Configurazione dell'assegnazione dell'indirizzo IP statico agli utenti AnyConnect tramite l'autorizzazione RADIUS

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Configurazione della VPN ad accesso remoto con autenticazione AAA/RADIUS tramite FMC Configura criterio di autorizzazione su ISE (server RADIUS) Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare l'autorizzazione RADIUS con un server Identity Services Engine (ISE) in modo che inoltri sempre lo stesso indirizzo IP a Firepower Threat Defense (FTD) per un utente Cisco AnyConnect Secure Mobility Client tramite l'indirizzo IP-Frame dell'attributo RADIUS 8.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect Secure Mobility Client
- protocollo RADIUS

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

• Windows 10 Pro

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazione della VPN ad accesso remoto con autenticazione AAA/RADIUS tramite FMC

Per una procedura dettagliata, fare riferimento a questo documento e a questo video:

- <u>Configurazione VPN ad accesso remoto AnyConnect su FTD</u>
- Configurazione iniziale di AnyConnect per FTD gestito da FMC

La configurazione VPN ad accesso remoto nella CLI del FTD è:

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

Configura criterio di autorizzazione su ISE (server RADIUS)

Passaggio 1. Accedere al server ISE e selezionare Amministrazione > Risorse di rete > Dispositivi di rete.

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			øσx	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 street of the street o		٥	DNS Resolutio	on Failure 9	41 less than	1 min ago			CPU		manitory colligio	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			****************					

Passaggio 2. Nella sezione Dispositivi di rete, fare clic su **Add** per elaborare le richieste di accesso RADIUS dall'FTD.

dentity Services Engine	Home + Context Visibility	 Operations 	Policy Administration	Work Centers			License Warning 🔺 🔍	
System Identity Management	Network Resources Device	ce Portal Manager	ment pxGrid Services + Feed	Service + Threat Centric NAC				
Network Devices Network Device G	roups Network Device Profiles	s External RAD	UUS Servers RADIUS Server Se	quences NAC Managers Extern	al MDM + Location Services			
•								
Network Devices	Network Devices							
Default Device							Selected 0 Tot	un 😌 🎡 🖕
Device Security Settings	/ Edit 4Add ChOupleate	@import @	Export • OGenerate PAC X	ielete +			Show Al	- 8
	Name 🔺	IP/Mask	Profile Name	Location	Туре	Description		
	DRIVERAP_ASA5506	172.16.255.2	🟥 Cisco 🙂	All Locations	All Device Types			

Immettere i campi **Nome** dispositivo di rete e **Indirizzo IP**, quindi selezionare la casella **Impostazioni autenticazione RADIUS**. Il **segreto condiviso** deve essere lo stesso valore utilizzato al momento della creazione dell'oggetto server RADIUS in FMC.

dentity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🔍	0 0	• ^
System Identity Management	Hotwork Resources Device Portal Management psGrid 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			
0				
Network Devices	Network Devices Lists New Network Device			
Default Device	* News ORDERS TO TO			
Device Security Settings	Particles Control - Contro			
	[₽ Address • * * P: 192.168.0.100 / 32	ŵ•		
	* Device Profile 🗰 Ciscol 👻 🕀			
	Model Name v			
	Software Version 📃 👻			
	* Network Device Group			
	Location Al Locations O Set. To Default			
	IPSEC Is IPSEC Device 📀 Set. To Default			
	Device Type 🛛 Al Device Types 🕐 🔰 Set. To Default			
	PADIUS Authentication Settings			
	RADIUS UDP Settings			- 1
	Protocol RADRUS			
	Shared Secret Show			
	Use Second Shared Secret 🗌 🕢			
	Show			
	CoA Port 1700 Set.To.Default			
	RADIUS DTLS Settings (2)			
	DILS Required a			~

Salvarlo con il pulsante alla fine della pagina.

Passaggio 3. Passare a Amministrazione > Gestione delle identità > Identità.

dealer Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Center	15		License Warring 🔺 🔍 😐 🔿 🗘
System Identity Management	Network Resources Device Portal Management pxGrid	System	Network Resources	pxGrid Services	
Network Devices Network Device C	2roups Network Device Profiles External RADIUS Servers	Deployment Licensing	Network Devices Network Device Groups	Feed Service	
0	No. of Barlow	Certificates	Network Device Profiles	Threat Centric NAC	
Network Devices	Network Devices	Maintenance	RADIUS Server Sequences	Third Party Vendors	Salarrad 0 Yotal 2 🚯 🔅 _
Default Device	/Edt -Add RyDupicate @Emport @Export - O	Upgrade Backup & Restore	NAC Managers External MDM		Show Al
Device Security Settings	Name	Admin Access	Location Services		
	□ DRMERAP_A 172.16.255.2 🗰 Cisco ⊕	Settings	Device Portal Management		
	□ DRIVERAP_F 192.168.0.10 🗰 Cisco ⊕	Identities	BYOD		
		Groups External Identity Sources	Certificate Provisioning Client Provisioning		
		Identity Source Sequences	Mobile Device Management		
		ominys	Custom Portal Files		
			Settings		
https://10.31.124.31:6012/admin/#a	dministration/administration_identitymanagement/ad	ministration_identitymanagemer	nt_identities		

Passaggio 4. Nella sezione Network Access Users, fare clic su **Add** per creare *user1* nel database locale di ISE.



Immettere nome utente e password nei campi **Nome** e **Password di accesso** e quindi fare clic su **Invia**.

dentity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺		
System Identity Management	Network Resources Device Portal Management pxGrid Service Freed Service Threat Centric NAC			
·Identities Groups External Iden	thy Sources Identity Source Sequences ▶ Settings			
0				
Users	Notoxi Access User List > New Tetwork Access User			
Latest Manual Network Scan Res	*Name Lusert Status 🖉 Enabled -			
	Emai			
	▼ Passwords			
	Pašsword Type: Internal Users 💌			
	Password Re-Enter Password			
	*Login Password			
	Enable Password Generate Password ()			
	• vser mormation			
	First Name			
	LastName			
	Description //			
	Change password on net login			
	* Account Disable Policy			
	Disable account if date exceeds 2021-11-21 (Vyyy-mm-dd)			
	▼ User Groups			
	Select an tem 🕜 — +			
	Setore Cancel			
<				>

Passaggio 5. Ripetere i passaggi precedenti per creare user2.



Passaggio 6. Andare a Policy > Policy Sets (Policy > Set di policy).



Passaggio 7. Fare clic sulla freccia > sul lato destro della schermata.

-dealer Id	entity Service	es Engine Home + Con	text Visibility + Operations	Policy Administration	Work Centers							icense Wa	iming 🔺	۹ و		
Policy S	ts Profiling	g Posture Client Provisioning	Policy Elements													
Policy	Sets										Reset Pol	cyset Hi	tcounts	Rese		Save
٠	Status	Policy Set Name	Description	Conditions					Allowed Proto	ols / Serve	r Sequence	н	ts	Actions	V	liew
Search																
						+										
	\odot	Default	Default policy set						Default Netwo	k Access	** +	1	7	¢		>
																_
																Save

Passaggio 8. Fare clic sulla freccia > accanto a **Criteri di autorizzazione** per espanderlo. A questo punto, fare clic sul simbolo + per aggiungere una nuova regola.

dentity	y Services	Engine Home Conte	xt Visibilit	y → Operations	* Policy	+ Administration	Work Centers								License	Warning 🔺	۹ ۵	•	o
Policy Sets	Profiling	Posture Client Provisioning	 Policy E 	Elements															
Policy Sets	s → Defa	ault												R	eset Policyset	t Hitcounts	Reset	t Sav	re
St	tatus	Policy Set Name	Descrip	notion	Cond	tions									Allowed Proto	cols / Serve	r Sequence	Hits	
Search																			
	0	Default	Default	policy set											Default Netwo	rk Access	×* +	17	
> Authentic	ation Poli	cy (3)																	
> Authoriza	ation Polic	y - Local Exceptions																	
> Authoriza	ation Policy	y - Global Exceptions																	
✓ Authoriza	ation Polic	<u>v (13)</u>																	
											R	Results							
•	Status	Rule Name	Cond	itions							P	rofiles		Security Group	6		Hits	Actions	
Search																			
	0	Wireless Black List Default	AND	Wireless_A	ccess p-Name EQ	UALS Endpoint Identit	ty Groups:Blacklist					×Blackhole_Wireless_Access	•	Select from list		• +	0	¢	
	0	Profiled Cisco IP Phones	48	IdentityGroup-Name	EQUALS En	dpoint Identity Groups	Profiled Cisco-IP-Pt	hone				× Cisco_IP_Phones	+	Select from list		• +	0	٥	1
	ø	Profiled Non Cisco IP Phones		Non_Cisco_Profiled,	Phones							×Non_Cisco_IP_Phones	+	Select from list		• +	0	٥	
	0	Unknown_Compliance_Redirect	AND	Network_Ac Compliance	cess_Auther	ntication_Passed Devices						× Cisco_Temporal_Onboard	+	Select from list		• •	0	¢	
	0	NonCompliant_Devices_Redirect	AND	Network_Ac	cess_Authen	ntication_Passed						× Cisco_Temporal_Onboard	+	Select from list		• +	0	¢	

Fornite un nome alla regola e selezionate il simbolo + nella colonna Condizioni (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

Fare clic nella casella di testo Editor attributi e fare clic sull'icona **Oggetto**. Scorrere verso il basso fino a individuare l'attributo *Nome utente RADIUS* e selezionarlo.

.ibrar	у		Editor														
Sea	rch by Name		0	Clic	k to ad	ld an attribu	ite										
Q		. 🛛 b 후	ъ	Select	attribu	te for condi	tion										1
	BYOD_is_Registered			0	Ēġ	•	۲	₽	Ĩ	F	♥			C	10	ີ່ເ	((:-
	Catalyst_Switch_Local_Web_Authentica tion	()			Dic	tionary				Attribut	te				D	Info	
P	Compliance Unknown Devices	(i)			A	I Dictionaries			~	Attribut	e				ID		^
	Compliant Devices	0		1	Mic	rosoft orola-Svmbo				MS-HC/	AP-Use -User-0	r-Name Sroup	•	6	2	() ()	
	Compliant_Devices	•		1	Net	work Access				AD-Use	r-DNS-	Domai	n			0	
	EAP-MSCHAPV2	0		1	Net	work Access				AD-Use	r-Join-F	Point				()	
2	EAP-TLS	()		1	Net	work Access				UserNa	ime					1	
2	Guest_Flow	(i)		1	Pas	siveID	_		_	Passive	ID_Us	ername				<i>i</i>	-
	MAC_in_SAN			1	Rad	tius tius				User-Na	ame asswor	d		1		() ()	٩
	Network_Access_Authentication_Passe d	()		1	Ruc	:kus				Ruckus	-User-(Groups		1	1	0	~
2	Non_Cisco_Profiled_Phones																
	Non_Compliant_Devices	0															
	Switch_Local_Web_Authentication	()															
0	Switch Web Authentication	(i)															

Mantieni **uguale** come operatore e immettere *user1* nella casella di testo accanto ad esso. Per salvare l'attributo, fare clic su **Use** (Usa).

brary		Editor					
Search by Name			Radius-User-Na	ame			
	9 1 O t 🤋	1	Equals	✓ user1			
BYOD_is_Registered	()		Set to 'Is not'			Duplicate	Save
Catalyst_Switch_Local_Web_Auther	ntica 🕡						
Compliance_Unknown_Devices	0			+ New AND	OR		
Compliant_Devices	0						
EAP-MSCHAPv2	0						
EAP-TLS	0						
Guest_Flow	0						
MAC_in_SAN	0						
Network_Access_Authentication_Pa d	sse 🕡						
Non_Cisco_Profiled_Phones	0						
Non_Compliant_Devices	()						
Switch_Local_Web_Authentication	()						
Switch Web Authentication							

La condizione per questa regola è ora impostata.

Passaggio 9. Nella colonna **Risultati/Profili**, fare clic sul simbolo + e scegliere **Crea nuovo profilo di autorizzazione**.

✓ Authori	zation Policy	y (13)					
				Results			
٠	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
1	0	Static IP Address User 1	Radius User-Name EQUALS user1	Select from list	Select from list • +		¢
				Create a New Authorization Profile			

Assegnare un **nome** al file e mantenere *ACCESS_ACCEPT* come **Tipo di accesso**. Scorrere fino alla sezione **Impostazioni avanzate attributi**.

Add New Standard Profile		3
Authorization Profile		^
* Name	StaticIPaddressUser1	
Description		
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	2010 CSCO + (1)	
Service Template		
Track Movement		
Passive Identity Tracking		
▼ Common Tasks		^
DACL Name		
IPv6 DACL Name		
ACL (Filter-ID)		12
ACL IPv6 (Filter-ID)		~
 Advanced Attributes 	Settings	~
		ve Cancel

Fate clic sulla freccia arancione e scegliete Raggio (Radius) > Indirizzo-IP-Frame-[8].

Add New Standard Profile Service Template				1	×
Track Movement 🔲 🕧					
Passive Identity Tracking					
	Radius				
 Common Tasks 	↓ ↓ ■ ↓ ○ ↓				1
DACL Name	Exercise MAND-1551				
_	Error-Cause[10]				
IPu6 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 	Framed-IPv6-Pool[100]				
Radius:Framed-IP-Address					
				_	
✓ Attributes Details					
Access Type = ACCESS_ACCEPT					
Framed-IP-Address =			11.		
			1114	~	1
¢				>	1
			Save	Cano	cel

Digitare l'indirizzo IP che si desidera assegnare in modo statico sempre a questo utente e fare clic su **Salva**.

Add New Standard Profile		×
Service Template		^
▼ Common Tasks		
Arespace IPv6 ACL Name	^	
ASA VPN		
AVC Profie 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

Passaggio 10. Scegliere il profilo di autorizzazione appena creato.

 Autho 	rization Policy	y (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
				Wireless_Access	DenyAccess	^			
	ø	Wireless Black List Default	AND	IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	NSP_Onboard		Select from list	0	¢
	0	Profiled Cisco IP Phones	-	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco-IP-Phone	Non_Cisco_IP_Phones	II.	Select from list +	0	0
	-				StatePaddressliter1	1			
	0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_Phones	Static_IP_address		Select from list	0	¢

La regola di autorizzazione è ora impostata. Fare clic su Salva.

dada ide	ntity Service	es Engine Home	Context Visibility	Operations -P	olicy Administration	Work Centers				License V	Varning 🔺	<u> २</u>	• •
Policy Se	ts Profiling	Posture Client Prov	isioning + Policy Element	ts									
Policy S	Sets → De	fault								Reset Policyset H	Hitcounts	Reset	Save
	Status	Policy Set Name	Description		Conditions					Allowed Protoco	ols / Server	Sequence	Hits
Search													
	0	Default	Default policy se	et						Default Network	Access	x * +	17
> Authe	entication Po	licy (3)											
> Autho	orization Poli	cy - Local Exceptions											
> Autho	prization Poli	cy - Global Exceptions											
✓ Author	orization Poli	cy (13)											
								Results					
٠	Status	Rule Name	Conditions					Profiles	Security	Groups		Hits	Actions
Search													
1	0	Static IP Address Use	r1 🔒 Radu	is-User-Name EQUA	ULS user1			*StaticlPaddressUser1	+ Select fro	om list •	+		٥

Verifica

Passaggio 1. Passare al computer client in cui è installato il client Cisco AnyConnect Secure Mobility. Connettersi all'headend FTD (qui viene utilizzato un computer Windows) e immettere le credenziali *utente1*.



Fare clic sull'icona dell'ingranaggio (nell'angolo in basso a sinistra) e selezionare la scheda **Statistiche**. Confermare nella sezione **Informazioni indirizzo** che l'indirizzo IP assegnato è effettivamente quello configurato nel criterio di autorizzazione ISE per questo utente.

🕙 Cisco AnyC	onnect Secure Mobility Client	-		(
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:23		_	IPv4	
۞			aliali cisco	÷

Cisco AnyConnect Secure Mob	ility Client	_		
AnyCon	nect Secure Mobility Client			(
rtual Private Network (V	PN) Diag	gnostics		
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			- •	
-)				×

L'output del comando debug radius all sull'FTD visualizza:

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 I log FTD mostrano: 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

I log di RADIUS Live su ISE mostrano:

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 23:63:19.72 Source Timestamp Received Tim 2021-09-22 23 53 19.72 Policy Server driverap-ISE-2-7 Event 5200 Authenticati user1 User 00 50 50 90 40 OF Calling Station Id 192.108.0.101 Windows10-Worksta Endpoint Profile nity Store Internal Users Authentication Ide Workstation ntity Group Audit Session Id 004000040000 PAP_ASCI Authentication Method Authentication Protocol PAP_ASCII Network Device DRIVERAP_FTD_7.0 Device Type All Device Types Location All Locations NAS IPv4 Address 0.0.0.0

Steps

- Stopp
 Stopp

 11011
 Resided RADUS Access Respect

 11011
 Resided RADUS Access Respect

 10010
 Evaluating Revise StateMonth

 10010
 Evaluating Servise StateMonth

 10011
 Evaluating Servise StateMonth

 10012
 Evaluating Servise StateMonth

 10013
 Evaluating Servise StateMonth

 10014
 Durates Revise StateMonth

 10015
 Evaluating StateMonth

 10016
 Evaluating StateMonth

 10016
 Evaluating StateMonth

 10016
 Evaluating StateMonth

 10017
 Evaluating StateMonth

 10018
 Evaluation PlaceMonth

 10018
 Evaluating Plac

- 24715 ISE has not confirmed locally previous su authentication for user in Active Directory
- 2415 auchentication for use in Advis Denotiny 1908: Evaluating Authentication Philop 2009: Looing as Endpaint in Internal Endpaint DStare 2421: Found Endpaint in Internal Endpaints DStare 2420: Found Endpaint in Internal Endpaints DStare 2420: Found Endpaint in Internal Endpaints DStare 2420: Statuset Authorization Philis StatistPedevacub 2020: Statuset Authorization Philis StatistPedevacub 2020: New accurring seals on testing in Sealson cache 11002: Returned RADUS Access-Accept

Toentry Services Engine	
NAS Port Type	Vitual
Authorization Profile	Static/PaddressUser1
Response Time	51 milliseconds
Other Attributes	
ConfigWersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PUCTx-Tunnel- Group Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0699505-3150-4215-a80a-6753645b456
In Third Parts Descine Eloss	false
CURRING AND AN RUTE Class To	
Ans Resained?)	A A A A A A A A A A A A A A A A A A A
	anneapharacter in aperatural
SelectedAuthenticationIdentity S	tores Internal Users
SelectedAuthenticationIdentity 5	tores AILAD_Join_Points
SelectedAuthenticationIdentityS	tores Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Statio IP Address User 1
15EPolicySetName	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

and an IR Address of	usert
Device IP Address	192.108.0.100
CPMSessionID	dba800640000db00614bc1d0
Called-Station-ID	192.168.0.100
CiscoW/Pair	mdo-bi-decise platformain, mdo-bi-decise platformain, mdo-bi-decise mac-00-50,505,604-60, mdo-bi-decise public mac-00-50,505,604-60, mdo-bi-decise platforman, the 20 Vibeau Vibeau Vibeau Vibeau platformain Vibeau Vibeau Vibeau Vibeau Vibeau Vibeau Vibeau glatasi histopistopistopistopistopistopistopistop
rsult	10 ÷ 50 101
s ult Framed 4P-Address Class	10.0.00.101 CACS.dba000460005114b;c140.dh;vesp;182.2.7;417464975223
Framed IP-Address Class cisco av pair	10 8 50 101 CAC5 uba0004400004000148x440 uhwaya-100-2/1417494978/23 prifika-akwa101000us10 f000408501

Passaggio 2. Connettersi all'headend FTD (qui viene utilizzato un computer Windows) e immettere le credenziali utente2.

S Cisco AnyConnect 192.168.0.100 X	N Cisco AnyConnect Secure Mobility Client —	×
Group: RA_VPN ✓ Username: user2 Password: ******	VPN: Contacting 192, 168, 0, 100. 192, 168, 0, 100 Connect	
OK Cancel	\$ ()	diala cisco

La sezione **Address Information** mostra che l'indirizzo IP assegnato è effettivamente il primo indirizzo IP disponibile nel pool locale IPv4 configurato tramite FMC.

Sisco AnyConnect Secure Mobil	ity Client	_		×
cisco AnyCon	nect Secure Mobility Client			()
Virtual Private Network (VF	PN)	Diagnostic	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	Ехро	rt Stats	•

L'output del comando debug radius all sull'FTD visualizza:

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 I log FTD mostrano:

<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

I log di RADIUS Live su ISE mostrano:

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
rthentication Details	
Source Timestamp	2021-09-23 00:00:08.488
Received Timestamp	2021-09-23 00:00:06:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Usemame	user2
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	c0a800540000d000814bc387
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCI
Network Device	DRIVERAP_FTD_7.0
	All Device Types
Device type	
Location	All Locations

Steps: 111 Attable standard and standard sta

æ.,	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/PDC7x-3unnel- Group Name	RA_VPN
	OriginalUserName	use2
	NetworkDeviceProfileId	b0099505-3150-4215-a80e-6753d45b/55c
	IsThirdPartyDeviceFlow	false
	CVPN3000/ASA/PD/7x-Client-Type	2
	AcsSessionID	driverap-15E-2-7/417484978/24
	SelectedAuthenticationIdentityStore	Internal Users
	SelectedAuthenticationIdentityStore	AILAD_Join_Points
	SelectedAuthenticationIdentityStores	o Quest Users
	Authentication Status	AuthenticationPassed
	identityPolicyMatchedRule	Default
	AuthorizationPolicyMatchedRule	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
	Device Type	Device Type#All Device Types

cisco-av-pair	profile-name=Windows10-Workstation
esult.	CACS: cbs8005400004000614bc367; driversp-15E-2-7/41749497E/24
CiscoW/Pair	India-di-dialogi adjatementa, India-di-dialogi adjatementa, India-di-dialogi adjatementa (36,000,46,41,000,000, India-di-dialogi adjatementa (36,000,46,41,000,000, India-di-dialogi adjatementa, Ins. YMAeek Y (14,000,000, India-di-dialogi adjatementa), India-di-dialogi adjatementa (14,000,000,000,000,000,000,000,000,000,0
CPMSessionID Called-Station-ID	cba800640000d000014bc387 192.198.0.100
Device IP Address	192.108.0.100
RADIUS Username	user2
EnableFlag	Enabled
Name	Endpoint Identity Groups Profiled Workstation

Nota: Per evitare conflitti di indirizzi IP duplicati tra i tuoi client AnyConnect, è necessario utilizzare intervalli di indirizzi IP diversi per l'assegnazione degli indirizzi IP sia sul pool locale IP FTD che sui criteri di autorizzazione ISE. Nell'esempio di configurazione, il protocollo FTD è stato configurato con un pool locale IPv4 compreso tra 10.0.50.1 e 10.0.50.100, quindi il server ISE assegna un indirizzo IP statico pari a 10.0.50.101.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Su FTD:

debug radius all

ISE:

Registri attivi RADIUS