ASA 8.3:使用ACS 5.X的TACACS身份驗證

目錄

 簡介

 必要條件

 需求

 採用元件

 慣例

 設定

 網路圖表

 使用CLI配置ASA以從ACS伺服器進行身份驗證

 使用ASDM配置ASA以從ACS伺服器進行身份驗證

 擦ACS配置為TACACS伺服器

 驗證

 疑難排解

 錯誤: AAA將AA伺服器組tacacs中的TACACS+伺服器x.x.x.標籤為失敗

 相關資訊

<u>簡介</u>

本文檔提供有關如何配置安全裝置以對使用者進行網路訪問驗證的資訊。

<u>必要條件</u>

<u>需求</u>

本文檔假設自適應安全裝置(ASA)完全可運行且配置為允許思科自適應安全裝置管理器(ASDM)或 CLI進行配置更改。

註:有關如何允許ASDM遠端配置裝置的詳細資訊,請參閱<u>允許ASDM進行HTTPS訪問</u>。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •思科自適應安全裝置軟體版本8.3及更高版本
- •思科自適應安全裝置管理器6.3版及更高版本
- •思科安全存取控制伺服器5.x

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。

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

<u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定:



注意:此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

使用CLI配置ASA以從ACS伺服器進行身份驗證

為ASA執行以下配置以從ACS伺服器進行身份驗證:

!--- configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+ ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on. ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco !--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa authentication http console cisco LOCAL

注意:在ASA上使用<u>username cisco password cisco privilege 15</u> 命令建立本地使用者,以便在 ACS不可用時通過本地身份驗證訪問ASDM。

使用ASDM配置ASA以從ACS伺服器進行身份驗證

ASDM過程

完成以下步驟,以便從ACS伺服器配置ASA進行身份驗證:

1. 選擇Configuration > Device Management > Users/AAA > AAA Server Groups > Add以建立 AAA Server Group。

nfiguration > Dev	rice Management	> Users/AAA > AAA S	erver Groups			
AA Server Groups	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add Edit Delete
ervers in the Selected	d Group		Interface		Timenuk	Add
Server Mark of B	naan waa		a Rollinge		THOOR.	Edit

2. 在Add AAA Server Group視窗中提供AAA Server Group詳細資訊,如下所示。使用的協定是 TACACS+,且建立的伺服器群組是cisco。

🛓 Add AAA Serve	r Group		×	
Server Group:	cisco			
Protocol:	TACACS+	~		
Accounting Mode:	🔘 Simultaneous	💿 Single		
Reactivation Mode:	 Depletion 	🔘 Timed		
Dead Time: 10	minut	es		
Max Failed Attempts:	3			
ОК	Cancel	Help		
				按一下「OK」

3. 選擇Configuration > Device Management > Users/AAA > AAA Server Groups,然後在 Servers in the Selected Group下按一下Add以新增AAA伺服器。

berver aroup	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
isco	TACAC5+	Single	Depletion	10	3	Edit
						Delete
vers in the Selected	d Group					

4. 在Add AAA Server視窗中提供AAA Server詳細資訊,如下所示。使用的伺服器組是cisco。

8.165.29		
8.165.29		
		seconds
	_	
•		
		8

OK」,然後按一下「Apply」。您將看到AAA Server Group和AAA Server在ASA上配置。 5. 按一下「Apply」。

Co	nfiguration > Device	Management	> Users/AAA > AAA S	erver Groups		
A	AA Server Groups					
	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
	cisco	TACACS+	Single	Depletion	10	3
	ware in the Colorhod C					
26	Fivers in the selected G	oup		Televine		Timerak
	Server Name or IP Ad	dress		Interface	Timeout	
L	192,100,105,29			amz		
	LDAP Attribute Ma	n				
	Contraction of the					
					Apply Res	et

6. 選擇Configuration > Device Management > Users/AAA > AAA Access > Authentication, 然 後點選HTTP/ASDM和SSH旁邊的覈取方塊。然後選擇cisco作為伺服器組,然後按一下 Apply。

Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication Authorization Accounting
Enable authentication for administrator access to the ASA.
Require authentication to allow use of privileged mode commands
Enable Server Group: LOCAL Server Group fails
Require authentication for the following types of connections
FITP/ASDM Server Group: cisco V Use LOCAL when server group fails
Serial Server Group: LOCAL S Use LOCAL when server group fails
SSH Server Group: cisco V Use LOCAL when server group fails
Telnet Server Group: tac Use LOCAL when server group fails
Apply Reset

將ACS配置為TACACS伺服器

完成以下步驟即可將ACS配置為TACACS伺服器:

1. 選擇**Network Resources > Network Devices and AAA Clients**,然後按一下**Create**以將ASA新 增到ACS伺服器。

cisco Cisco Secure Ad	cs
▶ 💮 My Workspace	Network Resources > Network Devices and AAA Clients
Image: Network Resources Network Device Groups	Network Devices
Location Device Type Network Devices and AAA Clients Default Network Device	Filter: Match it Go Name IP / Mask NDG:Location NDG:Device Type Description No data to display No data to display
	Create Duplicate Edit Delete File Operations Export

2. 提供有關客戶端的必需資訊(ASA在此為客戶端),然後按一下Submit。這樣可以將ASA新增到 ACS伺服器。詳細資訊包括ASA的IP地址和TACACS服務器詳細資訊。

cisco Cisco Secure A	cs			acsailman EMEAAC
Cisco Cisco Secure A Cisco S	Vatwork Resolutions > 1444 Natwork Resolutions > 1444 Description ACS Natwork Device Gro Location Device Type IP Address © Single IP Ad © IP: 192.168.165 © = Required fields	o to ASA All Device Types dress P Range(s) 3	Select Select	Athentication Options TACACS+ Shared Betret Cisco Shared Betret Cisco Shale Connect Device Ciacaty TACACS+ Single Connect Buppert TACACS+ Draft Compliant Single Connect RADIJS Shared Sacret:
	Submit Cancel			

您將看到客戶端Cisco被新增到ACS伺服器。

cisco Cisco Secure A	cs						
- + 💮 MyWorkspace	Network	Resources	> Netw	ork Devices and AAA (Clients		
🔻 🦣 Network Resources	Netw	ork Device	:5				
 Network Device Groups Location Device Type 	Filte	r		Match If.	~	00 🗢	
Network Devices and AAA Clients		Name	*	IP / Mask	NDG:Location	NDO:Device Type	Description
Default Network Device External RADIUS Servers		Cisco		192.168.165.3/32	All Locations	All Device Types	ACS to ASA
Users and identity Stores							
→ Sp Policy Elements							
Access Policies							
 Monitoring and Reports 							
🔸 🥞 System Administration							

3. 選擇Users and Identity stores > Internal Identity Stores > Users, 然後按一下Create以建立新 使用者。

cisco Cisco Secure A	CS
🕞 🖌 My Workspace	Users and identity Stores > Internal identity Stores > Users
 Network Resources 	Internal Users
Identity Groups	Filler: Match if: Go 🔫
Internal Identity Stores Users Hosts	Status User Name Identity Group Description No data to display
 External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Authorities Certificate Authorities Certificate Authorities Certificate Sequences Policy Elements 	
Access Policies Monitoring and Reports	
System Administration	
	Create Duplicate Ect Delete Change Password File Operations Export

4. 提供名**稱、密碼和啟用密碼**資訊。**啟用密碼**是可**選的**。完成後,按一下Submit。

cisco Cisco Secure Ad	S accadmin EMEAAC
 MyWorkspace Network Resources Second Methods Stores Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA Securit Dioken Servers RADIUS Identity Stores Securities Certificate Authentics Certificate Authentics Certificate Authentics Certificate Authentics Certificate Authentics Monitoring and Reports System Administration 	Users and kientity Stores + Internal identity Stores + Loors + Create General • Nama: isca Description: Test User • Identity Group: All Groups Password Information Password Information Password nust • Contain 4 - 32 characters • Password: • Contain 4 - 32 characters • Confirm • Confirm Password: • Confirm • Change password on next login Enable Password: User Information • Password in user • Password: • Confirm • Change password on next login Password: • Description • Confirm • Confirm • Password: • Confirm • Confirm • • Required fields • • • • • • • • • • • • • • • • • • •
	Submit Cance

您將看到正在將使用者cisco新增到ACS伺服器。

cisco Cisco Secure A	cs
🕞 🖌 😚 My Workspace	Users and identity Stores > Internal identity Stores > Users
Network Resources	Infernal Lisers
Given Stores General Identity Stores Identity Groups	Filter: Match if: Go 🗢
 Internal Identity Stores 	Status User Name 🔺 Identity Group Description
Hosts + External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Authorities Identity Store Sequences	All Groups Test User
System Administration	



使用本節內容,確認您的組態是否正常運作。

使用**test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco**命令 檢查配置是否正常工作。此圖顯示身份驗證成功,並且連線到ASA的使用者已由ACS伺服器進行身 份驗證。

🖆 Command Line Interface

Command						
💿 Single Line	O Multiple Line		🔽 Enable con	itext sensitive h	elp (?)	
test aaa-server	authentication cisco hos	192.168.165.2	9 username cis	co password cis	0	~
Response:						
Result of the	command: "test a	aa-server a	uthenticat	ion cisco h	ost 192.	168.165.
INFO: Attempt	ing Authenticatio	n test to T	P address	<192 168 16	E 29> /+	imeout:
INFO: Authent	ication Successfu	1	r auuress		0.200 (0	Lifeodo.
N	111				C chan a	
					Clear R	esponse
	Send	Close	Hel	P		

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

錯誤:AAA將AAA伺服器組tacacs中的TACACS+伺服器x.x.x.標籤為失敗

此消息表示Cisco ASA丟失了與x.x.x.和服器的連線。確保tcp 49上從ASA到伺服器x.x.x.来具有有效

的連線。您還可以將TACACS+伺服器的ASA超時從5增加至所需的秒數,以防出現網路延遲。 ASA不會向FAILED伺服器x.x.x.x傳送身份驗證請求。但是,它將使用aaa-server組tacacs中的下一 個伺服器。

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援頁
- Cisco ASA 5500系列自適應安全裝置命令參考
- 思科調適型資安裝置管理員
- IPsec協商/IKE通訊協定支援頁面
- <u>思科安全存取控制伺服器(Windows專用)</u>
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems