Configurer l'attribution d'adresses IP statiques aux utilisateurs AnyConnect via l'autorisation RADIUS

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Diagramme du réseau Configuration du VPN d'accès à distance avec authentification AAA/RADIUS via FMC Configurer la stratégie d'autorisation sur ISE (serveur RADIUS) Vérification Dépannage

Introduction

Ce document décrit comment configurer l'autorisation RADIUS avec un serveur ISE (Identity Services Engine) afin qu'il transfère toujours la même adresse IP à Firepower Threat Defense (FTD) pour un utilisateur spécifique du client Cisco AnyConnect Secure Mobility via l'adresse IP tramée RADIUS Attribute 8.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FTD
- Firepower Management Center (FMC)
- ISE
- Client de mobilité sécurisée Cisco AnyConnect
- protocole RADIUS

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- FMCv 7.0.0 (build 94)
- FTDv 7.0.0 (build 94)
- ISE 2.7.0.356
- AnyConnect 4.10.02086

• Windows 10 Pro

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Diagramme du réseau



Configuration du VPN d'accès à distance avec authentification AAA/RADIUS via FMC

Pour une procédure pas à pas, reportez-vous à ce document et à cette vidéo :

- <u>Configuration VPN d'accès à distance AnyConnect sur FTD</u>
- <u>Configuration AnyConnect initiale pour FTD géré par FMC</u>

La configuration VPN d'accès à distance sur l'interface CLI FTD est la suivante :

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

Configurer la stratégie d'autorisation sur ISE (serveur RADIUS)

Étape 1. Connectez-vous au serveur ISE et accédez à Administration > Network Resources > Network Devices.

dealer Identity Services Engine	Home •	Context Visibility	Operations	Policy	• A	dministration	+ Work Center	5							License Warnin	ng 🔺 🔍	0 0 0	
Summary Endpoints	Guests	Vulnerability	Threat	+	Sy	stem		Network Reso	ources	pxGrid Services							۰ ه	
METRICS Total Endpol	ints 0	1	Active Endpo	vints Ø	U U U U U U U U U U U U U U U U U U U	Jeensing Jentificates Jopping Jaintenance Jpgrade Backup & Restore Idmin Access Settings entity Management dentities Jroups	et	Network Dev Network Dev External RAC RADIUS Sen NAC Manage External MDM Location Ser Device Portal Blackist BYOD Certificate Pr	Ace Groups Ace Profiles XUS Servers ver Sequences ers M Nices Management rovisioning	Feed Service Profiler Threat Centric NAC Third Party Vendors	2	Aut	henticated Guests Ø	0	BYOD Endpoints @	0	- Q	
AUTHENTICATIONS dentity Group Norm) ork.Device Fa	aluro Reason		80) 10 S	External Identity So dentity Source Sec Settings	turces quences	Client Provis Mobile Devic My Devices Custom Port Settings	ioning te Management tal Files		×		ENDPOINTS O				e ល x	
inter_users: [100%]_	()				driv	ea5506: [10	00%]	0				workstations: [100%]	0			
∃ BYOD ENDPOINTS ⁰				øø	×	# ALAR	MS 0				gox		# SYSTEM SUMM	ARY 0			øøх	U.
Type Profile						Severity	Name	C	Occu Last Oc	curred	^	`	1 node(s)				All * 24HR *	
	No data	available.				~	Name						driverap-ISE-2-7		Mamon Linna	Authoritical	ion Latency	
		- forder to taken the		and the state of		٥	DNS Resolutio	on Failure 9	41 less than	1 min ago			CPU		mannary collige	Paraterioca	on canny	
ps//10.51.124.31:0012/admin/#a	aministratio	nyadministratio	netwoncesou	urces/admi	inistratio	on_networkres	.ources_device	es a la setti d	1600 love three	1 min ann			****************					

Étape 2. Dans la section Périphériques réseau, cliquez sur **Ajouter** pour qu'ISE puisse traiter les demandes d'accès RADIUS à partir du FTD.

dentity Services Engine	Home + Context Visibility	Operations	Policy Administ	ation • Work Centers			License Warning 🔺	
System identity Management	Network Resources Device	ce Portal Manager	ment pxGrid Services +	eed Service + Threat Centri	e NAC			
Network Devices Network Device G	roups Network Device Profile	s External RAD	UUS Servers RADIUS Serv	r Sequences NAC Manager	s External MDM + Location Services			
•								
Network Devices	Network Devices							
Default Device							Selecte	d 0 Total 1 🧐 🎡 🖕
Device Security Settings	/ Edit -Add	Dimport @	Export • OGenerate PAC	XDelete +			Show AI	- 8
	Name 🔺	IP/Mask	Profile Name	Location	Type	Description		
	DRIVERAP_ASA5506	172.16.255.2	dia Cisco 🙂	All Locations	All Device Types			

Entrez les champs **Nom** du périphérique réseau et **Adresse IP**, puis cochez la case **Paramètres d'authentification RADIUS**. Le **secret partagé** doit être la même valeur que celle utilisée lors de la création de l'objet RADIUS Server sur FMC.

dentity Services Engine	Home + Contact Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🍳 😑 🧿 🌣 ^
System Identity Management	Herknerk Resources + Device Portal Management prGrid Service + Feed Service + Threat Centric NAC	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
6		
Network Devices	Network Devices List > New Retwork Device	
Default Device		
Device Security Settings	name (DRUPERA-FID_7.0	
	Description	
		@ *
	* Device Profile I atta Cisco 💌 🕀	
	MOOR FRAME	
	Software Version +	
	* Network Device Group	
	Location Allocations O Set To Default	
	University Al Dece Types O Section man	
	RADUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Shared Secret	
	Use Second Shared Secret 🗌 🕢	
	Show	
	CoA Port 1700 Set. To. Default	
	RADUS DTLS Settings (7)	
	DTLS Required 🗌 🕡	~

Enregistrez-le avec le bouton à la fin de cette page.

Étape 3. Accédez à Administration > Identity Management > Identities.

dealer Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Center	\$		License Warning 🔺 🤍 😐 🔿 🗢
System Identity Management	Network Resources Device Portal Management pxGrid	System	Network Resources	pxGrid Services	
Network Devices Network Device C	Groups Network Device Profiles External RADIUS Servers	Deployment	Network Devices Network Device Groups	Feed Service	
0		Certificates	Network Device Profiles	Profiler	
Network Devices	Network Devices	Logging Maintenance	External RADIUS Servers RADIUS Server Sequences	Threat Centric NAC Third Party Vendors	
Default Device		Upgrade	NAC Managers		Selected 0 Yotal 2 😵 🐳 🖬
Device Security Settings	/Edit -Add L_Duplcate @Import @Export - OK	Backup & Restore Admin Access	External MDM Location Services		Show Al Y
	Name DP/Mask Profile Name	Settings	Device Portal Management		
	DRIVERAP_A. 172.16.0.10 # OKO @	Identity Management	Blacklist		
		Groups	BYOD Certificate Provisioning		
		External Identity Sources	Client Provisioning		
		Identity Source Sequences Settings	Mobile Device Management My Devices		
			Custom Portal Files		
			Settings		
https://10.31.124.31:6012/admin/#a	administration/administration_identitymanagement/ad	ministration_identitymanagemen	t_identities		

Étape 4. Dans la section Network Access Users, cliquez sur **Add** afin de créer *user1* dans la base de données locale d'ISE.



Entrez le nom d'utilisateur et le mot de passe dans les champs **Nom** et **Mot de passe de connexion**, puis cliquez sur **Envoyer**.

dealer Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺		o i
System Identity Management	Network Resources Device Portal Management psGrid Service Feed Service Threat Centric NAC			
·Identities Groups External Identi	ny Sources Identity Source Sequences + Settings			
0				
Users	Network Access Users List > New Network Access User			
Latest Manual Network Scan Res	•Name user1 Status C Enabled +			
	Email			
	▼ Passwords			
	Password Type: Internal Users +			
	Password Re-Enter Password			
	*Login Password ++++++ Generate Password @			
	Enable Password Generate Password ()			
	* User Information			
	First Name			
	LastName			
	▼ Account Options			
	Description			
	Change password on next login			
	* Account Disable Policy			- 1
	Disable account if date exceeds 2021-11-21 (yyy-mm-dd)			
	* User Groups			
	Select an item 🖉 — 🕂			
	Submit Cancel			
<				>

Étape 5. Répétez les étapes précédentes afin de créer user2.



Étape 6. Accédez à Stratégie > Jeux de stratégies.



Étape 7. Cliquez sur la flèche > à droite de l'écran.

adaada cisco	identity Servic	es Engine Home + Con	text Visibility	Policy Administration Work Centers			License Warning		
Polic	r Sets Profilin	g Posture Client Provisioning	Policy Elements						
Polic	y Sets					•	eset Policyset Hitcou	nts Reset	Save
+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server	Sequence Hits	Actions	View
Sea	ch								
					+				
	0	Default	Default policy set			Default Network Access	* * + 17	¢	>
								Reset	Save

Étape 8. Cliquez sur la flèche > en regard de **Stratégie d'autorisation** pour la développer. Cliquez maintenant sur le symbole + afin d'ajouter une nouvelle règle.

cisco lidenti	ny services	Engine Home Contex	d Visibilit	ty + Operations	Policy Administration	Work Centers					License Warning 🔺	<u> </u>	0 0	0
Policy Sets	Profiling	Posture Client Provisioning	 Policy I 	Elements										
Policy Se	ts → Defa	ault								Re	set Policyset Hitcount	Res	et Sav	ve
	Status	Policy Set Name	Descrip	ption	Conditions						Allowed Protocols / Serve	er Sequenc	e Hits	ŧ.
Search														
	0	Default	Default	policy set							Default Network Access	×* 4	17	
> Authent	tication Poli	cy (3)												
> Authoria	zation Polic	y - Local Exceptions												
> Authoria	zation Polic	y - Global Exceptions												
✓ Authoriz	zation Polic	<u>y (13)</u>												
								Results						
•	Status	Rule Name	Cond	litions				Profiles		Security Groups		Hits	Actions	4
Search														
	0	Wreless Black List Default	AND	Wireless_Ac	ccess			×Blackhole Wireless Access	+	Select from list	- +	0	ø	
	Ť.,		1110	4 IdentityGroup	p-Name EQUALS EndpointIden	tity Groups:Blacklist								
	ø	Profiled Cisco IP Phones	48	IdentityGroup Name E	EQUALS Endpoint Identity Group	s Profiled Cisco-IP-Phor	ne	×Cisco_JP_Phones	+	Select from list	- +	0	٥	
	0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_	Phones			(×Non_Cisco_IP_Phones)	+	Select from list	· +	0	٥	
	0	Inimum Compliance Redired		Network_Acc	cess_Authentication_Passed			x Cisco Temporal Onhosof		Salart from list	- 4		~	
	0	contrain_complainte_realeu	AND	Compliance	_Unknown_Devices			(*	
	0			Network_Acc	cess_Authentication_Passed			(Outertham Est			~	
	0	wonCompliant_Devices_Redirect	AND	Non_Compli	liant_Devices			× Cisco_Temporal_Onboard	Τ.	beliect from list	• •	0	¢	

Entrez un nom pour la règle et sélectionnez le symbole + dans la colonne Conditions.

✓ Author	zation 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

Cliquez dans la zone de texte Éditeur d'attributs et cliquez sur l'icône **Objet**. Faites défiler la liste vers le bas jusqu'à ce que vous trouviez l'attribut *Nom d'utilisateur RADIUS* et que vous le choisissiez.

ibrary		Editor														
Search by Name		•	Clic	ck to add	d an attribu	te										
♀ □ ▲ ⊕ 早 ₽ ₽ 0 0 0	106 🕫 🗟	5	Select	attribut	e for condi	tion				_						
BYOD_is_Registered	()		•	Ē	•	۲	<u>P</u>	đ	F		2	Ē	© 🚺		ີະ	
Catalyst_Switch_Local_Web_Authentition	ica 🕡			Dict	onary				Attribu	te			ID		Info	
Compliance_Unknown_Devices	0		1	Al	Dictionaries			~	Attribut	e AP-Use	r-Name	•	60		<i>(</i> i)	^
Compliant_Devices	()		1	Moto	rola-Symbol				Symbol	-User-0	Group		12		<i>i</i>	
EAP-MSCHAPv2	()		1	Netv	vork Access				AD-Use	r-DNS-	Domair	n			()	
EAP-TLS	()		1	Netv	vork Access				AD-Use	r-Join-F	Point				(i) (i)	
Guest_Flow	()		1	Pas	siveID				Passive	ID_Us	ername				0	
MAC_in_SAN	()		1	Rad	us				User-N	ame			1		0	٩
Network_Access_Authentication_Pass	se 🕡		1	Ruci	kus				Ruckus	-User-(Groups		1		() ()	~
Non_Cisco_Profiled_Phones	()					-	-		-	-	-	-	-	-	-	-
Non_Compliant_Devices	1															
Switch_Local_Web_Authentication	<i>i</i>)															
Switch Web Authentication	<i>(</i>)															

Conservez **Equals** en tant qu'opérateur et entrez *user1* dans la zone de texte à côté. Cliquez sur **Use** afin d'enregistrer l'attribut.

brar	у		Editor					
Sear	rch by Name			Radius-User-Na	me			
9		0 b 🕈	1	Equals	v user1			
	BYOD_is_Registered			Set to 'Is not'			Duplicate	
	Catalyst_Switch_Local_Web_Authentica tion	()						
	Compliance_Unknown_Devices	()			+ New AND	OR		
	Compliant_Devices							
	EAP-MSCHAPv2							
	EAP-TLS							
	Guest_Flow							
	MAC_in_SAN	0						
	Network_Access_Authentication_Passe d							
	Non_Cisco_Profiled_Phones	0						
	Non_Compliant_Devices							
	Switch_Local_Web_Authentication	0						
	Switch Web Authentication							

La condition de cette règle est maintenant définie.

Étape 9. Dans la colonne **Résultats/Profils**, cliquez sur le symbole + et choisissez **Créer un nouveau profil d'autorisation**.

✓ Author	rization Policy	y (13)					
				Results			
•	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
1	0	Static IP Address User 1	Radus User-Name EQUALS user1	Select from list	Select from list 🔹 🛨		¢
				Create a New Authorization Profile			

Donnez-lui un **nom** et conservez *ACCESS_ACCEPT* comme **type d'accès**. Faites défiler jusqu'à la section **Paramètres des attributs avancés**.

Add New Standard Profile			×
Authorization Profile		^	
* Name	StaticIPaddressUser1		
Description			
* Access Type	ACCESS_ACCEPT *		
Network Device Profile	And Cisco + D		
Service Template			
Track Movement			
Passive Identity Tracking			
▼ Common Tasks			
DACL Name			
IPv6 DACL Name			
ACL (Filter-ID)			
ACL IPv6 (Filter-ID)		~	
 Advanced Attributes 	Settings	~	I
<	Start Sta	>	
	Jave	Cancel	2

Cliquez sur la flèche orange et choisissez Radius > Framed-IP-Address-[8].

Add New Standard Profile Service Template			×
Track Movement 🔲 🕧			
Passive Identity Tracking 🔲 🕧			
R	adius		
Tommon Tacks			
Common Tasks		•	
DACL Name	Foress-VI ANID-1561		
	Error-Cause[10]		
IPv6 DACL Name	Filter-ID[11]		
	Framed-AppleTalk-Link-[37]		
	Framed-AppleTalk-Network[38]		
ACL (Fiter-ID)	Framed-AppleTalk-Zone(39)		
	Framed-Compression[13]		
ACL IPv6 (Filter-ID)	Framed-Interface-Id-(96)	~	
	Framed-IP-Address[8]		
	Framed-tP-Netmask[9]		
	Framed-IPv6-Address[168]		
 Advanced Attributes Setting 	Framed-IPv6-Pool[100]		
Radius:Framed-IP-Address			
▼ Attributes Details			
Access Type = ACCESS ACCEPT			
Framed-IP-Address =			
			~
<		>	
		Save	ncel

Tapez l'adresse IP que vous souhaitez affecter de manière statique à cet utilisateur et cliquez sur **Enregistrer**.

Add New Standard Profile		×
Service Template		^
▼ Common Tasks		
Airespace IPv6 ACL Name	^	
🗆 ASA VPN		
AVC Profile Name		
UPN Lookup	~	
▼ Advanced Attributes Settings		
Radus:Framed-IP-Address 💽 = 10.0.50.101 💿 = +		
★ Attributes Details Access Type = ACCESS_ACCEPT Framed-IP-Address = 10.0.50.101		~
	Save Ca	ncel

Étape 10. Sélectionnez maintenant le profil d'autorisation nouvellement créé.

 Autho 	rization Polic	y (13)							
					Results				
T	Status	Rule Name	Cond	tions	Profiles		Security Groups	Hits	Actions
Search									
1	ø	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	+	Select from list • +		¢
				Wreless Access	Derwiccess	^			
	\odot	Wireless Black List Default	AND	IdentityGroup Name EQUALS Endpoint Identity Groups:Blacklist	NSP_Onboard		Select from list • +	0	٥
					Non_Cisco_IP_Phones	2			
	\odot	Profiled Cisco IP Phones	44	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco-IP-Phone	PermitAccess		Select from list • +	0	\$
	0	Profiled Non Cisco IP Phones	8	Non_Cisco_Profiled_Phones	StaticiPaddressUser1		Select from list • +	0	0
			_		Static_IP_address	~			

La règle d'autorisation est maintenant définie. Click Save.

iden	tity Service	es Engine Home + Co	ontext Visibility	Policy Administration	Work Centers				License Warning 🔺	<u>२</u> •	•
Policy Sets	Profiling	Posture Client Provisioning	Policy Elements								
olicy Se	ets → De	fault						Reset P	olicyset Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions				Allowe	d Protocols / Server	Sequence	Hits
earch											
	0	Default	Default policy set					Defa	It Network Access	* * +	17
Auther	ntication Po	blicy (3)									
Author	rization Poli	icy - Local Exceptions									
Author	rization Poli	icy - Global Exceptions									
Author	rization Poli	icy (13)									
						1	Results				
•	Status	Rule Name	Conditions				Profiles	Security Groups		Hits	Actions
Search											
1	0	Static IP Address User 1	Radius-User-Name	EQUALS user1			* StaticlPaddressUser1	+ Select from list	× +		٥

Vérification

Étape 1. Accédez à la machine cliente sur laquelle le client Cisco AnyConnect Secure Mobility est installé. Connectez-vous à votre tête de réseau FTD (un ordinateur Windows est utilisé ici) et entrez les informations d'identification *user1*.



Cliquez sur l'icône du rapport (coin inférieur gauche) et accédez à l'onglet **Statistiques**. Confirmez dans la section **Address Information** que l'adresse IP attribuée est effectivement celle configurée sur la stratégie d'autorisation ISE pour cet utilisateur.

🕙 Ci	sco AnyC	Connect Secure Mobility Client			×
ĺ		VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnec	t
00:0	00:23				IPv4
0	i				alialia cisco

		8
AnyCon	nect Secure Mobility Client	(
rtual Private Network (V	PN) Diagnostics	
eferences Statistics Route Deta	ails 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:	00:01:49	
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		^ _
	Decet Evport St	tate

La sortie de la commande debug radius all sur FTD affiche :

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).....

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 Les journaux FTD affichent : 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

02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 |AK..X...1

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

Les journaux RADIUS Live sur ISE montrent :

Event	5200 Authentication succeeded
Isername	user!
Endpoint Id	00.50.55.95.45.57 ()
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Statio IP Address User 1
Authorization Result	StaticiPaddressUser1

2021-09-22 23:53:19:72 Source Timestamp 2021-09-22 23:53:19.72 Received Tin Policy Serve driverap-ISE-2-7 Event 5200 Authenticat user1 User 00 50 50 90 40 07 192.168.0.101 Windows10-Works Internal Users Authentication Workstation Audit Session Id 014800040000 PAP_ASCI Authentication Method PAP_ASCII DRIVERAP_FTD_7.0 Authentication Protocol Network Device All Device Types Device Type Location All Locations NAS IPv4 Address 0.0.0.0

Steps

- Sector 1951 Residued RADUS Access Resource 1951 Residued RADUS Access Resource 1957 RADUS greated a new section 1959 Residued greans Benefactor Relay 1959 Residued greans Benefactor Relay 1959 Residued Sector Relay 1959 Sectores Benefactor Relay 1959 Relay Sectores Relay 1950 Relay Sectores Relay Sectores Relay 1950 Relay Sectores Relay Sectores Relay 1950 Relay Sectores Relay Sectores

- 24715 ISE has not confirmed locally previous to authentication for user in Active Directory
- 2415 autoetication for use in Adrive Directory 19036 Extendent Autorization Pellity 24205 Looling us Endpoint in Internal Endpoints (20 24211: Found Endpoint in Internal Endpoints (20 24211: Found Endpoint in Internal Endpoints (20 2421): Selected Autorization Politie StaticPaddree 20001: Mais sessione policy passed

- 22080 New accounting session created in Session cache 11082 Returned RADIUS Access-Accept

NAS Port Type	Vitual
Authorization Profile	Static/PaddressUser1
Response Time	61 milliseconds
Other Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PDC7x-Tunnel- Group Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0599505-3150-4215-a00e-6753d45bf56o
Is ThirdPartyDeviceFlow	false
CVPN3000/ASA/PDX7x-Client-Type	2
AcsSessionID	driversp-ISE-2-7/417494978/23
SelectedAuthenticationIdentityStore	es Internal Users
SelectedAuthenticationIdentityStore	es All_AD_Join_Points
SelectedAuthenticationIdentityStore	es. Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Statio IP Address User 1
ISEPolicySettiame	Default
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

esult	
Called-Station-ID CiscoWPair	192 158 8 100 mdo Rundenia platformalis, mdo Rundenia platformalis, platformalisti Stationo resultati Visiona 4 10 0006, mdo Rundenia platformalisti Stationo resultati stationa formatione maintenamente stationa formatione stationa formatione st
CPMSessionID	dba800040000d000014bc1d0
Device IP Address	192.168.0.100
EnableFlag	Enabled

Étape 2. Connectez-vous à votre tête de réseau FTD (un ordinateur Windows est utilisé ici) et entrez les informations d'identification user2.

S Cisco AnyConnect 192.168.0.100 ×	🚳 Cisco AnvConnect Secure Mobility Client — 🗆	×
Group: RA_VPN ~ Username: user2 Password: ******	VPN: Contacting 192.168.0.100. 192.168.0.100	
OK Cancel	\$ ()	allalla cisco

La section **Address Information** indique que l'adresse IP attribuée est effectivement la première adresse IP disponible dans le pool local IPv4 configuré via FMC.

Sisco AnyConnect Secure Mobil	ity Client	÷.		×
cisco AnyCon	nect Secure Mobility Client			()
Virtual Private Network (VF	PN)	Diagnostics	s	
Preferences Statistics Route Detail	ls 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	Expor	rt Stats	

La sortie de la commande debug radius all sur FTD affiche :

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 Les journaux FTD affichent :

<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

Les journaux RADIUS Live sur ISE montrent :

Event	5200 Authentication succeeded
Jsemane	use/2
Endpoint Id	00.50.56.96.46.6F B
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess
thentication Details	
iource Timestamp	2021-09-23 00:00:06:488
leceived Timestamp	2021-09-23 00:00:06:488
folicy Server	driverap-ISE-2-7
went	5200 Authentication succeeded
Isemame	user2
iser Type	User
and an a loss that	00.50.56.96.46.6F
conditional re-	
Calling Station Id	192.168.0.101
Calling Station Id	192.168.0.101 Windows10-Workstation
Calling Station Id	192, 168, 0, 101 Windows10-Workstation Internal Uses
Emploint in Calling Station Id Endpoint Profile Authentication Identity Store dentity Group	192,168.0.101 Windows15-Workstation Internal Oters Workstation
creptions to Calling Station Id Indpoint Proble Webentication Identity Store dentity Group Audit Session Id	192 188 8 101 Wendows 10-Portestation Internal Dees Workstation divelacióococcoccoccocco
Interpretent to Calling Station Id Indepoint Profile Webertication Identity Store dentity Group kudit Session Id Kuthentication Method	152 168 8 191 Windows/O-Workston Internal Uwe Workston diae00040000001614x:087 Pag_a520
Calling Station Id Calding Station Id Endpoint Profile Authentication Identity Store dentity Group Audit Session Id Authentication Method Authentication Protocol	192 168 8 191 Windows10-Winkstein Internal Uwes Worksteinn ulwi0004000000014exb07 PAP_ADCI PAP_ADCI
Calling States Id Codposed Profile Kuthentication Identity Store detelly Group Kuthentication Method Kuthentication Method Kuthentication Protocol Intervork Device	192 198 0 191 Witchen 194 Rythation Internat Uses Workstein Iske000400000001 Houb97 RAP_ASICS RAP_ASICS RAP_ASICS
Lange Basine V Lating Basine Ma Indiposit Profile Authentication Identity Store dentity Oroup Latit Session M Latitettication Method Authentication Protocol leterorik Device Profice Type	192 198 0 191 Wickewith Makatalan Internal Uses Wakatalan debalook40000.0000 (kuckt) NPL_ASCI NPL_ASCI DMVEMA_FTD_7 2 Al Device Types
Carling Station Md Carling Station Md Endpood Profile Authentication Identity Store Identity Group Audit Session Id Kuthentication Method Authentication Protocol Vetwork, Device Jevice Type Location	192 168 J 191 Wickows M Albunation Internal Uses Worksakon Maladose Addose M Albunation PAP_AGO: PAP_AGO: DRV:EMA_JTD_7 0 All Devices Al Londow

Steps			
11001	Received RADIUS Access-Request		
11017	RADI/S greated a new session		
15049	Evaluating Policy Group		
15008	Evaluating Service Selection Policy		
15041	Evaluating Identity Policy		
15048	Queried PIP - Normalised Radius.RadiusFlowType (4 times		
22072	Selected identity source sequence - All_User_ID_Stores		
15013	Selected Identity Source - Internal Users		
24210	Looking up User in Internal Users IDStore - user2		
24212	Found User in Internal Users IDStore		
22037	Authentication Passed		
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory		
15035	Evaluating Authorization Policy		
24209	Looking up Endpoint in Internal Endpoints IDStore - user2		
24211	Found Endpoint in Internal Endpoints IDStore		
15048	Queried PIP - Radius User-Name		
15048	Queried PIP - Radius.NAS-Port-Type		
15048	Queried PIP - EndPoints LogicalProfile		
15048	Queried PIP - Network Access AuthenticationStatus		
15016	Selected Authorization Profile - PermitAccess		
22081	Max sessions policy passed		
22080	New accounting session created in Session cache		

NAS Port Time	Vist-al
Authorization Profile	Parmitteness
Resources Time	No alliana
response rane	and the dependence
Other Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PIX7x-Tunnel- Group Name	RA_VPN
OriginalUserName	use2
NetworkDeviceProfileId	b0099505-3150-4215-a00e-6753d45b/56o
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PDC7x-Client-Type	2
AcsSessionID	driverap-158-2-7/417494978/24
SelectedAuthenticationIdentityStore	es Internal Users
SelectedAuthenticationIdentityStore	es All_AD_Join_Points
SelectedAuthenticationIdentityStore	es Quest Users
Authentication Status	AuthenticationPassed
identityPolicyMatchedRule	Default
Authorization Policy Matched Rule	Basic_Authenticated_Access
15EPolicySetName	Default
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

LicenseTypes	Base license consumed	
cisco-av-pair	profile-name+Windows10-Workstation	
Class	CACS:d0a800540000.d000814bc387.driverap-ISE-2-7/417494578/24	
esult		
	uk-30544370718078278196712421844218446858627178370388603 84465880344, auditession-4m05a800440000061464367, ip-pump-4m152.68.0.101, opa-pumh-fbue	
CiscoWPair	mich 40-46-los platformain. mich 30-46-los (march 20:000, 20:00-40:00, 20:00-40:00, 2	
Called-Station-ID	192.168.0.100	
CPMSessionID	c0a800640000.d000614bc367	
Device IP Address	192.168.0.100	
RADIUS Username	ute/2	
EnableFlag	Enabled	
Name	Endpoint Identity Groups Profiled Workstation	
IP SEC		

Note: Vous devez utiliser différentes plages d'adresses IP pour l'attribution d'adresses IP à la fois sur le pool local IP FTD et les stratégies d'autorisation ISE afin d'éviter les conflits d'adresses IP en double parmi vos clients AnyConnect. Dans cet exemple de configuration, FTD a été configuré avec un pool local IPv4 de 10.0.50.1 à 10.0.50.100 et le serveur ISE attribue l'adresse IP statique 10.0.50.101.

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Sur FTD :

• debug radius all

Sur ISE :

• Journaux en direct RADIUS