FireSIGHT系統與ACS 5.x的整合,用於 RADIUS使用者身份驗證

目錄

 簡介

 必要條件

 需求

 採用元件

 組態

 ACS 5.x配置

 配置網路裝置和網路裝置組

 在ACS中新增身份組

 將本地使用者新增到ACS

 配置ACS策略

 FireSight管理中心配置

 FireSight管理器系統策略配置

 啟用外部身份驗證

 驗證

 相關思科支援社群討論

簡介

本檔案介紹將Cisco FireSIGHT管理中心(FMC)或Firepower受管裝置與思科安全存取控制系統 5.x(ACS)整合以進行遠端驗證撥入使用者服務(RADIUS)使用者驗證所需的配置步驟。

必要條件

需求

思科建議您瞭解以下主題:

- 通過GUI和/或外殼進行FireSIGHT系統和受管裝置的初始配置
- 在ACS 5.x上配置身份驗證和授權策略
- •基本RADIUS知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 思科安全存取控制 系統 5.7(ACS 5.7)
- Cisco FireSight管理員中心5.4.1

以上版本是當前可用的最新版本。所有ACS 5.x版本和FMC 5.x版本均支援此功能。

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。

組態

ACS 5.x配置

配置網路裝置和網路裝置組

 在ACS GUI中,導航到Network Device Group,按一下Device Type並建立裝置組。在後面的 示例螢幕截圖中,已配置裝置型別FireSight。 在後續步驟中,將在授權策略規則定義中引用此 裝置型別。 按一下「Save」。

► 🖓 My Workspace	Network Resources > Network Device Groups > Device Type > Edit: "Device Type:All Device Types:FireSight"
Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device	Device Group - General Image: Parent: FireSight Image: Parent: All Device Types Select
External Proxy Servers OCSP Services Users and Identity Stores	♥ = Required fields
 Policy Elements Access Policies 	
Monitoring and Reports System Administration	

• 在ACS GUI中,導覽至**Network Device Group**,單擊**NetworkDevices and AAA clients**並新增 裝置。 提供描述性名稱和裝置IP地址。 FireSIGHT管理中心在以下示例中定義。



- 在Network Device Groups中,將Device Type配置為與以上步驟中建立的裝置組相同。
- 選中Authentication Options旁邊的框,選中RADIUS覈取方塊,然後輸入將用於此NAD的 Shared secret key。 注意:稍後在FireSIGHT管理中心上配置RADIUS伺服器時,將再次使用 相同的共用金鑰。 要檢視純文字檔案鍵值,請按一下Show按鈕。 按一下「Submit」。
- 對需要RADIUS使用者身份驗證/授權以進行GUI和/或外殼訪問的所有FireSIGHT管理中心和受 管裝置重複上述步驟。

在ACS中新增身份組

• 導航到**使用者和身份庫,**配置**身份組**。在此示例中,建立的身份組為「FireSight管理員」。此 組將連結到以下步驟中定義的授權配置檔案。



將本地使用者新增到ACS

導航到使用者和身份庫,在內部身份庫部分中配置使用者。輸入本地使用者建立所需的資訊
 ,選擇上一步中創建的身份組,然後按一下提交。

My Workspace	Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"
▶ ♣ Network Resources	
👻 🐴 Users and Identity Stores	General Status: Enchlad A
Identity Groups Internal Identity Stores	Description:
Users	C Identity Group: All Groups:FireSight Administrator Select
Hosts External Identity Stores 	Email Address:
LDAP	
Active Directory	Account Disable
RADIUS Identity Servers	Disable Account if Date Exceeds: 2015-Nov-01 iiii (yyyy-Mmm-dd)
Certificate Authorities	Disable account after 3 successive failed attempts
Certificate Authentication Profile	
Identity Store Sequences	Password Hash
Policy Elements	Applicable only for Internal Users to store password as hash.
Construction Access Policies	Enable Password Hash Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.
Monitoring and Reports	
System Administration	Password Lifetime
a self mar market	Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled
	User Information There are no additional identity attributes defined for user records
	Creation/Modification Information
	Date Wed Sep 02 13:15:56 UTC 2015 Created:
	Date Wed Sep 02 23:12:39 UTC 2015
	Date Wed Sep 02 13:15:56 UTC 2015
	¢ = Required fields
and the second second second second	Submit Cancei

配置ACS策略

• 在ACS GUI中, 導航至Policy Elements > Authorization and Permissions > Network Access >

Authorization Profiles。 略為FireSight管理員。

使用描述性名稱建立新的授權配置檔案。在下面的示例中,建立的策

► 🔂 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"
Itel Network Resources	
Big Users and Identity Stores	General Common Tasks RADIUS Attributes
🔹 🎭 Policy Elements	Ame: FireSight Administrator
 Session Conditions Date and Time 	Description: Comparison of the second sec
Custom Network Conditions 	
 Authorization and Permissions Network Access 	
Authorization Profiles Device Administration	
Named Permission Objects	
Access Policies	
Monitoring and Reports	
System Administration	

• 在RADIUS attributes頁籤中,新增用於授權上面建立的身份組的手動屬性,然後按一下Submit

My Workspace	Policy Elements > Authorizat	tion and Permissions > Network Acces	ss > Authorization Profiles > 1	Edit: "FireSight Administrator"
Image:				
B Users and Identity Stores	General Common T	Tasks RADIUS Attributes		
- Or Policy Elements	Common Tasks Attribu	utes		
	Attribute	Туре	Value	
Session Conditions				
 Network Conditions 				
 Authorization and Permissions 				
 Network Access 				
Authorization Profiles				
Device Administration	Manually Entered			
Named Permission Objects	Attribute	Туре	Value	
Access Policies	Class	String	Groups:FireSig	ht Administrator
Monitoring and Reports				
System Administration				
· ·				
	Add Λ Edit V	✓ Replace Λ Delete		
	Dictionary Type:	RADIUS-IETF		
	S RADIUS Attribute:	Class	Select	
	Attribute Type:	String		
	Attribute Value:	Static		
		Groups:FireSight Administrator		
	* = Poquired fields			
	Submit Cancel			

- 導覽至Access Policies > Access Services > Default Network Access > Authorization 並為 FireSight管理中心管理會話配置新的授權策略。以下示例使用NDG:裝置型別與與上述步驟 中配置的裝置型別和身份組匹配的身份組條件。
- 此策略隨後作為結果與上述配置的FireSight管理員授權配置檔案相關聯。 按一下「Submit」。



FireSight管理中心配置

FireSight管理器系統策略配置

- 登入到FireSIGHT MC,然後導航到System > Local > User Management。 按一下External Authentication頁籤。 按一下+ Create Authentication Object按鈕,為使用者身份驗證/授權新 增新的RADIUS伺服器。
- 選擇RADIUS作為驗證方法。 輸入RADIUS伺服器的描述性名稱。 輸入主機名/IP地址和 RADIUS金鑰。 金鑰應與以前在ACS上配置的金鑰匹配。 (可選)輸入備份ACS服務器主機 名/IP地址(如果存在)。
 Overview Analysis Policies Devices Objects AMP

					Local > User Management	Updates	Licenses	Mor
Users	User Roles	External Authentication						
		External Authentication Ob Authentication Method Name *	RADIUS C					
		Description Primary Server						
		Host Name/IP Address * Port * RADIUS Secret Key	172.18.75.172 1812	ex. IP or host	name			
		Backup Server (Optional)						
		Host Name/IP Address Port RADIUS Secret Key	1812	ex. IP or host	name			

• 在 **RADIUS特定引數** 節,在本示例中,Class=Groups:FireSight管理員值對映到FireSight管理 員組。 這是ACS作為ACCESS-ACCEPT的一部分返回的值。 按一下 **儲存** 要儲存配置,或繼 續下面的驗證部分以測試對ACS的身份驗證。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	11
Administrator	Class=Groups:FireSight Administrator

•在**外殼訪問過濾器**下,輸入逗號分隔的使用者清單以限制外殼/SSH會話。

Shell Access Filter	
Administrator Shell Access	user1, user2, user3
Jser List	

啟用外部身份驗證

最後,完成以下步驟,以便在FMC上啟用外部驗證:

- 1. 導覽至System > Local > System Policy。
- 2. 在左側面板中選擇External Authentication。
- 3. 將Status變更為Enabled(預設為停用)。
- 4. 啟用新增的ACS RADIUS伺服器。
- 5. 儲存策略並在裝置上重新應用策略。

驗證

• 要針對ACS測試使用者身份驗證,請向下滾動至Additional Test Parameters部分,並輸入 ACS使用者的使用者名稱和密碼。 按一下「Test」。 成功測試將獲得緣色成功: 瀏覽器視窗 頂部的Test Complete消息。

Additional Test Parameters		
User Name	test	
Password	••••	

Success Test Complete.	×	
• 要檢視測試身份驗證的結果,請轉到 測試輸出 部分 。 在下面的示例螢幕截圖中,請注意「radiusauth	,然後按一下 顯示詳細資訊 旁邊的 黑1 n - response: 從ACS接收的「	马箭頭

|Class=Groups:FireSight Administrator|」值。 此值應與上面在FireSIGHT MC上配置的本地 FireSight組關聯的Class值匹配。 按一下「**Save**」。

Test Output	
Show Details	•
User Test	check_auth_radius: szUser: test RADIUS config file: /var/tmp/_bcEn4h_wF/radiusclient_0.conf radiusauth - response: User-Name=test radiusauth - response: Class=Groups:FireSight Administrator radiusauth - response: Class=CACS:acs/229310634/47 "test" RADIUS Authentication OK check_is_radius_member attrib match found: Class=Groups:FireSight Administrator - Class=Groups:FireSight Administrator ********* role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
*Required Field	
	Save Test Cancel