為安全防火牆機箱管理器(FCM)配置ISE RADIUS身份驗證

目錄

簡介

本文檔介紹如何為使用ISE的安全防火牆機箱管理器配置RADIUS授權/身份驗證訪問的過程。

必要條件

需求

思科建議瞭解以下主題:

- 安全防火牆機箱管理員(FCM)
- 思科身分辨識服務引擎(ISE)
- RADIUS 驗證

採用元件

- Cisco Firepower 4110安全裝置FXOS v2.12
- 思科身份服務引擎(ISE) v3.2修補4

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。

設定

組態

安全防火牆機箱管理員

步驟 1.登入到Firepower機箱管理器GUI。 步驟 2.導航至平台設定

verview Interfaces	Logical Devices	Security Engine Platfo	orm Settings)	System Tools Help admir
FPR4K-1-029A78B Model: Cisco Fire	172.16.0.130 power 4110 Secur	rity Appliance Ver	sion: 2.12(0.8) Op	perational State: O p	perable	Chassis Uptime 0	0:06:02:19 也 の①
ONSOLE MGMT USB	Powe	er 2 - Removed	Network Module 1	Network N	Iodule 2 : Empty	Network Module	3 : Empty
FAULTS 3(3) CRITICAL	D(O) MAJOR	3 5 DOWN @ UP	INSTANCES O O DOWN	1 1 UP	LICENSE Smart Agent UNREGISTERED	INVENTORY 1(1) 6(6) ⊜ Security Engine ☆ Fans	1(2) ⇒ Power Supplies
Select All Faults Cancel Sel	elected Faults Acknowled	lge				*	
Severity	Description			Cause	Occurrence	Time	Acknowledged
CRITICAL	FPGA version lower that	an 2.00 is detected. A critical u	pgrade from the firmwar	fpga-upgrade-requir	red 1	2022-02-20T22:32:45.64	1 no
	Network Module 3 remo	oved when in online state. It is	recommended to set m	module-suprise-remo	oval 1	2022-11-07T09:03:02.02	2 no
Successful Login in last 24 hrs -	View Details Thu Feb 01	2024 at 17:00:55 from - 172.16.	0.35				البداد » cisco

步驟 3.從左側選單中按一下over AAA。 選擇Radius並增加新的RADIUS提供程式。

Overview Interfaces Logic	al Devices Security Engine	Platform Settings		System	Tools Hel	o admin
NTP	LDAP RADIUS TACACS					
SSH						
SNMP	Properties					
HTTPS	Timeout:* 5 Secs					
► AAA						
Syslog	Retries:* 1					
DNS	RADIUS Providers					
FIPS and Common Criteria					0	Add
Access List			and a	A	_	_
MAC Pool	Hostname	Order	Service	Auth Port		
Resource Profiles						
Network Control Policy						
Chassis URL						
	Save Cancel					
8 Successful Login in last 24 hrs - View D	Details Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35				cisco

步驟 4.使用Radius提供者要求的資訊填入提示選單。按一下「OK」(確定)。

Overview Interfaces Logi	cal Devices Security Engin	e Platform Settings			System Tools Help	admin
NTP SSH SNMP HTTPS AAA	LDAP RADIUS TACAC	S Add RADIUS Provider		(7) X		
Sysiog DNS FIPS and Common Criteria Access List MAC Pool Resource Profiles Network Control Policy Chassis URL	RADIUS Providers Hostname	Hostname/FQDN/IP Address:* Order:* Key: Confirm Key: Authorization Port:* Timeout:* Retries:*	172.16.0.12 lowest-available ••••••• 1812 5 1	Set: No	Auth Port	Add
8 Successful Login in last 24 hrs - <u>View I</u>	Save Cancel	rom - 172.16 0.35	ОК	Cancel		altatu cisco

步驟 5.導航到系統>使用者管理

Overview Interfaces Logi	cal Devices Security Engin	Platform Settings			System Too	ls Help admin
_			Configuration	Licensing	Updates U	Jser Management
SSH						-
SNMP	Properties					
HTTPS	Timeout:* 5 Secr					
► AAA	Retries.* 1					
Syslog	PADILIS Providers					
DNS	TADIOS FIORACIS					
FIPS and Common Criteria						Add 🔾
Access List	Hostname	Order	Service	Auth Port		
Resource Profiles	172.16.0.12	1	authorization	1812		6
Network Control Policy						
Chassis URL						
	8 - E					
	2					
	Save Cancel					
line 24 hors - Marriel	Detaile 175-15-5 01 2024 -1 17 00 55 1	17216026				مانيان
avascript:void(0) ast 24 nrs - view	Details Thu Feb 01 2024 at 17:00:55 f	om - 172.16.0.35				CISCO

步驟 6.點選Settings頁籤並將下拉選單中的Default Authentication設定為Radius,然後向下滾動並 儲存配置。

Overview Interfaces Logical	Device	es Security Engine Platform Settings			System	Tools Help admin
			Configuration	Licensing	Updates	User Management
Local Users Settings						
Default Authentication	Local Local	*Local is fallback authentication method				
Console Authentication	RADIUS LDAP	• -				
Remote User Settings	TACACS					
Remote User Role Policy	None	No-Login				
Local User Settings						
Password Strength Check	Enabl	e				
History Count	5	(0-disabled,1-15)				
Change Interval	48	✓ (1-730 hours)				
Change Count	2	(1-10)				
No Change Interval		(1-730 hours)				
Days until Password Expiration	0	(0-never,1-9999 days)				
Password Expiration Warning Period	0	(0-9999 days)				
Expiration Grace Period	0	(0-9999 days)				
Password Reuse Interval	0	(0-disabled,1-365 days)				
Session Timeout(web UI,ssh,telnet)	600	(0-never.3600 seconds)				
8 Successful Login in last 24 hrs - <u>View Deta</u>	<u>ails</u> Thu I	Feb 01 2024 at 17:00:55 from - 172.16.0.35				cisco



注意:此時已完成FCM組態。

身分辨識服務引擎

步驟 1. 新增網路裝置。

導航到位於左上角的漢堡圖示= > Administration > Network Resources > Network Devices > +Add。

= Cisco ISE			Administration • Netw	rork Resources			🔺 Evaluation Mode 18 Days Q 🕐 균로 🚭
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More \vee
Network Devices	Notwork	k Dovince					
Default Device Device Security Settings	Network	k Devices					Salastad & Testi A C B
	0 Edit + A4	dd 🚺 Duplicate 🕁 Import	① Export 🗸 👌 Generate PA	C 🍵 Delete 🗸			
	□ Name	e 🔿 IP/Mask	Profile Name	Location Type		Description	
				No data available	,		

步驟 2. 填寫有關新網路裝置資訊請求的引數。

2.1選中RADIUS覈取方塊

2.2配置與FCM Radius配置相同的共用金鑰。

2.1向下滾動並按一下「Submit(提交)」。

Cisco ISE			Administration	n - Network Resour	ces			A Evaluation Mode 18 Days	20	p 8 0	- 1
Network Devices	Network Device Groups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors	Location Services				
Network Devices Default Device Device Security Settings	Network Devices List > New Network Device Network Devices										
	Name FPR-4110 Description										
	II PARMEN - *P: 172.16.0	130 [/] 32 O									
	Device Profile A Cisco	<u> </u>									
	Model Name EPR-4110	v									
	Software Version 2.12 Network Device Group	~									
	Location All Locations	👻 Set To Defau	•								
	IPSEC Is IPSEC Device	Set To Defaul	•								
	Device Type All Device Types	Set To Defaul	•								
	RADIUS Authentication Set	lings									
	RADIUS UDP Settings										
	Protocol RADIUS	Show									
	Use Second Shared Secret 🕥										
	Second Shared Secret		Show								

步驟 3.驗證新裝置是否顯示在「網路裝置」下。

≡ Cisco ISE		Administration · Netv	vork Resources			A Evaluation Mode 18 D	ays Q	35	0 B
Network Devices	Network Device Groups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors	More \vee		
Network Devices Default Device Device Security Settings	Network Devices					Select	ed 0 Total 1	8	0
	🖉 Edit 🕂 Add 📋 Duplicate 🅁 Import	🖞 Export 🖂 🔒 Generate PAG	Delete 🗸					~	V
	Name	lame Location	Туре	Description					
	□ FPR-4110 172.16.0 ﷺ Cisc	All Locations	All Device Types						

步驟 4. 建立所需的使用者身份組。導航到位於左上角的漢堡圖示≡ > Administration > Identity Management > Groups > User Identity Groups > +增加

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 🕥 🔎
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 18 O		Selected 0 Total 9 🧭 🚳
> 🛅 Endpoint Identity Groups		$\sim abla$
> 🗅 User Identity Groups	Name Description	
	KALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	GROUP_ACCOUNTS (default) Default GROUP_ACCOUNTS (default) User Group	
	□ ≹ GuestType_Contractor (default) Identity group mirroring the guest type	
	C & GuestType_Daily (default) Identity group mirroring the guest type	
	C & GuestType_SocialLogin (default) Identity group mirroring the guest type	
	C & GuestType_Weekly (default) Identity group mirroring the guest type	
	ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	

步驟 5.設定管理員使用者身份組的名稱,然後點選提交以儲存配置。

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💿 👼
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups > New User Identity Group Identity Groups * Name FPR-4110-Admin User Group for Administrator. Description Submit	Cancel

5.1對唯讀使用者重複相同的程式。

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 🕥 👼
Identities Groups External Iden	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Group: > New User Identity Group * Name FPR-4110-ReadOnly User Group for Read Only Users. Description	omit Cancel

步驟 6.驗證使用者身份組下顯示的新使用者組。

Cisco ISE	Administr	tration - Identity Management	🔺 Evaluation Mode 18 Days Q 🛞 🕫
dentities Groups External Iden	dity Sources Identity Source Sequences Sett	tings	
Identity Groups	User Identity Groups		
< 🐮 🗼	🖉 Edit 🕂 Add 🔋 Delete 🗸 🕁 Import 🖒 Exp	v noq	Selected 0 Total 11 🤪
> 🛅 User Identity Groups	Name Desc	scription	
	ALL_ACCOUNTS (default) Defi	fault ALL_ACCOUNTS (default) User Group	
	C # Employee Defi	fault Employee User Group	
	☐ Ž FPR-4110-Admin Use	er Group for Administrator.	
	☐ 😤 FPR-4110-ReadOnly Use	er Group for Read Only Users.	
	C & GROUP_ACCOUNTS (default) Defa	fault GROUP_ACCOUNTS (default) User Group	
	C & GuestType_Contractor (default) Ider	ntity group mirroring the guest type	
	GuestType_Daily (default)	ntity group mirroring the guest type	
	C & GuestType_SocialLogin (default) Ider	ntity group mirroring the guest type	
	GuestType_Weekly (default)	ntity group mirroring the guest type	
	OWN_ACCOUNTS (default) Defi	fault OWN_ACCOUNTS (default) User Group	

步驟 7. 建立本地使用者並將他們增加到其對應組。 導航到漢堡圖示≡ >管理>身份管理>身份> +增 加。

≡ Cisco ISE	Administration - Identity Management	▲ Evaluation Mode 18 Days Q ⑦ 등립 @
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 0 😂 🔕
		~ 10
	Status Username \wedge Description First Name Last Name Email Address User Identity Groups Admin	
	No data available	

7.1增加具有管理員許可權的使用者。設定名稱和口令,分配給FPR-4110-Admin,然後向下滾動並 按一下Submit以儲存更改。

E Cisco	o ISE				Administration - Identity Management	A Evaluation Mode 18 Days	209	78 0
Identities	Groups	External Identity Sources	Identity Source Sequences	Settings				
Users Latert Manual Net	work Scan Res.	V Network Access Username Status Account Name Alas Emai Password Type: IP Password Type: IP Password Type: IP Password Type: IP Password Infention Password Entert O	s User cisce_admin Cisce_admin Cisce_admin Cisce_admin Cisce constructions					
		* Login Password Enable Password > User Informatii > Account Optio > Account Disab	In the Policy	Re-Enter Password	Generate Password O			
		E FPR-4110-A	dmin 🗸 🛈 🌒					

7.2增加具有只讀許可權的使用者。設定名稱和口令,並將其分配給FPR-4110-ReadOnly,然後向 下滾動並按一下Submit以儲存更改。

E Cisco ISE		Administration - Identity Management	🔺 Evaluation Mode 18 Days Q. 💿 🕼 💿
Identities Groups Ext	ternal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	 ✓ Network Access User * Username cisce_readonly Status Ended ✓ Account Name Allas O Email 		
	Password System Users Password Type: Internet Users Password Lifetime: With Experision O Password all experts in 60 days Netword Splites ①		
	Password Re-Criter Password * Login Password Dashe Password > User Information	Generate Password O Generate Password O	
	Account Options Account Disable Policy		
	✓ User Groups E FPR-4110-ReadOnly ✓ ③ ●		

7.3驗證使用者是否在網路訪問使用者下。

😑 Cisco ISE	Ad	Iministration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🕼	0
Identities Groups Exte	nal Identity Sources Identity Source Sequences Settings			
Users Latest Manual Network Scan Res	Network Access Users			
			Selected 0 Total 2 👩 🧔	
	$ / \ {\rm Ent} \ \ + \ {\rm Add} \ \ \otimes \ {\rm Change Status} \ \lor \ \ \oplus \ {\rm Import} \ \ \oplus \ {\rm Export} \ \lor \ \ \otimes \ {\rm Change Status} \ \lor \ \ \oplus \ {\rm Import} \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ {\rm Import} \ \ \odot \ \ \oplus \ \ \ \ \oplus \ \ \ \ \oplus \$		$M \sim - \nabla$	
	Status Username 🔿 Description First Name Last Name Email Ad	Idress User Identity Groups Admin		
	BEnabled 1 cisco_admin	FPR-4110-Admin		
	Enabled 1 cisco_readonly	FPR-4110-ReadOnly		

第8步:為管理員使用者建立授權配置檔案。

FXOS機箱包括以下使用者角色:

- 管理員-對整個系統的完整讀寫存取權。預設管理員帳戶預設分配此角色,且無法更改。
- 唯讀-對沒有修改系統狀態之許可權的系統組態唯讀存取權。
- 操作-對NTP配置、智慧許可的Smart Call Home配置和系統日誌(包括系統日誌伺服器和故障)的讀寫訪問許可權。對系統的其餘部分具有讀取許可權。
- AAA -對使用者、角色和AAA配置的讀寫訪問許可權。對系統其餘部分的讀取許可權

每個角色的屬性:

cisco-av-pair=shell : roles="admin"

- cisco-av-pair=shell : roles="aaa"
- cisco-av-pair=shell : roles="operations"
- cisco-av-pair=shell : roles="read-only"



附註:本檔案僅定義管理屬性和唯讀屬性。

導航到Burger圖示≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

定義授權配置檔案的名稱,將訪問型別保留為ACCESS_ACCEPT,並在Advanced Attributes Settings下增加cisco-av-pair=shell:roles="admin" with,然後按一下Submit。

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 17 Day	n Q	0 53	•
Dictionaries Conditions	Results				
Authentication > Autherization >	Authorization Profile 5 FPR-4110-Admins Authorization Profile				
Authorization Profiles Downloadable ACLs	* Name FPR-4110-Admins				
	Description				
Profiling > Posture >	* Access Type ACCESS_ACCEPT Y				
Client Provisioning	Network Device Profile 🟥 Disco 🗸 🗇				
	Service Template				
	Agentiess Posture				
	Passive identity Tracking 🗆 🕐				
	ACL IPv6 (Fitter-ID)				
	Advanced Attributes Settings				
	End Ciscocisco-av-pair v *				
	Attributes Details Access Type = ACCESS, ACCEPT etico-av-par = sheltrates="behavit"				
		Submit		Cancel	

8.1 重複以上步驟,為只讀使用者建立授權配置檔案。這次使用值read-only Administrator建立 RADIUS類。

= Cisco ISE			Policy - Policy Elements		Evaluation Mode 18 Days	Q ()	9 Q	
Dictionaries Conditions	Results							
Authentication >	Authorization Profiles > New A	wthorization Profile						
Authorization Profiles Downloadable ACLs	* Name	FPR-4110-ReadOnly						
Profiling >	Description							
Posture >	 Access Type 	ACCESS_ACCEPT ~						
Client Provisioning	Network Device Profile	±t Cisco ∨⊕						
	Service Template Track Movement Agentiess Posture Passive Identity Tracking							

ACL IPv6 (Filter-ID)		
✓ Advanced Attributes Settings		
Cisco:cisco-av-pair v ahelt:roles*'read-only* v +		
✓ Attributes Details Access type = ACCESS_ACCEP1 docs-av-pair = 3-ddLordes_*read-only*		
	Submit	Cancel

第9步:建立與FMC IP地址匹配的策略集。這是為了防止其他裝置向使用者授予訪問許可權。

導航到≡ > Policy > Policy Sets > Add icon sign(位於左上角)。

≡ Cisco ISE	Policy - Policy Sets	🛕 Evaluation Mode 17 Days Q 💿 😼 🕹
Policy Sets		Reset Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
	+	
Default Default policy set		Default Network Access 🥜 🕂 58 🚳 🕨
		Reset Save

9.1新行位於策略集的頂部。按一下Add圖示配置新條件。

🕘 Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Seque	ince Hits	s Actions	View
Q Search								
۲	New Policy Set 1			+	Select from list	+	ô	>
٥	Default	Default policy set			Default Network Access	+ 58	命	>
							694	

9.2為RADIUS NAS-IP-Addressattribute增加匹配FCM IP地址的頂部條件,然後按一下使用。

Libr	ary														
Se	arch	by Nar	ne												
0	173	0	*	0	₽	٢	8	8	2	昰	0	1	o	Ł	φ.
::	F 5	G													
:	e 0	atalys	t_Swit	tch_L	ocal_	Web_	Authe	enticat	ion						
8	F R	adius													
8	F 5	witch_	Local	_Wet	_Aut	hentic	ation								
::	! s	witch,	Web,	Auth	entica	ition									
8	e v	/ired_l	802.1	×											
::	e v	/ired_l	MAB												
::	e v	/ireles	s_802	.1X											
:	e v	/ireles	s_Acc												
8	e v	/ireles	s_MA	в											
8	e v	/LC_W	/eb_A	uthen	ticati	on									

Editor

Ŷ

🗸 Attri	Select attribute for condit	tion			
		P 100 12 12 10	1 0 b	Transformed and the second sec	g value View
not'	Dictionary	Attribute	ID Info	Duplicate	Save
	All Dictionaries	Attribute	ID		>
	Microsoft	MS-User-IPv4-Address	61 🕕		
	Network Access	ISE Host Name	0		
	Radius	DNS-Server-IPv6-Address	169 🕕		
	Radius	Framed-IP-Address	8 ()		Save
	Radius	Framed-IPv6-Address	168 🕕		
	Radius	NAS-IP-Address	4 🕕		
	Radius	Stateful+IPv6+Address-Pool	172 ①		



9.3完成後,按一下Save。

≡ Cisco	ISE		Policy · Policy Sets		A Evaluation M	rde 17 De	<mark>00 0</mark>	0	58 ¢
Policy Sets				Reset	Reset Policys	et Hitcor	unts		Save
Status	Policy Set Name	Description	Conditions	Allowed Protocol	/ Server Seque	nce H	fits A	ctions	View
Q Search									
۰	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🐼 🗸	+		¢	>
۰	Default	Default policy set		Default Network	liccess 🧷	+ 5		(2)	>
								_	
						Re	eset		Save



提示:在本練習中,我們允許使用預設網路訪問協定清單。您可以建立一個新清單,並根 據需要縮小其範圍。

步驟 10. 透過按一下行末尾的>圖示檢視新的策略集。

Policy Sets		Reset Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q. Search		
New Policy Set 1	Rediss-NAS-IP-Address EQUALS 172.16.0.130	Default Network Access 🗷 🗸 +

10.1 展開Authorization Policy 選單,然後按一下in (+)增加新條件。

\vee	Authorization	n Policy (1)						
					Results			
	 Status 	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
	Q Search	h						
	۰	Authorization Rule 1		+	Select from list	Select from list	0 +	礅

10.2設定條件以匹配DictionaryIdentity Groupwith AttributeName Equals User Identity Groups: FPR-4110-Admins(在步驟7中建立的組名)並按一下Use。

Ciscale				Delleur	Balley Cale						A	0 ×	
y Se	Conditions Studio												
Statu	Library	Editor											
	Search by Name	_	Identity	iroup-Na	lame								
			Equals	Sele	ect attribute for conditio	n			×				
	ii 🖪 56 💿		Set to 'Is	•	백 0 🔹 0 묘	⊕ 8 © 2 !	01	0 t 🕈	-	C	Duplicate		
then	E BYOD_is_Registered				Dictionary	Attribute	ID	Info					
uthon	E Catalyst_Switch_Local_Web_Authentication				All Dictionaries	Attribute	ID						
uthori	: Compliance_Unknown_Devices			-	IdentityGroup	Description							
	E Compliant_Devices				IdentityGroup	Name		0					
⊛ s	E EAP-MSCHAPv2				InternalUser	IdentityGroup		0					
9	EAP-TLS				PassiveID	PassiveID_Groups		0					
	E Guest_Flow			-	administrator	ExternalGroups		0					
	II 🖪 MAC_in_SAN 💿												
	E Network_Access_Authentication_Passed												
	:: ONn_Cisco_Profiled_Phones												
	E Non_Compliant_Devices												
	🗄 👩 Radius 💿												
	# F Switch_Local_Web_Authentication												
										Close	Us		

brary		Editor			
Search by Name			IdeniityGroup Name		1
• · · · • • · · · · · · · · · · · · · ·	10 E 🕈		Equals View Identity Groups: \$PR-4110-		
: E 50		*	Admin V		
BYOD_is_Registered			Set to 'is not'	Save	l
Catalyst_Switch_Local_Web_Authentication			NEW AND OR		
Compliance_Unknown_Devices					
Compliant_Devices					
EAP-MSCHAPv2					
EAP-TLS					
Cuest_Flow					
MAC_in_SAN					
Network_Access_Authentication_Passed					
Non_Cisco_Profiled_Phones					
Non_Compliant_Devices					
Radius					

第10.3步驗證新條件是否在授權策略中配置,然後在配置檔案下增加使用者配置檔案。

V Authorization Policy (1)												
			Results									
💿 Statu	s Rule Name	Conditions			Profiles		Security Groups		Hits	Actions		
Q Searc	a.											
۰	Authorization Rule 1	A IdentityGroup Name EQUALS User Identity Groups:/FR-4110-Admin			FPR-4110-Admins \times	~+	Select from list	~+		٨		
۰	Default				DenyAccess	1+	Select from list	1+	۰	\$		

Save

步驟 11.在步驟9中,針對唯讀使用者重複相同的程式,然後按一下「儲存」。

驗證

1. 嘗試使用新的RADIUS憑證登入FCM GUI

2. 切換作業選項至Burger 圖示= > Operations > Radius > Live logs。

3. 顯示的資訊會顯示使用者是否成功登入。

=	Cisco ISE								Operations	· RADIUS									A Evaluation I	Aode 17 Days	9.0	58 O
Live	Logs Live Sessie	ns																				
	Misconfigured Supplic	ants 🕕				Misconfigured	I Network Devices 💿				RADIUS Drop	• 0			c	lient Stopped Resp	onding 🕕				Repeat Co	unter 🕕
	0						0				1					0					C)
	Ø 😂 Reset Repeat C	ounta 🖞 Deport To	~														Refs Ne	esh ver	Latest 20	records 🗸	Within Last 3 hou Filter V	<u> </u>
	Time	Status	De	tails	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address		Network De	Device Port	Identity Group	Posture	Server	Mdm Ser	IMEISV		Usecasi
	×				<u>~</u>	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~	Network Devic	Device Port	Identity Group	Posture St	Server	Mdm Serve	IMEISV		Usecase
	Feb 03, 2024 01:5 Feb 03, 2024 01:5	0.48.9	6			cisco_readonly cisco_admin			New Polic	New Polic	FPR-4110			FPR-411D FPR-411D		User Identity Group		marpatinISE marpatinISE				

4. 從Secure Firewall機箱CLI驗證已記錄使用者角色。

FPR4K-1-029A78B# scope security FPR4K-1-029A78B /security # show remote-user detail Remote User cisco_admin: Description: User Roles:	FPR4K-1-029A78B# scope security serve	se r service-profile	
Name: admin Name: read-only FPR4K-1-029A78B /security #	FPR4K-1-029A78B# scope FPR4K-1-029A78B /secur Remote User cisco_admi Description: User Roles: Name: admin Name: read-only FPR4K-1-029A78B /secur	security ity # show remote-user detail n: /	

1. 透過ISE GUI,導航到漢堡圖示≡ >操作> Radius >即時日誌。

1.1驗證日誌會話請求是否到達ISE節點。

1.2若為失敗狀態,請檢閱階段作業的詳細資訊。

= Cisco ISE	Ope	erations - RADIUS	Evaluation Mode	18 Days Q 💿 🕫 🔯
Live Logs Live Sessions				
Misconfigured Supplicants 💿	Misconfigured Network Devices 🕕	RADIUS Drops 🕕	Client Stopped Responding 🕥	Repeat Counter 🕕
0	1	1	0	3
ට් 🖯 Reset Repeat Counts 🖞 Export To 🗸			Refresh Show Never V Latest 20 reco	Inds v Uthin Value
Time Status Deta	tails Repea Identity Endpoint ID	Endpoint Authenti Authoriz IP A	Address Network De Device Port Identity Group Posture	a Server Mdm Se
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic Authorizatic IP A	Address 🗸 Network Device Device Port Identity Group Posture	Sta Server Mdm Sen
Feb 02, 2024 07:32:18.8 O	cisco_admin	Default >> Default	FPR-4110 User Identity Group:	marpatinISE
Feb 02, 2024 07:23:20.1	cisco_readonly	Default >> Default >> PermitAcc	FPR-4110 User identity Groups	marpatinISE
Feb 02, 2024 07:15:32.2	cisco_admin	Default >> Default >> PermitAcc	FPR-4110 User identity Groups	marpatiniSE

2. 對於未顯示在RADIUS即時日誌中的請求,檢視UDP請求是否透過資料包捕獲到達ISE節點。

導航到Burger圖示≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dump。增加新的捕獲 並將檔案下載到本地電腦,以檢視UDP資料包是否到達ISE節點。

2.1填寫所需資訊,向下滾動並按一下Save。

E Cisco ISE	Operations - Troubleshoot	Liveluation Mode 17 Days Q. (2) 🖓 🕼
Diagnostic Tools Downloa	ad Logs Debug Wizard	
General Tools ~ RADIUS Authentication TroubL	TCP Durgs > New	
Execute Network Device Com Evaluate Configuration Validat Posture Troubleshooting Agentiess Posture Troublesho	Add ToP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear. Hist Name* margatistSE v	
EndPoint Debug TCP Dump	Natsaink Martice*	
TrustSec Tools	Gigabelt Ehernet D (Lip, Kunning) 🔍 🕖	
	(g) host 172.16.0.130 (g) host 10.77.122.123 and not (10.177.122.119	

2.2選取並啟動擷取。



2.3當ISE捕獲運行時,嘗試登入到安全防火牆機箱

2.4停止ISE中的TCP轉儲並將檔案下載到本地電腦。

2.5檢視流量輸出。

預期輸出:

資料包No1。透過埠1812 (RADIUS)從安全防火牆向ISE伺服器發出請求 資料包No2。ISE伺服器答覆接受初始請求。



關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。