Konfigurieren von ISE Radius-Authentifizierung für Secure Firewall Chassis Manager (FCM)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Radius-Autorisierungs-/Authentifizierungszugriffs für den sicheren Firewall-Chassis-Manager mit der ISE beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, in den folgenden Bereichen über Kenntnisse zu verfügen:

- Secure Firewall Chassis Manager (FCM)
- Cisco Identity Services Engine (ISE)
- RADIUS-Authentifizierung

Verwendete Komponenten

- Cisco FirePOWER 4110 Security Appliance FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2 Patch 4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Konfigurationen

Sicherer Firewall-Chassis-Manager

Schritt 1: Melden Sie sich bei der Firepower Chassis Manager-GUI an. Schritt 2: Navigieren zu Plattformeinstellungen

verview Interface	s Logical De	vices Security Engine P	latform Settings				System	ı Tools Help adn
FPR4K-1-029A78 Model: Cisco Fi	B 172.16	.0.130 D Security Appliance	Version: 2.12(0.8)	perational State: Op	erable	Chassis Up	time 00:06:02	2:19 じ の①
DNSOLE MGMT USB		Power 2 - Removed	Network Module 1	7 8	Iodule 2 : Empty	Network	k Module 3 : Emp	ty
FAULTS 3(3) ⊗ CRITICAL	0(0) (MAJOR	INTERFACES 3 5 OWN @ U	INSTANCES O OOWN	1 @ UP	LICENSE Smart Agent UNREGISTERED	INVENTORY 1(1) Security Engine	6(6) ☆ Fans ≠	1(2) Power Supplies
Select All Faults Cancel	Selected Faults	Acknowledge				*		
Severity	Description			Cause	Occurrence	Time	e	Acknowledged
CRITICAL	FPGA version	lower than 2.00 is detected. A criti	cal upgrade from the firmwar	fpga-upgrade-requir	red 1	2022-02-20722	2:32:45.641	no
	Network Modu	ule 3 removed when in online state	. It is recommended to set m	module-suprise-remo	oval 1	2022-11-07T09	9:03:02.022	no
uccessful Login in last 24 h	rs - <u>View Details</u> Tr	hu Feb 01 2024 at 17:00:55 from - 17	2.16.0.35					ينياني ciso

Schritt 3: Klicken Sie im Menü links auf AAA. Wählen Sie Radius und fügen Sie einen neuen RADIUS-Anbieter hinzu.

Overview Interfaces Logic	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			and a	1.11 P. 1	_	_	_
MAC Pool	Hostname	Order	Service	Auth Port			
Resource Profiles							
Network Control Policy							
Chassis URL							
	Saus Canad						
	Save Cance						
Successful Login in last 24 hrs - View D	etails Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35					

Schritt 4: Füllen Sie das Aufforderungsmenü mit den vom Radius Provider angeforderten Informationen aus. Klicken Sie auf 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

Schritt 5: Navigieren Sie zu System > Benutzerverwaltung.

Overview Interfaces Logi	cal Devices Security Engin	e Platform Settings		Sy	stem ⁴ Tools Help admin
			Configuratio	on Licensing Up	dates User Management
SSH SNMP	Properties				↑
HTTPS	Timeout:* 5 Sec:	;			
Syslog DNS FIPS and Common Criteria	Retries:* 1 RADIUS Providers				Add
Access List	Hostname	Order	Service	Auth Port	
Resource Profiles Network Control Policy Chassis URL	172.16.0.12	1	authorization	1812	26
	Save Cancel				
avascript:void(0) last 24 hrs - View	Details Thu Feb 01 2024 at 17:00:55 f	rom - 172.16.0.35			ululu cisco

Schritt 6: Klicken Sie auf die Registerkarte Einstellungen, und legen Sie im Dropdown-Menü die Standardauthentifizierung auf Radius fest. Scrollen Sie dann nach unten, und speichern Sie die Konfiguration.

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



Hinweis: Die FCM-Konfiguration ist zu diesem Zeitpunkt abgeschlossen.

Identity Service Engine

Schritt 1: Hinzufügen eines neuen Netzwerkgeräts

Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Network Resources > Network Devices > +Add.

			Administration · Netv	vork Resources			🛦 Evaluation Mode 18 Days Q 💮 🕫 🚭
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 0 🦪 🔕
	2 Edit + Ad	td 🚺 Duplicate 🕁 Import	🗄 Export 🗸 🛛 👌 Generate P/	AC 👩 Delete 🗸			\sim \sim 14
	Name	e 🔿 IP/Mask	Profile Name	Location Type		Description	
				No data available			

Schritt 2: Geben Sie die Parameter an, die für die Informationen zu den neuen Netzwerkgeräten angefordert wurden.

2.1 Aktivieren Sie das Kontrollkästchen RADIUS.

2.2 Konfigurieren Sie den gleichen Shared Secret-Schlüssel wie in der FCM Radius-Konfiguration.

2.1 Blättern Sie nach unten, und klicken Sie auf Senden.

🔳 Cisco ISE	Administration - Network Resources	A Evaluation Mode 18 Days	1 0 9	8 Q
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 Device			
	Description			
	E #A60HH · · *P: 172.16.6.130 / 32 •			
	Device Profile Image: Control Image:			
	Subware Venion 2,12			
	Location All Locations V Set To Default			
	IPSEC Is IPSEC Device V Set To Default			
	Device Type: All Device Types V Set To Default			
	RADIUS Authentication Settings			
	MADUS LUP Settings Protocol RADUS			
	Shared Secret Show			
	Second Shared Share			

Schritt 3: Überprüfen Sie, ob das neue Gerät unter "Netzwerkgeräte" angezeigt wird.

	Administration - Netw	ork Resources			A Evaluation Mode 18 Days Q	0	59	ø
Network Device Groups Network Device P	rofiles External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors More \vee			
Network Devices								
	l mar A para co A como para	6 page 11			Selected 0 Total	10	0	
Name \sim IP/Mask	Profile Name Location	Туре	Description			A1 ~	v	
FPR-4110 172.16.0	🚔 Cisco 🕕 All Locations	All Device Types						
	Network Device Groups Network Device P	Network Device Groups Network Device Profiles External RADIUS Servers Network Devices Import © Expert © © Generate PAG Name © IP/Mask Profile Name Location Import © FPR-4110 172.16.0 @ Cisco © All Locations	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers Network Devices Immont I P/Mask Profile Name Location Type Description Immont I P/Mask Profile Name Locations All Device Types Immont I Device Types	Network Device Groups Network Device Profile External RADIUS Server RADIUS Server Sequence NAC Manages External RADIUS Network Devices Image: Comparison of the profile Image: Comparison of the pro	Network Device Drougs Network Device Profile External RADIUS Servers RADIUS Servers NAC Managers External MDM acklind Direct Connectors Mere	Accesse columnitation - Network Resources ADDUS Servers Ser	Administration - Network Besources NaC Managers External NDM pxdrid Direct Connectors More Network Device Brougs Network Device Profiles External RADUUS Servers RADUUS Servers Sequences NAC Managers External NDM pxdrid Direct Connectors More Image: Server Devices Image: Server Devices<

Schritt 4: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zum Burger-Symbol ≡ in der oberen linken Ecke > Administration > Identity Management > Groups > User Identity Groups > + Add.

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 💿 🕫 🖨
Identities Groups External Identi	ity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 10 N		Selected 0 Total 9 🧭 🚳
> Endpoint Identity Groups	2 Edit + Add Delete V & Import D Export V	$\sim ~ \nabla$
> 🛅 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	
	□ 👫 OWN_ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	

Schritt 5: Legen Sie einen Namen für die Admin User Identity Group fest, und klicken Sie auf Submit (Senden), um die Konfiguration zu speichern.

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💮 👼
Identities Groups External Ide		
) Guser identity droups	Description	Cancel

5.1 Wiederholen Sie den gleichen Vorgang für schreibgeschützte Benutzer.

=	Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🖓 🖗
lde	entities Groups Ex	xternal Identity S	surces Identity Source Sequences Settings	
	Identity Groups EQ C THE > Endpoint identity C > User identity Group	User Iden aroups ps De	tentify Groups > New User Identify Group tity Group ame FPR-4110-ReadOnty User Group for Read Only Users.	
				Juliu

Schritt 6: Überprüfen Sie, ob die neuen Benutzergruppen unter Benutzeridentitätsgruppen angezeigt werden.

E Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 18 Days Q 🕥 🕞
Jentities Groups External Identi	ty Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< The second sec	∥ Edit + Add 🚯 Delete ∨ 🕁 Import 🖒 Export ∨	Selected 0 Total 11 🧭 🚳
> 🛅 User Identity Groups	Name ^ Description	
	ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	C & Employee Default Employee User Group	
	□ ≹ FPR-4110-Admin User Group for Administrator.	
	KFR-4110-ReadOnly User Group for Read Only Users.	
	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	
	C & GuestType_SocialLogin (default) Identity group mirroring the guest type	
	GuestType_Weekly (default) Identity group mirroring the guest type	
	KOWN_ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	
	A Radius	

Schritt 7. Erstellen Sie die lokalen Benutzer, und fügen Sie sie ihrer entsprechenden Gruppe hinzu. Navigieren Sie zum Burger-Symbol ≡ > Administration > Identity Management > Identities > + Add.

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days Q 😗 🗖 🔯
Identities Groups Ex	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 Hinzufügen des Benutzers mit Administratorrechten. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie FPR-4110-Admin zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🖓 💿
Identities Groups E	ternal Identity Sources Identity Source Sequences Settings		
Users Lettert Manual Network Scen Res	✓ Network Access User * Usemane claca_dmin Satura ■ Crubied ~ Account Name Alas ● Email ● ✓ Password S ● Password Type: intermet Users • Password Type: ● ● Password S ● ● Password S ● ● Password Type: ● ● Password ant experts 00 mps ● O New Classies 00 ●		
	Passeord Be-Criter Passeord	Cenerate Pasanote Cenerate Pasanote	

7.2 Fügen Sie den Benutzer mit Lesezugriff hinzu. Legen Sie einen Namen und ein Kennwort fest, und weisen Sie sie FPR-4110-ReadOnly zu. Scrollen Sie nach unten, und klicken Sie auf Submit (Senden), um die Änderungen zu speichern.

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q, 💿 🕼 🚳
Identities Groups E	ternal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	✓ Network Access User * Usersana * Usersana Siatus Account Name Allas Emai		
	Password Type: Internet Users Password Lifetime: Who Equivation ③ Password Lifetime: Never Explose ③ Never Explose ③ Desearch Bit force Desearch		
	* Login Password	Generate Password Image: Constant Password	
	> User Information		
	Account Disable Policy		
	✓ User Groups E FPR-4110-ReadOny ✓ ① ●		

7.3 Überprüfen Sie, ob sich die Benutzer unter Netzwerkzugriffsbenutzer befinden.



Schritt 8: Erstellen Sie das Autorisierungsprofil für den Administrator-Benutzer.

Das FXOS-Chassis umfasst die folgenden Benutzerrollen:

- Administrator Vollständiger Lese- und Schreibzugriff auf das gesamte System. Dem Standardadmin-Konto ist diese Rolle standardmäßig zugewiesen und kann nicht geändert werden.
- Read-Only Schreibgeschützter Zugriff auf die Systemkonfiguration ohne Berechtigung zum Ändern des Systemstatus.
- Betrieb Lese- und Schreibzugriff auf die NTP-Konfiguration, die Smart Call Home-Konfiguration für Smart Licensing und Systemprotokolle, einschließlich Syslog-Server und Fehler. Lesezugriff auf das übrige System.
- AAA Lese- und Schreibzugriff auf Benutzer, Rollen und AAA-Konfiguration. Lesezugriff auf das übrige System

Attribute für jede Rolle:

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

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

```
cisco-av-pair=shell:roles="operations"
```

```
cisco-av-pair=shell:roles="schreibgeschützt"
```



Hinweis: In dieser Dokumentation werden nur die Attribute admin und read-only definiert.

Navigieren Sie zum Burger-Symbol ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Definieren Sie einen Namen für das Autorisierungsprofil, belassen Sie den Zugriffstyp ACCESS_ACCEPT, und fügen Sie unter Erweiterte Attributeinstellungen cisco-avpair=shell:roles="admin" mit hinzu, und klicken Sie auf "Senden".

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 17 Days	• Q	0;	20
Dictionaries Conditions	Results				
Authentication >	Authorization Profile Authorization Profile				
Authorization Profiles	* Name EOP_4110.54mins				
Downloadable ACLs	Description				
Profiling	* Access Type				
Posture >	ACCESS_ACCEPT				
Client Provisioning >	Network Device Profile III: Class VIII Service Template C Track Movement C Agenties Posture C Passive Identity Trackling C				
	ACL IPv6 (Fitter-ID)				
	Advanced Attributes Settings				
	Image: Cisco.cisco-av-pair * sheltroles**admin* v = +				
	Attributes Details Access type = ACCESS_ACCEPT dice-ar-pair = aheltraises="admin"				
		Submit		Canc	el

8.1 Wiederholen Sie den vorherigen Schritt, um das Autorisierungsprofil für den schreibgeschützten Benutzer zu erstellen. Erstellen Sie diesmal die Radius-Klasse mit dem Wert read-only anstelle von Administrator.

= Cisco ISE				Policy - Policy Elements		A Evaluation Mode 18 Days	9,0	5	0
Dictionaries Condition	1S	Results							
Authentication	~ ~	Authorization Profiles > New J Authorization Profile	Authorization Profile						
Authorization Profiles Downloadable ACLs		* Name Description	FPR-4110-ReadOnly]					
Profiling	>	* Access Type							
Client Provisioning	2	Network Device Profile	±Cisco ∨⊕	_					
		Service Template Track Movement Agentiess Posture Passive Identity Tracking							

ACL IPv6 (Filter-ID)		
Advanced Attributes Settings		
"Ciscoctisco-av-pair V shelt:roles="read-only" V = +		
Attributes Details Access Type + ACCESS ACCEPT disco-ar-year - athetosies-"read-only"		
	Submit	Cancel

Schritt 9: Erstellen eines Policy Sets, das mit der IP-Adresse des FMC übereinstimmt Auf diese Weise wird verhindert, dass andere Geräte den Benutzern Zugriff gewähren.

Navigieren Sie zu \equiv > Policy > Policy Sets > Add icon sign in der oberen linken Ecke.

= Cisco ISE			Policy · Policy Sets	A Evaluation Mode	17 Days	۵ ۵	Ø 0
Policy Sets				Reset Reset Policyset	Hitcounts		Save
Status Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
Q Search							
			+				
O Default	Default policy set			Default Network Access 🧳 🖉 +	58	<u>@</u>	>
					Reset		Save

9.1 Eine neue Zeile wird an die Spitze Ihrer Policy Sets gesetzt. Klicken Sie auf das Symbol Hinzufügen, um eine neue Bedingung zu konfigurieren.

🕣 Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequ	ience Hi	its Action	View
Q Searc								
٥	New Policy Set 1			+	Select from list	e +	ŵ	>
0	Default	Default policy set			Default Network Access	۶ + 54	\$	>

9.2 Fügen Sie eine Top-Bedingung für ein RADIUS NAS-IP-Adressattribut hinzu, das mit der FCM-IP-Adresse übereinstimmt, und klicken Sie dann auf Verwenden.

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

Radius-NAS-IP-Addres Equals V Attri	s Select attribute for condit	ion			X Wrong value	52 ¢
Set to 'Is not'	Dictionary	Attribute	L O	는 후 Info	Duplicate Save	
	All Dictionaries ~	Attribute MS-User-IPv4-Address	ID 61	0		*
	Network Access	ISE Host Name		0		
	Radius Radius	DNS-Server-IPv6-Address Framed-IP-Address	8	0		Save
	Q Radius	Framed-IPv&-Address	168	0		
	Radius Radius	NAS-IP-Address Stateful-IPv6-Address-Pool	4	0		



9.3 Klicken Sie abschließend auf Speichern.

≡ 0	Cisco IS	SE		Policy - Policy Sets		A Evaluation Mode	17 Days	Q (0)	6 R
Policy	Sets				Reset	Reset Policyset	Hitcounts		Save
۲	Status	Policy Set Name	Description	Cenditions	Allowed Protocol	s / Server Sequenc	e Hits	Actions	View
Q	Search								
	۰	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network	Access 🛛 🗸 🕂		(2)	>
	۰	Default	Default policy set		Default Network	Access 🥒 🕂	58		>
								_	
							Reset		Save



Tipp: Für diese Übung haben wir die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

Schritt 10. Zeigen Sie den neuen Richtliniensatz an, indem Sie auf das > Symbol am Ende der Zeile klicken.

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	Radius NAS-IP-Address EQUALS 172.16.0.130	Default Network Access 💿 🗸 + 🚳 🕨

10.1 Erweitern Sie das Menü Autorisierungsrichtlinie, und klicken Sie auf (+), um eine neue

Bedingung hinzuzufügen.

√ Au	V Authorization Policy (1)												
					Results								
۲	Status Rule Name	Conditions			Profiles	Security Groups	Hitr	s Actions					
	Q Search												
	Authorization Rule 1		+		Select from list	# Select from list	<i>•</i> +	 					

10.2 Legen Sie die Bedingungen so fest, dass sie mit der Dictionaryldentity-Gruppe mit AttributeName gleich User Identity Groups:FPR-4110-Admins (dem in Schritt 7 erstellten Gruppennamen) übereinstimmen, und klicken Sie auf Use (Verwenden).

Se Co	onditions Studio			hallan	Ballau Pate					A	0	×
Libra	ary	Editor										
Statu	arch by Name		IdentityG	iroup-Na	me						0	Э
			Equals	Sele	ct attribute for conditio	n		×				
	E 5G 0		Set to 'Is	•	12 O 🔹 🔍 🖳	9888	0 1	0 t 🕈		Duplicate	Save	
uthen	BYOD_is_Registered 0				Dictionary	Attribute	ID	Info				
uthor	Catalyst_Switch_Local_Web_Authentication				All Dictionaries	Attribute	ID					
uthon	Compliance_Unknown_Devices			-	GWA MartinGroup	CWA_ExternalGroups		0				
8	Compliant_Devices			-	IdentityGroup	Name		0				
s	E EAP-MSCHAPv2				InternalUser	IdentityGroup		0				
Q	EAP-TLS O				PassiveID	PassiveID_Groups						
8	Cuest_Flow O			•	adminstrator	ExternalGroups		0				
:	MAC_in_SAN O											
8	Network_Access_Authentication_Passed											
	Non_Cisco_Profiled_Phones											
8	Non_Compliant_Devices											
	🕫 Radius 📀											
	Switch_Local_Web_Authentication O											
									Ch	550	Use	

Conditions Studio		Rollan Rollan Color A Conservation	0	×
Search by Name	Editor	IdentityGroup Name		•
•	•	Equals Vuser identity Groups: SPR-4110- Admin	_	
ii 🖪 sa 💿	-	~		
E BYOD_is_Registered		Set to 'is not'	Save	
# E Catalyst_Switch_Local_Web_Authentication		NEW AND OR		
E Compliance_Unknown_Devices				
: Compliant_Devices				
E EAP-MSCHAPv2				
ii 📴 EAP-TLS 💿				
: Cuest_Flow 0				
H 🛛 MAC_In_SAN 💿				
E B Network_Access_Authentication_Passed				
II II Non_Cisco_Profiled_Phones				
E Non_Compliant_Devices				
🗄 🔋 Radius 💿				
# 🕅 Switch_Local_Web_Authentication ()				
		Close	Use	

Schritt 10.3 Überprüfen Sie, ob die neue Bedingung in der Autorisierungsrichtlinie konfiguriert ist, und fügen Sie dann unter "Profile" ein Benutzerprofil hinzu.

\vee Authorization	Policy (1)									
			Results							
 Status 	Rule Name	Conditions		Profiles		Security Groups		Hits	Actions	
Q. Search										
۰	Authorization Rule 1	R IdentityGrup Name EQUALS User Identity Grups:FPR-4110-Admin		FPR-4110-Admins \times	<u>~</u> +	Select from list	<u>~</u> +		٥	
۰	Default			DenyAccess	/ +	Select from list	1+	0	ŵ	

Schritt 11. Wiederholen Sie den gleichen Vorgang in Schritt 9 für schreibgeschützte Benutzer, und klicken Sie auf Speichern.

Überprüfung

1. Versuchen Sie, sich mit den neuen RADIUS-Anmeldeinformationen bei der FCM-GUI anzumelden.

- 2. Navigieren Sie zum Burger-Symbol ≡ > Operations > Radius > Live logs.
- 3. Die angezeigten Informationen zeigen an, ob ein Benutzer erfolgreich angemeldet wurde.

≡ Cisco ISE								Operations - RADIUS								🛦 Evaluation Mode 17 Days Q 💿 🕫 💿			58 0		
ive Logs	s Live Sessions																				
Misc	configured Supplicants 🕕				Misconfigured	Network Devices 📀				RADIUS Drop	• 0			c	lient Stopped Resp	onding 🕕				Repeat Co	unter 💿
	0					0				1					0					C)
ø	Seset Repeat Counts 1	🗄 Export To 🗸														N	resh rver	↓ Latest 20	records 🥪	Last 3 hou	ns v o
	Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address		Network De	Device Port	Identity Group	Posture	Server	Mdm Ser	IMEISV		Usecase
×				~	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~	Network Devic	Device Port	Identity Group	Posture 1	ta Server	Mdm Serve	IMEISV		Usecase
	Feb 03, 2024 01:51:51.0		ò		cisco_readonly			New Polic	New Polic	FPR-4110			EPR-411D		User Identity Group		marpatini58				
L	Feb 03, 2024 01:50:48.9		ō		cisco_admin			New Polic	New Polic	FPR-4110			FPR-4110		User Identity Group		marpatiniSE				

4. Rolle der protokollierten Benutzer in der Secure Firewall Chassis CLI überprüfen.



Fehlerbehebung

1. Navigieren Sie über die ISE-GUI zum Burger-Symbol ≡ > Operations > Radius > Live-Protokolle.

- 1.1 Überprüfen Sie, ob die Protokollsitzungsanforderung den ISE-Knoten erreicht.
- 1.2 Überprüfen Sie bei Status "Fehlgeschlagen" die Sitzungsdetails.

E Cisco ISE	c	Operations - 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
හි කිසෙන් Repeat Counts ක් Expert To 🗸			Never Show Latest 20 rec	ords v Hubin Last 3 hours v
Time Status	Details Repea Identity Endpoint ID	Endpoint Authenti Authoriz IP Add	dress Network De Device Port Identity Group Postur	re Server Mdm Sei
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic Authorizatic IP Ade	dress 🗸 Network Device Device Port Identity Group Posture	e Sta Server Mdm Sen
Feb 02, 2024 07:32:18.8 🧿	cisco_admin	Default >> Default	FPR-4110 User Identity Group:	marpadinISE
Feb 02, 2024 07:23:20.1	cisco_readonly	Default >> Default >> PermitAcc	FPR-4110 User identity Group:	marpadinISE
Feb 02, 2024 07:15:32.2	G cisco_admin	Default >> Default >> PermitAcc	FPR-4110 User Identity Group:	marpatinISE

2. Überprüfen Sie bei Anfragen, die nicht in Radius Live-Protokollen angezeigt werden, ob die

UDP-Anfrage den ISE-Knoten über eine Paketerfassung erreicht.

Navigieren Sie zum Burger-Symbol ≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dump. Fügen Sie eine neue Erfassung hinzu, und laden Sie die Datei auf Ihren lokalen Computer herunter, um zu überprüfen, ob die UDP-Pakete beim ISE-Knoten eintreffen.

2.1 Füllen Sie die gewünschten Informationen aus, scrollen Sie nach unten und klicken Sie auf Speichern.

E Cisco ISE	Operations - Troubleshoot	🛦 Evaluation Mode 17 Days Q. (1) 🕼 🖗
Diagnostic Tools Downloa	ad Logs Debug Wizard	
General Tools ~	10P Dung 3 New	
Execute Network Device Com	Add TCP Dump	
Evaluate Configuration Validat	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.	
Posture Troubleshooting Agentiess Posture Troublesho EndPoint Debug	Hijst Nane* marpatixISE V	
TCP Dump Session Trace Tests	Nereok Norrisce* GigabitEthemet 0 [Up, Running] ()	
Trustfiec Tools	Faur (ip host 172.16.0.130) (ip host 10.77.122.123 and not (i) 10,177.122.119	

2.2 Auswahl und Start der Erfassung.

E Cisco ISE	Operations - Trout	bleshoot						🛦 Evaluation Mode 17 Days Q. 🔘 🕫 🔘				
Diagnostic Tools Download	d Logs	Debug Wizard										
General Tools 🗸 🗸	The	TCP Dump utility page is to n	monitor the contents of pack	ets on a network interface an	d troubleshoot problems on	the network as	they appe	ar				
RADIUS Authentication Troubl												Rows/Page 1 → I < 1 / 1 > I Go 1 Total Rows
Execute Network Device Com Evaluate Configuration Validat	ø	Add 2 Edt () Train 1	✓ ■ Start ⊖ Step ::	E. Download								riter 🗸 - 🔶
Posture Troubleshooting		Host Name	Network Interface	Filter	File Name	Reposito	File S	Number of	Time Limit	Promiscuous M	O Status	
Agentiess Posture Troublesho EndPoint Debug		marpatintSE.marpatin.com	GigabitEthemet 0 [Up, Run	ip host 172.16.0.130	marpatiniSE_GigabitEthemet		10	1	5	false	RUNNING	
TCP Dump												
Session Trace Tests												
TrustSec Tools												

2.3 Versuchen Sie, sich beim sicheren Firewall-Chassis anzumelden, während die ISE-Erfassung ausgeführt wird.

2.4 Stoppen Sie den TCP-Dump in der ISE, und laden Sie die Datei auf einen lokalen Computer herunter.

2.5 Überprüfen der Datenverkehrsausgabe

Erwartete Ausgabe:

Paket Nr. 1 Anfrage von der sicheren Firewall an den ISE-Server über Port 1812 (RADIUS) Paket Nr. 2 Die Antwort des ISE-Servers akzeptiert die erste Anforderung.

	•			🚄 marpatinISE_GigabitEthernet 2.pc	ip							
4	· 🖄 🖄 📹 🕲 🕭 🔳	२ 🗢 🗢 😫 쥼	👲 🗔 🔳 🤅	e e e 🛄								
📕 Appl	📕 Apply a display filter <\$\$/>											
No.	Time	Source	Destination	Length Protocol Message Transaction	ID Info							
	1 2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128 RADIUS	Access-Request id=22							
	2 2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186 RADIUS	Access-Accept id=22							

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.