Configuración de la Asignación de Dirección IP Estática a los Usuarios de AnyConnect mediante la Autorización RADIUS

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuración de VPN de acceso remoto con autenticación AAA/RADIUS a través de FMC Configuración de la política de autorización en ISE (servidor RADIUS) Verificación Troubleshoot

Introducción

Este documento describe cómo configurar la autorización RADIUS con un servidor de Identity Services Engine (ISE) para que siempre reenvíe la misma dirección IP a Firepower Threat Defense (FTD) para un usuario específico de Cisco AnyConnect Secure Mobility Client a través del atributo RADIUS 8 Framed-IP-Address.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMCv 7.0.0 (compilación 94)
- FTDv 7.0.0 (Compilación 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuración de VPN de acceso remoto con autenticación AAA/RADIUS a través de FMC

Para ver un procedimiento paso a paso, consulte este documento y este vídeo:

- Configuración de VPN de acceso remoto AnyConnect en FTD
- <u>Configuración de AnyConnect inicial para FTD gestionada por FMC</u>

La configuración VPN de acceso remoto en la CLI de FTD es:

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 Configuración de la política de autorización en ISE (servidor RADIUS)

Dago 1. Inicia agoión on al convider ISE y noveque basto Administration > Network Descure

Paso 1. Inicie sesión en el servidor ISE y navegue hasta Administration > Network Resources > Network Devices.

Home Home	Context Visibility	 Operations 	Policy	- Administration	Work Cente	rs				License Warnin	g 🔺 🔍 👘	
Summary Endpoints Gr	uests Vulnerability	Threat	+	System		Network Resources	pxGrid Services					٥
METRICS Total Endpoints @	1	Active Endpoir	nts 0	Licensing Certificates Löpging Maintenance Upprade Baciup & Rest Admin Access Settings Identity Manage Identity Gauss	ore	Network Device Groups Network Device Frolies External RAUIUS Servers RADIUS Server Sequences NAC Managers External MOM Location Services Device Portal Management Bioolists BYOD Certificate Provisionion	Feed Service Profiler Threat Centric NAC Third Party Vendors	-	Authenticated Guests 0	BYOD Endpoints @	0	ο
AUTHENTICATIONS dentity Group Network Devi	ce Failure Reason		ខ្ល	External Identit Identity Source Settings	y Sources Sequences	Client Provisioning Mobile Device Management My Devices Custom Portal Files Settings		×	ENDPOINTS O			a o x
interusers: [100%]	C			c	rivea5506: [1				workstations: [100%]	0		
BYOD ENDPOINTS 0			00	X II AL	ARMS 0		60	×	SYSTEM SUMMARY			e o x
Type Profile				Severity	Name	Occu Last Oc	curred	^	1 node(s)		/	II = 24HR =
Ne	o data available.				Name DNS Resolution	ion Ealizea 041 lass than	1 min ano		driverap-ISE-2-7 CPU	Memory Usage	Authenticatio	n Latency
://10.31.124.31:6012/admin/#admini	stration/administratio	n_networkresour	rces/admin	istration_network	resources_devie	ces have 4000 loss that	1 min and					

Paso 2. En la sección Network Devices (Dispositivos de red), haga clic en **Add** para que ISE pueda procesar las solicitudes de acceso RADIUS desde el FTD.

dealer Identity Services Engine	Home + Context Visibility	Operations	Policy Administration	Work Centers			License Warning 🔺 🔍	
System Identity Management	Network Resources Devic	ce Portal Management	pxGrid Services + Feed S	ervice + Threat Centric NAC				
Network Devices Network Device G	roups Network Device Profile:	s External RADIUS S	ervers RADIUS Server Sequ	ences NAC Managers Externa	al MDM Location Services			
•								
Network Devices	Network Devices							
Default Device			1				Selected 0	Total 1 😵 🎬 🖕
Device Security Settings	Edt 4-Add Dupicate	Dimport Deport	t • OGenerate PAC XDek	ite *			Show AI	* 6
	Name ·	IP/Mask Pro	ofile Name	Location	Type	Description		
	U DRIVEROP_ASA5506	1/2.10.255.2	CSC0 1	All Locations	Al Device Types			

Ingrese los campos **Nombre** y **Dirección IP** del dispositivo de red y luego marque la casilla **Configuración de autenticación de RADIUS**. El **secreto compartido** debe ser el mismo valor que se utilizó cuando se creó el objeto de servidor RADIUS en FMC.

<pre> i idead decade i idead decade</pre>	dentity Services Engine	Home + Context Visibility + Operations + Policy +Administration + Work Centers	License Warning 🔺 🔍	0 0	0
• Nucci Decision Nucci Decision Nucci Decision Nucci Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Decision • Dec	System Identity Management	Holtwork Resources Device Portal Management psGrid Service Freed Service Threat Centric NMC			
Petero Daces Petero Petero	Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Servers NAC Managers External NDM + Location Services			
Identified Image: Control Device Device Strandy Strangs Image: Control Device Image: Control Device Strandy Strangs Image: Control Device Strandy Strangs Image: Control Device Strandy Strangs Image: Control Device Strandy Strangs Image: Control Device Strandy Strangs Image: Control Device Strange Image: Control Device Strange Image: Con	0				
Detect beter ************************************	Network Devices	Network Devices List > New Hetwork Device			
Device Skourdy Settings	Default Device	Name DENERAL STD. 7.0.			
• Orece Prefer • P[122.168.0.00 / 122 • Orece Prefer • Orece Pref	Device Security Settings				
PAdeu • • • • • • • • • • • • • • • • • • •					
Cede Patie @ Catoo @ @ Model Patie Software Version Versence Provide Catoo Bettings RADUIS Authentication Settings RADUIS Authentication Settings Verse Second Shared Setting Verse Second Shared Setting Cat Part [2000 Set To Default. Cat Part [2000 Set To D		P Address + *P: 192.168.0.100 / 32	۵.		
* Decce Prefie @ Good @ @ Model Name					
Concer Produit Concer • Concer Produit Concer • Concert Produit Concert • Concert Produit Concert • Concert Produit Concert • Concert • Concert• Concert • Concert• Concert • Concert• C					
Model Name Software Version * Network Device Group Location PSEC BurSEC Device C Set. To Default PSEC Device Types S Set. To Default Device Types S Set. To Default S Device Types S Set. To Default S S Device Types S Set. To Default S S S S S S S S S S S S S S S S S S S		Device Profile det Cisco Device			
Model Name Software Version * Network Device Grose Leation Alcoatons PBEC BISEC Device C Set. To Default PBEC BISEC Device C Set. To Default Device Type All Device Types C Set. Ta Default Device Type All Device Types C Set. Ta Default Device Types C Set. Ta Default BADNUS UUP Settings RADNUS UUP Settings Use Second Shared Secret CaA Pert 1700 Set. To Default BADNUS DULS Settings ()					
Sthurst Version Sthurst Version Sthurst Version Sthurst Version St		Model Name 🔹			
Network Device Group Location Allocations ③ Set Te Default. PPGC []: SPSC Device ③ Set Te Default. Device Type: ④ Set Te Default. Device Type: ⑤ Set Te Device Te OPC Te O		Software Version 🔹			
Lecation Allocations © Set. To Default PSEC IN PSEC Device © Set. To Default Device Type I Device Type © Set. To Default Convorting I Device Types © Set. To Default RADUS UDP Settings Protocol RADUS BADUS UDP Settings Protocol RADUS Use Second Shared Secret © CaA Pert 1700 Set. To Default RADUS DTLS Settings ©		* Network Device Group			
Leadon Al Leadon O Set Ta Default. PREC IS PSEC Device O Set. Ta Default. Device Type Al Device Types O Set. Ta Default. Concernment of the set of the					
POSC B PSSC Device Set To Default. Divide Type F ADDUS Authentication Settings RADIUS Authentication Settings RADIUS UP Settings RADIUS Protocol RADIUS F Shared Secret CoA Pot T TO TO Sat To Default. RADIUS DILS Settings ()		Location Al Locations 📀 Set. To Default			
Device Type Al Device Types Set. Ta Default RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS Protocol RADIUS Duse Second Shared Secret CoA Port 1700 Set. Ta Default RADIUS DIL, S Settings ()		IPSEC Is IPSEC Device 📀 Set To Default			
RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS Shared Secret CoA Pot 1700 Set. To Default RADIUS DILS Settings ()		Device Type At Device Types O Set. To Default			
Protocol RADIUS RADIUS UDP Settings Protocol RADIUS Protocol RADIUS Protocol RADIUS Protocol RADIUS CoAPed 1700 Show CoAPed 1700 Sho					
Protocol RADRUS Protocol RADRUS Shared Secret CoA Pot Show CoA Pot Show RADRUS DILS Settings ()		RADIUS Authentication Settings			
RADUS UDP Settings Protocol RADUS Protocol RADUS Shared Secret Use Second Shared Secret CoA Pot 1200 Set. To Default RADUS DTLS Settings ()					
Protocol RADRUS Shared Secret Shared Use Second Shared Secret CoA Port 1700 Set. To Default. RADRUS DTLS Settings ()		RADUS UDP Settings			_
		Protocol RADIUS			_
Use Second Shared Secret 🗍 🛞 Show. CoA Port 1700 Set. To Default. RADUS DTLS Settings 👔		*Shared Secret show			_
CoA Port 1700 Set: To Default. RADUS DTLS Settings ()		Use Second Shared Secret 🔲 🕖			
CoA Port 1200 Set. To Default. RADUS DTLS Settings (j)		Show			
RADUS DTLS Settings (j)		CoA Port 1700 Set To Default			
		RADIUS DTLS Settings ()			
DTLS Required _ ()		DTLS Required 🗍 🕡			,

Guárdelo con el botón situado al final de esta página.

Paso 3. Vaya a Administración > Gestión de identidades > Identidades.

dealer Identity Services Engine	Home + Context Visibility + Operation	s → Policy •Administration → W	Vork Centers		License Warning 🔺 🤍 😐 🔿 🗢
System Identity Management	Network Resources Device Portal Manap	ement pxGrid E System	Network Resources	pxGrid Services	
Network Devices Network Device C	Groups Network Device Profiles External RA	ADIUS Servers Deployment	Network Devices	Feed Service	
0		Certificates	Network Device Profiles	Profiler	
Network Devices	Network Devices	Logging	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 Loupicate @Import @	Export • OG Backup & Restore Admin Access	External MDM Location Services		Show Al Y
	Name IP/Mask Pro	ofile Name Settings	Device Portal Management		
	DRIVERAP_A. 172.16.235.2	Cisco @ Identity Management	Blacklist	Blacklist	
		Identities	BYOD Certificate Provisioning		
		External Identity Source	es Client Provisioning		
		Identity Source Sequen Settings	ices Mobile Device Management My Devices		
		crange.	Custom Portal Files		
			Settings		
https://10.31.124.31:6012/admin/#a	dministration/administration_identityma	nagement/administration_identityma	nagement_identities		

Paso 4. En la sección Usuarios de acceso a la red, haga clic en **Agregar** para crear *user1* en la base de datos local de ISE.



Ingrese el nombre de usuario y la contraseña en los campos **Name** y **Login Password**, y luego haga clic en **Submit**.

- deset Monthly Services Engine Home + Context Visibility + Operators + Policy - Administration + Work Centers License Warming &		1
System -identity Management Network Resources Device Portal Management pricind Services Fineat Centric NAC		
- Sdentbles Circups External Identity Sources Identity Sources Identity Sources Identity Sources Identity Sources - Sdentbles		
•		
Uses NMMMR Access Uses Here Retwork Access User		
Lahst Manual Network Scan Res + Included ALACERS USer Name Loss1 Status C Enabled - Enabled -		
* Passwords		
Password Type: Internal Users +		
Password Re-Enter Password		
*Login Password		
Enable Password Generate Password ()		
* User Information		
FirstName		
LastName		
Description //		
Change password on next login		t,
▼ Account Disable Policy		L
Disable account if date exceeds 2021-11-21 (yyy-mm-dd)		L
* User Groups		
Select an Rem 📀 — 🕂		
[Submt] Gancel		,
C		>

Paso 5. Repita los pasos anteriores para crear user2.



Paso 6. Navegue hasta Política > Conjuntos de Políticas.



Paso 7. Haga clic en la flecha > a la derecha de la pantalla.

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

Paso 8. Haga clic en la flecha > junto a **Política de autorización** para expandirla. Ahora, haga clic en el símbolo + para agregar una nueva regla.

dentity Service	es Engine Home	of Visibility	Operations	Policy Administration	Work Centers					License Warning 🔺		0 0
Policy Sets Profilin	g Posture Client Provisioning	 Policy El 	lements									
Policy Sets → D Status	Policy Set Name	Descript	tion	Conditions					Reset	Policyset Hitcounts wed Protocols / Serve	Reset	Save
Search												
0	Default	Default p	olicy set						D	efault Network Access	×* +	17
> Authentication F	olicy (3)											
> Authorization Po	licy - Local Exceptions											
> Authorization Po	licy - Global Exceptions											
Authorization Po	licy_(13)											
							Results					
Status	Rule Name	Condit	lions				Profiles		Security Groups		Hits	Actions
Search												
Ø	Wreless Black List Default	AND	Wireless_Acc	ess			×Blackhole Wireless Access	+	Select from list	- +	0	ø
		7440	4 IdentityGroup	Name EQUALS EndpointIden	tty Groups:Blacklist							
0	Profiled Cisco IP Phones	48.	IdentityGroup-Name Ef	QUALS Endpoint Identity Group	s Profiled Cisco-IP-Phor	ne	Clsco_IP_Phones	+	Select from list	- +	0	٥
0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_P	Phones			[×Non_Cisco_IP_Phones]	+	Select from list	- +	0	٥
0			Network_Acce	ess_Authentication_Passed			(construction)		Palast from 1st			
0	Unknown_Compliance_Redired	AND	Compliance_	Unknown_Devices			- Cisco_remporal_Onboard	-	oeieu num list		0	¥
0			Network_Acce	ess_Authentication_Passed			(Relation int			~
0	NonComprant_Devices_Redirect	AND	Non_Complia	ant_Devices			(*Cisco_temporal_Onboard)	-	Detect month list	• •	0	¥ .

Proporcione un nombre a la regla y seleccione el símbolo + bajo la columna **Condiciones**.

✓ Author	ization Policy	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

Haga clic en el cuadro de texto Editor de atributos y haga clic en el icono **Asunto**. Desplácese hacia abajo hasta que encuentre el atributo *RADIUS User-Name* y elijalo.

ibrar	у		Editor													
Sear	rch by Name		0	Click to add an attribute												
♥ 🛱		. 🛛 t 😤	ß	Select	attribu	e for cond	tion				_					
	BYOD_is_Registered			0	Ē	•	۲	₽	Ĩ	P	♥	2	P	©	<mark>ا</mark> د	(•
	Catalyst_Switch_Local_Web_Authentica tion	1			Dic	tionary				Attribu	te			ID	Info	
	Compliance_Unknown_Devices	()			A	I Dictionaries			~	Attribut	e AP-Use	r-Name		60	Ø	^
	Compliant_Devices			1	Mot	orola-Symbo	1			Symbol	-User-O	Group		12	0	
	EAP-MSCHAPv2	0		1	Net	work Access				AD-Use	r-DNS-	Domair	n		<i>(i)</i>	
	EAP-TLS			1	Net	work Access work Access				AD-Use	r-Join-F	Point			() ()	
	Guest_Flow	0		1	Pas	siveID				Passive	ID_Us	ername			()	
8	MAC_in_SAN	0		1	Rad	lius				User-N	ame asswor	d		1	() ()	٩
	Network_Access_Authentication_Passe d	0		1	Ruc	kus				Ruckus	-User-(Groups		1	0	~
	Non_Cisco_Profiled_Phones														 	-
	Non_Compliant_Devices	٢														
	Switch_Local_Web_Authentication															
	Switch Web Authentication	()														

Mantenga **Equals** como el operador e introduzca *user1* en el cuadro de texto junto a él. Haga clic en **Usar** para guardar el atributo.

orary	Edito	or		
Search by Name		Radius·Us	ser-Name	
	9101₹	Equals	v user1	
BYOD_is_Registered	0	Set to 'Is not'	r	Duplicate S
Catalyst_Switch_Local_Web_Authen	itica 🕡			
Compliance_Unknown_Devices	0		H New AND	OR
Compliant_Devices	0			
EAP-MSCHAPv2	0			
EAP-TLS				
Guest_Flow				
MAC_in_SAN	0			
Network_Access_Authentication_Pa	sse 🕡			
Non_Cisco_Profiled_Phones	0			
Non_Compliant_Devices				
Switch_Local_Web_Authentication				
Switch Web Authentication				

La condición para esta regla está ahora establecida.

Paso 9. En la columna **Resultados/Perfiles**, haga clic en el símbolo + y elija **Crear un nuevo perfil** de autorización.

✓ Authorizat	tion Policy	(13)					
				Results			
٠ ۽	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
1	0	Static IP Address User 1	1 Radius User-Name EQUALS user1	Select from list	Select from list 🔹 🔸		٥
			Winter Ameri	Create a New Authorization Profile			

Asigne un **Nombre** y mantenga *ACCESS_ACCEPT* como el **Tipo de acceso**. Desplácese hacia abajo hasta la sección **Configuración avanzada de atributos**.

Add New Standard Profile		×
Authorization Profile		^
* Name	StaticIPaddressUser1	
Description		
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	2880 CECO + ①	
Service Template		
Track Movement		
Passive Identity Tracking		
 Common Tasks 		
DACL Name		î
IPv6 DACL Name		
ACL (Filter-ID)		
ACL IPv6 (Filter-ID		~
w Advanced Attributes	Pattinge	_
Advanced Attributes		\ <u>`</u>
	Sa	ve Cancel

Haga clic en la flecha naranja y elija Radius > Framed-IP-Address-[8].

Add New Standard Profile Service Template			×
Track Movement 🔲 🕧	D		
Passive Identity Tracking 🔲 🕧	D		
	Radius		
Tommon Tacke			
· common rusks	4 • ■ •	^	
DACL Name	E Ecress-VLAND-155		
	Error-Cause[101]		
IPv6 DACL Name	u FiterID-[11]		
	u 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)	~	
	E Framed-IP-Address(8)		
	Framed-IP-Netmask[9]		
	Framed IPv6-Address-[168]		
 Advanced Attributes Settin 	ng 🗉 Framed IPv6-Pool[100] 💙		
Radius:Framed-IP-Address			
▼ Attributes Details			
Access Type = ACCESS ACCEPT			
Framed-IP-Address =			
		l	\sim
<		>	
		Save	ancel

Escriba la dirección IP que desea asignar de forma estática siempre a este usuario y haga clic en **Guardar**.

Add New Standard Profile		×
Service Template		^
▼ Common Tasks		
Airespace IPv6 ACL Name	^	
ASA VPN		
AVC Profie Name		
UPN Lookup	×	
× Advanced Attributes Sattings		
Radus:Framed-IP-Address 10.0.50.101 +		
▼ Attributes Details		
Access Type = ACCESS_ACCEPT Framed-IP-Address = 10.0.50.101		
	Save Car	ncel

Paso 10. Ahora, elija el perfil de autorización recién creado.

 Autho 	rization Polic	y (13)							
					Results				
T	Status	Rule Name	Cond	itions	Profiles		Security Groups	Hits	Actions
Search									
1	0	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	+	Select from list • +		٥
				History Arran	Cisco_webAber	^			
	\odot	Wireless Black List Default	AND	da IdentifyGroup Name EQUALS Endocint Identify Groups Blacklist	NSP_Onboard		Select from list 🔹 🕇	0	\$
					Non_Cisco_IP_Phones				
	\odot	Profiled Cisco IP Phones	42.	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	Static/PaddressUser1		Select from list +	0	0
					Static_IP_address	~			

La regla de autorización está ahora establecida. Click Save.

dudu Iden	tity Service	s Engine Home	Context Visibility Operat	ions Policy Administration	Work Centers			License	Warning 🔺	९ 🛛 🛛	• •
Policy Sets	Profiling	Posture Client Provi	sioning + Policy Elements								
Policy Se	ets → De	fault						Reset Policyset	Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions				Allowed Protoc	ols / Server Se	equence	Hits
Search											
	0	Default	Default policy set					Default Network	k Access ×	+	17
> Authen	ntication Po	iicy (3)									
> Author	ization Poli	cy - Local Exceptions									
> Author	ization Poli	cy - Global Exceptions									
 Author 	ization Poli	cy (13)									
							Results				
•	Status	Rule Name	Conditions				Profiles	Security Groups	н	lits	Actions
Search											
1	0	Static IP Address User	1 L Radius-User-	Name EQUALS user1			×StaticlPaddressUser1	Select from list	- +		٥

Verificación

Paso 1. Desplácese hasta el equipo cliente en el que está instalado el cliente Cisco AnyConnect Secure Mobility. Conéctese a la cabecera FTD (aquí se utiliza una máquina con Windows) e introduzca las credenciales *user1*.



Haga clic en el icono del engranaje (esquina inferior izquierda) y desplácese a la pestaña **Estadísticas**. Confirme en la sección **Información de Dirección** que la dirección IP asignada es ciertamente la configurada en la política de autorización de ISE para este usuario.

🕙 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 Mobi	ility Client —		
AnyCon	nect Secure Mobility Client		(
rtual Private Network (V	PN) Diagnostics		
eferences Statistics Route Deta	ails Firewall Message History		
			^
Connection Information	3	•	
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		~	
			v

La salida del comando debug radius all en FTD muestra:

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 Los registros de FTD muestran: 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

Los registros en directo de RADIUS en ISE muestran:

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 Received Tim 2021-09-22 23:53:19.72 Policy Serve driverap-ISE-2-7 Event 5200 Authenticat user1 User 00 50 50 90 40 07 192.168.0.101 Calling Static Windows10-Works Internal Users Authentication I Workstation Rity Group Audit Session Id 04800840000 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

- 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 Philos 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 Philos Statict/Redexaulty 2020: Statuset Authorization Philos Statict/Redexaulty 2020: New accurring sealon zealate in Sealion cache 11002: Returned RADUS Access-Accept

NAS Port Type	Virtual
Authorization Profile	StatidPaddressUser1
Response Time	51 milliseconds
ther Attributes	
Config'versionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PD/7x-Tunnel-	RA_VPN
Originallisediame	used
Congonality services	
networkDeviceProtietd	50099505-3150-4215-8808-073334568566
Is ThirdPartyDeviceFlow	false
CVPN3000/ASA/PD/7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417494978/23
SelectedAuthenticationIdentityStore	a Internal Users
SelectedAuthenticationIdentityStore	s All_AD_Join_Points
SelectedAuthenticationIdentityStore	s Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Statio IP Address User 1
15EPolicySettame	Default
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations
Desides Tree	

user1 192,108.0.100 dba500540000.d000514bc140
192.168.0.100 cbx80054000c0000514bc1d0
dba800540000d000514bc1d0
192,168.0.100
mdn Dhordevice jalaformani, mdn Dhordevice jalaformani, mdn Dhordevice jalaformani, sano 200 65 64-04.00 mdn Dhordevice jalaformani, mdn Dhordevice, mdn Dhordevice,
10.0.60.101
CACS.dba800840000x800814bc1d8.driverap-ISE-2-7/417494978/23
profile-name=Windows10-Workstation
Base license consumed

Paso 2. Conéctese a la cabecera FTD (aquí se utiliza una máquina con Windows) e introduzca las credenciales del usuario2.

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	Ci altalta cisco

La sección **Información de dirección** muestra que la dirección IP asignada es, de hecho, la primera dirección IP disponible en el conjunto local IPv4 configurado a través de FMC.

🚳 Cisco AnyConnect Secure Mob	lity Client	<u> -</u>		×
cisco AnyCon	nect Secure Mobility Clien	it		()
Virtual Private Network (V	PN)	Diagnostic	s	
Preferences Statistics Route Deta	ils 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	ort Stats.	

La salida del comando debug radius all en FTD muestra:

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 Los registros de FTD muestran:

<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

Los registros en directo de RADIUS en ISE muestran:

Event	5200 Authentication succeeded
Usemame	use2
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 00:00:06:488
Received Timestamp	2021-09-23 00:00:06:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Usemane	use2
User Type	User
Endpoint Id	00.50.56.96.46.6F
	192 168 0 101
Calling Station Id	
Calling Station Id Endpoint Profile	Windows10-Workstation
Calling Station Id Endpoint Profile Authentication Identity Store	Windows10-Workstation Internal Oters
Calling Station Id Endpoint Profile Authentication Identity Store Identity Group	Windows10-Wolstation Internal Uses Workstation
Calling Station Id Endpoint Profile Authentication Identity Store Identity Group Audit Session Id	Windows 10-Wolstation Internet Uters Workstein stabil0044000000000 Heuden
Calling Station Id Endpoint Profile Authentication Identity Store Identity Group Audit Session Id Authentication Method	Windows 10-Woldstation Different Uses Workstation state006400000000014ext87 PAP_ACCI
Calling Station Id Endpoint Profile Authentication Identify Store Identity Croup Audit Session Id Authentication Method Authentication Protocol	Windows 5 Volketation Internal Uses Wolkstoon I Islando 5 Volketation I Islando 5 Volketatio I Islando 5 Volketation I Islando 5 Volketation I Islando

NAS IPv4 Address 0.0.0.0

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS 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
15036	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 LogicalPhofile
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 Type	Vitual
Authorization Profile	PermitAccess
Response Time	202 milliseconds
Other Attributes	
ConfigVersionId	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
OriginalUserflame	use/2
NetworkDeviceProfileId	b0099505-3150-4215-a80e-8753d45b/58o
IsThirdPartyDeviceFlow	faise
CVPN3000/ASA/PIX7x-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
15EPolicySettame	Default
Identity SelectionMatchedRule	Default
DTL 5 Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

IPSEC	IPSEC#Is IPSEC Device#No	
Name	Endpoint Identity Groups Profiled Workstation	
EnableFlag	Enabled	
RADIUS Username	use/2	
Device IP Address	192.108.0.100	
CPMSessionID	c0x800040000c000014bc367	
Called-Station-ID	192.168.0.100	
Cisco/WPair	India Barkajas (Jatamania, India Barkajas (Jatamania, India Barkajas (Jatamania, Jata) (Jata) (Jata) India Barkajas (Jata) (Jata) (Jata) India Barkajas (Jata) (Jata) (Jata) India Barkajas (Jata) (Jata) (Jata) India Barkajas (Jata) (Jata) (Jata) India Barkajas India Barkajas I	
esult		
Class	CACS:c0x800040000d000814bc387.driverap-ISE-2-7/417484978/24	
cisco-av-pair	profile-name=Windows10-Workstation	
	Barry Deserve and and a second second	

Session Events

Nota: Debe utilizar diferentes rangos de direcciones IP para la asignación de direcciones IP tanto en las políticas de agrupación local de IP FTD como en las de Autorización de ISE para evitar conflictos de direcciones IP duplicadas entre sus Clientes de AnyConnect. En este ejemplo de configuración, FTD se configuró con un conjunto local IPv4 de 10.0.50.1 a 10.0.50.100 y el servidor ISE asigna dirección IP estática de 10.0.50.101.

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

En FTD:

debug radius all

En ISE:

• Registros activos RADIUS