IPS 7.X:使用ACS 5.X作為Radius伺服器配置示例 的使用者登入身份驗證

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> 慣例 <u>設定</u> 使用IME配置IPS以從ACS伺服器進行身份驗證 將ACS配置為RADIUS伺服器 <u>驗證</u> <u>疑難排解</u> 相關資訊

<u>簡介</u>

本文提供如何使用RADIUS伺服器設定使用者登入驗證的Cisco入侵防禦系統(IPS)的相關資訊。 ACS用作RADIUS伺服器。

<u>必要條件</u>

<u>需求</u>

本文檔假定Cisco Intrusion Prevention System(IPS)已完全正常運行且已配置為允許Cisco Intrusion Prevention System Manager Express(IME)或CLI更改配置。除了本地AAA身份驗證外,您現在還可 以配置RADIUS伺服器以執行感測器使用者身份驗證。Cisco Intrusion Prevention System 7.0(4)E4及更高版本提供將IPS配置為對使用者帳戶使用AAA RADIUS身份驗證的功能,這有助於操 作大型IPS部署。

注意:沒有在IPS上啟用記帳的選項。IPS 7.04中支援RADIUS身份驗證,但不支援TACACS或授權 或記帳。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •思科入侵防禦系統版本7.0(4)E4及更高版本
- •入侵防禦系統管理員Express版本7.1(1)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。

<u>慣例</u>

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。

使用IME配置IPS以從ACS伺服器進行身份驗證

完成以下步驟,以便將IPS新增到IME,然後配置IPS以從ACS伺服器進行身份驗證:

1. 選擇Home > Devices > Device List > Add,以便將IPS新增到IME。



2. 完成Add Device視窗中的欄位(如此處所示),以便提供有關IPS的詳細資訊。此處使用的感 測器名稱為IPS。按一下「OK」(確定)。

C Add Device	×						
Sensor Name:	,IPS						
Sensor IP Address:	192.168.165.8						
Web Server Port:	443						
Communication protocol —							
⊙ Use encrypted connection (https)						
O Use non-encrypted connect	ion (http)						
Authentication							
Configuration User Name:	cisco						
Configuration Password:	••••••						
Use the Same Account for Configuration and Event Subscription (This is not recommended):							
Event Subscription User Name:	cisco						
Event Subscription Password:	•••••						
Event Start Time (UTC)							
Most Recent Alerts							
Start Date (YYYY:MM:DD):							
Start Time (HH:MM:SS):							
Exclude alerts of the following severity level(s)							
🔲 Informational 🔂 Low [Medium 🔄 High						
	ж Cancel						

3. 按一下「**Yes**」以接受憑證並繼續https連線到感應器。您必須接受該證書,才能連線並訪問感 測器。



4. 選擇Configuration > IPS > Sensor Setup > Authentication,然後完成以下步驟:按一下「 RADIUS Server」單選按鈕,以選擇「RADIUS Server」作為驗證裝置。提供RADIUS Authentication引數,如下所示。選擇Local和RADIUS作為控制檯身份驗證,以便在 RADIUS伺服器不可用時使用本地身份驗證。按一下「Apply」。

Username	Role	Status	Add
isco	Administrator	Active	
ervice	Service	Active	Edit
etwork Access ID: 0P5 Allow Local Authentication if all Rac	Default User Role: Administrator		
Allow Local Authentication if all Rad	aus Servers are Uniresponsive		
	20		
Server IP Address: 192.168.165.2			
Server IP Address: 192.168.165.2 Authentication Port: 1812	Secondary Radius Server (optional) (3)		
Server IP Address: 192.168.165.2 Authentication Port: 1812 Timeout (seconds): 3	Secondary Radius Server (optional)		
Server IP Address: 192.168.165.2 Authentication Port: 1812 Timeout (seconds): 3	Secondary Radius Server (optional)		

將ACS配置為RADIUS伺服器

完成以下步驟,將ACS配置為RADIUS伺服器:

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

 My Workspace Metwork Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers System Administration 	
 Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Servers Vers and Identity Stores No data to display 	
 Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers No data to display Filter: Match if: Marne IP / Mask NDG:Location NDG:Device Type No data to display	
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Image: Client Se	
Network Devices and AAA Clients Default Network Device External RADIUS Servers Image: Control of the servers <th>Description</th>	Description
External RADIUS Servers	Description
Weers and Identity Stores Over Policy Elements Constraints Monitoring and Reports System Administration	
Policy Elements Access Policies Monitoring and Reports System Administration	
Access Policies Monitoring and Reports System Administration	
Monitoring and Reports System Administration	
System Administration	
	-

 提供客戶端所需的資訊(IPS是此處的客戶端),然後按一下Submit。這樣,IPS就可以新增 到ACS伺服器。詳細資訊包括IPS的IP地址和RADIUS服務器詳細資訊。

Description:	IPS	
Network Devic	Groups	
Location	All Locations	Select
Device Type	All Device Types	Select
IP Address Single O IP: 192.16	P Address P Range(s) 3.165.8	Authentication Options TACACS+ Shared Secret Single Connect Device Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Sup

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
► 💮 MyWorkspace	Users and kiently Stores > Internal kiently Stores > Users
Network Resources	Internal Users
 B Users and identify Stores 	
Identity Groups	
Internal Identity Stores Users	Status User Name 🔺 Identity Group Description
Hosts	No data to display
External Identity Stores	
Active Directory	
RSA SecuriD Token Servers	
RADIUS Identity Servers Certificate Authorities	
Certificate Authentication Profile	
Identity Store Sequences	
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	
	Create Duplicate Edit Delete Change Password File Operations Export

4. 提供名稱和密碼資訊。完成後,按一下Submit。

General		
o Name:	IPS Status: Enabled	
Description:	IPS access	
Identity Group:	All Groups Se	lect
Password Inform	nation	Enable Password Information
Password must:		Password must:
 Contain 4 	- 32 characters	 Contain 4 - 32 characters
Password:	•••••	Enable Password:
Confirm Password:	*****	Confirm Password:
🖸 Change p	bassword on next login	
User Information		
Max User Per Session:	1	
• = Required fiel	1s	



使用本節內容,確認您的組態是否正常運作。

嘗試用新建立的使用者登入IPS。使用者通過身份驗證後,檢查ACS上的報告。



按一下「Authentications-RADIUS-Today」以檢視當前報告。

cisco Cisco Secure A	CS View						
Monitoring and Reports Dashboard Alarms Inbox Thresholds Schedules	Dashboard General Troubleshooting Authentication Trends ACS Health Top 5 Alarms Minimum Severity: Info						
 ■ Reports Favorities Shared ♥ Catalog ■ Troubleshooting Connectivity Tests ACS Support Bundle Emert Troubleshooter 	Severity © Critical Alarm My Favorite Reports	Name ACS - System Errors ACS - Waming Alarm	Date Fri Apr 2	22 01:34:00 formation Alarm	Cause Alarm caused by A		
Konitoring Configuration	Favorite Name ACS - Configuration / ACS - System Errors Buthentications - RAU Authentications - RAU Authentications - TAO Authentications - TAO	Audit - Today - Today DIUS - Today DIUS - Yesterday CACS - Today CACS - Yesterday	Re AC AC AA AA AA	eport Name CS Instance>ACS_Co CS Instance>ACS_Syst A Protocol>RADIUS_ A Protocol>RADIUS_ A Protocol>TACACS_ A Protocol>TACACS_	nfiguration_Audit tem_Diagnostics Authentication Authentication Authentication Authentication		

此圖顯示,連線到IPS的使用者由ACS伺服器進行身份驗證。

	Showing P	age 1	of 1						Goto Paç	je: Go	
AAA Protocol > RADIUS Authentication											
Authentication Status : Pass or Fail Date : April 29, 2011 (Last 30 Minutes Last Hour Last 12 Hours Today Yesterday Last 7 Days Last 30 Days)											
Generated on April 29, 2011 1:31:12 AM UTC											
2 Reload											
Pass	×-Fail	^q -c	lick for de	stails	₿ =Mou	isə oyer iten	n for additi	onal information			
	Logged At		RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address
Apr 29,	11 1:25:51.8	06 AM	1		Q.	IPS	127.0.1.1	Default Network Access	PAP_ASCI	<u>PS</u>	<u>192.168.165.8</u>

<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 。

<u>疑難排解</u>

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco IPS 4200系列感應器支援頁面
- Cisco IPS 4200系列感測器命令參考
- Cisco IPS管理員Express版本
- 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