配置FireSIGHT系統以將警報傳送到外部系統日誌 伺服器

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>傳送入侵警報</u> <u>傳送運行狀況警報</u> <u>第1部分:建立系統日誌警報</u> <u>第2部分:建立運行狀況監視器警報</u> 傳送影響標誌、發現事件和惡意軟體警報

簡介

儘管FireSIGHT系統在其Web介面內提供了各種事件檢視,但您可能希望配置外部事件通知以促進 對關鍵系統的持續監控。您可以將FireSIGHT系統配置為生成警報,在生成以下任一警報時通過電 子郵件、SNMP陷阱或系統日誌通知您。本文描述如何配置FireSIGHT管理中心以在外部系統日誌 伺服器上傳送警報。

必要條件

需求

思科建議您瞭解系統日誌和FireSIGHT管理中心。此外,防火牆中必須允許系統日誌埠(預設為 514)。

採用元件

本檔案中的資訊是根據軟體版本5.2或更新版本。

注意:本文中的資訊是根據特定實驗室環境內的裝置所建立,並使用已清除(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。

傳送入侵警報

1.登入到FireSIGHT管理中心的Web使用者介面。

2.導航至Policies > Intrusion > Intrusion Policy。

3.按一下要應用的策略旁邊的編輯。

4.按一下Advanced Settings。

5.在清單中找到Syslog Alerting,並將其設定為Enabled。

Overview Analysis Policie	es Devices Objects FireAMP	Healt	h System Help v admin v
Access Control Intrusion > In	ntrusion Policy Network Discovery	Application Detectors Files Users	Correlation Actions •
Edit Policy			
Policy Information	Advanced Settings		< Back
Variables	V Performance Settings		
Rules	Event Queue Configuration	Enabled Opicabled	/ Edit
FireSIGHT Recommendations	Even queue composition	Chabled Obsabled	e une
 Advanced Settings 	Latency-Based Packet Handling	Enabled O Enabled Disabled	
Policy Layers	Latency-Based Rule Handling	C Enabled 📀 Disabled	
	Performance Statistics Configuration	Enabled Disabled	🥔 Edit
	Regular Expression Limits	Enabled Oisabled	🥖 Edit
	Rule Processing Configuration	Enabled Oisabled	🥜 Edit
	🐨 External Responses		0
	SNMP Alerting	🗌 Enabled 🛛 🙆 Disabled	=
	Syslog Alerting	Enabled Oisabled	🥖 Edit 🗸

6.按一下Syslog Alerting右側的Edit。

7.在Logging Hosts欄位中鍵入系統日誌伺服器的IP地址。

8.從下拉選單中選擇適當的Facility和Severity。除非將系統日誌伺服器配置為接受特定設施或嚴重性的警報,否則可以將這些警報保留為預設值。

Overview Analysis Policies	Devices Objects FireAMP		Health	System Hel	o ▼ admin ▼
Access Control Intrusion > Int	rusion Policy Network Discovery	Application Detectors Files	Users	Correlation	Actions •
Edit Policy					
Policy Information	Syslog Alerting				< Back
Variables	Settings				
Rules	Leasing Marte	(Classia ID address a		a sector of Hark's	
FireSIGHT Recommendations	Logging Hosts	(Single IP address o	r comma-seg	parated list)	
Advanced Settings	Facility AUTH V				
Back Orifice Detection	Priority EMERG V				
Checksum Verification					
DCE/RPC Configuration		Revert to Defaults			
DNS Configuration					
Event Queue Configuratio					
FTP and Telnet Configurat					
Global Rule Thresholding					
GTP Command Channel C					

9.按一下此螢幕左上角附近的Policy Information。

10.按一下Commit Changes按鈕。

11.重新應用入侵策略。

附註:為了生成警報,請在訪問控制規則中使用此入侵策略。 如果未配置訪問控制規則,則 將此入侵策略設定為用作訪問控制策略的預設操作,然後重新應用訪問控制策略。

現在,如果在該策略上觸發了入侵事件,則還會向在入侵策略上配置的系統日誌伺服器傳送警報。

傳送運行狀況警報

第1部分: 建立系統日誌警報

1.登入到FireSIGHT管理中心的Web使用者介面。

2.定位至**策略>操作>預警**。

Overview	v Ana	lysis	Polici	es C	Devices	Ob	jects	F	ireAMP			Hea	alth	System	Help 🔻	admin 🔻
Access Cor	ccess Control Intrusion • Files		Net	Network Discovery			Application Detectors			Users Co		lation	Actions + Alerts			
					Po	licies	Rule Ed	litor	White List	Traffic Profiles	Alerts	Remedi	iations	Groups	Health Mor	itor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts					s	Advanced Malware Protection Alerts										
														0	Create Aler	t•
Name											Тур	pe	Int	Use	Enabled	

3.選擇Web介面右側的Create Alert。



4.按一下Create Syslog Alert。系統將顯示配置彈出視窗。

5.提供預警的名稱。

6.在**主機**欄位中填寫系統日誌伺服器的IP地址。

7.如果需要,更改系統日誌伺服器的埠(預設埠為514)。

8.選擇適當的Facility和Severity。

Create Syslog	Alert Configuration		?	×
Name]
Host]
Port	514]
Facility	ALERT		;)
Severity	ALERT		\$)
Tag				
		Save	Cancel	

9.按一下Save按鈕。您將返回Policies > Actions > Alerts頁。

10.啟用系統日誌配置。



第2部分: 建立運行狀況監視器警報

以下說明描述了配置健康監控警報的步驟,該警報使用您剛剛建立的系統日誌警報(在上一節中):

1.轉至Policies > Actions > Alerts頁,然後選擇Health Monitor Alerts,該頁位於頁面頂部。

Overview	v Anal	ysis	Policie	s De	vices	Obj	jects F	ireAMP			Health	System	Help 🔻	admin 🔻
Access Co	ccess Control Intrusion • File		Files	les Network Discovery		Application Detectors		Users Cor		relation	Actions + Alerts			
					Poli	cies	Rule Editor	White List	Traffic Profiles	Alerts	Remediatio	ns Groups	Health Mon	itor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts					Advanced Malware Protection Alerts									
												0	Create Aler	t •
Name										Тур	e I	n Use	Enabled	

2.為健康警報命名。

3.選擇Severity(按住CTRL鍵的同時按一下可用來選擇多個嚴重性型別)。

4.在**Module**列中,選擇要向其傳送警報的系統日誌伺服器的運行狀況模組(例如,磁碟使用情況)。

5.從Alerts列中選擇以前建立的syslog警報。

6.按一下Save按鈕。

傳送影響標誌、發現事件和惡意軟體警報

您還可以配置FireSIGHT管理中心,以便針對具有特定影響標誌、特定型別的發現事件和惡意軟體 事件的事件傳送系統日誌警報。為此,您必須執行<u>第1部分:建立系統日誌</u>警報,然後配置要傳送到 系統日誌伺服器的事件型別。為此,您可以導航到Policies > Actions > Alerts頁,然後選擇所需警報 型別的頁籤。

Overview	Analysis	Polici	es Dev	vices Ot	ojects I	FireAMP			Health	System	Help 🔻	admin 🔻
Access Co	ss Control Intrusion • Files		Network	Network Discovery		Application Detectors		ers Cor	relation	Actions + Alerts		
				Policies	Rule Editor	White List	Traffic Profiles	Alerts	Remediation	s Groups	Health Moni	itor Alerts
Alerts	erts Impact Flag Alerts Discovery Event Alerts				Advance	ed Malware P						
										٥	Create Alert	•
Name								Тур	e Ir	1 Use	Enabled	

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)。