳輸。

使用檔案控制功能,您可以選擇監控(檢測)、阻止或允許檔案上傳和下載的傳輸。例如,可以實施阻止使用者下載執行檔的檔案策略。

利用網路AMP功能,您可以選擇希望通過常用協定監控的檔案型別,並將SHA 256雜湊、檔案中的 後設資料,甚至檔案本身的副本傳送到思科安全情報雲進行惡意軟體分析。根據檔案分析,雲會將 檔案雜湊的性質返回為乾淨或惡意。

檔案控制和面向Firepower的AMP可以配置為檔案策略,並用作整體訪問控制配置的一部分。與訪 問控制規則關聯的檔案策略檢查滿足規則條件的網路流量。

附註:確保FirePOWER模組具有保護/控制/惡意軟體許可證,以便配置此功能。若要驗證許可 證,請選擇Configuration > ASA FirePOWER Configuration > License。

為檔案控制/網路AMP配置檔案策略

配置檔案訪問控制

登入到ASDM並選擇Configuration > ASA Firepower Configuration > Policies > Files。此時將顯示 New File Policy對話方塊。

輸入新策略的名稱和可選說明,然後按一下**儲存ASA Firepower更改**選項。系統將顯示File Policy Rule頁面。

ASA FirePOWER Configur 🗗 🗜	Configuration > A9	5A FirePOWER Con	figuration > Policies > Files			
Policies	-	_			and correct	
Access Control Policy Intrusion Policy					Compare Policies	v File Policy
🔁 Files	-					
SSL	File Policy	New File Po	licy	? ×	ed	
Identity Policy		Name	File_Access_Control		Add a new policy	
Object Management Object Management Local Object Management Object		Store A	SA FirePOWER Changes	ancel		

按一下Add File Rule以將規則新增到檔案策略。檔案規則使您可以精細控制要記錄、阻止或掃描惡 意軟體的檔案型別。

應用協定: 將應用協定指定為Any(預設)或特定協定(HTTP、SMTP、IMAP、POP3、FTP、 SMB)。

傳輸方向:指定檔案傳輸的方向。根據應用協定,可以是Any或Upload/Download。您可以檢查檔 案下載的通訊協定(HTTP、IMAP、POP3、FTP、SMB)和檔案上傳的通訊協定(HTTP、SMTP、 FTP、SMB)。使用**Any**選項可檢測通過多個應用程式協定的檔案,而不管使用者是傳送還是接收檔案。

Action:指定檔案訪問控制功能的操作。操作可以是Detect Files或Block Files。Detect File操作將生成事件,而Block Files操作將生成事件並阻止檔案傳輸。使用Block Files 操作,可以選擇選擇Reset Connection以終止連線。

File Type Categories:選擇要阻止檔案或生成警報的檔案型別類別。

檔案型別:選擇檔案型別。「檔案型別」選項提供了更精細的選項來選擇特定的檔案型別。

選擇Store ASA Firepower Changes選項以儲存配置。

Application Protocol	Any	Action 🗙 Block Files	v		
Direction of Transfer	Any	▼			
ile Type Categories	20	File Types		Selected File Categories and Types	6
 Archive Multimedia Executables PDF files Encoded Graphics System files 	18 30 11 2 2 6 12	All types in selected Categories Image: TZ (7-Zip compressed file) Image: TZ (7-Zip compressed file) Image: ACCDB (Microsoft Access 2007 file) Image: AMF (Advanced Module Format for digita) Image: AMF (Advanced Module Format for digita) <tr< td=""><td>Add</td><td>Category: Archive</td><td></td></tr<>	Add	Category: Archive	

配置網路惡意軟體防護(網路AMP)

登入到ASDM並導航到Configuration > ASA Firepower Configuration > Policies > Files。 系統將顯示File Policy頁面。現在,按一下「新建檔案策略」(New File Policy)對話方塊。

輸入新策略的Name和可選的Description,然後按一下Store ASA Firepower Changes選項。系統將 顯示File Policy Rules頁面。

ASA FirePOWER Configur 🗗 🕴	Configuration > ASA Fire	POWER Configurat	ion > Policies > Files		
Policies Access Control Policy Ontrol Policy Ontrol Policy Ontrol Policy Ontrol Policy Ontrol Policy SSL	Default SSL SSL Policy	Policy			
Actions Alerts Identity Policy DNS Policy Double Management Cocal Cocal Configuration	File_Policy File_Access_Contro Network file Access C	New File Polic Name Description	Cy // Network_Malware_Protection Network AMP	? ×	Compare Policies New File Policy
Information	including the Access of	Store ASA	FirePOWER Changes Cancel		

按一下Add File Rule選項將規則新增到檔案策略。檔案規則使您可以精細控制要記錄、阻止或掃描 惡意軟體的檔案型別。

```
應用協定:指定Any(預設)或特定協定(HTTP、SMTP、IMAP、POP3、FTP、SMB)
```

傳輸方向:指定檔案傳輸的方向。它可以是Any或根據應用協定上傳/下載。您可以檢查檔案下載的 通訊協定(HTTP、IMAP、POP3、FTP、SMB)和檔案上傳的通訊協定(HTTP、SMTP、FTP、 SMB)。使用Any選項可檢測通過多個應用程式協定的檔案,無論使用者傳送或接收檔案。

Action:對於網路惡意軟體防護功能,操作可以是**惡意軟體雲查詢**或**阻止惡意軟體。**操作**惡意軟體雲** 查詢僅生成事件,而操作**阻止惡意軟體**生成事件並阻止惡意軟體檔案傳輸。

附註: Malware Cloud Lookup 和Block Malware 規則允許Firepower計算SHA-256雜湊並將其 傳送到雲查詢過程,以確定通過網路傳輸的檔案是否包含惡意軟體。

檔案型別類別:選擇特定的檔案類別。

檔案型別: 選擇特定的檔案型別以獲得更精細的檔案型別。

選擇Store ASA Firepower Changes選項以儲存配置。

pplication Protocol	Any	 Action Block Malware 		
irection of Transfer	Any	▼		
le Type Categories		File Types	Selected File Categories and Type	25
Office Documents	16	Search name and description	Category: PDF files	6
Archive	17	All types in selected Categories	Category: Executables	6
Multimedia	2	TT (7-7in compressed file)	Category: Archive	6
Executables	7	ARI (Compressed archive file)		
PDF files	1	BINARY DATA (Universal Binary/Java By	Add	
	0	BINERY (Macintosh BinHey 4 Compresse		
Encoded	0	BIT (heir 2 compressed analyse)		
EncodedGraphics	U	E DZ (DZIPZ compressed archive)		
 Encoded Graphics System files 	2			
 Encoded Graphics System files 	2	CPIO_CRC (Archive created with the cpio		

附註:檔案策略按以下規則操作順序處理檔案:攔截優先於惡意軟體檢查,後者優先於簡單的 檢測和記錄。

如果您配置基於網路的高級惡意軟體防護(AMP),並且Cisco Cloud錯誤地檢測到檔案的處置情況 ,則可以使用SHA-256雜湊值將檔案新增到檔案清單,以提高將來檢測檔案處置情況的效果。根據 檔案清單的型別,您可以執行以下操作:

要將檔案視為雲分配了乾淨處置,請將該檔案新增到乾淨清單。

•要將檔案視為雲分配了惡意軟體性質,請將檔案新增到自定義清單中。

要配置此配置,請導航到Configuration > ASA FirePOWER Configuration > Object Management > File List,然後編輯清單以新增SHA-256。

ASA FirePOWER Configur 리 무	Configuration > ASA FirePOWER Configurat	ion > Object Management > FileList		
Device Management			Silter	
Object Management Object Management	Name	Number of Entries		
Port Security Zones	Clean-List	0		Ø 🗄
Application Filters	Custom-Detection-List	2		00
Individual Objects Object Groups GeoLocation Variable Set Variable Variable Variable Variable Variable Variable Variable Variable Variable Variable				

為檔案策略配置訪問控制策略

導航到Configuration > ASA Firepower Configuration > Policies > Access Control Policy,然後建立 新的Access rule或編輯現有的Access Rule,如下圖所示。

要配置檔案策略,操作應為Allow。導航到Inspection頁籤,然後從下拉選單中選擇File Policy。

要啟用日誌記錄,請導航logging選項,然後選擇適當的日誌記錄選項和**日誌檔案**選項。按一下 Save/Add按鈕儲存配置。

選擇Store ASA Firepower Changes選項以儲存AC策略更改。

Logging: files: Event Viewer
Inspection Logging Comm

部署訪問控制策略

導航到ASDM的**Deploy**選項,然後從下拉選單中選擇**Deploy Firepower Change**選項。按一下 **Deploy**選項部署更改。

Access Control Policy: Default Allow All Traffic	
Intrusion Policy: Balanced Security and Connectivity	
Intrusion Policy: No Rules Active	
Intrusion Policy: IPS_Policy	
U	
U System Policy: Default	
Sensor Policy: firepower	

導航到監控> ASA Firepower監控>任務狀態。確保任務必須完成才能應用配置更改。

附註:在5.4.x版本中,要將訪問策略應用到感測器,需要按一下**Apply ASA FirePOWER Changes**。

監視檔案策略事件的連線

要檢視由與檔案策略相關的Firepower模組生成的事件,請導航到**Monitoring > ASA Firepower** Monitoring > Real Time Eventing。

e Eventing							
All ASA FirePOWER Even	nts Connection In	trusion File Malware File	Security Intelligence				
lter							
Reason=File Monitor 🗱							
Refresh R	ate 5 seconds	• 1/7/16 12:06:30) PM (IST)				±Ш
Receive Times							
	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	s
1/6/16 1:29:48 PM	Action	First Packet 1/6/16 11:38:29 AM	Last Packet 1/6/16 1:26:46 PM	Reason File Monitor	Initiator IP 192.168.20.3	Responder IP 10.76.76.160	6
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM	Action Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM	Reason File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50	6
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM 1/5/16 9:22:57 PM	Allow Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM 1/5/16 9:16:21 PM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM 1/5/16 9:22:56 PM	Reason File Monitor File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50 46.43.34.31	5 5
1/6/16 1:29:48 PM 1/6/16 2:21:23 AM 1/5/16 9:22:57 PM 1/5/16 9:21:27 PM	Action Allow Allow Allow Allow	First Packet 1/6/16 11:38:29 AM 1/6/16 2:16:47 AM 1/5/16 9:16:21 PM 1/5/16 9:15:15 PM	Last Packet 1/6/16 1:26:46 PM 1/6/16 2:18:21 AM 1/5/16 9:22:56 PM 1/5/16 9:21:26 PM	Reason File Monitor File Monitor File Monitor File Monitor	Initiator IP 192.168.20.3 192.168.20.3 192.168.20.3 192.168.20.3 192.168.20.3	Responder IP 10.76.76.160 13.107.4.50 46.43.34.31 46.43.34.31	€ 5 5

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

確保檔案策略已正確配置為協定/方向/操作/檔案型別。 確保訪問規則中包含正確的檔案策略。

確保訪問控制策略部署成功完成。

監控連線事件和檔案事件(Monitoring > ASA Firepower Monitoring > Real Time Eventing),驗證流 量是否達到正確的規則。

相關資訊

• 技術支援與文件 - Cisco Systems