# FMCでのRAVPN証明書認証とISE認可の設定

## 内容

はじめに 前提条件 要件 使用するコンボーネント 設定 ステップ1:信頼できるCA証明書のインストール ステップ2:ISE/RADIUSサーバグループおよび接続プロファイルの設定 ステップ3:ISEの設定 ステップ3.1:ユーザ、グループ、および証明書認証プロファイルの作成 ステップ3.2:認証ポリシーの設定 ステップ3.3:許可ポリシーの設定

#### <u>確認</u>

<u>トラブルシュート</u>

## はじめに

このドキュメントでは、FMCのCSFによって管理されるRAVPN接続での証明書認証に対する ISEサーバ認可ポリシーの設定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。

- ・シスコセキュアファイアウォール(CSF)
- Cisco Secure Firewall Management Center(FMC)
- Cisco Identity Services Engine ( ISE )
- ・ 証明書の登録とSSLの基本』を参照してください。
- 認証局(CA)

使用するコンポーネント

このドキュメントの内容は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Clientバージョン5.1.6
- Cisco Secure Firewallバージョン7.2.8
- Cisco Secure Firewall Management Centerバージョン7.2.8

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

#### ステップ1:信頼できるCA証明書のインストール



注:CA証明書がサーバ認証に使用したものと異なる場合は、この手順に従う必要がありま す。同じCAサーバがユーザ証明書を発行する場合は、同じCA証明書を再度インポートす る必要はありません。

Firewall Management Center Devices / Certificates	Overview Ana	lysis Policies	Devices O	bjects Integration
Name	Domain	Enrollment Type	Status	
√ 🚥 FTD1				
cisco.com	Global	PKCS12 file	CA ID	Server Certificate
InternalCAServer	Global	Manual (CA Only)	CA O ID	Internal CA certificate

a.に移動し、Devices > CertificatesをクリックしAddます。

b. trustpoint nameを入力し、CA情報の下の登録タイプとしてManualを選択します。

c.CA Onlyをチェックし、信頼できる/内部のCA証明書をpem形式で貼り付けます。

d. Skip Check for CA flag in basic constraints of the CA Certificateにチェックマークを付けて、Saveをクリックします。

## Add Cert Enrollment

Add Cert Enrollmen	[	0
Name*		
Description		
CA Information Ce	rtificate Parameters Key Rev	vocation
Enrollment Type:	Manual  CA Only Check this option if you do not require from this CA	) e an identity certificate to be created
CA Certificate:	BEGIN CERTIFICATE MIIB/ zCCAWigAwIBAgIBATANBgkqhki G9w0BAQsFADATMREwDwYDV QQDEwhDQVNI cnZlcjAeFw0yNDEwMTcxMDU5 MDBaFw0yNTExMjAxMDU5MDB aMBMxETAPBgNVBAMT CENBU2VydmVyMIGfMA0GCSq GSIb3DQEBAQUAA4GNADCBiQ	
Validation Usage:	IPsec Client SSL Client SSL Client Skip Check for CA flag in basic control	SSL Server
		Cancel Save

e. Cert Enrollmentの下で、先ほど作成したドロップダウンからtrustpointを選択して、Addをクリックし ます。

## Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

?

Device*:			
FTD1		•	
Cert Enrollment*: InternalCAServer		• +	
Cert Enrollment Deta	ils:		
Name: Enrollment Type: Enrollment URL:	InternalCAServer Manual (CA Only) N/A		
			Cancel Add

## ステップ2:ISE/RADIUSサーバグループおよび接続プロファイルの設定

a. Objects > AAA Server > RADIUS Server Groupに移動し、Add RADIUS Server Groupをクリックします。Enable authorize onlyオプションをチェックします。



警告: Enable authorize onlyオプションにチェックマークが入っていない場合、ファイア ウォールは認証要求を送信します。ただし、ISEは要求とともにユーザ名とパスワードを 受信することを想定しており、パスワードは証明書で使用されません。その結果、ISEは 要求を認証に失敗したとマークします。

## Edit RADIUS Server Group

Name:*				
ISE_Authorization	n			
Description:	]			
Group Accounting	Mode:			
Single	•			
Retry Interval:*	(1-10) Seconds			
10				
Realms:				
	•			
Enable authoriz	ze only			
Enable interim	account update			
Interval:*	(1-120) hours			
24				
Enable dynamic authorization				
Port:*	(1024-65535)			

b. Add (+)アイコンをクリックし、IPアドレスまたはホスト名を使用してRadius server/ISE serverを追加します。

0

## Edit RADIUS Server

#### IP Address/Hostname:\*

ISELocal

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:*	(1-65535)			
1812				
Key:*				
••••				
Confirm Key:*				
••••				
Accounting Port:	(1-65535)			
1813				
Timeout: (1-	300) Seconds			
10				
Connect using:				
Routing      Specific	Interface 🕕			
Default: Management,	/Diagnostic 🖌	+		
Redirect ACL:				
	T	+		
			Cancel	Save

C. Devices > Remote Access configurationに移動します。new connection profileを作成し、認証方式をClient Certificate Onlyに設定します。認可サーバで、前の手順で作成したサーバを選択します。

Allow connection only if user exists in authorization databaseオプションにチェックマークを付けます。この設定

Edit Connection Profile	?
Connection Profile:* FTD_CertAuth	
Group Policy:* DfltGrpPolicy  +	
Edit Group Policy Client Address Assignment AAA Aliases	
Authentication Authentication Method: Client Certificate Only  Enable multiple certificate authentication	
<ul> <li>Map username from client certificate</li> </ul>	
Map specific field	
Primary Field: Secondary Field:	
CN (Common Name)	
<ul> <li>Use entire DN (Distinguished Name) as username</li> </ul>	
Authorization Authorization Server: ISE_Authorization (RADIUS)	
Allow connection only if user exists in authorization database	-
Accounting	
Cancel Sav	/e

クライアント証明書からのマップユーザ名は、証明書から取得した情報を参照してユーザを識別 します。この例では、デフォルトの設定を使用していますが、ユーザの識別に使用する情報に応 じて変更できます。

をクリックします。Save

d. Advanced > Group Policiesに移動します。右側にあるAdd (+)アイコンをクリックします。

Firewall Management	nt Center Overview	Analysis Po	licies Devices	Objects	Integration		Deploy	۹ (	<b>9</b> 🗘	👩 admin 🔻 🗄	SECURE
FTD_PolicyVPN											Cancel
Enter Description											
										Policy Assi	ignments (1)
							Local Realm: No	ne		Dynamic Access I	Policy: None
Connection Profile Access Inte	erfaces Advanced										
AnyConnect Client Images	Group Policies										
Address Assignment Policy	Group policy can be assigned to	VPN user through con	nection profile or by RAI	DIUS server du	ring authentication.						
Certificate Maps	Following are the group policies	that are associated wit	th this Remote Access V	PN configurati	on. Add a group policy	if it is required to be assigned by RADIUS server during	authentication.				-
Group Policies											+
LDAP Attribute Mapping	Name		Protocol			DNS Servers	VPN Filter				
Load Balancing	DfltGrpPolicy		SSL,IKEV2								/
V IPsec	Marketing Group		SSL IKEV2								11
KE Daliav											
IPsec/IKEv2 Parameters	IT_Group		SSL,IKEV2								/ <b>•</b>

e. group policiesを作成します。各グループポリシーは、組織グループと、各グループがアクセスで きるネットワークに基づいて設定されます。

Group Policy			Ø
Available Group Policy C +		Selected Group Policy	1
Q Search		DfltGrpPolicy	
DfltGrpPolicy	Add		
FTD1_GPCertAuth			-
FTD1_GPISE			
FTD1_GPLocalFull			
		Cancel	ОК
		Cancel	ОК

f.グループポリシーで、各グループに固有の設定を実行します。接続が成功した後に、バナーメッセージを追加して表示できます。

## Add Group Policy

Name:*					
IT_Group					
Description:					
General AnyCon	nect Advanced				
VPN Protocols	Banner:				
IP Address Pools	Maximum total size: 3999, Maximum characters in a line : 497. In case of a line spanning more than 497 characters, split the line into multiple lines.				
Banner	** Only plain text is supported (symbols '<' and '>' are not allowed)				
DNS/WINS	IT Group				
Split Tunneling					

g.左側の「group policies」を選択し、をクリックして右側に移動しますAdd。これにより、設定で使用されているグループポリシーが指定されます。

8

## **Group Policy**



0

#### e.変更を展開します。

### ステップ3:ISEの設定

ステップ3.1:ユーザ、グループ、および証明書認証プロファイルの作成

a. ISEサーバにログインし、Administration > Network Resources > Network Devicesに移動します。

Cisco IS	E (								
Da	ashboard	Context Visibility	Operations	Policy	Administration	Work C	Centers		
Recer	nt Pages	System		Network Resource	•	р×G	irid Services		
Use Poli Extu Cer Aut	rs cy Sets ernal Identity Sources tificate Provisioning horization Profiles	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore		Network Devices Network Device O Network Device F External RADIUS RADIUS Server S NAC Managers External MDM Location Services	Broups Profiles Servers equences	Sa Ci Di Sa Fee Pr	ummary Illant Management Illagnostics Jettings I <b>d Service</b> rofiler		
		Admin Access Settings		Device Portal Mana	igement	Thre	eat Centric NAC		
		Identity Management				וד	hird Party Vendors		
		Identities Groups External Identity Sources Identity Source Sequences		Certificate Provis Client Provisionin Mobile Device Ma My Devices	ioning 9 anagement				
Short Ctrl	cuts + // - Expand menu - Collapse menu	Settings		Custom Portal Fil Settings	es				
Make	a wish							(	R

b. Addをクリックして、ファイアウォールをAAAクライアントとして設定します。

Netv	work	Devices				
🖉 Edit	+ Add	Duplicate	ني Import 🔥 Export 🗸	🔒 Generate PAC 👔	) Delete 🗸	
	Name	∧ IP/Mask	Profile Name	Location	Туре	Description
	FTD		tto Cisco (i)	All Locations	All Device Types	

c. ネットワークデバイスのNameフィールドとIP Addressフィールドを入力してから、RADIUS Authentication Settingsボックスにチェックマークを入れて、Shared Secret.を追加します。この値は、 FMCでRADIUSサーバオブジェクトが作成されたときに使用された値と同じでなければなりませ ん。をクリックします。Save

Network Devices List	Network Devices List > FTD					
Network Devices						
Name	FTD					
Description						
IP Address	✓ * IP : / 32	<b>發</b>				
	—					



RADIUS Authentication Settings

**RADIUS UDP Settings** 

Protocol	RADIUS	
Shared Secret		Show
Use Second	Shared Secret (i)	,

d. Administration > Identity Management > Groupsに移動します。

Cisco ISE	Q What page are you looking	i for?				
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	System		Network Resour	ces	pxGrid Services	
Live Logs Users Policy Sets External Identity Sources Certificate Provisioning	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access		Network Devic Network Devic Network Devic External RADIU RADIUS Server NAC Managers External MDM Location Servi	es e Groups e Profiles IS Servers Sequences 	Summary Client Management Diagnostics Settings Feed Service Profiler	
	Settings		Device Portal Ma	anagement	Threat Centric NAC	
Shortcuts	Identity Management Identities Groups External Identity Sources Identity Source Sequences Settings		Blocked List BYOD Certificate Pro Client Provisio Mobile Device My Devices Custom Portal	visioning ning Management Files	Third Party Vendors	
Ctrl + (/) - Expand menu esc) - Collapse menu			Settings			6

e. User Identity Groupsをクリックし、次にAddをクリックします。

### グループ名を入力し、 Submitをクリックします。

Identity Groups	User Identity Groups	
< 🖀 💩	🖉 Edit 🕂 Add 👩 Delete 🗸 🕁 Import 🏠 Export 🗸	
> 🗅 User Identity Groups	Name   Description	
	Group X	
	🗋 🍕 IT Group	
	C A Marketing Group	

User Identity Groups > New User Identity Group

Identity Gr	oup		
* Name	IT_Group		
Description			
		Submit	Cancel
		_	

注:この手順を繰り返して、必要な数のグループを作成します。

d. Administration > Identity Management > Identitiesに移動します。

Cisco ISE	Q What page are you looking	for?	_			
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	System		Network Resour	es	pxGrid Services	
Groups Network Devices Live Logs Users Policy Sets	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access		Network Devic Network Devic Network Devic External RADIU RADIUS Server NAC Managers External MDM Location Servic	es e Groups e Profiles IS Servers Sequences	Summary Client Management Diagnostics Settings Feed Service Profiler	
	Settings		Device Portal Ma	inagement	Threat Centric NAC	
	Identity Management Identities Groups External Identity Sources Identity Source Sequences		Blocked List BYOD Certificate Prov Client Provision Mobile Device My Devices	visioning ning Management	Third Party Vendors	
Shortcuts	Settings		Custom Portal Settings	Files		
Ctrl + (/) - Expand menu						6

e. Addをクリックして、サーバローカルデータベースに新しいユーザを作成します。

UsernameコマンドとLogin Passwordコマンドを入力します。次に、このページの最後に移動し、User Groupを選択します。

をクリックします。Save

Network Access Users

🖉 Edit	+ Add	$\circledast$ Change Status $\lor$	/ 山 Import 合 Export	V 📋 Dele	ete 🗸 📋 Du	plicate		
	Status	Username	∧ Description	First Name	Last Name	Email Address	User Identity Grou Admin	
	🗹 Enabled	9 user1					IT Group	
	Z Enabled	9 user2					Marketing Group	

#### ✓ Network Access User

* Username user1		
Status Enabled V		
Email		
✓ Passwords		
Password Type: Internal Users 🗸		
Password	Re-Enter Password	
* Login Password	••••••	Generate Password (i)
Enable Password		Generate Password (i)
v User Groups		



注:内部ユーザを作成するには、ユーザ名とパスワードを設定する必要があります。証 明書を使用して実行されるRAVPN認証には必要ありませんが、これらのユーザはパスワ ードを必要とする他の内部サービスに使用できます。したがって、必ず強力なパスワー ドを使用してください。

f. Administration > Identity Management > External Identify Sourcesに移動します。



g. AddをクリックしてCertificate Authentication Profileを作成します。

証明書認証プロファイルは、クライアント証明書の検証方法を指定します。これには、証明書の どのフィールドをチェックできるかが含まれます(サブジェクト代替名、共通名など)。

External Identity Sources	Certi	ificate Authe	nticatior	n Profile
> 🛅 Certificate Authentication Profile	0 Edit	+ Add Duplicate	Delete	
Active Directory		Name	~	Description
🗖 LDAP	U	Name	~	Description
ODBC		Certificate_Profile		Certificate Authorization Profile.
RADIUS Token				
C RSA SecurID				
SAML Id Providers				
Social Login				

#### Certificate Authentication Profiles List > Certificate\_Profile

#### **Certificate Authentication Profile**

* Name	Certificate_Profile
Description	Certificate Authorization Profile.
Identity Store	[not applicable] V
Use Identity From	Certificate Attribute Subject - Common Name      (i)     Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) (i)
Match Client Certificate Against Certificate In Identity Store ()	<ul> <li>Never</li> <li>Only to resolve identity ambiguity</li> <li>Always perform binary comparison</li> </ul>

ステップ3.2:認証ポリシーの設定

認証ポリシーは、要求がファイアウォールと特定の接続プロファイルから発信されることを認証 するために使用されます。

a. Policy > Policy Setsに移動します。

🔀 Cisco ISE	Q What page are you lookin					
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	Policy Sets		Profiling			
Groups Settings Identity Source Sequences	Posture		Client Provisioning	1		
Policy Sets Authorization Profiles	Policy Elements					
	Dictionaries Conditions Results					
Shortcuts						
Ctrl + // - Expand menu						
esc - Collapse menu						

画面右側の矢印をクリックして、デフォルトの認可ポリシーを選択します。

Policy Sets					Reset Policys	et Hitcount:	•	Save
🕂 Statu	s Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits A	ctions	View
Q Sear	sh							
				+				
0	Default	Default policy set			Default Network Access 🛛 🖂 +	23	\$	>
						Reset		Save

b. Authentication Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、 add (+)アイコンをクリックして新しいルールを追加します。

$\sim$ Authentication Policy (2)					
🕀 Status Rule Name	Conditions		Use	Hits	Actions
Q Search					

### ルールの名前を入力し、add (+)アイコンを条件列で選択します。

✓ Authent	tication Policy (2)					
⊕ s	tatus Rule Name	Conditions		Use	Hits	Actions
	Search					
1	RAVPN_CentUsers		+	Internal Users ( ) ~ > Options		{ô}}

c. Attribute Editorテキストボックスをクリックし、NAS-IP-Addressアイコンをクリックします。ファ イアウォールのIPアドレスを入力します。

Conditions Studio		
Library	Editor	
Search by Name	Click to add an attribute	$\otimes$
	Select attribute for condition	
Catalyst_Switch_Local_Web_Aut hentication	<ul> <li>▼□</li> <li>□</li> <li>⊕</li> <li>₽</li> <li>□</li> <li>₽</li> <li>₽</li> <li>0</li> <li>0</li> <li>1</li> <li>0</li> <li></li></ul>	
EAP-MSCHAPv2	Dictionary Attribute ID Info	
🗄 🗐 EAP-TLS	All Dictionaries V nas X ID	)
# E MAC_in_SAN	Radius NAS-IP-Address 4 (1)	

d. Newをクリックし、他の属性Tunnel-Group-nameを追加します。FMCで設定されたConnection Profileの名前 を入力します。

### **Conditions Studio**

#### Library

Search by Name

EAP-MSCHAPv2

EAP-TLS

E MAC\_in\_SAN

#### Editor Radius-NAS-IP-Address 0 Equals 🗸 : E Catalyst\_Switch\_Local\_Web\_Aut () Click to add an attribute A... Select attribute for condition 0 0 1 C -8 Ę. F . P Dictionary Attribute ID Info Switch\_Local\_Web\_Authenticatio All Dictionaries 🗸 tunnel-group-name × Cisco-VPN3000 CVPN3000/ASA/PIX7x-Tunnel-Group-Name 146 Po : E Switch\_Web\_Authentication

### Conditions Studio

Library	Editor		~
	<del>چ</del> یا	Radius·NAS-IP-Address	× ×
Catalyst_Switch_Local_Web_Aut (	D	Cisco-VPN3000·CVPN3000/ASA/PIX7x-Tunnel-Group-Na	8
EAP-MSCHAPv2	D	Equals V FTDLCertAuth	
EAP-TLS	D		
E MAC_in_SAN	D	+ NEW AND OR	
: Switch_Local_Web_Authenticatio	D	Set to 'Is not' Duplicate Save	L

e. Use列で、作成したCertificate Authentication Profileを選択します。これにより、ユーザの識別に使用 されるプロファイルで定義された情報が指定されます。

√ Aut	Authentication Policy (2)								
Ð	Status	Rule Name	Con	ditions	Use	Hits	Actions		
Q Search									
	0	RAVPN-CertUsers	11.	VerlfyCertAuth	Certificate_Profile ( ) > Options	7	ŵ		

をクリックします。Save

ステップ3.3:許可ポリシーの設定

 $^{\otimes}$ 

8

×

<u></u>

0 × a. Authorization Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、「 add (+)」アイコンをクリックして新しいルールを追加します。

$\sim$ Authorization Policy (13)					
		Results			
(+) Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					

#### ルールの名前を入力し、Conditions列の下のadd (+)アイコンを選択します。

$\scriptstyle \smallsetminus$ Authorization Policy (13)						
			Results			
(+) Status Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Q Search						
IT_Group_Policy		+	Select from list $\sim$ +	Select from list $\vee$ +		\$

b. Attribute Editorテキストボックスをクリックし、Identity groupアイコンをクリックします。Identity group - Name属性を選択します。

Conditions Studio															
Library		Editor													_
Search by Name				_Group										۲	$\otimes$
	L 🛛 ½ 🛜			Int	ernalUse	er∙lder	ntityGr	oup						8	
BYOD_is_Registered	0		Selec	ct attrib	ute for	con	ditio	n						-	×
Catalyst_Switch_Local_Web_Aut	0	A ×	<b>Q</b>	<b>\$</b>	*	۲	₽	Ş	7 0	Ø	©	1	٥	ĥ	Ģ
Compliance_Unknown_Devices	0			Dictio	nary			Attril	ute		ID		Info		
Compliant_Devices	0			All Dict	ionaries	~		Attrib	ute		ID				
EAP-MSCHAPv2	0		*	CWA				CWA_	ExternalG	roups			0		
EAP-TLS	0			Identity	Group			Name	ption		 		0		
: E Guest_Flow	0			Internal	User			Identi	/Group		 		0		
: 🗐 IT_Group	0		484	Passive	D			Passiv	eID_Grou	ps			0		

演算子として<sub>Equals</sub>を選択し、ドロップダウンメニューの矢印をクリックして使用可能なオプショ ンを表示し、User Identity Groups: を選択します。

## Conditions Studio

Library		Editor					
Search by Name			E IT_G	roup			$^{\otimes}$
	<del>چ</del> بڑ 🕲			InternalUse	er∙ldenti	ityGroup	8
BYOD_is_Registered	0		â	Equals	~	Choose from list or type	~ #
Catalyst_Switch_Local_Web_Aut	0	<u>A</u> ~				User Identity Groups:GuestType_Soc	alLogin (default)
	•					<ul> <li>User Identity Groups:GuestType_We</li> </ul>	ekly (default)
: E compliance_onknown_bevices	0		+			User Identity Groups:IT Group	
Compliant_Devices	0		Set to 'ls	not'		User Identity Groups:Marketing Grou	р
EAP-MSCHAPv2	0					User Identity Groups:OWN_ACCOUN	ITS (default)

c. Profilesカラムでadd (+)アイコンをクリックし、Create a New Authorization Profileを選択します。

∨ Aut	horization	Policy (13)									
						Results					
Ð	Status	Rule Name	Cond	litions		Profiles		Security Groups		Hits	Actions
Q Search											
	0	IT Group Policy	AND		IT_Group	Select from list	+	Select from list	~+		ŝ
	IT_Group_	···_····	JAND AND	R InternalUser-IdentityGroup EQUALS User Identity Groups:IT Group			· · · ·		152		
		Wireless Black List Default	AND	E	Wireless_Access	Create a New Authorization Profile		au' Select from list $ imes +$			ŝ
	·	there are the training		8	IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist						252

## profile を入力し<sub>Name</sub>ます。

* Name	IT_Group_Profile		
Description			
* Access Type	ACCESS_ACCEPT	~	
Network Device Profile	dette Cisco ∨⊕		
Service Template			
Track Movement			
Agentless Posture			
Passive Identity Tracking			

#### Authorization Profile

Common Tasksに移動し、ASA VPNをチェックします。次に、group policy nameを入力します。これは、 FMCで作成したコマンドと同じである必要があります。

✓ Common Tasks		
🗹 ASA VPN	IT_Group	~
AVC Profile Name		
UDN Lookup		

#### 次に来る属性は、各グループに割り当てられました。

Attributes Details
 Access Type = ACCESS\_ACCEPT
 Class = IT\_Group

[Save] をクリックします。



注:作成した各グループに対して、「ステップ3.3:許可ポリシーの設定」を繰り返しま す。

## 確認

1. コマンドshow vpn-sessiondb anyconnectを実行し、ユーザが正しいグループポリシーを使用しているかどうかを確認します。

<#root>

firepower#

show vpn-sessiondb anyconnect

Session Type : AnyConnect

Username : user1

Index : 64 Public IP : Assigned IP : 192.168.55.2 Protocol : AnyConnect-Parent : AnyConnect Premium License : AnyConnect-Parent: (1)none Encryption Hashing : AnyConnect-Parent: (1)none Bytes Tx : 15084 Bytes Rx : 99611 Group Policy : IT\_Group Tunnel Group : FTD\_CertAuth : 22:21:43 UTC Tue Oct 22 2024 Login Time Duration : 3h:03m:50s : 0h:41m:44s Inactivity VLAN Mapping : N/A VLAN : none Audt Sess ID : 96130a0f0004000067182577 Security Grp : none Tunnel Zone : 0 Username : User2 : 70 Index Assigned IP : 192.168.55.3 Public IP : : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol License : AnyConnect Premium : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing Bytes Tx : 15112 Bytes Rx : 19738 Group Policy : Marketing\_Group Tunnel Group : FTD\_CertAuth : 01:23:08 UTC Wed Oct 23 2024 Login Time Duration : 0h:02m:25s : 0h:00m:00s Inactivity VLAN Mapping : N/A VLAN : none Audt Sess ID : 96130a0f0004600067184ffc Security Grp : none Tunnel Zone : 0 firepower#

 グループポリシーでは、ユーザが正常に接続したときに表示されるバナーメッセージを設定 できます。各バナーを使用して、認可を受けているグループを識別できます。

Cisco AnvConnect		
	<ul> <li>Cisco AnyConnect Secure Mobility Client</li> <li>VPN: Please respond to banner.</li> </ul>	– – ×
	FTD1_CertAuth	Connect

Cisco AnyConnect		
Marketing Group		
	🚳 Cisco AnyConnect Secure Mobility Client —	
	VPN: Please respond to banner.	Connect
	<b>\$</b> (i)	alialia cisco

3. ライブログで、接続が適切な許可ポリシーを使用しているかどうかを確認します。をクリッ ク<sub>Details</sub>して、認証レポートを表示します。

E Cisco ISE	Operations · RADIUS						
Live Logs Live Sessions							
Misconfigured Supplicants 🕕	Misconfigured Network Devices 🕕	RADIUS Drops ①	Client Stopped Responding 🕕	Repeat Counter 🕕			
0	0	0	0	0			
ට් Refresh 🕁 Reset Repeat Counts ሳ Export 1	o ~		Refresh Show Latest 100 re	c↓ Within Last 30 minu↓ ▼Filter ↓			
Time Status	Details Repea Identity	Endpoint ID Endpoint Authenti	Authoriz Authoriz IP Address Network De Do	evice Port Identity G			
Oct 25, 2024 08:38:03.6	o user1	Windows1 Default	Default >> IT_Group				
Oct 25, 2024 08:38:03.6	user1	Windows1 Default	Default >> IT_Group FTD	User Identit			

Records Shown: 2

Last Updated: Fri Oct 25 2024 14:42:41 GMT-0600 (GMT-06:00)

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

1. 証明書認証のCSFの診断CLIからデバッグを実行できます。

debug crypto ca 14 debug webvpn anyconnect 255 debug crypto ike-common 255

2. AAAデバッグを使用して、ローカル属性またはリモート属性(あるいはその両方)の割り当て を確認します。

debug aaa common 255 debug aaa shim 255 debug aaa authentication debug aaa authorization debug radius all

ISEで次を実行します。

1. Operations > RADIUS > Live Logsに移動します。

8	Cisco ISE	Q What page are you looking for?							
	Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers			
	Recent Pages Policy Sets Authorization Profiles Results External Identity Sources Groups	RADIUS Live Logs Live Sessions TACACS		Threat-Centric NAM Troubleshoot Diagnostic Tools Download Logs Debug Wizard	C Live Logs				
		Adaptive Network Control Policy List Endpoint Assignment		Reports					
	Shortcuts Ctrl + [] - Expand menu esc) - Collapse menu					G	3		

Live Logs Live Sessions

Misconfigured Supplicants ①	Misconfigured N	letwork Devices 🕕		RADIUS Dro	ps 🕕		Client Stop	ped Respond	ing 🕕		Rej	oeat Counter 🕕
0		0		0				3				0
Ø Refresh 🕁 Reset Repeat Counts එ Export	To 🗸							Refresh Never	~	Show Latest 20	recov L	thin ast 3 hours ↓ ▼ Filter ↓ @
Time Status	Details Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address	Ne	etwork De	Device Por	t Identity G
×	~	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~ N	etwork Device	Device Port	Identity Gro
Oct 23, 2024 01:26:29.3	0	User2		Windows1	Default	Default >>	Marketing		FT	D		User Identity
Oct 23, 2024 01:22:29.3 0	0	User2					DenyAccess		FT	D		User Identity
Oct 23, 2024 01:21:46.9 0	i a	User2					DenyAccess		FT	D		User Identity
Oct 23, 2024 01:16:33.4 0	9	User2					DenyAccess		FT	D		User Identity
Oct 22, 2024 10:25:14.1	0	user1		Windows1	Default	Default >>	IT_Group		FT	D		User Identit
Oct 22, 2024 10:24:18.9	à	user1		Windows1	Default	Default >>	IT_Group		FT	D		User Identit

Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00)

Records Shown: 6

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。