Secure Firewall Chassis Manager(FCM)用のISE Radius認証の設定

内容

はじめに

このドキュメントでは、ISEを使用したSecure Firewall Chassis Manager(SFM)のRADIUS許可/認証アクセスを設定する方法のプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

- ・ Cisco Firepower 4110セキュリティアプライアンスFXOS v2.12
- ・ Cisco Identity Services Engine(ISE)v3.2パッチ4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。こ のドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始 しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を 十分確認してください。

設定

コンフィギュレーション

セキュアファイアウォールシャーシマネージャ

ステップ 1 : Firepower Chassis Manager(FCM)のGUIにログインします。 ステップ 2 : Platform Settingsに移動します。

FPR4K-1-029A78	s Logical De B 172.16	vices Security Engin	Platform S	Settings				Sys	tem Tools Help ad
Model: Cisco Fi	repower 411	0 Security Appliance	Version:	2.12(0.8) Of	perational State: O	perable	Chassi	s Uptime 00:0	6:02:19 (J P (J)
ONSOLE MGMT USB		Power 2 - Removed		Network Module 1	7 7 8	Module 2 : Empty	Net	work Module 3 :)	Empty
FAULTS 3(3) © CRITICAL	0(0) MAJOR	INTERFACES 3 DOWN	5 100	INSTANCES O O DOWN	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	1	Time	Acknowledged
CRITICAL	FPGA version	lower than 2.00 is detected	A critical upgrade	e from the firmwar	fpga-upgrade-requ	ired 1	2022-02-20	DT22:32:45.641	no
	Network Mode	ule 3 removed when in onlir	e state. It is recon	nmended to set m	module-suprise-rem	oval 1	2022-11-0	7T09:03:02.022	no
uccessful Login in last 24 h	rs - <u>View Details</u> T	hu Feb 01 2024 at 17:00:55 f	rom - 172.16.0.35						2 alta cis

ステップ 3:左側のメニューからAAAをクリックします。 RadiusとAdd a new RADIUS providerを選択します。

verview Interfaces Logic	al Devices Security Engine	Platform Settings		System	n Tools Help	admin
NTP	LDAP RADIUS TACACS					
SSH						
SNMP	Properties					
HTTPS	Timeout:* 5 Secs					
AAA	Petries.*					
Syslog	PADILIS Provider					
DNS					_	
FIPS and Common Criteria						Add
Access List	Hostname	Order	Service	Auth Port		
MAC POOI						
Network Control Policy						
Chassis URL						
	Same Canad					
	Save					
uccessful Login in last 24 hrs - <u>View D</u>	Petails Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35				cisc

ステップ 4:プロンプトメニューに、RADIUSプロバイダーに関する必要な情報を入力します。 [OK] をクリックします。

NTP SSH SMMP HTTPS AAA Syslog DNS FIPS and Common Criteria Access List MAC Pool Resource Profiles Network Control Policy Chassis URL Imeout:* Ser Imeout:* Ser Network Control Policy Chassis URL Imeout:* Ser Imeout:* Ser Imeout:* Ser Chassis URL Imeout:* Ser Ser Imeout:* Ser Ser Imeout:* Ser Retries:* Imeout:* Ser Ser Imeout:* Ser Ser Imeout:* Ser Ser Imeout:* Ser Ser Imeout:* Ser Retries:* Imeout:* Ser Retries:* Imeout:* Ser Retries:*	Overview Interfaces Logi	cal Devices Security Engin	e Platform Settings			System Tools Help admin
Sysiog DNS FIPS and Common Criteria Access List MAC Pool Resource Profiles Network Control Policy Chassis URL Authorization Port:* Immeout:* Retries:* Authorization Port:* Immeout:* Retries:* Order:* Muthorization Port:* Immeout:* Retries:* Immeout:* Sysion Immeout:* Immeout:*	NTP SSH SNMP HTTPS	LDAP RADIUS TACAC Properties Timeout:* 5 Sec	S			
Timeout:* 5 Secs Retries:* 1 OK Cancel	Syslog DNS FIPS and Common Criteria Access List MAC Pool Resource Profiles Network Control Policy Chassis URL	Retries:* 1 RADIUS Providers Hostname	Add RADIUS Provider Hostname/FQDN/IP Address:* Order:* Key: Confirm Key: Authorization Port:*	172.16.0.12 lowest-available ••••••• 1812	Set: No	ort
		Save Cancel	Timeout:* Retries:*	5 1 ОК	Secs	

ステップ 5: System > User Managementの順に移動します。

Overview Interfaces Logic	al Devices Security Engine	Platform Settings			System ⁴ Tools Help adr
			Configuratio	n Licensing	Updates User Managem
SSH SNMP HTTPS	Properties				†
AAA Syslog DNS FIPS and Common Criteria	Retries:* 1 RADIUS Providers				a Add
Access List MAC Pool	Hostname	Order	Service	Auth Port	
Resource Profiles Network Control Policy Chassis URL	172.16.0.12	1	authorization	1812	25
	Save				
iavascript:void(0) last 24 hrs - View (Details Thu Feb 01 2024 at 17:00:55 fro	m - 172.16.0.35			مالية

手順 6 : Settingsタブをクリックして、ドロップダウンメニューからDefault Authenticationを Radiusに設定し、スクロールダウンして設定を保存します。

Overview Interfaces Logica	al Device	es Security Engine Platform Settings			System	Tools Help ad	min
			Configuration	Licensing	Updates	User Managem	ent
Local Users Settings							
Default Authentication	Local Local	*Local is fallback authentication method					
Console Authentication	RADIUS LDAP	• •					
Remote User Settings	TACACS	5					
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				(1) (15	() CO



注:FCMの設定はこの時点で完了しています。

アイデンティティサービスエンジン

ステップ1:新しいネットワークデバイスを追加します。

左上隅にあるバーガーアイコン≡ージ> Administration > Network Resources > Network Devices > +Addに移動します。

≡ Cisco ISE			Administration · Net	work 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 🧭 🚳
	0 Edit + Ad	d Duplicate 🕁 Import	🗄 Export 🗸 🛛 🙆 Generate Pi	AC 🚦 Delete 🗸			$\sim 10^{-10}$
	Name	∧ IP/Mask	Profile Name	Location Type		Description	
				No data available			

ステップ2:新しいネットワークデバイス情報に関して要求されるパラメータを入力します。

2.1 RADIUSチェックボックスのチェック

2.2 FCM RADIUS設定と同じ共有秘密キーを設定します。

2.1下にスクロールして、Submitをクリックします。

🔳 Cisco ISE	E Administration - Network Resources	🛦 Evaluation Mode 18 Days Q, 🛞 💭 🕀
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxG	rid Direct Connectors Location Services
Network Devices Default Device Device Security Settings	Network Device List > knew Network Device Network Device Network Device Network Device Network Device	
	Description	
	Device Profile III Coco 🗸 🗸	
	Model Name EPR-4110 V	
	Software Version 2.12	
	Location All Locations V Set To Default	
	IPSEC Is IPSEC Device V Set To Default	
	Device Type All Device Types Set To Default	
	ADJUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS Shared Secret Show	
	Use Second Shared Secret 📀	
	Second Shared Show	

ステップ3:[ネットワークデバイス]に新しいデバイスが表示されていることを確認します。

≡ Cisco ISE		Administration - Netw	vork Resources			A Evaluation Mode 18 Days Q	0 [,70 ·	ø
Network Devices Net	twork 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	쇼 Export > 은 Generate PAC	D 🚦 Delete 🗸			Selected 0 Total 1	8 • ~	© 7	
	Name ∧ IP/Mask Profile FPR-4110 172.16.0, m Cisc	Name Location	Type All Device Types	Description					

ステップ 4: 必要なユーザIDグループを作成します。左上隅にあるバーガーアイコン≡ージ> Administration > Identity Management > Groups > User Identity Groups > + Addに移動します

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 💮 📈 💮
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 18 0		Selected 0 Total 9 🧭 🚳
> 🛅 Endpoint Identity Groups		$\sim \nabla$
> 🛅 User Identity Groups	Name Description	
	ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	Employee 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	
	A OWN_ACCOUNTS (default) Default OWN_ACCOUNTS (default) User Group	

ステップ 5:管理者ユーザIDグループの名前を設定して、Submitをクリックし、設定を保存しま す。

≡ Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 🛞 💮
Identities Groups E	xternal Identity Sources Identity Source Sequences Settings	
Identity Groups	Broups > New User Identity Group Broups * Name PR-4110-Admin User Group for Administrator. Description	Submit

5.1読み取り専用ユーザに対して同じプロセスを繰り返します。

≡ Cisc	o ISE			Administra	ation - Identity Management		A Evaluation Mode 18 Days	2 0 2	0
Identities	Groups	External Ide	ntity Sources	Identity Source Sequences Settin	ngs				
Identity G	Endpoint Identity Gi	ay Groups roups	User Identity Grou Identity Grou * Name Description	os > New User Identity Group P FPR-4110-ReadOnly User Group for Read Only Users.		Submit	Cancel		

手順 6:新しいユーザグループがユーザIDグループの下に表示されていることを確認します。

E Cisco ISE	Administration	Jentity Management 🛕 Evaluation Mode 18 Days Q 💿 🕫 🔅
dentities Groups External Ide	tity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 12 0		Selected 0 Total 11 🧷 🔕
> 🛅 Endpoint Identity Groups	/ Edit + Add 🔋 Delete 🗸 🕁 Import 🗅 Export 🗸	$\nabla \sim m$
> 🛅 User Identity Groups	Name Description	
	ALL_ACCOUNTS (default) Default A	CCOUNTS (default) User Group
	Default Er	yee User Group
	C 😤 FPR-4110-Admin User Grou	r Administrator.
	☐ ≹ FPR-4110-ReadOnly User Grou	r Read Only Users.
	GROUP_ACCOUNTS (default) Default G	P_ACCOUNTS (default) User Group
	GuestType_Contractor (default) Identity g	mirroring the guest type
	GuestType_Daily (default) Identity g	mirroring the guest type
	GuestType_SocialLogin (default) Identity g	mirroring the guest type
	GuestType_Weekly (default) Identity g	mirroring the guest type
	OWN_ACCOUNTS (default) Default O	ACCOUNTS (default) User Group
	Radius	

手順 7: ローカルユーザを作成し、対応するグループに追加します。 バーガーアイコン≡ > Administration > Identity Management > Identities > + Addに移動します。

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	ai \sim $~$ ∇
	Status Username A Description First Name Last Name Email Address User Identity Groups Admin	
	No data available	

7.1管理者権限を持つユーザを追加する。名前とパスワードを設定し、それをFPR-4110-Adminに 割り当て、スクロールダウンしてSubmitをクリックし、変更を保存します。

E Cisco	ISE				Administration - Identity Management	A Evaluation Mode 18 Days (201	78 0	
Identities	Groups	External Identity Sources	Identity Source Sequences	Settings					
Ukers	work Scan Res.	 Vetwork Acces Usemane Status Account Name Alias Email Passwords Password Lifetime: With Expiration Password all reg Never Expiration 	s User Sites.admin Enabled ~ In solution The solution of th	De-Enter Password					
		Enable Passerd Enable Passerd User Informati Account Optio Account Disab User Groups User Groups E #PR-4110-A	in ns le Palicy enn v () ()		Generate Passenet				

7.2読み取り専用権限を持つユーザを追加する。名前とパスワードを設定し、それをFPR-4110-ReadOnlyに割り当てます。スクロールダウンして、Submitをクリックし、変更を保存します。

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q. 💿 🕼 🚭
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings		
Users Latert Manual Network Scan Res	Vetwork Access User tuserame cisco.readonly Status		
	Passwords Password Type: Internet Users Password Lifetime: With Experises 0 Presence and experts #0 days Never Expires 0		
	Password Re-Criter Password * Login Password Enable Password > User Information	Generate Password O Generate Password O	
	Account Options Account Disable Policy User Groups		
	🗄 FPR-4110-ReadOnly 🗸 🕘 🔮		

7.3ユーザがNetwork Access Usersの下にあることを確認する。

😑 Cisco ISE	Ad	Iministration - Identity Management	A Evaluation Mode 18 Days Q ()	58 Ø
Identities Groups Exte	nal Identity Sources Identity Source Sequences Settings			
Users Latest Manual Network Scan Res	Network Access Users			
			Selected 0 Total 2	3 0
	🖉 Edit — + Add — 🛞 Change Status — 🕁 Import 🛆 Expert — 🍵 Delete — 🕞 Deleteration		AL ~	V
	Status Username 🔿 Description First Name Last Name Email Ad	Idress User Identity Groups Admin		
	Enabled 1 cisco_admin	FPR-4110-Admin		
	Enabled 1 cisco_readonly	FPR-4110-ReadOnly		

ステップ8:Adminユーザの許可プロファイルを作成します。

FXOSシャーシには、次のユーザロールが含まれます。

- 管理者:システム全体への読み取り/書き込みアクセス権を付与します。デフォルトの管理 者アカウントにはデフォルトでこのロールが割り当てられ、変更することはできません。
- 読み取り専用:システムの状態を変更する権限のない、システム設定への読み取り専用アクセス。
- 操作:NTP設定、Smart Licensing用のSmart Call Home設定、およびsyslogサーバと障害を 含むシステムログへの読み取りおよび書き込みアクセス。システムの他の部分への読み取り アクセス。
- AAA:ユーザ、ロール、およびAAA設定への読み取り/書き込みアクセス。システムの他の 部分への読み取りアクセス

各ロールの属性

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

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

cisco-av-pair=shell:roles="操作"

cisco-av-pair=shell:roles="読み取り専用"



注:このドキュメントでは、admin属性とread-only属性のみを定義しています。

バーガーアイコン≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

許可プロファイルの名前を定義し、アクセスタイプをACCESS_ACCEPTのままにして、 Advanced Attributes Settingsでcisco-av-pair=shell:roles="admin"を追加し、Submitをクリックし ます。

≡ Cisco ISE	Policy - Policy Elements	Evaluation Mode 17 Day	a Q	05	a ¢
Dictionaries Conditions	Results				
Authentication >	Authorization Profile 3 FPR-4110-Admins Authorization Profile				
Authorization Profiles	* Name FPR-4110-Admins				
Downloadable ACLs	Description				
Profiling > Posture >	* Access Type ACCESS_ACCEPT V				
Client Provisioning >	Network Device Profile actions block actions				
	ACL IPv6 (Filter-ID)				
	✓ Advanced Attributes Settings □ Clacoxisco-av-pair ✓ * shelt:roles* admin* ✓ = +				
	Attributes Details Access Type = ACCESS_ACCEPT doc-burgar = 3hdtroles="aonie"				

8.1前の手順を繰り返して、読み取り専用ユーザの許可プロファイルを作成します。今回は Administratorではなく、read-onlyの値でRadiusクラスを作成します。

= Cisco ISE			Policy · Policy Elements			4	Evaluation Mode 18 Days	Q (2)	59	٥
Dictionaries Conditions	Results									
Clisco ISE Cicionaries Condition Authorization Authorization Conversion Client Previolenting Client Previolentin		Authorization Profile								
Authorization Profiles	* Name	FPR-4110-ReadOnly								
	Description			1						
Profiling										
Posture	 Access Type 	ACCESS_ACCEPT ~								
Client Provisioning	Network Device Profile	± Cisco ∨⊕								
	Service Template Track Movement Agentiess Posture Passive Identity Tracking									

ACL IPv6 (Filter-ID)		
Advanced Attributes Settings Image: Ciscocisco-av-pair v * shelt:roles=*read-only* v = +		
Attributes Details Access type - ACCESS, ACCEPT		
Globa-výar = thetroises "read-only"	Submit	Cancel

ステップ9:FMC IPアドレスに一致するポリシーセットを作成します。これは、他のデバイスがユ ーザにアクセス権を付与するのを防ぐためです。

左上隅の≡> Policy > Policy Sets >Add icon signに移動します。

= 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				
			+	
O Default	Default policy set			Default Network Access 🥜 🕂 58 🔅 🕨
				Reset Save

9.1新しい品目がポリシーセットの一番上に表示されます。Addアイコンをクリックして、新しい 条件を設定します。

🕣 Statu	s Policy Set Name	Description	Conditions		Allowed Protocols / Server Seq	uence	Hits Actio	s View
Q Sear	h							
٥	New Policy Set 1			+	Select from list	0 +	ŵ	>
٥	Default	Default policy set			Default Network Access	0 +	50 (j)	>

9.2 FCM IPアドレスに一致するRADIUS NAS-IP-Addressattributeのトップ条件を追加し、Useを クリックします。

Library	
Search by Name	
	0 E 🕈
ii 📄 5G	
E Catalyst_Switch_Local_Web_Authentication	
🗄 🖪 Radius	
# E Switch_Local_Web_Authentication	
: Bwitch_Web_Authentication	
# 📳 Wired_802.1X	
: B Wired_MAB	
: [] Wireless_802.1X	
# 🗄 Wireless_Access	
# 📑 Wireless_MAB	
# B WLC_Web_Authentication	

Editor

Ŷ

adius-NAS-IP-Address	Selec	t attribute for conditio	n 🛛 🖉 🗏 O	T) L P	X Wrong value	View
t to 'is not'		Dictionary	Attribute	ID	Info	Duplicate Save	
		All Dictionaries	Attribute	ID			>
	۰	Microsoft	MS-User-IPv4-Address	61	0		>
	•	Network Access	ISE Host Name		0		
	۰	Radius	DNS-Server-IPv6-Address	169	0		
	۰	Radius	Framed-IP-Address	8	0		iave
	•	Radius	Framed-IPv6-Address	168	0		
	•	Radius	NAS-IP-Address	4	0		
	۰	Radius	Stateful-IPv6-Address-Pool	172	0		



9.3完了したら、Saveをクリックします。

=	Cisco I	SE		Policy - Policy Sets		A Evaluation	Mode 17	Days (Q (0)	6 BJ
Polic	y Sets				Reset	Reset Poli	cyset Hite	counts		Save
۲	Status	Policy Set Name	Description	Conditions	Allowed Protoco	ols / Server Sec	quence	Hits	Actions	View
3	λ Search									
	۰	New Policy Set 1		Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Networ	k Access 🛛	\sim +		<u>م</u>	>
	۰	Default	Default policy set		Default Network	(Access	0+	58	(2)	>
									_	
							1	Reset		Save



ヒント:この演習では、デフォルトのNetwork Access Protocolsリストを許可しています 。新しいリストを作成し、必要に応じてリストを絞り込むことができます。

ステップ10:行の最後にある>アイコンをクリックして、新しいポリシーセットを表示します。

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 Authorization Policy メニューを展開し、(+)をクリックして新しい条件を追加します。

$\sim A$	uthorization	n Policy (1)						
					Results			
0	Status	Rule Name	Conditions		Profiles	Security Groups	Hit	Actions
	Q Search	h						
	۰	Authorization Rule 1		+	Select from list	/ + Select from list	0 +	礅

10.2 DictionaryIdentity Groupwith AttributeName Equals User Identity Groups: FPR-4110-Admins(ステップ7で作成したグループ名)に一致する条件を設定し、Useをクリックします。

See ICC			n	-Fau	Balley Cote						A Destruction of	1. de 13 De e	0
Conditions Studio												0	×
Library		Editor											
Search by Name			IdentityGr	oup-Na	me							0	ð
	. O E 🕈		Equals	Sala	st attribute for conditi								
ii 😑 sa			Set to 'is	•		£ ∞ 2	E 0 1	0 E 9	Ě		Duplicate	Save	
BYOD_is_Registered					Dictionary	Attribute	ID	Info					
Catalyst_Switch_Local_Web_Authentication					All Dictionaries	Attribute	ID						
on E Compliance_Unknown_Devices				÷	CWA	CWA_ExternalGroups		0					
E Compliant_Devices					IdentityGroup	Name		0					
E EAP-MSCHAPv2				4	InternalUser	IdentityGroup		0					
🗄 📑 EAP-TLS				٠	PassiveID	PassiveID_Groups							
: Guest_Flow				*	adminstrator	ExternalGroups		0					
🗄 📋 MAC_In_SAN													
E Network_Access_Authentication_Passed													
E Non_Cisco_Profiled_Phones													
E Non_Compliant_Devices													
🗄 👩 Radius													
Switch_Local_Web_Authentication													
										Close		Use	

orary	Edito		
earch by Name		IdentityGroup-Name	
	10 E 🕈	Equals User Identity Groups:FPR-4110- *	
E 50	0	Admin	H
BYOD_is_Registered		Set to 'is not'	Duplicate Save
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			
Switch_Local_Web_Authentication			

手順10.3:許可ポリシーで新しい条件が設定されていることを確認し、Profilesの下にユーザプロファイルを追加します。

✓ Authorizatio	n Policy (1)						
			Results				
 Status 	Rule Name	Conditions	Profiles	Security Groups		Hits A	lctions
Q Searc	h						
٥	Authorization Rule 1	A IdentityGroup Name EQUALS User Identity Groups:/FPR-4110-Admin	FPR-4110-Admins ×	+ Select from list	~+		٨
۰	Default		DenyAccess	+ Select from list	1+	0	٨
					Reset		Save

ステップ 11ステップ9で同じプロセスを読み取り専用ユーザに繰り返し、保存をクリックします。

確認

1. 新しいRADIUSクレデンシャルを使用して、FCM GUIへのログインを試行します。

2. バーガーアイコンに移動します= > Operations > Radius > Live logs。

3. 表示される情報は、ユーザーが正常にログインしたかどうかを示します。

≡ Cisco ISE							Operation	s · RADIUS									A Evaluation N	Aode 17 Days	9.0	58 Ø
Live Logs Live Ses	ions																			
Misconfigured Supp	cants 🕕			Misconfigured	d Network Devices 💿				RADIUS Drop	HS ()			c	lient Stopped Resp	onding 🕕				Repeat Co	unter 🕕
0					0				1					0					C	
හි ්ට Reset Reper	Counts 🖞 Export To 🗸														Refre	h Ir s	Latest 20	records 👳	Within Last 3 hou Filter 🗸	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 Sta	Server	Mdm Serve	IMEISV		Usecase
Feb 03, 2024 0	\$1:\$1.0	ò		cisco_readonly			New Polic	New Polic	FPR-4110			FPR-4110		User Identity Group	I	marpatinISE				
Feb 03, 2024 0	50:48.9	0		cisco_admin			New Polic	New Polic	FPR-4110			FPR-4110		User Identity Group		marpatinISE				

4. Secure Firewall Chassis CLIからLogged usersロールを検証します。



トラブルシュート

1. ISE GUIで、バーガーアイコン= > Operations > Radius > Live logsの順に移動します。

1.1ログセッション要求がISEノードに到達しているかどうかを検証します。 1.2失敗ステータスについては、セッションの詳細を確認します。

≡ Cisco ISE	Ope	erations - RADIUS	🛕 Evaluation Mode 18	Days Q @ 58 @
Live Logs Live Sessions				
Misconfigured Supplicants 🔘	Misconfigured Network Devices 🕕	RADIUS Drops 💿	Client Stopped Responding 💿	Repeat Counter 🕕
0	1	1	0	3
හි 🖯 Reset Repeat Counts 🖞 Export To 🗸			Never V Latest 20 record	is ↓ Within Last 3 hours ↓ Filter ↓ ♦
Time Status Deta	tails Repea Identity Endpoint ID	Endpoint Authenti Authoriz IP Ad	ddress Network De Device Port Identity Group Posture	. Server Mdm Sei
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic Authorizatic IP Ad	ddress 🧹 Network Device Device Port Identity Group Posture Sta	a Server Mdm Sen
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	cisco_admin	Default >> Default >> PermitAcc	FPR-4110 User Identity Groups	marpatin/SE

2. RADIUSライブログに表示されない要求(UDP要求がISEノードに到達しているかどうかをパ ケットキャプチャを介して確認する)の場合。

burgerアイコン≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dumpの順に移動します 。UDPパケットがISEノードに到着しているかどうかを確認するために、新しいキャプチャを追 加し、ファイルをローカルマシンにダウンロードします。

2.1必要な情報を入力し、下にスクロールしてSaveをクリックします。

E Cisco ISE	Operations - Troubleshoot	A Evaluation Mode 17 Days	۹ ۵	58	0
Diagnostic Tools Downloa	d Logs Debug Wizard				
General Tools \vee	TCP Dump 2 New				
RADIUS Authentication Troubl Execute Network Device Com Evaluate Configuration Validat	Add TCP Dump Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.				
Posture Troubleshooting Agentiess Posture Troublesho	Ngot Nama* marpatist\$E v				
EndPoint Debug TCP Dump Session Trace Tests	Network Interface" (gigsbitthement 0 (Up, Running) v)				
Trustliec Tools					
	E g: (p host 10.77.122.123 and not				
	10.177.122.119				

2.2キャプチャを選択して開始します。

E Cisco ISE			Operations - Trou	bleshoot			🛦 Evaluation Mode 17 Days Q. (2) 🕫 (2)					
Diagnostic Tools Download	Diagnostic Tools Download Logs Debug Wizard											
Renard Table												
RADIUS Authentication Troubl												Rows/Page 1 → < < 1 / 1 > > Ge 1 Total Rows
Execute Network Device Com Evaluate Configuration Validat	ø	Add / Edit () Truck S	✓ ■ Start ⊖ Stop →	Download								riter 🗸 - 🔶
Posture Troubleshooting		Host Name	Network Interface	Filter	File Name	Reposito	File S	Number of	Time Limit	Promiscuous M	Status	_
Agentiess Posture Troublesho EndPoint Debug		marpatin25E.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 ISEキャプチャの実行中にセキュアファイアウォールシャーシへのログインを試みる
2.4 ISEでTCPダンプを停止し、ファイルをローカルマシンにダウンロードします。
2.5トラフィック出力のレビュー
予想される出力:

パケット番号1。セキュアファイアウォールからISEサーバへのポート1812(RADIUS)経由の要求 パケット番号2ISEサーバが最初の要求を受け入れて応答します。



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。