使用思科身份服務引擎(Radius)的AsyncOS外部 身份驗證

目錄

簡介
必要條件
需求
採用元件
背景資訊
設定
網路圖表
步驟1.建立身份驗證的身份組。
步驟2.建立本地使用者以進行身份驗證。
步驟3.建立授權配置檔案。
步驟4.建立授權範疇
驗證
疑難排解
相關資訊

簡介

本檔案介紹在郵件安全裝置(ESA)/安全管理裝置(SMA)和思科身份服務引擎(ISE)之間成功實施使用 RADIUS的外部身份驗證所需的配置。

必要條件

需求

思科建議您瞭解以下主題:

- •驗證、授權及記帳(AAA)
- RADIUS類屬性。
- Cisco ISE身份管理和授權策略。
- Cisco ESA/SMA使用者角色。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ISE 2.4
- Cisco ESA 13.5.1、13.7.0
- Cisco SMA 13.6.2

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

相關產品

未測試「使用的元件」部分中列出的版本以外的版本。

背景資訊

Radius CLASS屬性

用於記帳,這是RADIUS伺服器包含在所有記帳資料包中的任意值。

類屬性在ISE(RADIUS)中按組配置。

當使用者被視為其屬性為25的ISE/VPN組的一部分時,NAC根據身份服務引擎伺服器(ISE)中配置的 對映規則實施策略。

設定

網路圖表



身份服務引擎接受來自ESA/SMA的身份驗證請求,並將其與使用者身份和組進行匹配。

步驟1.建立身份驗證的身份組。

登入ISE伺服器並建立身份組:

導航到Administration -> Identity Management -> Groups -> User Identity Group。如下圖所示。



附註:Cisco建議為分配的每個ESA/SMA角色在ISE中使用身份組。

步驟2.建立本地使用者以進行身份驗證。

在此步驟中,建立新使用者或分配已存在的使用者到我們在步驟1中建立的身份組。請登入到ISE並

導航到Administration->Identity Management->Identities,然後建立新使用者或分配給您建立的組中的用戶。如下圖所示。

Network Access Users List > New Networ	k Access User	
Network Access User		
* Name ESA_admin		
Status 🔽 Enabled 👻		
Email admins@mydomain.com		
▼ Passwords		
Password Type: Internal Users	•	
Password	Re-Enter Password	
* Login Password		Generate Password (i)
Enable Password		Generate Password (i)
 User Information 		
First Name		
Last Name	Anvconnect	
	St Dot1X	
 Account Options 		
Description		4
Description		
Change password on next login \Box		
 Account Disable Policy 		
Disable account if date exceeds	GuestType_Contractor (default)	/y-mm-dd)
	SuestType_Daily (default)	
▼ User Groups	T. Guest type_weekly (default)	
Select an item		
Submit Cancel		

步驟3.建立授權配置檔案。

無需授權配置檔案即可成功完成RADIUS身份驗證,但不會分配角色。要完成設定,請導**覽至** Policy->Policy Elements->Results->Authorization->Authorization profile。

附註:為每個要分配的角色建立一個授權配置檔案。

Authorization Profiles > Aav	ega_ESA_Admin
Authorization Profile	
* Name	ESA_Admin
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	titte Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
Common Tasks Web Authentication (I Airespace ACL Name ASA VPN AVC Profile Name	Local Web Auth)
 Advanced Attribute 	s Settings
Select an item	

附註:確保使用radius類屬性25並指定名稱。此名稱必須與AsyncOS(ESA/SMA)上的配置匹 配。 在圖3中,管理員是CLASS屬性名稱。

步驟4.建立授權策略。

最後一步允許ISE伺服器識別使用者登入嘗試並對映到正確的授權配置檔案。

在授權成功的情況下,ISE會返回一個訪問接受並沿授權配置檔案中的CLASS值定義。

導航到Policy > Policy Sets > Add(+符號)

Γ	+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
6	Search									
	/	ø	New Policy Set 1			+	Select from list 🔹 🕇		٥	>

指定名稱並選擇加號以新增所需的條件。本實驗環境使用Radius。NAS-IP-Address。儲存新策略。

oliolo Ide	entity Ser	rvices Engine	Home	Context Visibility	Operations	▼ Policy	Administration	Work Centers		1	License	Warning 🔺	O,	0 (o o
Policy Se	ets Prof	filing Posture Cli	ent Provisio	ning + Policy Eleme	nts					Click here to	o do visibility	setup Do not	show th	is again.	×
_															
Policy S	Sets									Rese	t Policyse	t Hitcounts		Reset	Save
+	Status	Policy Set Name		Description		Condition	S		AI	lowed Protocols	/ Server Se	equence	Hits	Actions	View
Search															
	Ø	ESA_Policy					twork Access-Device IP /	Address EQUALS 10.122.1	111.238	Default Network Ac	cess >	· · +	16	¢	>

為了正確匹配授權請求,必須新增條件。**選擇**

圖示並新增條件。

實驗室環境使用InternalUser-IdentityGroup並匹配每個授權配置檔案。

✓ Auth	orization F	Policy (5)							
					Results				
+	Status	Rule Name	Cond	itions	Profiles	Security Groups		Hits	Actions
Search	h								
	ø	ESA Monitor	牛	InternalUser-IdentityGroup EQUALS User Identity Groups:ESA_Monitor	ESA_Monitors	Select from list	- +	0	٥
	Ø	ESA HelpDesk	48-	InternalUser-IdentityGroup EQUALS User Identity Groups:HelpDesk	ESA_admin +	Select from list	- +	0	٥

步驟5.啟用對AsyncOS ESA/SMA的外部身份驗證。

登入AsyncOS裝置(ESA/SMA/WSA)。 並**導航到System Administration > Users > External** Authentication > Enable External Authentication on ESA。

Edit External Authentication

External Authentication Settings	
Enable External Authentication	
Cancel	Submit

提供以下值:

- RADIUS伺服器主機名
- 連接埠
- 共用金鑰
- 超時值(秒)
- •驗證通訊協定

選擇**將外部身份驗證的使用者對映到多個本地角色(推薦)**。如下圖所示。

Edit External Authentication

RADIUS 🔁							
RADIUS Server Hostname	Port	Share	d Secret	Timeout Value (in seconds)	Authent	ication	Add Row
x.x.x.x	1812	•••••	••••	5	PAP	0	Ŵ
0 seconds							
Map externally auther	ticated u	sers to r	multiple local ro	les. (recomme	ended)		
RADIUS CLASS Att	ribute		Role 🥐			A	dd Row
Administrators			Administrator	· 🜔			Ŵ
Monitors			Operator	0			ŵ
RADIUS CLASS attri	<i>butes are</i> enticated	e <i>case-se</i> users to	ensitive. the Administra	ator role.			
	RADIUS Image: Constraint of the second s	RADIUS Server Hostname Port X.X.X.X 1812 0 seconds • Map externally authenticated u RADIUS CLASS Attribute Administrators Monitors RADIUS CLASS attributes are • Map all externally authenticated	RADIUS Image: Constraint of the second s	RADIUS Port Shared Secret RADIUS Server Port Shared Secret Hostname Port Isla X.X.X.X 1812 Isla 0 seconds seconds 0 seconds RADIUS CLASS Attribute Role ? Administrators Administrator Monitors Operator RADIUS CLASS attributes are case-sensitive. Map all externally authenticated users to the Administrator	RADIUS Image: Second secon	RADIUS Image: Server Hostname Port Shared Secret Timeout Value (in seconds) X.X.X.X Image: Im	RADIUS Port Shared Secret Timeout Value (in seconds) RADIUS Server Port Shared Secret Timeout Value (in seconds) Image: Seconds Image: Seconds Image: Seconds Image: Seconds Image: Seconds Image: Seconds Image: Seconds </td

附註: Radius CLASS Attribute MUST Match with the attribute Name defined in Step 3(在 對映為ASA VPN的常見任務下)。

驗證

請登入您的AsyncOS裝置,確認已授予訪問許可權且已正確分配分配的角色。如圖所示,具有訪客 使用者角色。

ULLIIII CISCO U	V000			Email Security Appliance is
CISCO Email Secur	ity Virtual Appliance			
Monitor				
My Dashboard				
				🃜 Printable PDF
Attention — À You ca Some > Ove	an customize this "My Dashboard" modules are added for you by de rview.	page by addi fault. The Ove	ing report modules from different r erview page can be accessed from	eports. Monitor
Attention — A You ca Some > Ove	an customize this "My Dashboard" modules are added for you by de rview.	page by addi fault. The Ove	ing report modules from different r erview page can be accessed from	eports. Monitor
Attention — A You ca Some > Ove System Overview Overview > Status	an customize this "My Dashboard" modules are added for you by de rview.	page by addi fault. The Ove	ing report modules from different r erview page can be accessed from Overview > Quarantines - Top 3 by 1	eports. Monitor Disk Usage (Policy and Virus)
Attention — A You ca Some > Ove System Overview Overview > Status	an customize this "My Dashboard" modules are added for you by de rview. System Status:	page by addi fault. The Ove	ing report modules from different r erview page can be accessed from Overview > Quarantines - Top 3 by 1 No quarantines are available	eports. Monitor Disk Usage (Policy and Virus)
Attention — A You ca Some > Ove System Overview Overview > Status	an customize this "My Dashboard" modules are added for you by de rview. System Status: Incoming Messages per hour:	page by addi ault. The Ove	ing report modules from different r erview page can be accessed from Overview > Quarantines - Top 3 by I No quarantines are available	eports. Monitor Disk Usage (Policy and Virus)
Attention — A You ca Some > Ove System Overview Overview > Status	an customize this "My Dashboard" modules are added for you by de rview. System Status: Incoming Messages per hour: Messages in Work Queue:	page by addi fault. The Ove	ing report modules from different r erview page can be accessed from Overview > Quarantines - Top 3 by I No quarantines are available	reports. Monitor



如果登入嘗試在ESA上失敗,則顯示消息「無效使用者名稱或密碼」。問題可能出在授權策略上。

登入到ESA,從External Authentication選擇Map all external authenticated users to the Administrator role。

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

提交並提交更改。進行新的登入嘗試。如果登入成功,請仔細檢查ISE Radius授權配置檔案 (CLASS屬性25)和授權策略設定。

<u>ISE 2.4</u>
<u>AsyncOS</u>