RADIUS認証によるAnyConnectユーザへのスタ ティックIPアドレス割り当ての設定

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント <u>設定</u> <u>ネットワーク図</u> <u>FMCによるAAA/RADIUS認証を使用したリモートアクセスVPNの設定</u> <u>ISE(RADIUSサーバ)での認可ポリシーの設定</u> <u>確認</u> トラブルシュート

概要

このドキュメントでは、Identity Services Engine(ISE)サーバを使用してRADIUS認可を設定し、 RADIUS属性8 Framed-IP-Addressを使用して、特定のCisco AnyConnectセキュアモビリティクラ イアントユーザのFirepower Threat Defense(FTD)に常に転送する方法についてを説明します。

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。

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect セキュア モビリティ クライアント
- RADIUS プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- •FMCv 7.0.0(ビルド94)
- FTDv 7.0.0(ビルド94)
- ISE:2.7.0.356
- AnyConnect 4.10.02086
- Windows 10 Pro

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、初期(デフォルト)設定の状態から起動しています 。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

ネットワーク図



FMCによるAAA/RADIUS認証を使用したリモートアクセスVPNの設定

手順については、次のドキュメントとビデオを参照してください。

- FTD での AnyConnect Remote Access VPN の設定
- FMCによって管理されるFTDの初期AnyConnect設定

FTD CLIでのリモート・アクセスVPNの構成:

ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0

interface GigabitEthernet0/0
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0

aaa-server ISE_Server protocol radius aaa-server ISE_Server host 172.16.0.8 key ***** authentication-port 1812 accounting-port 1813

crypto ca trustpoint RAVPN_Self-Signed_Cert enrollment self fqdn none subject-name CN=192.168.0.100 keypair <Default-RSA-Key> crl configure ssl trust-point RAVPN_Self-Signed_Cert

webvpn enable Outside_Int http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache no disable error-recovery disable group-policy DfltGrpPolicy attributes vpn-tunnel-protocol ikev2 ssl-client user-authentication-idle-timeout none webvpn anyconnect keep-installer none anyconnect modules value none anyconnect ask none default anyconnect http-comp none activex-relay disable file-entry disable file-browsing disable url-entry disable deny-message none tunnel-group RA_VPN type remote-access tunnel-group RA_VPN general-attributes

tunnel-group RA_VPN general-attributes address-pool AC_Pool authentication-server-group ISE_Server tunnel-group RA_VPN webvpn-attributes group-alias RA_VPN enable

ISE(RADIUSサーバ)での認可ポリシーの設定

ステップ1:ISEサーバにログインし、[Administration] > [Network Resources] > [Network Devices]に移動します。

deate Identity Services Engine	Home	Context Visibility	Operations	Policy	- Administra	tion • Work	Centers					Licens	e Warning 🔺 🔍		5 f
Summary Endpoints	Guests	Vulnerability	Threat	+	System		Network	Resources	pxGrid Services					¢.	-
METRICS Total Endpol	ints 0	1	Active Endpo	vints Ø	Licensing Certificate: Logging Maintenan Upgrade Backup & I Admin Acc Settings Identities Groups	i ce Restore ess sagement	Network Network External RADIUS NAC Ma External Location Device P Blacklis BYOD Centrics	Cherice Groups R Device Profiles i RADIUS Servers Server Sequences anagers MDM n Senices ortal Management it ate Provisioning	Feed Service Profiler Threat Centric NAC Third Party Vendors	-	Authenticated Guests @	BYOD Endp	oints 0	- 0 0; >	
AUTHENTICATIONS	ork Device	Failure Reason		80	External Id Identity So Settings	entity Sources arce Sequences	Client P Mobile (My Devi Custom Settings	Provisioning Device Management ices 1 Portal Files 8		×	ENDPOINTS			e o x	
inter_ussens: [100%]_	(2				drivea550	D6: [100%]	0			workstations: [1				
₿ BYOD ENDPOINTS ●				0 9	×	ALARMS 0			6	дaх	# SYSTEM SUMM	ARY O		gox	
Type Profile					Seve	rity Name		Occu Last O	ccurred	^	1 node(s)			All = 24HR =	
	No dat	a available.				¥ Name					driverap-ISE-2-7	Memory Lisage	Authentics	ition Latency	
tor://10.21.124.21:6012/admin/#a	desisietesti	on/administration	naturatives	ureae (admi	nistration cot	DNS Re	esolution Failure	941 less that	n 1 min ago		010		Patricia		
short in a rule a rule relagimit a	on manada	on you minimise action	Chermonicesou	in coy outfill		ional esources.	previnces a lagenti	4600 loss the	0.1 min 200						×

ステップ2:[Network Devices]セクションで[**Add**]をクリックし、ISEがFTDからのRADIUSアクセス 要求を処理できるようにします。

dentity Services Engine	Home + Context Visibility	 Operations 	Policy Administration	n Vork Centers			License Warning 🔺	9 0 0
System Identity Management	Network Resources Device	e Portal Manager	nent pxGrid Services + Fee	d Service + Threat Centric N	UAC CONT			
Network Devices Network Device G	roups Network Device Profile	s External RAD	IUS Servers RADIUS Server S	equences NAC Managers	External MDM + Location Services			
•								
Network Devices	Network Devices							
Default Device		1					Selecte	d 0 Total 1 🧐 🎡 🖕
Device Security Settings	/ Edit	@ Import	Export • OGenerate PAC X	Delete +			Show Al	• 6
	Name •	IP/Mask	Profile Name	Location	Type	Description		
	DRIVERAP_ASA5506	172.16.255.2	Cisco 🗠	All Locations	All Device Types			

ネットワークデバイスの[**名前**]フィールド**と[IPアドレ**ス]フィールドを入力し、[**RADIUS** Authentication Settings]ボックスをオンにします。[Shared Secret]は、FMC上のRADIUSサーバオ ブジェクトの作成時に使用された値と同じである必要があります。

esce Identify Services Engine	Home + Context Visibility + Operations + Policy +Administration + Work Centers	License Warning 🔺 🔍	0 0	• ^
System Identity Management	Helwork Resources Device Portal Management puCrid Service Feed Service Threat Centric NAC			
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services			
0				
Network Devices	Notoxis Davids List New Network Device Notoxis Davids			
Default Device	* Name ORDERAD CTO 2			
Device Security Settings				
	with a second seco			
	▼ Address * 192:168.0.100 / 32	ŵ•		
	* Device Profile (mc. Carrol +) (ff)			
	Model Name 🔹			
	Software Version +			
	* Network Device Group			
	VILCADORS C Sectoreau			
	Set To Default			
	Device Type Al Device Types 📀 Set. To Default			
	RADUS Authentication Settings			
	RADIUS UOP Settings			- 11
	Protocol RADNUS			
	* Shared Secret Shared Secret			
	Use Second Shared Secret 🔲 🛞			
	Show			
	CoA Port 1700 Set To Default			
	RADIUS DTL.S Settings ()			
	DTLS Required 🗖 🕢			~

このページの最後にあるボタンで保存します。

ステップ3:[Administration] > [Identity Management] > [Identities]に移動します。

-disdu- cisco Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Center	8		License Warning	A 9 0	0 0
Vetrity Services Engine System • Identity Management • Network Devices Network Device Default Devices Device Device Security Settings Device Security Settings	Home • Context Visibility • Operation: • Policy • Network Resources • Device Profiles betwork Device Profiles betwork Device Profiles • Retwork Devices Policy	Administration Voir Center System Desloyment Licensing Centralize Logging Magnate Backup & Relative Administration Centry Magnate Centry Management Centry Management Centry Management Centry Secure Se	Network Resources Network Devices Network Device Profiles Estimati Recht/S Bevers Ref Managens Estimati Recht/S Bevers Estimati Moti Location Senices Device Pertal Management Blacitist BYOD Crefticate Provisioning Creft Provisioning Creft Provisioning Collet Provisioning Collet Provisioning Collet Provisioning Collet Provisioning Custom Pertal Files Settings	patiend Services Feed Service Proller Threat Centric NAC Third Party Vendors	Licenze Waning	Selected 0 Year 2	● ● ● ● ● ● ● ● ●
11tps://10.31.124.31:6012/admin/#	administration/administration_identitymanagement/adm	ninistration_identitymanagement	Lidentities				

ステップ4:[Network Access Users]セクションで、[*Add*]をクリックしてISEのローカルデータベー スに*user1*を作成します。



[名前]フィールドと[ログインパスワー**ド]フィールド**にユーザ名と**パスワード**を入力し、[送信]を クリック**します**。

dentify Services Engine Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺		0
System *-Identity Management Network Resources Device Portal Management puGrid Services Feed Service Threat Centric IVAC			
- Identities Groups External Identity Sources I Identity Source Sequences In Settings			
Uses version Access Users Lus > new remover Access User			
Latest Manual Network Scan Res.			
owna K Endold +			
Emai			
* Passwords			
Password Type: Informal Users •			
Password Re-Enter Password			
*Logn Password Generate Password @			
Enable Password Generate Password 0			
* loss Information			
- vage antonimotori			
HER REAL			
LastName			
Description /			
Change password on net login			- 4
			- 1
✓ Account Unsate Poncy			
□ Disable account if date exceeds 2021-11-21 (0999-mm-dd)			
▼ User Groups			
Select an item 📀 — 🕂			
			- 1

ステップ5:前のステップを繰り返して、user2を作成します。



ステップ6:[Policy] > [**Policy Sets]に移動します**。



ステップ7:画面の右側*にある矢印*をクリックします。

obaba ide	ntity Service	es Engine Home + Con	text Visibility + Operations	Policy Administration	Work Centers License Warnin			
Policy Se	ts Profiling	Posture Client Provisioning	Policy Elements					
Policy S	Sets				Reset Policyset Hitco	nts Re	iset	Save
•	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits	Action	s	View
Search								
					+			
					•			_
	\odot	Default	Default policy set		Default Network Access * * 17	\$		>
						R	Iset	Save

ステップ8:[Authorization Policy]の横にある矢印*>をクリックし*て、**[Authorization Policy]**を展開します。次に、+記号をクリックして新しい規則を追加します。

		AL VISIDIN	 Operations 	Policy Administration	n + work Genters			cicense training		
cy Sets Profiling	g Posture Client Provisioning	 Policy E 	lements							
y Sets → De	efault							Reset Policyset Hitcour	nts Re:	set Sr
Status	Policy Set Name	Descrip	tion	Conditions				Allowed Protocols / Ser	ver Sequent	ce Htt
ch										
0	Default	Default p	uticy set					Default Network Access	×* •	+ 1
thentication Pr	olicy (3)									
thorization Pol	licy - Local Exceptions									
uthorization Pol	licy - Global Exceptions									
uthorization Do	Sev (40)									
DUINA KOUNT P O	551,154									
÷.						Results				
+ Status	Rule Name	Condit	lons			Results Profiles	Security Gr	oups	Hits	Action
• Status	Rule Name	Condi	tions			Results Profiles	Security Gr	oups	Hits	Action
Status earch	Rule Name	Condi	tions	cess		Results Profiles	Security Gr	oups	Hits	Action
* Status earch	Rule Name Wireless Black List Default	Condi	tions Wireless_Acc ab. identityGroup	cess Name EQUALS Endpoint Iden	ntly Groups Blacklist	Results Profiles (*Blackhole_Wireless_Access)	Security Gr	oups	Hits 0	Action
* Status earch ©	Rule Name Wireless Black List Default Profiled Cisco IP Phones	Condit AND	Wireless_Acc & IdentityGroup IdentityGroup-Name El	cess Name EQUALS Endpoint iden QUALS Endpoint identity Group	nthy Groups Blacklist Jpp Profiled Cisco-IP-Phone	Results Profiles Blachole, Wireless, Access Carol JP, Phones	Select trom Select trom	oups	Hits 0 0	Action ©
Status sarch	Rule Name Wireless Black List Default Profiled Cisco IP Phones Profiled Non Cisco IP Phones	Condit AND	tions Wireless_Acc MinethyGroup IdenthyGroup-Name Ei Non_Cisco_Profiled_P	cess - Name EQUALS Endpoint Iden QUALS Endpoint Idently Group Phones	ntly Groups Blacklist ups Profiled Claco-IP-Phone	Results Profiles Results Resu	Security Gr Select from Select from Select from	oups	Hits 0 0	Action O
Status Aarch © ©	Rule Name Wreless Black List Default Profiled Claco IP Phones Profiled Non Claco IP Phones	Condit AND 4	Itons Wireless_Acc Mireless_Acc MentlyGroup Name Ei Non_Cisco_Profiled_F	cess Name EQUALS Endpoint Iden QUALS Endpoint Idently Group Phones	ntly Groups Blacklist ups Profiled Clisco-IP-Phone	Results Profiles REachole_Wireless_Access (*Clsco_P_Phones) (*Non_Clsco_P_Phones)	Security Gr	oups	Hits 0 0	Actor
status earch	Rule Name Vireless Black List Default Profiled Cisco IP Phones Profiled Non Cisco IP Phones Uninnown_Compliance_Redired	Condit AND 4 AND	tions Utreless_Acc Utreless_Acc Utreless_Acc Utreless_Acc Utreless_Acc Utreless_Acc Utreless_Acc Non_Cisco_Profiled_P Non_Cisco_Profiled_P Non_Cisco_Profiled_P	cess Name EQUALS Endpoint Iden QUALS Endpoint Identity Croup Phones ess_Authentication_Passed	ntly Groups Blackfist ups Profiled Cisco-IP-Phone	Results Profiles REachole_Wireless_Access RCIsco_IP_Phones RNIN_CISco_IP_Phones ROISCO_TEMPORIL_ORDORING	Security Gr Select from Select from Select from Select from Select from Select from	st v +	Hits 0 0 0 0	Action O O
status earch	Rule Name Wreless Black List Default Profiled Cisco IP Phones Profiled Non Cisco IP Phones Unitnown_Compliance_Redired	Condition of the second	Itons Wireless_Acc Wireless_Acc Wireless_Acc MidentlyGroup IdentlyGroup Name El Non_Cisco_Profiled_P Non_Cisco_Profiled_P Network_Acc Compliance_ Compliance_	cess Name EQUALS Endpoint iden QUALS Endpoint identity Croup Phones ess_Authentication_Passed Unincom_Devices	ntly Groups Blacklist ups Profiled Claco-IP-Phone	Results Profiles (* Blachole_Wireless_Access) (* Clsco_P_Phones) (* No_Clsco_P_Phones) (* Clsco_Temporal_Onboard)	Security Gr Select term Select term Select term Select term Select term	sist v +	Hits 0 0 0 0 0	Action
earch earch Constraints Cons	Rule Name Wreless Black List Default Profiled Cisco IP Phones Profiled Non Cisco IP Phones Unknown_Compliance_Redrect	Condition of the second	bons Wireless_Acc wireless_Acc stanth/Group Name E Non_Cisco_Profiled_F Non_Cisco_	cess Name EQUALS Endpoint Identity CRUALS Endpoint Identity Croup Phones ess_Authentication_Passed Unitrovem_Devices ess_Authentication_Passed	ntty Groups Blacklist ups Profiled Clace-IP-Phone	Results Profiles * Blachole, Wireless, Access * Disco_P_Phones * Non_Cisco_P_Phones * Disco_Temporal_Onboard	Security Gr	nups	Hits 0 0 0	Action O

ルールに名前を付け、[条件]列の下の+記号を選択します。

✓ Author	ization Polic	y (13)						
					Results			
٠	Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Search								
1	ø	Static IP Address User 1		+	Select from list	Select from list • +		٥

[Attribute Editor]テキストボックスをクリックし、[Subject]アイコンを**クリック**します。[*RADIUS User-Name*]属性が見つかるまで下にスクロール*し、そ*れを選択します。

librar	у		Editor														
Sea	rch by Name			Click to add an attribute													
Q		🛛 t: 🦻	ťs	Select	attribute	for condit	ion										
	BYOD_is_Registered	<i>(</i>)		•	-	- &	۲	<u>P</u>	Ĩ	F	ॎ	2		9 👤	C	Ê;	
	Catalyst_Switch_Local_Web_Authentica tion	0			Dictio	onary				Attribut	e			ID		Info	
	Compliance_Unknown_Devices	0			All	Dictionaries			~	Attribut	e					•	^
0	Compliant_Devices	<i>(</i>)		1	Micros	soft ola-Symbol				MS-HC/	VP-Use	r-Name Group		60 12		() ()	
	EAP-MSCHAPv2	()		1	Netwo	ork Access				AD-Use	r-DNS-	Domair	ı			<i>(i</i>)	
0	EAP-TLS			1	Netwo	ork Access				AD-Use	r-Join-F	oint				(i)	
0	Guest_Flow	<i>(</i>)		1	Passi	velD				Passive	ID_Use	ername				() ()	
	MAC_in_SAN	()		1	Radiu	IS				User-Na	ame			1		()	
	Network_Access_Authentication_Passe	0		1	Radiu Rucku	IS				User-Pa Ruckus	usswor -User-C	d Groups		2		() ()	~
	Non_Cisco_Profiled_Phones	1															
	Non_Compliant_Devices																
	Switch_Local_Web_Authentication	<i>i</i>															
0	Switch Web Authentication																

演算子と**して[等**しい]を選択し、その横*のテキ*ストボックスにuser1と入力します。[**Use**]をクリッ ク**し**、属性を保存します。

Con	ditions Studio						
ibra.	у		Editor				
Sea	rch by Name			Radius-User-Nan	ne		
•		b 🖗	1	Equals	user1		
	BYOD_is_Registered			Set to 'Is not'			Duplicate
	Catalyst_Switch_Local_Web_Authentica tion	0					
	Compliance_Unknown_Devices				+ New	AND OR	
	Compliant_Devices	<i>(i</i>)					
	EAP-MSCHAPv2	0					
	EAP-TLS						
	Guest_Flow	<i>(i</i>)					
	MAC_in_SAN	٢					
	Network_Access_Authentication_Passe d	1					
	Non_Cisco_Profiled_Phones	()					
	Non_Compliant_Devices	()					
	Switch_Local_Web_Authentication	0					
8	Switch Web Authentication	()					

これで、このルールの条件が設定されました。

ステップ9:[**Results/Profiles**]列で、+記号をクリックし、[**Create a New Authorization Profile]を選** 択します。

✓ Autho	ization Policy	y (13)					
٠	Obstac	Proje Manuel		Results	Security Crowne		1. Sec.
Search	Status	Rule Name	Conditions	Proties	accurry Groups	HIIS	Actions
1	0	Static IP Address User 1	L Radius User-Name EQUALS user1	Select from list	Select from list 🔹 🕈		¢
				Create a New Authorization Profile			

名前を指定し、ACCESS_ACCEPTをアクセスタイプとして保**持します**。[Advance Attributes Settings]セクションまで**スクロールダウン**します。

Add New Standard Profile		>
Authorization Profile		^
* Name	StaticIPaddressUser1	
Description		
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	the Cisco 💌 🕀	
Service Template		
Track Movement		
Passive Identity Tracking		
 Common Tasks 		
DACL Name		
IPv6 DACL Name		
ACL IPv6 (Filter-ID)	~
		_
Advanced Attributes	Settings	, v
		Save Cancel

オレンジ色の矢印をクリックし、[Radius] > [Framed-IP-Address---[8]を選択します。

Add New Standard Profile Service Template				×
Track Movement			í	
Darriva Identify Tracking 🖂 🖉				
Passive submicky macking [] ()				
	Radius			
▼ Common Tasks				
			^	
DACL Name	Egress-VLANID[56]			
	Error-Cause[101]			
IPv6 DACL Name	Filter-ID[11]			
	Framed-AppleTalk-Link[37]			
_	Framed-AppleTalk-Network{38}			
ACL (Filter-ID)	Framed-AppleTalk-Zone(39)			
	Framed-Compression[13]			
ACL IPv6 (Filter-ID)	Framed-Interface-Id[96]		\sim	
	Framed-IP-Address[8]			
	Framed-IP-Netmask[9]			
	Framed-IPv6-Address[168]			
 Advanced Attributes Settin 	9 🗉 Framed-IPv6-Pool[100]			
Radius:Framed-IP-Address				
			- 1	
Access Type = ACCESS ACCEPT				
Framed-IP-Address =		4		
		Mt.		,
<			>	
		Save	Can	sel

このユーザーに常に静的に割り当てるIPアドレスを入力し、[保存]をクリ**ックします**。

Add New Standard Profile		×
Service Template Track Movement Tracking To C		^
▼ Common Tasks	_	
Arespace IPv6 ACL Name	^	
AVC Profile Name		
UPN Lookup	~	
✓ Advanced Attributes Settings Radius:Framed-IP-Address 10.0.50.101 ● <li< td=""><td></td><td></td></li<>		
▼ Attributes Details Access Type = ACCESS_ACCEPT Framed-IP-Address = 10.0.50.101	Save Ca	▼ ncel

ステップ10:ここで、新しく作成した認可プロファイルを選択します。

✓ Authorization Policy (13)									
					Results				
T	Status	Rule Name	Cond	tions	Profiles		Security Groups	Hits	Actions
Search									
/	0	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	+	Select from list • +		٥
				Misalass Arrass	CISCO_WebAble	^			
	\odot	Wireless Black List Default	AND	Instruct_needs	NSP Opboard		Select from list 🔹 🕇	0	¢
				Internet/output marine booms a bindown internet output previous	Non_Cisco_IP_Phones				
	\odot	Profiled Cisco IP Phones	48	IdentityGroup Name EQUALS Endpoint Identity Groups.Profiled:Cisco-IP-Phone	PermilAccess		Select from list • +	0	\$
	0	Profiled Non Cisco IP Phones	8	Non_Cisco_Profiled_Phones	StaticIPaddressUser1		Select from list + +	0	0
			-		Static_IP_address	~			

これで、認可ルールがすべて設定されました。[Save] をクリックします。

esce Iden	tity Service	es Engine H	iome + Cont	eid Visibility	+ Operations	* Policy	+ Administration	Work Centers	s				License Warn	ing 🔺	् •	•
Policy Sets	s Profiling	Posture Clie	nt Provisioning	 Policy Elen 	nents											
Policy Se	<u>ets</u> → De	fault										Re	set Policyset Hito	ounts	Reset	Save
	Status	Policy Set Nam	e	Description	ı	Condit	lions						Allowed Protocols /	Server S	Sequence	Hits
Search																
	0	Default		Default polic	ty set								Default Network Acce	155	* * +	17
> Auther	ntication Po	olicy (3)														
> Author	rization Poli	icy - Local Except	tions													
> Author	rization Poli	icy - Global Excep	ptions													
✓ Author	rization Poli	icy (13)														
										Results						
•	Status	Rule Name		Condition	15					Profiles		Security Groups			Hits	Actions
Search																
1	ø	Static IP Addres	s User 1	1 R	adius-User-Name	EQUALS use	r1			×StaticlPaddressUser1	+	Select from list		F		¢

確認

ステップ1:Cisco AnyConnectセキュアモビリティクライアントがインストールされているクライ アントマシンに移動します。FTDヘッドエンド(ここではWindowsマシンを使用)に接続し、 *user*1クレデンシャルを*入力し*ます。



歯車のアイコン(左下の角)をクリックして、[Statistics] タブに移動します。[Address Information]セクションで、割り当てられたIPアドレスが、このユーザのISE認証ポリシーで設定 されているIPアドレスであることを確認します。

🚳 Cisco A	nyConnect Secure Mobility Client	-		×
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:23			IP	v4
ن 🌣			 C	lulu isco

Cisco AnyConnect Secure Mobility Client -						
AnyCon	nect Secure Mobility Clie	nt		(
rtual Private Network (V	PN)	Diagnostic	s			
eferences Statistics Route Deta	ails Firewall Message History					
				^		
Connection Information	<u></u>		- ^			
State:	Connected					
Tunnel Mode (IPv4):	Tunnel All Traffic					
Tunnel Mode (IPv6):	Drop All Traffic					
Dynamic Tunnel Exclusion:	None					
Dynamic Tunnel Inclusion:	None					
Duration:	00:01:49					
Session Disconnect:	None					
Management Connection State:	Disconnected (user tunnel active)					
Address Information			- •			
Client (IPv4):	10.0.50.101					
Client (IPv6):	Not Available					
Server:	192.168.0.100					
Bytes						
DYLCS				h.d.		

FTDでのdebug radius allコマンドの出力は次のとおりです。

firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0x9000)
radius mkreq: 0x13
alloc_rip 0x0000145d043b6460
new request 0x13 --> 3 (0x0000145d043b6460)
got user 'user1'
got password
add_req 0x0000145d043b6460 session 0x13 id 3
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101
RADIUS packet decode (authentication request)

RADIUS packet decode (response)

Raw packet data (length = 136)....

02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 |AK..X...1 7d aa 38 1e 01 07 75 73 65 72 31 08 06 0a 00 32 | }.8...user1....2 65 19 3d 43 41 43 53 3a 63 30 61 38 30 30 36 34 | e.=CACS:cOa80064 30 30 30 30 61 30 30 36 31 34 62 63 30 32 64 | 0000a000614bc02d 3a 64 72 69 76 65 72 61 70 2d 49 53 45 2d 32 2d | :driverap-ISE-2-37 2f 34 31 37 34 39 34 39 37 38 2f 32 31 1a 2a | 7/417494978/21.* 00 00 00 09 01 24 70 72 6f 66 69 6c 65 2d 6e 61 |\$profile-na 6d 65 3d 57 69 6e 64 6f 77 73 31 30 2d 57 6f 72 | me=Windows10-Wor 6b 73 74 61 74 69 6f 6e | kstation Parsed packet data.... Radius: Code = 2 (0x02)Radius: Identifier = 3 (0x03)Radius: Length = 136 (0x0088)Radius: Vector: 0CAF1C414BC4A658DEF392317DAA381E Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07)Radius: Value (String) = 75 73 65 72 31 | user1 Radius: Type = 8 (0x08) Framed-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.0.50.101 (0x0A003265) Radius: Type = 25 (0x19) Class Radius: Length = 61 (0x3D)Radius: Value (String) = 43 41 43 53 3a 63 30 61 38 30 30 36 34 30 30 30 | CACS:c0a80064000 30 61 30 30 30 36 31 34 62 63 30 32 64 3a 64 72 | 0a000614bc02d:dr 69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4 31 37 34 39 34 39 37 38 2f 32 31 | 17494978/21 Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 42 (0x2A)Radius: Vendor ID = 9 (0x0000009) Radius: Type = 1 (0x01) Cisco-AV-pair Radius: Length = 36 (0x24)Radius: Value (String) = 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win 64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati 6f 6e | on rad_procpkt: ACCEPT Got AV-Pair with value profile-name=Windows10-Workstation RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0x0000145d043b6460 session 0x13 id 3 free_rip 0x0000145d043b6460 radius: send queue empty FTD のログは次のとおりです。 firepower# <omitted output> Sep 22 2021 23:52:40: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.101/60405 to 192.168.0.100/443 for TLSv1.2 session Sep 22 2021 23:52:48: %FTD-7-609001: Built local-host Outside_Int:172.16.0.8 Sep 22 2021 23:52:48: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 : user = user1 Sep 22 2021 23:52:48: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user1 Sep 22 2021 23:52:48: %FTD-6-113008: AAA transaction status ACCEPT : user = user1 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.radius["1"]["1"] = user1 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.radius["8"]["1"] = 167785061 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute

aaa.radius["25"]["1"] = CACS:c0a800640000c000614bc1d0:driverap-ISE-2-7/417494978/23 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.grouppolicy = DfltGrpPolicy Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.ipaddress = 10.0.50.101 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.username = user1 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.username1 = user1 Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.username2 = Sep 22 2021 23:52:48: %FTD-7-734003: DAP: User user1, Addr 192.168.0.101: Session Attribute aaa.cisco.tunnelgroup = RA_VPN Sep 22 2021 23:52:48: %FTD-6-734001: DAP: User user1, Addr 192.168.0.101, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy Sep 22 2021 23:52:48: %FTD-6-113039: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> AnyConnect parent session started. <omitted output> Sep 22 2021 23:53:17: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.101/60412 to 192.168.0.100/443 for TLSv1.2 session Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv4 address request' message queued Sep 22 2021 23:53:17: %FTD-7-737035: IPAA: Session=0x0000c000, 'IPv6 address request' message queued Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv4 address request' Sep 22 2021 23:53:17: %FTD-6-737010: IPAA: Session=0x0000c000, AAA assigned address 10.0.50.101, succeeded Sep 22 2021 23:53:17: %FTD-7-737001: IPAA: Session=0x0000c000, Received message 'IPv6 address request' Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: no IPv6 address available from local pools Sep 22 2021 23:53:17: %FTD-5-737034: IPAA: Session=0x0000c000, IPv6 address: callback failed during IPv6 request Sep 22 2021 23:53:17: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User <user1> IP <192.168.0.101> No IPv6 address available for SVC connection Sep 22 2021 23:53:17: %FTD-7-609001: Built local-host Outside_Int:10.0.50.101 Sep 22 2021 23:53:17: %FTD-5-722033: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> First TCP SVC connection established for SVC session. Sep 22 2021 23:53:17: %FTD-6-722022: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> TCP SVC connection established without compression Sep 22 2021 23:53:17: %FTD-7-746012: user-identity: Add IP-User mapping 10.0.50.101 -LOCAL\user1 Succeeded - VPN user Sep 22 2021 23:53:17: %FTD-6-722055: Group <DfltGrpPolicy> User <user1> IP <192.168.0.101> Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086 Sep 22 2021 23:53:17: %FTD-4-722051: Group

```
ISEのRADIUS Liveログには次のように表示されます。
```

Event	5200 Authentication succeeded
Isemame	user1
Endpoint Id	00.50.58.98.48.67 (0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Statio IP Address User 1
Authorization Result	StaticiPaddressUser1

Source Timestamp	2021-09-22 23:53:19.72
Received Timestamp	2021-09-22 23:53:19.72
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Usemame	usert
User Type	User
Endpoint Id	00.50.56.96.45.6F
Calling Station Id	192.108.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	x0x8000540000x0000514bx1x0
Authentication Method	PAP_ASCI
Authentication Protocol	PAP_ASCI
Network Device	DRIVERAP_FTD_7.0
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	0.0.0.0

Steps

- Stopp
 Stopp

 1991
 Residued RADUS Access Respond

 1991
 Residued Printy Ghoup

 1994
 Residued printy Stopp

 1994
 Residued Stopp

 1995
 Selected Stopp

 1994
 Selected Stopp

 1995
 Selected Stopp

 1994
 Selected Stopp

 1994
 Selected Stopp

 1995
 Selected Stopp

 1995
 Selected Stopp

 1997
 Selected Stopp

 1998
 Selected Stopp

 199

- 2027
 Automiciation Passed

 2116
 Rist and colomed today previous subsetul machine automiciation for use in Adam Directory

 2028
 Evaluation Automiciation Pulicy

 2029
 Evaluation Automiciation Pulicy

 2020
 Evaluation Pulicy

 2021
 Fund Endpairs In Internal Endpairs Distore

 2021
 Evaluation Pulicy in Internal Endpairs Distore

 2031
 Second Endpairs In Internal Endpairs Distore

 2035
 Execution Second Endpairs

 2036
 Max eservice policy seaml

 2038
 Resources Anotysic

 11952
 Reshumed RADUS Access-Accept

en internet of the office	
NAS Port Type	Vitual
Authorization Profile	Static/PaddressUser1
Response Time	51 milliseconds
Other Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Redus
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
CVPN3000/ASA/P0/7x-Tunnel- Group Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0099505-3150-4215-a80e-6753d45bf56o
Is ThirdPartyDeviceFlow	faite
CVPN3000/A SA/PDX7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417494978/23
SelectedAuthenticationIdentity Sto	res Internal Users
Selected Authentication Identity Sto	res All AD Join Points
Selected & theories stical deaths fits	as front then
Authentication Status	AdmentionEnned
Marth Pales Matched Pale	Pada di
Authorization Dalign Matched Dale	State ID Address Lines 1
AuthorizationPolicyMatchedRule	Statio IP Address Geer 1
15t Policy Settlame	Delani
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types

IPSEC	IPSEC#s IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPMSessionID	dba800040000.0000014bc1d0
Called-Station-ID	192,108.0.100
CiscoW/Pair	ndn inndering klatmenkin, mön inndering klatmenkin, nön inndering klatmenking (h. 1932), mön inndering klatmenking) (h. 1932), mön inndering klatmenking) (h. 1932), mön inndering klatmenking (h. 1932), mön inndering klatmenking (h. 1932), glabar HEFFELDOFFEL
Result	10.0.50 101
Class	CACS v0x500540000x000514br140 driveran ISE 2.7341749497823
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed
Session Events	

ステップ2:FTDヘッドエンド(ここではWindowsマシンを使用)に接続し、user2のクレデンシャ ルを入力します。

S Cisco AnyConnect 192.168.0.100 ×	🕥 Cisco AnyConnect Secure Mobility Client — 🗌	×
Group: RA_VPN ~ Username: user2 Password: ******	VPN: Contacting 192.168.0.100. 192.168.0.100 Connect	
OK Cancel	\$ (i)	cisco

[Address Information] セクションでは、割り当てられたIPアドレスが、FMCを介して設定された IPv4ローカルプールで使用可能な最初のIPアドレスであることが示されています。

Sisco AnyConnect Secure Mobil	ity Client	<u> </u>		х
cisco AnyCon	nect Secure Mobility Client			()
Virtual Private Network (VF	N)	Diagnostics	s	
Preferences Statistics Route Detail	s Firewall Message History			
Connection Information				^
State:	Connected			
Tunnel Mode (IPv4):	Tunnel All Traffic			
Tunnel Mode (IPv6):	Drop All Traffic			
Dynamic Tunnel Exclusion:	None			
Dynamic Tunnel Inclusion:	None			
Duration:	00:01:05			
Session Disconnect:	None			
Management Connection State:	Disconnected (user tunnel active)			
Address Information			- •	
Client (IPv4):	10.0.50.1			
Client (IPv6):	Not Available			
Server:	192.168.0.100			
Bytes			_ ^	
				¥
	Reset	Expo	rt Stats	•

FTDでの**debug radius allコマンド**の出力は次のとおりです。

firepower# SVC message: t/s=5/16: The user has requested to disconnect the connection.
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL

np_svc_destroy_session(0xA000)
radius mkreq: 0x15
alloc_rip 0x0000145d043b6460
new request 0x15 --> 4 (0x0000145d043b6460)
got user 'user2'
got password
add_req 0x0000145d043b6460 session 0x15 id 4
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.0.101

RADIUS packet decode (authentication request)

RADIUS packet decode (response)

-----Raw packet data (length = 130).... 02 04 00 82 a6 67 35 9e 10 36 93 18 1f 1b 85 37 |q5..6.....7 b6 c3 18 4f 01 07 75 73 65 72 32 19 3d 43 41 43 | ...O..user2.=CAC 53 3a 63 30 61 38 30 30 36 34 30 30 30 30 30 62 30 | S:c0a800640000b0 30 30 36 31 34 62 63 30 61 33 3a 64 72 69 76 65 | 00614bc0a3:drive 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 31 37 34 | rap-ISE-2-7/4174 39 34 39 37 38 2f 32 32 1a 2a 00 00 00 09 01 24 | 94978/22.*....\$ 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win 64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dows10-Workstati 6f 6e | on Parsed packet data.... Radius: Code = 2(0x02)Radius: Identifier = 4 (0x04)Radius: Length = 130 (0x0082)Radius: Vector: A667359E103693181F1B8537B6C3184F Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07)Radius: Value (String) = 75 73 65 72 32 | user2 Radius: Type = 25 (0x19) Class Radius: Length = 61 (0x3D)Radius: Value (String) = 43 41 43 53 3a 63 30 61 38 30 36 34 30 30 30 30 | CACS:c0a80064000 30 62 30 30 30 36 31 34 62 63 30 61 33 3a 64 72 | 0b000614bc0a3:dr 69 76 65 72 61 70 2d 49 53 45 2d 32 2d 37 2f 34 | iverap-ISE-2-7/4 31 37 34 39 34 39 37 38 2f 32 32 | 17494978/22 Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 42 (0x2A)Radius: Vendor ID = 9 (0x0000009) Radius: Type = 1 (0x01) Cisco-AV-pair Radius: Length = 36 (0x24)Radius: Value (String) = 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 69 6e | profile-name=Win 64 6f 77 73 31 30 2d 57 6f 72 6b 73 74 61 74 69 | dowslo-Workstati 6f 6e | on rad_procpkt: ACCEPT Got AV-Pair with value profile-name=Windows10-Workstation RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0x0000145d043b6460 session 0x15 id 4 free_rip 0x0000145d043b6460 radius: send queue empty FTD のログは次のとおりです。

<omitted output> Sep 22 2021 23:59:26: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.101/60459 to 192.168.0.100/443 for TLSv1.2 session Sep 22 2021 23:59:35: %FTD-7-609001: Built local-host Outside_Int:172.16.0.8 Sep 22 2021 23:59:35: %FTD-6-113004: AAA user authentication Successful : server = 172.16.0.8 : user = user2Sep 22 2021 23:59:35: %FTD-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user2 Sep 22 2021 23:59:35: %FTD-6-113008: AAA transaction status ACCEPT : user = user2 Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.radius["1"]["1"] = user2 Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.radius["25"]["1"] = CACS:c0a800640000d000614bc367:driverap-ISE-2-7/417494978/24 Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.grouppolicy = DfltGrpPolicy Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.username = user2 Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.username1 = user2 Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.username2 = Sep 22 2021 23:59:35: %FTD-7-734003: DAP: User user2, Addr 192.168.0.101: Session Attribute aaa.cisco.tunnelgroup = RA_VPN Sep 22 2021 23:59:35: %FTD-6-734001: DAP: User user2, Addr 192.168.0.101, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy Sep 22 2021 23:59:35: %FTD-6-113039: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> AnyConnect parent session started. <omitted output> Sep 22 2021 23:59:52: %FTD-6-725002: Device completed SSL handshake with client Outside_Int:192.168.0.101/60470 to 192.168.0.100/443 for TLSv1.2 session Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv4 address request' message queued Sep 22 2021 23:59:52: %FTD-7-737035: IPAA: Session=0x0000d000, 'IPv6 address request' message queued Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv4 address request' Sep 22 2021 23:59:52: %FTD-5-737003: IPAA: Session=0x0000d000, DHCP configured, no viable servers found for tunnel-group 'RA_VPN' Sep 22 2021 23:59:52: %FTD-7-737400: POOLIP: Pool=AC_Pool, Allocated 10.0.50.1 from pool Sep 22 2021 23:59:52: %FTD-7-737200: VPNFIP: Pool=AC_Pool, Allocated 10.0.50.1 from pool Sep 22 2021 23:59:52: %FTD-6-737026: IPAA: Session=0x0000d000, Client assigned 10.0.50.1 from local pool AC_Pool Sep 22 2021 23:59:52: %FTD-6-737006: IPAA: Session=0x0000d000, Local pool request succeeded for tunnel-group 'RA_VPN' Sep 22 2021 23:59:52: %FTD-7-737001: IPAA: Session=0x0000d000, Received message 'IPv6 address request' Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: no IPv6 address available from local pools Sep 22 2021 23:59:52: %FTD-5-737034: IPAA: Session=0x0000d000, IPv6 address: callback failed during IPv6 request Sep 22 2021 23:59:52: %FTD-4-722041: TunnelGroup <RA_VPN> GroupPolicy <DfltGrpPolicy> User <user2> IP <192.168.0.101> No IPv6 address available for SVC connection Sep 22 2021 23:59:52: %FTD-7-609001: Built local-host Outside_Int:10.0.50.1 Sep 22 2021 23:59:52: %FTD-5-722033: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> First TCP SVC connection established for SVC session. Sep 22 2021 23:59:52: %FTD-6-722022: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> TCP SVC connection established without compression Sep 22 2021 23:59:52: %FTD-7-746012: user-identity: Add IP-User mapping 10.0.50.1 - LOCAL\user2 Succeeded - VPN user Sep 22 2021 23:59:52: %FTD-6-722055: Group <DfltGrpPolicy> User <user2> IP <192.168.0.101> Client Type: Cisco AnyConnect VPN Agent for Windows 4.10.02086

Sep 22 2021 23:59:52: %FTD-4-722051: Group

ISEのRADIUS Liveログには次のように表示されます。

Event	5200 Authentication succeeded	
Usemame	use/2	
Endpoint Id	00.50.56.96.46.6F 🕀	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Basic_Authenticated_Access	
Authorization Result	PermitAccess	
thentication Details		
Source Timestamp	2021-09-23 00:00:08.488	
Received Timestamp	2021-09-23 00:00:08.488	
Policy Server	driverap-ISE-2-7	
Event	5200 Authentication succeeded	
Usemame	Seeu	
User Type	User	
Endpoint Id	00.50.50.90.40.0F	
Calling Station Id	192.168.0.101	
Endpoint Profile	Windows10-Workstation	
Authentication Identity Store	Internal Users	
Identity Group	Workstation	
Audit Session Id	d0a000540000d000614bc387	
Authentication Method	PAP_ASCI	
Authentication Protocol	PAP_ASCI	
Network Device	DRIVERAP_FTD_7.0	
	All Davies Tones	

Identity Services Engine	
NAS Port Type	Vitual
Authorization Profile	PermitAccess
Response Time	202 milliseconds
Other Attributes	
ConfigWersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
CVPN3000/ASA/PIX7x-Tunnel- Group Name	RA_VPN
OriginalUserName	use2
NetworkDeviceProfileId	b0599505-3150-4215-a80e-8753d45b/55o
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/POX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/24
SelectedAuthenticationIdentityStore	s Internal Users
SelectedAuthenticationIdentityStore	s All_AD_Join_Points
SelectedAuthenticationIdentityStore	s Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basiq_Authenticated_Access
15EPolicySetName	Default
Identity SelectionMatchedRule	Default
DTL 5 Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

Name	Endpoint Identity Groups Profiled Workstation	
EnableFlag	Enabled	
RADIUS Username	use/2	
Device IP Address	192.168.0.100	
CPMSessionID	c0a800540000d000514bc367	
Called-Station-ID	192.168.0.100	
Cisco/WPair	India Sin-Applica (Jatamonic), India Sin-Applica (Jatamonic), India Sin-Applica (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (Jata) (Jata) (Jata) (Jata) (Jata) India Sin-Applica (Jata) (
esult		
Class	CACS.cba800640000d000614bc367.driverap-ISE-2-7/417494978/24	
cisco-av-pair	profile-name=Windows10-Workstation	
	Base license consumed	

Session Events

注: AnyConnectクライアント間で重複するIPアドレスの競合を避けるには、FTD ipローカ ルプールとISE認可ポリシーの両方でIPアドレス割り当てに異なるIPアドレス範囲を使用す る必要があす。この設定例では、10.0.50.1から10.0.50.100までのIPv4ローカルプールを使 用してFTDが設定され、ISEサーバは10.0.50.101の静的IPアドレスを割り当てます。

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。

FTD :

debug radius all

ISE:

• RADIUS ライブ ログ