Configuración de la autenticación RADIUS de ISE para el administrador de chasis de firewall seguro (FCM)

Contenido

Introducción

Este documento describe el proceso de configuración del acceso de autorización/autenticación Radius para Secure Firewall Chasis Manager con ISE.

Prerequisites

Requirements

Cisco recomienda tener conocimiento de los siguientes temas:

- Administrador de chasis de firewall seguro (FCM)
- Cisco Identity Services Engine (ISE)
- Autenticación RADIUS

Componentes Utilizados

- Dispositivo de seguridad Cisco Firepower 4110 FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2, parche 4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuraciones

Administrador de chasis de firewall seguro

Paso 1. Inicie sesión en la GUI de Firepower Chassis Manager.

Paso 2. Vaya a Configuración de la plataforma

FPR4K-1-029A78 Model: Cisco F	B 172.16	0.130) Security Appliance	e Version:	2.12(0.8) Of	perational State: O f	perable	Chassis	Uptime 00:00	5:02:19 じ の①
NSOLE MGMT USB	-	Power 2 - Removed	ı 🍽	Network Module 1	Network N	lodule 2 : Empty	Netw	vork Module 3 : I	mpty
FAULTS		INTERFACES		INSTANCES		LICENSE	INVENTORY		
3(3) ⊗ CRITICAL	O(O)	3 OOWN	5 100	0	1 @ UP	Smart Agent	1(1) Security Engine	6(6) ☆ Fans	1(2) ⇒ Power Supplies
Select All Faults Cance	Selected Faults	cknowledge							
Severity	Description				Cause	Occurrence	т	ime	Acknowledged
	FPGA version	ower than 2.00 is detect	ed. A critical upgrad	e from the firmwar	fpga-upgrade-requi	red 1	2022-02-20	T22:32:45.641	no
	Network Modu	le 3 removed when in on	line state. It is recor	mmended to set m	module-suprise-rem	oval 1	2022-11-07	T09:03:02.022	no

Paso 3. En el menú de la izquierda, haga clic sobre AAA. Seleccione Radius y Add a new RADIUS provider.

Overview Interfaces Logica	al Devices Security Engine	Platform Settings			System Tools	: Help	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	Hartson	Order	Constant Sector	Auth Part		-	
MAC Pool	Hostname	Order	Service	Auth Port			
Resource Profiles							
Network Control Policy							
Chassis URL							
	Save Cancel						
	Sare Sarva						
8 Successful Login in last 24 hrs - View De	etails Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35					cisco

Paso 4. Rellene el menú de prompt con la información solicitada del proveedor de Radius. Click OK.

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH SNMP HTTPS	LDAP RADIUS TACACS Properties Timeout.* 5 Secs	1			
AAA Syslog DNS FIPS and Common Criteria Access List	Retries:* 1 RADIUS Providers	Add RADIUS Provider Hostname/FQDN/IP Address:* Order:*	172.16.0.12 lowest-available		Add
MAC Pool Resource Profiles Network Control Policy Chassis URL	rostname	Key: Confirm Key: Authorization Port:* Timeout:*	••••••• ••••••• 1812 5	Set: No	
	Save Cancel	Retries.*	1	Cancel	
8 Successful Login in last 24 hrs - <u>View</u>	Details Thu Feb 01 2024 at 17:00:55 fr	om - 172.16.0.35			ոլիսիս cisco

Paso 5. Vaya a System > User Management .

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings		Sys	em ⁴ Tools Help admin
			Configuratio	on Licensing Upd	ates User Management
SSH					
SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
► AAA	Retries.* 1				
Syslog	PADILIS Providers				
DNS	Indios Providers				
FIPS and Common Criteria					O Add
Access List	Hostname	Order	Service	Auth Port	
Resource Profiles	172.16.0.12	1	authorization	1812	<i>d</i> 6
Network Control Policy					
Chassis URL					
	Save Cancel				
					ا بابيان
vascript:void(0) last 24 hrs - View	Details Thu Feb 01 2024 at 17:00:55 fro	om - 172.16.0.35			cisco

Paso 6. Haga clic en la ficha Settings (Parámetros) y establezca Default Authentication (Autenticación predeterminada) en el menú desplegable Radius. A continuación, desplácese hacia abajo y guarde la configuración.

Overview Interfaces Logica	al 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	Enab	le				
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 - View De	<u>etails</u> Thu	Feb 01 2024 at 17:00:55 from - 172.16.0.35				cisco



Nota: la configuración de FCM ha finalizado en este punto.

Identity Service Engine

Paso 1. Agregue un nuevo dispositivo de red.

Navegue hasta el icono de hamburguesa ≡ ubicado en la esquina superior izquierda > Administración > Recursos de red > Dispositivos de red > +Agregar.

			Administration • Netv	work Resources		🛦 Evaluation Mode 18 Days Q 💮 😼 🔯
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers External N	DM pxGrid Direct Connectors More ~
Network Devices						
Default Device	Networ	k Devices				
Device Security Settings						Selected 0 Total 0 🦪 🔕
	0 Edit + A	dd 🚺 Duplicate 🕁 Import	🗄 Export 🗸 🛛 🙆 Generate Pr	AC 🔋 Delete 🗸		all \sim $-\nabla$
	Nam	e 🗠 IP/Mask	Profile Name	Location Type	Description	
				No data available		

Paso 2. Rellene los parámetros solicitados para la información de los nuevos dispositivos de red.

- 2.1 Marque la casilla RADIUS
- 2.2 Configure la misma clave secreta compartida que en la configuración Radius de FCM.
- 2.1 Desplácese hacia abajo y haga clic en Enviar.

🔳 Cisco ISE	Administration - Network Resources	A Evaluation Mode 18 Days Q (0) 528 (0)
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	
	E PAGPHS V *P: 172,166,130 / 32 O	
	Device Prote at Coco Y O	
	Model Name \$P92-4110 V	
	Software Version 2.12	
	Network Device Group	
	Location Al Locations V Set To Default	
	IPSC IN PSC Device v Set To Default	
	Device Type All Device Types v Set To Default	
	RADIUS Authentication Settings	
	RADIUS UOP Settings	
	Protocol RADUS	
	Shared Secret Show	
	Ute Second Shared Second	
	Beend Shared Shared Share	

Paso 3. Validar que el nuevo dispositivo se muestra en Dispositivos de red.

≡ Cisco ISE		Administration - Network	work Resources			A Evaluation Mode 18 Days Q (5	0
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	Network Devices							
Device Security Settings						Selected 0 Total 1	0 0	į.
	🖉 Edit 🕂 Add 🚺 Duplicate 🥁 Impor	t 🏦 Export 🗸 👌 Generate PA	C 📋 Delete 🗸			Al	~ 7	
	🗌 Name 🗠 IP/Mask Profile	Name Location	Туре	Description				
	FPR-4110 172.16.0 # Cit	All Locations	All Device Types					

Paso 4. Cree los grupos de identidad de usuario necesarios. Navegue hasta el icono de hamburguesa ≡ ubicado en la esquina superior izquierda > Administración > Administración de identidad > Grupos > Grupos de identidad de usuario > + Agregar

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 🕐 🕫 🖗
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 18 O		Selected 0 Total 9 🔗 💿
> Endpoint Identity Groups	2 Edit + Add Delete V & Import D Export V	All \sim ∇
> 🗁 User Identity Groups	Name Description	
	ALL_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	
	GuestType_Daily (default) Identity group mirroring the guest type	
	GuestType_SocialLogin (default) Identity group mirroring the guest type	
	☐ ≹ GuestType_Weekly (default) Identity group mirroring the guest type	
	ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	

Paso 5. Establezca un nombre para el Admin User Identity Group y haga clic en Submit para guardar la configuración.

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💿 🕫 🚭
Identities Groups External Ide	antity Sources Identity Source Sequences Settings	
SQ C SQ C SB C Endpoint identity Groups C User identity Groups	User Identity Groups > New User Identity Group Image: Terminal state in the s	Cancel

5.1 Repita el mismo proceso para los usuarios de ReadOnly.

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q () 등정 🗇
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
Edentity Groups C C S C C C C C C C C C C C C C	User Identity Groups > New User Identity Group: Identity Group * Name FPR-4110-ReadOnly User Group for Read Only Users. Description	Submit Gancel

Paso 6. Valide que los nuevos grupos de usuarios aparezcan en Grupos de identidades de usuarios.

E Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 18 Days Q 🛞 🖉
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 🐮 🔷	🖉 Eas 🕂 Add 🌘 Delete 🗸 🕁 Import 🖒 Export 🗸	All V
> 🛅 User Identity Groups	Name	
	ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	□ 😤 FPR+4110+Admin User Group for Administrator.	
	User Group for Read Only Users.	
	□ 👫 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	
	🗌 📲 GuestType_SocialLogin (default) Identity group mirroring the guest type	
	🗌 🦂 GuestType_Weekly (default) Identity group mirroring the guest type	
	ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	
	🗌 😽 Radius	

Paso 7. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya al icono de hamburguesa \equiv > Administration > Identity Management > Identities > + Add.

E Cisco ISE	Administration - Identity Management	Administration - Identity Management						
Identities Groups Ext	ternal Identity Sources Identity Source Sequences Settings							
Users Latest Manual Network Scan Res	Network Access Users							
		Selected 0 Total 0 💋 🔞						
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🛆 Export 🗸 📋 Delete 🗸 📋 Duplicate	$_{ m All}$ \sim $~$ ∇						
	Status Username A Description First Name Last Name Email Address User Identity Groups Admin							
	No data available							

7.1 Agregue el usuario con derechos de administrador. Establezca un nombre, una contraseña y asígneselos a FPR-4110-Admin, desplácese hacia abajo y haga clic en Enviar para guardar los cambios.

E Cisc	o ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q	0 58	0	Ī
Identities	Groups	External Identity Sources Identity Source Sequences Settings					
Users Latent Manual Ne	twork Scan Res	V Network Access User Usernane Clico, admin Status Count Name Alas Cmat Cmat					
		Password Uniters Password Uniters With Express Of the system With Express O Neuron Express O					
		Password Petror Password	Generate Passwort				
		User Information Account Options Account Disable Policy					
		∨ User Groups E 1998-4110-Admin v ⊙					

7.2 Agregue el usuario con derechos de sólo lectura. Establezca un nombre y una contraseña y asígneselos a FPR-4110-ReadOnly, desplácese hacia abajo y haga clic en Submit para guardar los cambios.

= Cisc	o ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q. 🔘 🕼 🕼
Identities	Groups	External Identity Sources Identity Source Sequences Settings		
Users Latest Manual Ne	twork Scan Res	V Network Access User Useramia cisco_readonly Status E Gradeed V		
		Account Name Alias		
		Passwords Password Type: Internet Users Password Liferime: With Exploration ① Password with explorement New Construct Details New Construct Details		
		Password Re-Enter Password * Login Password Chable Password	Generate Password	
		User Information Account Options Account Disable Policy		
		✓ User Groups I FPR-4110-ReadOMy ✓ ③ ●		

7.3 Valide que los usuarios estén en Usuarios de acceso a la red.



Paso 8.Cree el perfil de autorización para el usuario administrador.

El chasis FXOS incluye las siguientes funciones de usuario:

- Administrador: acceso de lectura y escritura completo a todo el sistema. La cuenta de administrador predeterminada tiene asignada esta función de forma predeterminada y no se puede cambiar.
- Sólo lectura: acceso de sólo lectura a la configuración del sistema sin privilegios para modificar el estado del sistema.
- Operaciones: acceso de lectura y escritura a la configuración de NTP, la configuración de Smart Call Home para Smart Licensing y los registros del sistema, incluidos los servidores de registro del sistema y los fallos. Acceso de lectura al resto del sistema.
- AAA: acceso de lectura y escritura a usuarios, roles y configuración AAA. Acceso de lectura al resto del sistema

Atributos para cada función:

```
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"
```



Nota: Esta documentación sólo define los atributos admin y read-only.

Vaya al icono de hamburguesa ≡ > Política > Elementos de política > Resultados > Autorización > Perfiles de autorización > +Agregar.

Defina un nombre para el perfil de autorización, deje el tipo de acceso como ACCESS_ACCEPT y en Advanced Attributes Settings agregue cisco-av-pair=shell:roles="admin" con y haga clic en Submit.

≡ Cisco I	SE	Policy - Policy Elements	A Evaluation Mode 17 Days	Q	0 57	0
Dictionaries	Conditions	Results				
Authentication	>	Authorization Profile Authorization Profile				
Authorization Profil	les	* Name EPR-4110-Admiss				
Downloadable ACL	La	Description				
Profiling	>	* Access Type ACCESS_ACCEPT V				
Client Provisioning	>	Network Device Profile Case Case				
		ACL IPv6 (Fitter-ID)				
		Advanced Attributes Settings ^{III} Cisco:cisco-av-pair v * shelt:roles=*admin* v = +				
		Attributes Details Access type = ACCESS_ACCET dice-ar-pair = dheltrobes="admini"				
			Submit		Cancel	

8.1 Repita el paso anterior para crear el perfil de autorización para el usuario de sólo lectura. Cree la clase Radius con el valor read-only en su lugar Administrator esta vez.

= Cisco ISE	E Cisco ISE						Evaluation Mode 18 Days	Q () 55	a o
Dictionaries Conditio	ons	Results								
Authentication	~	Authorization Profiles > New J Authorization Profile	Authorization Profile							
Authorization Profiles Downloadable ACLs		* Name	FPR-4110-ReadOnly							
		Description								
Profiling	>									
Posture	>	- Access Type	ACCESS_ACCEPT ~							
Client Provisioning	>	Network Device Profile	tta Cisco 🗸 🕀							
		Service Template Track Movement Agentiess Posture Passive Identity Tracking								

ACL IPv6 (Filter-ID)		
✓ Advanced Attributes Settings □ Ciscoxisco-av-pair ✓ * sheltroles**read-only* ✓ = +		
 ✓ Attributes Details: 		
Access Type = ACCESS_ACCEPT disct-ar-pair = sheltsrole="read-only"	h.	
	Submit	Cancel

Paso 9.Cree un conjunto de políticas que coincida con la dirección IP de FMC. Esto es para evitar que otros dispositivos concedan acceso a los usuarios.

Navegue hasta ≡ Policy > Policy Sets >Agregar icono de signo en la esquina superior izquierda.

= Cisco I	SE			Policy · Policy Sets			Evaluation Mode 1	7 Days	۵ ۵	9 0
Policy Sets						Reset	Reset Policyset H	litcounts		Save
Status	Policy Set Name	Description	Conditions			Allowed Protoco	ls / Server Sequence	Hits	Actions	View
Q Search										
				+						
۰	Default	Default policy set				Default Network	Access 🥜 🕂	58	ø	>
								Reset		Save

9.1 Se coloca una nueva línea en la parte superior de los conjuntos de políticas. Haga clic en el icono Add para configurar una nueva condición.

🕕 Sta	tus	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sec	quence	Hits A	ctions	View
Q Se	arch									
	9	New Policy Set 1			+	Select from list	0 +		ŵ	•
	9	Default	Default policy set			Default Network Access	<i>o</i> +	58	合	>

9.2 Agregue una condición superior para el atributo RADIUS NAS-IP-Addressque coincida con la dirección IP de FCM y, a continuación, haga clic en Usar.

Library								
Search by Name								
● I ⑦ E S 8 7 ₽ ₽ 0 ₽ 0	F 🕹							
:: 🖻 sG								
E Catalyst_Switch_Local_Web_Authentication								
🗄 📄 Radius								
: Switch_Local_Web_Authentication								
B Switch_Web_Authentication								
:: B Wired_802.1X								
E Wired_MAB								
E Wireless_802.1X								
E Wireless_Access								
H Wireless_MAB								
# B WLC_Web_Authentication								

Editor

Ŷ

quals 🗸 Attri	Select attribute for c	ondition	1	9 E 🕈	X Wrong value	0
iet to 'Is not'	Dictionary	Attribute	ID	Info	Duplicate Save	
	All Dictionaries	Attribute	ID			
	Microsoft	MS-User-IPv4-Address	61	0		
	Network Access	ISE Host Name		0		
	• Radius	DNS-Server-IPv6-Address	169	0		
	Radius	Framed-IP-Address	8	0		
	Radius	Framed-IPv&-Address	168	0		
	Radius	NAS-IP-Address	4	0		
	Radius	Stateful+IPv6+Address+Pool	172	0		



9.3 Una vez completado, haga clic en Guardar.

≡ Cisco	ISE		Policy - Policy Sets		A Evaluation Mode 1	7 Days	Q (0)	58 ¢
Policy Sets	1			Reset	Reset Policyset Hi	tcounts		Save
🕣 Statu	is Policy Set Name	Description	Conditions	Allowed Protocols	/ Server Sequence	Hits	Actions	View
Q Sea	ch							
٥	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🛛 🗸 +		(2)	•
٥	Default	Default policy set		Default Network A	iccess 🖉 +	58		•
							_	
						Reset		Save



Sugerencia: para este ejercicio hemos permitido la lista Protocolos de acceso a la red predeterminados. Puede crear una lista nueva y reducirla según sea necesario.

Paso 10. Para ver el nuevo conjunto de políticas, pulse el icono > situado al final de la fila.

Policy Sets		Reset Reset Policyset Hitcounts Save
(+) Status Policy Set Name Descrip	tion Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
New Policy Set 1	Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Network Access 🤕 🗸 + 🔯 🏹

10.1 Expanda el menú Authorization Policy y haga clic en (+) para agregar una nueva condición.

	Authorization Dation (2)								
~	Authorization Policy (1)								
				Results					
	Status Rule Name	Conditions		Profiles	Security Groups	Hits	Actions		
	Q Search								
	Authorization Rule 1		+	Select from list 🥒 +	Select from list 🥒	+	\$		

10.2 Establezca las condiciones para que coincidan con el grupo DictionaryIdentity con AttributeName es igual a User Identity Groups: FPR-4110-Admins (el nombre de grupo creado en el paso 7) y haga clic en Use.

Cisco IC	Conditions Studio			a East	Rollins: Cote					A Post	0	×
	Library	Editor										
Statu	Search by Name		Identity	roup-Nar	me							•
	9 III 0 * 0 9 II 0 II 0 1 9		Equals	Selec	ct attribute for conditio	n						
	ii 👩 50 💿		Set to 'Is	•	리 모	₽ ₽ ∞ 2 8	01	0 t 🕈	Ĵ	Duplic	da Save	
Authen	E BYOD_is_Registered				Dictionary	Attribute	ID	Info				
Authori	: Catalyst_Switch_Local_Web_Authentication				All Dictionaries	Attribute	ID					· .
Authori	E Compliance_Unknown_Devices			-	IdentityGroup	Description		0				
	E Compliant_Devices				IdentityGroup	Name		0				
💿 is	EAP-MSCHAPv2				InternalUser	IdentityGroup		0				
Q	🗄 📑 EAP-TLS 📀			-	PassiveID	PassiveID_Groups		0				
	: O Guest_Flow			-	administrator	Externaruroups		0				
	E MAC_in_SAN O											
	E Setwork_Access_Authentication_Passed											
	: Non_Cisco_Profiled_Phones											
	E Non_Compliant_Devices											
	🗄 📋 Radius 📀											
	E P Switch_Local_Web_Authentication											
										Close	Use	•

brary	Edir	or	
Search by Name		IdentityGroup Name	6
0 1 2 4 9 9 9 8 8 8 9	10 E 🕈	Equals User Identity Groups: FPR-4110-	
. 50			
BYOD_is_Registered		Set to 'is not'	plicate Save
Catalyst_Switch_Local_Web_Authentication		NEW AND OR	
Compliance_Unknown_Devices			
Compliant_Devices			
EAP-MSCHAPv2			
🗄 📳 EAP-TLS			
Guest_Flow			
MAC_in_SAN			
B Network_Access_Authentication_Passed			
Non_Cisco_Profiled_Phones			
Non_Compliant_Devices			
🔋 🔋 Radius			
Switch_Local_Web_Authentication			

Paso 10.3 Valide que la nueva condición esté configurada en la política de autorización, luego agregue un perfil de usuario bajo Perfiles.

~ Authorization	Policy (1)		Results				
📀 Status	Rule Name	Conditions	Profiles	Security Groups		fits A	Actions
Q Search							
۰	Authorization Rule 1	R. IdentityGroup-Name EQUALS User Identity Groups:FPR-4110-Admin	FPR-4110-Admins ×	→ Select from list	\sim +		٨
۰	Default		DenyAccess	🖉 🕂 Select from list	1+	0	٨

Paso 11. Repita el mismo proceso en el paso 9 para los usuarios de sólo lectura y haga clic en Guardar.

Verificación

- 1. Intente iniciar sesión en la GUI de FCM con las nuevas credenciales de Radius
- 2. Navegue hasta el icono de hamburguesa ≡ > Operaciones > Radio > Registros en vivo.
- 3. La información mostrada indica si un usuario ha iniciado sesión correctamente.

=	≡ Cisco ISE						Operations	· RADIUS								A Evaluation	9.0	58 Ø			
Live	Logs	Live Sessions																			
	Misco	infigured Supplicants 🕕				Misconfigured	Network Devices 💿				RADIUS Drop	• 0			Client Stopped Resp	ionding 🕕				Repeat Co	unter 🕕
		0					0				1				0					0	
	ø	5 Reset Repeat Counts	₫ Export To ∨													Ref Ne	ver	Latest 20	records 🤟	Last 3 hour	o - 10
		Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address	Network (e Device Port	Identity Group	Posture	Server	Mdm Ser	IMEISV		Usecasi
	\times				~	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network D	vic Device Port	Identity Group	Posture St	a Server	Mdm Serve	IMEISV		Usecase
		Feb 03, 2024 01:51:51.0		i i		cisco_readonly			New Polic	New Polic	FPR-4110		FPR-4110		User Identity Group		marpatiniSE				
		Feb 03, 2024 01:50:48.9		0		cisco_admin			New Polic	New Polic	FPR-4110		FPR-4110		User Identity Group		marpatinISE				

4. Valide el rol de usuarios registrados desde la CLI del chasis de firewall seguro.

<pre>FPR4K-1-029A78B# security</pre>	scope se server		service-pro	ofile	
FPR4K-1-029A78B#	scope_sec	urity			
Remote User cisco	security a _admin:	# show	remote-user	detail	
User Roles:	010				
Name: rea	ad-only	#			
	,				

Troubleshoot

1. En la GUI de ISE , vaya al icono de hamburguesa ≡ > Operaciones > Radio > Registros en directo.

- 1.1 Valide si la solicitud de sesión de registro está llegando al nodo ISE.
- 1.2 Para ver el estado de error, revise los detalles de la sesión.

≡ Cisco ISE	(Operations - RADIUS	Livaluation 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
Ø ⇔Reset Repeat Counts di Export To ∨			Befresh Show Never V Latest 20 reco	rds v Uthin Last 3 hours v
Time Status	Details Repea Identity Endpoint ID	Endpoint Authenti Authoriz IP	Address Network De Device Port Identity Group Posture	Server Mdm Sei
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic IP	Address 🗸 Network Device Device Port Identity Group Posture	Sta Server Mdm Ser
Feb 02, 2024 07:32:18.8 🔮	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 Group:	marpatinISE
Feb 02, 2024 07:15:32.2	o cisco_admin	Default >> Default >> PermitAcc	FPR-4110 User Identity Groups	marpatin/SE

2. Para las solicitudes que no se muestran en los registros de Radius Live , revise si la solicitud UDP está llegando al nodo ISE a través de una captura de paquetes.

Vaya al icono de hamburguesa ≡ > Operaciones > Solución de problemas > Herramientas de diagnóstico > Volcado de TCP. Agregue una nueva captura y descargue el archivo en su máquina local para revisar si los paquetes UDP llegan al nodo ISE.

2.1 Rellene la información solicitada, desplácese hacia abajo y haga clic en Guardar.



2.2 Seleccione e inicie la captura.

E Cisco ISE			Operations - Trout	bleshoot						🛦 Evaluation Mode 17 Days Q. 🔘 🖟 🔘		
Diagnostic Tools Downloa	Diagnostic Tools Download Logs Debug Wizard											
General Tools ~	The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear and the second secon											
RADIUS Authentication Troubl												Rows/Page 1 → < < 1 / 1 > > Go 1 Total Rows
Execute Network Device Com Evaluate Configuration Validat	ø	Add 2 Edt () Train y	Start O Stop	Download								mer 🗸 - 💠
Posture Troubleshooting		Host Name	Network Interface	Filter	File Name	Reposito	File S	Number of	Time Limit	Promiscuous M	Status	
Agentiess Posture Troublesho EndPoint Debug	8	marpatinISE.marpatin.com	GigabitEthemat 0 [Up, Run	ip host 172.16.0.130	marpatinISE_GigabitEthernet		10	1	5	false	RUNNING	
TCP Dump												
Session Trace Tests												
TrustSec Tools												

- 2.3 Intento de registro en el chasis de firewall seguro mientras se ejecuta la captura de ISE
- 2.4 Detenga el volcado de TCP en ISE y descargue el archivo en un equipo local.
- 2.5 Revise la salida del tráfico.

Resultado esperado:

Paquete nº 1. Solicitud del firewall seguro al servidor ISE a través del puerto 1812 (RADIUS) Paquete nº 2. Respuesta del servidor ISE que acepta la solicitud inicial.



Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).