使用ASDM(機箱內管理)配置系統/流量事件的 Firepower模組日誌記錄

目錄

簡介 必要條件 需求 採用元件 背景資訊 設定 配置輸出目標 步驟1.系統日誌伺服器配置 步驟2.SNMP伺服器配置 用於傳送流量事件的配置 為連線事件啟用外部日誌記錄 為入侵事件啟用外部日誌記錄 為IP安全情報/DNS安全情報/URL安全情報啟用外部日誌記錄 為SSL事件啟用外部日誌記錄 用於傳送系統事件的配置 為系統事件啟用外部日誌記錄 驗證 疑難排解 相關資訊 相關思科支援社群討論

簡介

本檔案介紹Firepower模組的系統/流量事件以及將這些事件傳送到外部日誌記錄伺服器的各種方法。

必要條件

需求

思科建議您瞭解以下主題:

- ASA(自適應安全裝置)防火牆、ASDM(自適應安全裝置管理器)知識。
- Firepower裝置知識。
- •系統日誌、SNMP協定知識。

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

事件型別

Firepower模組事件可以分為兩種型別:-

- 1. 流量事件(連線事件/入侵事件/安全情報事件/SSL事件/惡意軟體/檔案事件)。
- 2. 系統事件(Firepower作業系統(OS)事件)。

設定

配置輸出目標

步驟1.系統日誌伺服器配置

要為通訊事件配置系統日誌伺服器,請導航到Configuration > ASA Firepower Configuration > Policies > Actions Alerts,然後點選Create Alert下拉選單並選擇Create Syslog Alert**選項。**輸入系 統日誌伺服器的值。

名稱:指定唯一標識系統日誌伺服器的名稱。

主機:指定Syslog伺服器的IP地址/主機名。

連接埠:指定系統日誌伺服器的埠號。

設施: 選擇系統日志伺服器上配置的任何設施。

嚴重性: 選擇系統日誌伺服器上配置的任意嚴重性。

標籤: 指定要與系統日誌消息一起顯示的標籤名稱。

Gisco ASDM 7.5(2) for ASA - 192.168	3.20.1				1.1		• •
File View Tools Wizards Windo	ow Help			Type topic to sear	th	Go	aha
Home Sconfiguration Mor	itoring 🔚 Deploy 👻 🔇	Refresh 🕜 Ba	ick 🔘 Forward 🛛 🦓 Help			CIS	co
Device List Bookmarks	Configuration > ASA Fire	POWER Configura	tion > Policies > Actions Alerts				
Device List 🗇 🕂 🗡							
💠 Add 📋 Delete 🚿 Connect	Alerts						
Find: Go					0	Create Alert	-
	Name			Туре	In Use	Enabled	
ASA FirePOWER Configur 🗗 🕂							
Policies		Edit Syslog	Alert Configuration		? X		
Access Control Policy		Name	Durke Conver		_		
		Name	Syslog_Server		- 10		
Rule Editor		Host	192.168.20.3				
SSL		Port	514				
Actions Alerts		Facility	ALERT		T		
DNS Policy		Severity			•		
Device Management		Severity	PEEN				
		Tag			_		
Device Setup							
Firewall			Store ASA FirePO	WER Changes Ca	incel		

步驟2.SNMP伺服器配置

要為流量事件配置SNMP陷阱伺服器,請導航到ASDM Configuration > ASA Firepower Configuration > Policies > Actions Alerts,然後點選Create Alert下拉選單並選擇Create SNMP Alert**選項。**

名稱:指定唯一標識SNMP陷阱伺服器的名稱。

陷阱伺服器: 指定SNMP陷阱伺服器的IP地址/主機名。

版本: Firepower模組支援SNMP v1/v2/v3。從下拉選單中選擇SNMP版本。

社群字串: 如果您選擇v1或v2 in Version 選項,請指定SNMP社群名稱。

使用者名稱:如果在Version選項中選擇v3,系統將提示User Name欄位。指定使用者名稱。

驗證: 此選項是SNMP v3配置的一部分。它提供基於雜湊的身份驗證

演算法使用MD5或SHA演算法。在Protocol下拉選單中,選擇雜湊演算法並輸入

Password 選項中的密碼。如果不希望使用此功能,請選擇None選項。

隱私:此選項是SNMP v3配置的一部分。它使用DES演算法提供加密。在**Protocol**下拉選單中,選擇 選項作為**DES**,並在**Password**欄位中輸入密碼。如果您不想使用資料加密功能,請選擇None選項 。

Alerts	ç					
	Edit SNMP A	ert Configuration SNMP Version V1/V2	? ×	•	Create Alert	×
Name	Name	SNMP_SERVER_1		Use	Enabled	
Syslog_Server	Trap Server	192.168.20.4		t Used		0
	Version	v2	T			
	Community String	Secret				
		Share ASA SizeDOWED Chapters	Cancel			
			Cancer			
Alerts						
	Edit SNMP A	ert Configuration SNMP Version V3	? X	•	Create Alert	•
Name	Name	SNMP_SERVER_1		Use	Enabled	
Syslog_Server	Trap Server	192.168.20.4		t Used		Ø 🖯
	Version	v3	T			
	User Name	user1				
	Authenticatio	'n				
	Protocol	MD5	•			
	Password	•••••				
	Privacy					
	Protocol	DES	T			
	Password	•••••				
	Engine ID	Example: 123456789a				
		Store ASA FirePOWER Changes				

用於傳送流量事件的配置

為連線事件啟用外部日誌記錄

當流量到達已啟用日誌記錄的訪問規則時,會生成連線事件。要為連線事件啟用外部日誌記錄,請 導航到(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy)編 輯訪問規**則**,然後導航到logging選項。

選擇日誌記錄選項**:在連線的開始和結束處**記錄**,或在連線結束時記錄**。導航到**將連線事件傳送到** 選項,並指定將事件傳送到何處。

若要將事件傳送到外部Syslog伺服器,請選擇**Syslog**,然後從下拉選單中選擇Syslog警報響應。或 者,您可以通過按一下add **icon**新增Syslog警報響應。

要將連線事件傳送到SNMP陷阱伺服器,請選擇**SNMP Trap**,然後從下拉選單中選擇SNMP警報響應。或者,您可以通過按一下新增**圖示**來新增SNMP警報響應。

onfiguration > ASA FirePOWER Con	iguration > Policies > [Access Control P	<u>olicy</u>				
ASA ASA FirePOWER							
Editing Rule - WebsiteBloc	k						
Name WebsiteBlock			Enabled	Move			
Action 🔀 Block with reset	~	IPS: no polic	ies Variables: n/a	Files: no inspection	Logging: connec	tions: Event Vie	wer, syslog, :
Zones Networks 🔺 Use	rs Applications	Ports URLs	🔺 ISE Attributes]	Inspection	Logging
Log at Beginning and End of Co	nnection		•				
\bigcirc Log at End of Connection							
O No Logging at Connection							
File Events:							
Log Files							
Send Connection Events to:							
🗹 Event Viewer							
Syslog (Connection Event only)	Syslog_Server			~ (3			
SNMP Trap SNMP_SERVER_1			~ (3				
							Save

為入侵事件啟用外部日誌記錄

當簽名(snort規則)與某些惡意流量匹配時,就會生成入侵事件。要啟用入侵事件的外部日誌記錄 ,請導航到ASDM Configuration > ASA Firepower Configuration > Policies> Intrusion Policy > Intrusion Policy。建立新的入侵策略或編輯現有入侵策略。導覽至Advanced Setting > External Responses。

若要將入侵事件傳送到外部SNMP伺服器,請在**SNMP警報**中選擇**Enabled**選項,然後按一下**Edit**選 項。

陷阱型別:陷阱型別用於警報中顯示的IP地址。如果網路管理系統正確呈現INET_IPV4地址型別 ,則可以選擇為Binary。否則,選擇為字串。

SNMP版本: 選擇其中一個版本2或版本3單選按鈕。

SNMP v2選項

陷阱伺服器:指定SNMP陷阱伺服器的IP地址/主機名,如下圖所示。

社群字串:指定團體名稱。

SNMP v3選項

陷阱伺服器:指定SNMP陷阱伺服器的IP地址/主機名,如下圖所示。

身份驗證密碼:指定身份驗證所需的密碼。SNMP v3使用雜湊函式對密碼進行身份驗證。

專用密碼:指定加密的密碼。SNMP v3使用資料加密標準(DES)分組密碼加密此密碼。

使用者名稱:指定使用者名稱。

Configuration > ASA FIREPOWER Config	uration > Policies > Intrusion Policy > Intrusion Policy				
Policy Information 🛦	SNMP Alerting < Bac	k			
Rules	Settings				
 Advanced Settings Global Rule Thresholding 	Trap Type 💿 as Binary 🔘 as String				
SNMP Alerting	SNMP Version Version Version Version 3				
Policy Layers	SNMP v2				
	Trap Server 192.168.20.3				
	Community String Secret				
Configuration > ASA FirePOWER Config	nuration > Policies > Intrusion Policy > Intrusion Policy				

Policy Information 🖄	SNMP Alerting	< Back
Rules	Settings	
Advanced Settings	Trap Type 💿 as Binary 🔘 as String	
Global Rule Thresholding	SNMB Version O Version R Version	
SNMP Alerting	Simp version U version2 U version3	
Policy Layers	SNMP v3	
	Trap Server 192.168.20.3	
	Authentication Password	
	Private Password (SNMP v3 passwords must be 8 or more characters)	
	Username user3	
	Revert to Defaults	

要將入侵事件傳送到外部系統日誌伺服器,請選擇選項 已啟用 在Syslog中 警報 然後按一下 編輯 選項,如下圖所示。

日誌記錄主機:指定Syslog伺服器的IP地址/主機名。

設施: 選擇任何合作室 配置的系統日誌伺服器。

嚴重性:選擇系統日誌伺服器上配置的任意嚴重性。

onfiguration > ASA FirePOWER Confi	guration > Policies > Intrusion Policy > Intrusion Policy	
Policy Information	Syslog Alerting	< Back
Rules	Settings	
 Advanced Settings Global Rule Thresholding SNMP Alerting 	Logging Hosts 192.168.20.3 (Single IP address or comma-separated list) Facility ALERT •	
Syslog Alerting	Priority EMERG V	
Policy Layers	Revert to Defaults	

為IP安全情報/DNS安全情報/URL安全情報啟用外部日誌記錄

當流量與任何IP地址/域名/URL安全情報資料庫匹配時,會生成IP安全情報/DNS安全情報/URL安全 情報事件。要啟用IP/URL/DNS安全情報事件的外部日誌記錄,請導航到(**ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy > Security Intelligence)**, 按圖中所示的**圖示**可啟用IP/DNS/URL安全情報的日誌記錄。按一下該圖示將提示一個對話方塊以 啟用日誌記錄,並提示一個選項以將事件傳送到外部伺服器。

若要將事件傳送到外部Syslog伺服器,請選擇**Syslog**,然後從下拉選單中選擇Syslog警報響應。或 者,您可以通過按一下新增圖示來新增系統日誌警報響應。

若要將連線事件傳送到SNMP陷阱伺服器,請選擇**SNMP Trap**,然後從下拉選單中選擇SNMP警報 響應。或者,您可以通過按一下新增圖示來新增SNMP警報響應。

Configuration > ASA FirePOWER Config	uration > Policies > Access Control P	olicy	6
ASA ASA FirePOWER			
Default Allow All Tra Enter a description	ffic		A Show Warnings
	¥ 2	Status: Access Control policy out-of-date on device	
Identity Policy: None	SSL Policy: None		
Rules Security Intelligence	HTTP Responses Advanced	Enable logging for DNS	blacklisting Evensts
Available Objects C C	Available Zones 🖒	DNS Policy: Default DNS Policy	Enable logging for IP SI Events Blacklist (2)
Networks URLs Global-Blacklist-for-URL URL Attackers URL Attackers URL Bogon URL Bots URL CnC URL Malware URL Open proxy		Add to Whitelist Image: Constraint of the second	Networks

為SSL事件啟用外部日誌記錄

當流量與啟用了日誌記錄的SSL策略中的任何規則匹配時,會生成SSL事件。若要為SSL流量啟用 外部日誌記錄,請導航到ASDM配置> ASA Firepower配置> 策略> SSL。編輯現有規則或建立新規 則,然後導航到logging 選項。選擇End of Connection 選項log。

然後導航到將連線事件傳送到,並指定將事件傳送到何處。

要將事件傳送到外部Syslog伺服器,請選擇**Syslog**,然後從下拉選單中選擇一個Syslog警報響應。 或者,您可以通過按一下新增圖示來新增系統日誌警報響應。

要將連線事件傳送到SNMP陷阱伺服器,請選擇**SNMP Trap**,然後從下拉選單中選擇SNMP警報響應。或者,您可以通過按一下新增圖示來新增SNMP警報響應。

<u>ontiguration > ASA FirePOWER Configuration > Po</u>	<u>licies</u> > <u>55L</u>						c
Default SSL Policy							
Editing Rule - SSL_Re_Sign							
Name SSL_Re_Sign		🕑 Enab	oled		Move into Cate	gory	▼ Stand
Action Decrypt - Resign 💌 wit	h Servertest			• c •	Replace Key		
Zones Networks Users Application	s Ports Category	Certificate	DN	Cert Status	Cipher Suite	Version]
Log at End of Connection							
Send Connection Events to:							
🕑 Event Viewer							
Syslog Syslog_Server		× (3					
SNMP Trap SNMP_SERVER_1		▼ €	3				

用於傳送系統事件的配置

為系統事件啟用外部日誌記錄

系統事件顯示Firepower作業系統的狀態。SNMP管理器可用於輪詢這些系統事件。

要配置SNMP伺服器以便從Firepower模組輪詢系統事件,需要配置系統策略,使資訊在firepower MIB(管理資訊庫)中可用,SNMP伺服器可以輪詢該資訊。

導航到ASDM Configuration > ASA Firepower Configuration > Local > System Policy,然後按一下 SNMP。

SNMP版本: Firepower模組支援SNMP v1/v2/v3。請指定SNMP版本。

社群字串:如果您在**SNMP版本選項中選擇**v1/v2,請在Community String欄位中鍵入SNMP社群 名稱。

使用者名稱: 如果您選擇v3</mark>選項in version選項。按一下Add User按鈕,並在使用者名稱欄位中指定 Username。

驗證: 此選項是SNMP v3配置的一部分。它使用MD5或SHA演算法提供基於雜湊消息身份驗證代碼 的身份驗證。選擇**Protocol** for hash algorithm,然後輸入密碼

在Password欄位中。如果不希望使用身份驗證功能,請選擇None選項。

隱私: 此選項是SNMP v3配置的一部分。它使用DES/AES演算法提供加密。選擇加密的協定,並在 Password(密碼)欄位中輸入密碼。如果您不需要資料加密功能,請選擇None選項。

Configuration > ASA FirePOWER Config	onfiguration > ASA FirePOWER Configuration > Local > System Policy				
Policy Name	Default				
Policy Description	Default System Policy				
Status: System policy out-of-date	on device				
	SNMP Version V	1//2			
Access List	Steller version v	1/ 12			
Access List	SNMP Version	/ersion 2 🔻			
Email Notification	Community String	ecret			
► SNMP					
STIG Compliance					
Time Synchronization					
Save Policy and Evit					
Configuration > ASA FirePOWER Confi	<u>quration > Local</u> > <u>Syste</u>	em Policy			
Policy Name	Default				
Policy Description	Default Cur	tare Deliau			
Policy Description	Derault Sys	tem Policy			
Status: System policy out-of-date	e on device				
	SNMP Versio	n V3			
Access List					
Email Notification	Username	user2			
► SNMP	Authentication Protoco	SHA 🔻			
STIG Compliance					
Time Synchronization	Authentication Passwo	ord			
	Verify Password	•••••			
Save Policy and Exit Cancel	Privacy Protocol	DES V			
	Privacy Password				
	verity rassword	••••••			
		Add			

:(MIB)FirepowerMIB(DCEALERT.MIB)(/etc/sf/DCEALERT.MIB)



目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

• 技術支援與文件 - Cisco Systems