Configure SSL Anyconnect Con Autenticación ISE Y Atributo De Clase Para Asignación De Políticas De Grupo

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar ASA ISE Troubleshoot Escenario de trabajo Situación no operativa 1 Situación no operativa 2 Situación no operativa 3 Video

Introducción

Este documento describe cómo configurar Secure Sockets Layer (SSL) Anyconnect con Cisco Identity Services Engine (ISE) para la asignación de usuarios a una política de grupo específica.

Amanda Nava, ingeniera del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- AnyConnect Secure Mobility Client versión 4.7
- Cisco ISE 2.4
- Cisco ASA versión 9.8 o posterior.

Componentes Utilizados

El contenido de este documento se basa en estas versiones de software y hardware.

- Adaptive Security Appliance (ASA) 5506 con la versión de software 9.8.1
- AnyConnect Secure Mobility Client 4.2.00096 en Microsoft Windows 10 de 64 bits.

• ISE versión 2.4.

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

En el ejemplo, los usuarios de Anyconnect se conectan directamente sin la opción de seleccionar un grupo de túnel del menú desplegable, ya que Cisco ISE los asigna a una política de grupo específica de acuerdo con sus atributos.

ASA

aaa-server

```
aaa-server ISE_AAA protocol radius
aaa-server ISE_AAA (Outside) host 10.31.124.82
key cisco123
AnyConnect
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
anyconnect enable
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool Remote_users
authentication-server-group ISE_AAA
group-policy DfltGrpPolicy attributes
banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
vpn-simultaneous-logins 0
vpn-tunnel-protocol ssl-client
group-policy RADIUS-USERS internal
group-policy RADIUS-USERS attributes
banner value YOU ARE CONNECTED TO ### RADIUS USER AUTHENTICATION###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list value SPLIT_ACL
group-policy RADIUS-ADMIN internal
group-policy RADIUS-ADMIN attributes
banner value YOU ARE CONNECTED TO ###RADIUS ADMIN AUTHENTICATION ###
vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
split-tunnel-network-list none
```

Nota: Con este ejemplo de configuración puede asignar la política de grupo a cada usuario de Anyconnect a través de la configuración de ISE. Como los usuarios no tienen la opción de seleccionar el grupo de túnel, están conectados al grupo de túnel DefaultWEBVPNGroup y a DfltGrpPolicy. Después de que se produce la autenticación y el atributo Class (Group-

policy) devuelve la respuesta de autenticación de ISE, el usuario se asigna al grupo correspondiente. En el caso de que el usuario no tenga aplicado un atributo Class, este usuario permanece en DfltGrpPolicy. Puede configurar los **vpn-simultáneos-logins 0** en el grupo DfltGrpPolicy para evitar que los usuarios sin política de grupo se conecten a través de la VPN.

ISE

Paso 1. Agregue ASA a ISE.

Para este paso, navegue hasta Administración>Recursos de red>Dispositivos de red.

dialo Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓ Network Devices Network Device G	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	
Network Devices	Network Devices
Default Device	* Name ASAv
Device Security Settings	Description
	IP Address 🔹 * IP : 10.31.124.85 / 32
	* Device Profile data Cisco 👻 🕀
	Software version 9,9
	* Network Device Group
	Location All Locations 🚫 Set To Default
	IPSEC No. Set To Default
	Device Type All Device Types Set To Default
	RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	* Shared Secret cisco123 Hide
	Use Second Shared Secret 🔲 🛞
	Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (i)

Paso 2. Crear grupos de identidad.

Definir grupos de identidad para asociar cada usuario al correcto en los siguientes pasos. Vaya a Administration>Groups>User Identity Groups.

diale Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	
System Identity Management Networe	k Resources ▶ Device Portal Management pxGrid Services ▶ Feed Service ▶ Threat Centric NAC	
Identities Groups External Identity Source	s Identity Source Sequences + Settings	
Identity Groups	User Identity Groups > RADIUS_ANYCONNECT_ADMIN Identity Group *Name RADIUS_ANYCONNECT Description Store Reset Member Users Users Users Status Email Username First Name Last Name © Enabled	Selected 0 Total 1 🏀 🎡 🖵 Show All 💌

Paso 3. Asociar usuarios a grupos de identidad.

Asociar usuarios al grupo de identidad adecuado. Vaya a Administración>Identidades>Usuarios.

dentity Services Engine	Home • Contex	xt Visibility	Policy Administration	n 🕨 Work Ce	nters									
System Identity Management	 Network Resources 	Device Portal Management	pxGrid Services + Feed	Service + Threa	t Centric NAC									
Identities Groups External Identity Sources Identity Source Sequences + Settings														
G														
Users	Network Acces	ss Users												
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Import	Export - XDelete -	Duplicate										
	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin						
	🗌 🛃 Enabled	👤 user1					RADIUS_ANYCONNECT							
	🗌 🛃 Enabled	👤 user2					RADIUS_ANYCONNECT_USER							
	🗌 🛃 Enabled	👤 user3												

Paso 4. Crear conjunto de políticas.

Defina un nuevo conjunto de políticas como se muestra en el ejemplo (todos los tipos de dispositivos) bajo condiciones. Vaya a **Policy>Policy sets.**

ahalo lo cisco	dentity Se	ervices Engine Home	Context Visibility	Policy Administration Work Centers	License Warning 🔺	Q	0 (o c
Policy S	Sets Pr	ofiling Posture Client Provisionin	ng + Policy Elements					
Policy	Sets					F	Reset	Save
Ð	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
	Ø	New Policy Set 1		DEVICE Device Type EQUALS All Device Types	Default Network Access 🛛 🗙 🕈 🕂	27	٥	>
	Ø	Default	Default policy set		Default Network Access * * +	0	٥	>
							Reset	Save

Paso 5. Cree una política de autorización.

Cree una nueva política de autorización con la condición adecuada para que coincida con el grupo de identidad.

cisco Id	entity Ser	rvices Engine Home	 Context Vi 	sibility 🔸	Operations	- Policy	 Administration 	÷١	Work Centers							Licen	se Warning 🏼	<u> </u>	. 😐	• •
Policy S	ets Pro	filing Posture Client Provi	sioning • Pol	icy Elements	i i															
Policy	Sets →	New Policy Set 1																	Reset	Save
	Status	Policy Set Name	Descrip	tion		Conditions	6									Allowed	Protocols /	Server	Sequence	e Hits
Search																				
	0	New Policy Set 1				₽ DE	VICE-Device Type EQ	QUALS	S All Device Types	s						Default	Network Acce	955	× • +	27
> Auth	entication	Policy (1)																		
> Auth	orization	Policy - Local Exceptions																		
		Defense Obstant Francisco																		
 Auth 	orization	Policy - Global Exceptions																		
✓ Auth	orization	Policy (3)																		
0												Rest	ults							
Ð	Status	Rule Name	Condi	tions								Profi	les		Securi	ity Groups			Hits	Actions
Search	h																			
	0	ISE CLASS ADMIN	AND	De De	EVICE Device Ty	/pe EQUAL	S All Device Types						et from list		Seler	rt from list				
		136_00A33_ADMIN	AND	AL Ide	entityGroup Nan	ne EQUALS	User Identity Groups	s:RADIL	NUS_ANYCONNEC	ECT										*
				모 DE	EVICE Device Ty	/pe EQUAL	S All Device Types					-								
1	Ø	ISE_CLASS_USER	AND	at Ide	entityGroup Nan	ne EQUALS	User Identity Groups	s:RADIL	US_ANYCONNEC	ECT_USER		Sele	ect from list	1	Selec	ct from list		• +	9	¢
	~	Defent											an Access		Salar	et from liet		- 4		~
	٢	Detaurt											enyAccess		30100	or morn mor			8	*

Reset Save

ØΧ

Librar	Y		Editor						
Sear	ch by Name	0 k ?		₽	DEVICE Dev Equals	rice Ty	pe All Device Types		,
	BYOD_is_Registered Catalyst_Switch_Local_Web_Authenticati on	0	AND ~	4	IdentityGroup Equals	o Nam	e ×User Identity Groups:RADIUS_ANYCON	INECT	
	Compliance_Unknown_Devices Compliant_Devices	© 0					+ New AND OR		
	EAP-MSCHAPv2 EAP-TLS	0		Set to 'Is no	r			Duplicat	te
_	Guest_Flow	0							
-	Network_Access_Authentication_Passed	0							
	Non_Cisco_Profiled_Phones Non_Compliant_Devices	0							
8	Switch_Local_Web_Authentication	0							
								Close	

Paso 6. Cree un perfil de autorización.

Conditions Studio

Cree un nuevo perfil de autorización con RADIUS: Atributo Class<Group-policy-ASA> y *Access Type: ACCESS_ACCEPT.

State Note Control State Note State State State State <								Results				
text · · · · · · · · · · · · · · · · · · ·	•	Status	Rule Name	Condit	ons			Profiles	Security Groups		Hits	Actions
<pre> CLUG_LOUG_LOUP AND CLUCES And Deck Type: CLUCE Dock Type CDULLS AND Deck Type: CLUCES_ADDREAM AND CLUCES Survivery Company MOULD_ANT/CONECT Current Time Addreamage Them CLUCES_ADDREAMAND CLUCES_ADDREAMANN CLUCES ADDREAMANN CLUCES ADDREAMANN CLUCES ADDREAMANN</pre>	Search											
<pre>> 0 BE_CLASS_JOANI AND a Mempdowphame TOULLS Use Memby Grapp MODUS_APPCODECT</pre>		~			DEVICE	Device Type EQUALS All Device Types		(all of the second seco	• Autom			
<pre></pre>		0	ISE_CLASS_ADMIN	AND	AL IdentityG	roup Name EQUALS User Identity Groups:RADIUS_ANYCONNEC	т	Create a New Authorization F	Profile	• •	1	Ŷ
V INC.CLASS_USER AND Image: Class_USER Image: Class_USER Image: Class_USER Image: Class_USER </td <td></td> <td>~</td> <td></td> <td></td> <td>DEVICE</td> <td>Device Type EQUALS All Device Types</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		~			DEVICE	Device Type EQUALS All Device Types						
O Defail Add New Standard Profile * Itamic Loss 5, MODE, ADMEN * Itamic Loss 5, MODE, ADMEN * Access Type ACCESS, ACCEPT * Advanced Attributes Settings	1	0	ISE_CLASS_USER	AND	A IdentityG	roup Name EQUALS User Identity Groups:RADIUS_ANYCONNEC	T_USER	Select from list	+ Select from list	* +	9	¢
Add Ixers Standard Profile Authorization Profile ************************************		0	Default					(×DenyAccess	+ Select from list	- +	8	٥
Add New Standard brofile Authorization Profile Usersplan												
Authorization Prolife * New (LKS_25_RADBS_ADMB) * New (LKS_25_RADBS_ADMB) * Access Type (LCCSS_ACCEFT) Network Device Profile (LCCSS_ACCEFT) Network Device Profile (LCCSS_ACCEFT) * Common Tasks * Advanced Attributes Settings * Advanced Attributes Settings * Advanced Attributes Details Access Type = CCCSS_ACCEFT Coss = RADBS-ADMB1 * Coss = RADBS-ADMB1 * Attributes Details Access Type = CCCSS_ACCEFT Coss = RADBS-ADMB1 * Coss = RADBS-ADMB1 * Coss = RADBS-ADMB1 * Attributes Details Access Type = CCCSS_ACCEFT Coss = RADBS-ADMB1 * Attributes Details Access Type = CCCSS_ACCEFT Coss = RADBS-ADMB1 * Coss = RADSADS-ADMB1 * Coss = RADBS-ADMB1 * Coss = RADSA	Add N	w Stan	dard Profile									×
Access Type A	Autho	vrizatio	* Name CLAS 25 RADUS	ADMIN						Î		
Advanced Attributes Settings Advanced Attributes Settings Attributes Detais Attributes Detais Attributes Detais 		(Description									
Network Device Profile Service Template Track Movement Passive Identity Tracking > Common Tasks This should be the Group-policy name • Advanced Attributes Settings • Advanced Attributes Settings • Attributes Details Access Type = ACCESS_ACCEPT Cases = RADZES_ACCEPT		* Ac	coess Type ACCESS_ACCEPT		ž							
Service Template Track Movement Pressive Identity Tracking Pressive Identity Tracking Common Tasks This should be the Group-policy name Advanced Attributes Settings ReduceClass Advanced Attributes Details Access Type = ACCUSS-ACCEPT Class = RADUS-ADMN Class = RADMN Class = RADUS-ADMN Class = RADMN Class = RADUS-ADMN	Netw	vik Devic	e Profile 🗮 Cisco 💌 🗇									
Service temperating Track Movement Pessive identify Tracking • Common Tasks • Common Tasks • Advanced Attributes Settings • Advanced Attributes Settings • Advanced Attributes Settings • Advanced Attributes Details Access Type = ACCESS, ACCEPT Class = RADUS-ADMIN		Canica	Tamalata 🖸									
Pessve identity Tracking Pessve identity Tracking Common Tasks This should be the Group-policy name Advanced Attributes Settings Exadus:Class Exadus:Class Class Exadus:Class Exadus:		Track	Novement C									
Common Tasks This should be the Group-policy name Advanced Attributes Settings Advanced Attributes Details Access Type = ACCESS_ACCEPT Class = RADJUS-ADMIN C	Passi	ve Identit	y Tracking T									
Common Tasks This should be the Group-policy name Advanced Attributes Settings Raduus:Class Raduus:Class Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN C												
Common Tasks This should be the Group-policy name Advanced Attributes Settings Radus:Class Radus:Class Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN C C C C C C C C C C C C C												
Advanced Attributes Settings Advanced Attributes Settings Radus:Class Advanced Attributes Details Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN C	► Ci	mmon	Tasks		Th	is should be the Group-po	olicy name					
Advanced Attributes Settings Radius:Class Advanced Attributes Settings Advanced Attributes Details Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN C C												
Radus:Class RADIUS-ADMIN Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN C C C C C C C C C C C C C	▼ A	lvanced	Attributes Settings		_					_ 1		
Attributes Details Access Type = ACCESS_ACCEPT Class = RADIUS-ADMN	Ra	dius:Clas	is 📀 =	ADIUS-A	MIN	÷ +						
Attributes Details Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN c			v							- 1		
Attributes Details Access Type = ACCESS_ACCEPT Class = RADIUS-ADMIN c												
Access Type = ACCESS_ACCEPT Class = RADBUS-ADMIN	▼ AI	tribute	s Details									
< · · · · · · · · · · · · · · · · · · ·	Acce Class	ss Type : i = RAD3	= ACCESS_ACCEPT US-ADMIN									
	<								4	> [×]		

Paso 7. Revise la configuración del perfil de autorización.

alialia cisco	Identit	y Services	s Engine	Home	▸ Context Visibility	 Opera 	tions	✓ Policy	 Administration 	Work Centers
Polic	y Sets	Profiling	Posture	Client Provis	ioning •Policy Ele	ments				
Dictio	onaries	 Condition 	ons v Re	esults						
				G						
► Auth	enticati	on		Autho	orization Profile				_	
▼ Auth	orizatio	n			* Name	CLASS_25_R	ADIUS_AD	MIN		
A		- Deeflee	_		Description					
Dov	nonzatio		_		* Access Type	ACCESS_ACC	CEPT			
▶ Prof	iling	IC AGES		Netw	ork Device Profile	🎎 Cisco 👻	\oplus			
▶ Post	ure				Service Template					
					Track Movement					
I Clier	nt Provis	sioning		Pass	ive Identity Tracking					
				► Ca	ommon Tasks					
				▼ A	Ivanced Attributes	s Settings				
				Ra	dius:Class	© •] = [RADIU	S-ADMIN	Ť	÷
				▼ A1	tributes Details					
				Acce	ess Type = ACCESS_A s = RADIUS-ADMIN	CCEPT				
				Save	Reset					

Nota: Siga la configuración tal como se muestra en la imagen anterior, Access_Accept, Class—[25], RADIUS-ADMIN es el nombre de la política de grupo (se puede cambiar).

La imagen muestra cómo debe ser la configuración. En el mismo conjunto de políticas, no tiene ninguna política de autorización, cada una coincide con el grupo de identidad necesario en la sección *condiciones* y utiliza la política de grupo que tiene en el ASA en la sección *Perfil.*

cisco Ide	entity Se	rvices Engine Home	 Context Vi 	isibility	 Operations 		 Administration 		 Work Centers 						Licens	e Warning 🔺	Q,	۲	• •
Policy Se	ets Pro	filing Posture Client Provisi	ioning + Pol	icy Elem	ents														
Policy S	Sets →	New Policy Set 1																Reset	Save
	Status	Policy Set Name	Descrip	tion		Condition	s								Allowed I	Protocols / S	Server S	Sequence	Hits
Search																			
	0	New Policy Set 1				🖵 DE	EVICE Device Type E	QUAL	LS All Device Types						Default N	Vetwork Acces	15	× • +	27
> Authe	entication	n Policy (1)																	
> Autho	orization	Policy - Local Exceptions																	
> Autho	orization	Policy - Global Exceptions																	
✓ Author	orization	Policy (3)																	
												Results							
+	Status	Rule Name	Condi	itions								Profiles		Security	Groups			Hits	Actions
Search																			
	~			무	DEVICE-Device	Type EQUAL	.S All Device Types					01.000 05 010000							~
	9	ISE_CLASS_ADMIN	AND	48.	IdentityGroup N	ame EQUALS	S User Identity Group	ps:RA	ADIUS_ANYCONNECT			× CLASS_25_RADIUS_A		Select h	rom list		T	1	Ŷ
	0			₽	DEVICE-Device	Type EQUAL	S All Device Types							Column (~
		ISE_CLASS_USER	AND	趣	IdentityGroup N	ame EQUALS	S User Identity Group	ps:RA	ADIUS_ANYCONNECT_US	SER		×CLASS_25_RADIUS_C	ISER T	Select	rom list		T	а	v
	ø	Default										× DenyAccess	+	Select f	rom list		+	8	¢
																		Reset	Save

Con este ejemplo de configuración, puede asignar la política de grupo a cada usuario de Anyconnect a través de la configuración de ISE basada en el atributo class.

Troubleshoot

Uno de los debugs más útiles es **debug radius**. Muestra detalles de la solicitud de autenticación de RADIUS y la respuesta de autenticación entre el proceso AAA y ASA.

debug radius

Otra herramienta útil es el comando test aaa-server. Ahora verá si la autenticación es ACEPTADA o NEGADA y los atributos ('class' atributo en este ejemplo) intercambiados en el proceso de autenticación.

test aaa-server authentication

Escenario de trabajo

En el ejemplo de configuración mencionado anteriormente **user1** pertenece a la política de grupo **RADIUS-ADMIN** de acuerdo con la configuración de ISE, se puede verificar si ejecuta la prueba aaa-server y debug radius. Resalte las líneas que deben verificarse.

ASAv# debug radius

ASAv#test aaa-server authentication ISE_AAA host 10.31.124.82 username user1 password ***** INFO: Attempting Authentication test to IP address (10.31.124.82) (timeout: 12 seconds)

RADIUS packet decode (authentication request)

 Raw packet data (length = 84)....

 01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73
 ...T..|.X"5^.|Hs

 04 9f 8c 74 01 07 75 73 65 72 31 02 12 ad 19 1c
 ...t.user1....

 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f 04 06 0a
 @.C..F.5.R.o...

 1f 7c 55 05 06 00 00 00 66 3d 06 00 00 00 55 1a
 ...Uure...

15 00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3dcoa-push= 74 72 75 65 | true Parsed packet data.... Radius: Code = 1 (0x01)Radius: Identifier = 30 (0x1E)Radius: Length = $84 (0 \times 0054)$ Radius: Vector: ACB67CE55822355E8E7C4873049F8C74 Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07)Radius: Value (String) = 75 73 65 72 31 user1 Radius: Type = 2 (0x02) User-Password Radius: Length = 18 (0x12)Radius: Value (String) = ad 19 1c 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f | ...@.C...F.5.R.o Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.31.124.85 (0x0A1F7C55) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x6Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5Radius: Type = 26 (0x1A) Vendor-Specific Radius: Length = 21 (0x15) Radius: Vendor ID = 9 (0x0000009)Radius: Type = 1 (0x01) Cisco-AV-pair Radius: Length = 15 (0x0F)Radius: Value (String) = 63 6f 61 2d 70 75 73 68 3d 74 72 75 65 coa-push=true send pkt 10.31.124.82/1645 rip 0x00007f03b419fb08 state 7 id 30 rad_vrfy() : response message verified rip 0x00007f03b419fb08 : chall_state '' : state 0x7 : reqauth: ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74 : info 0x00007f03b419fc48 session_id 0x80000007 request_id 0x1e user 'user1' response '***' app 0 reason 0 skey 'cisco123' sip 10.31.124.82 type 1

RADIUS packet decode (response)

Raw packet data (length = 188)																
02	1e	00	bc	9e	5f	7c	db	ad	63	87	d8	с1	bb	03	41	cA
37	3d	7a	35	01	07	75	73	65	72	31	18	43	52	65	61	7=z5user1.CRea
75	74	68	53	65	73	73	69	6f	6e	3a	30	61	31	66	37	uthSession:0a1f7
63	35	32	52	71	51	47	52	72	70	36	5a	35	66	4e	4a	c52RqQGRrp6Z5fNJ
65	4a	39	76	4c	54	6a	73	58	75	65	59	35	4a	70	75	eJ9vLTjsXueY5Jpu
70	44	45	61	35	36	34	66	52	4f	44	57	78	34	19	0e	pDEa564fRODWx4
52	41	44	49	55	53	2d	41	44	4d	49	4e	19	50	43	41	RADIUS-ADMIN.PCA

43 53 3a 30 61 31 66 37 63 35 32 52 71 51 47 52 CS:0a1f7c52RqQGR 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 6a 73 | rp6Z5fNJeJ9vLTjs 58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66 | XueY5JpupDEa564f 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f | RODWx4:iseamy24/ 33 37 39 35 35 36 37 34 35 2f 33 31 379556745/31 Parsed packet data.... Radius: Code = 2(0x02)Radius: Identifier = 30 (0x1E)Radius: Length = 188 (0x00BC) Radius: Vector: 9E5F7CDBAD6387D8C1BB0341373D7A35 Radius: Type = 1 (0x01) User-Name Radius: Length = 7 (0x07)Radius: Value (String) = 75 73 65 72 31 user1 Radius: Type = 24 (0x18) State Radius: Length = 67 (0x43)Radius: Value (String) = 52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 ReauthSession:0a 31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35 | 1f7c52RqQGRrp6Z5 66 4e 4a 65 4a 39 76 4c 54 6a 73 58 75 65 59 35 fNJeJ9vLTjsXueY5 4a 70 75 70 44 45 61 35 36 34 66 52 4f 44 57 78 JpupDEa564fRODWx 4 34 Radius: Type = 25 (0x19) Class Radius: Length = 14 (0x0E)Radius: Value (String) = 52 41 44 49 55 53 2d 41 44 4d 49 4e RADIUS-ADMIN Radius: Type = 25 (0x19) Class Radius: Length = 80 (0x50)Radius: Value (String) = 43 41 43 53 3a 30 61 31 66 37 63 35 32 52 71 51 | CACS:0alf7c52RqQ 47 52 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 | GRrp6Z5fNJeJ9vLT 6a 73 58 75 65 59 35 4a 70 75 70 44 45 61 35 36 | jsXueY5JpupDEa56 34 66 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 | 4fRODWx4:iseamy2 34 2f 33 37 39 35 35 36 37 34 35 2f 33 31 4/379556745/31 rad_procpkt: ACCEPT RADIUS ACCESS ACCEPT: normal termination RADIUS DELETE remove_req 0x00007f03b419fb08 session 0x80000007 id 30 free_rip 0x00007f03b419fb08 radius: send queue empty INFO: Authentication Successful

Otra manera de verificar si funciona cuando el usuario1 se conecta a través de Anyconnect, utilice el comando **show vpn-sessiondb anyconnect** para conocer la política de grupo asignada por el atributo de clase ISE.

ASAv# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : user1 Index : 28 Assigned IP : 10.100.2.1 Public IP : 10.100.1.3 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 Hashing: AnyConnect-Parent: (1) noneSSL-Tunnel: (1) SHA384DTLS-Tunnel: (1) SHA1Bytes Tx: 15604Bytes Rx: 28706 Group Policy : RADIUS-ADMIN Tunnel Group : DefaultWEBVPNGroup Login Time : 04:14:45 UTC Wed Jun 3 2020 Duration : 0h:01m:29s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6401010001c0005ed723b5 Security Grp : none

Situación no operativa 1

Si la autenticación falla en Anyconnect y el ISE responde con un RECHAZO. Debe verificar si el usuario está asociado a un **grupo de identidad de usuario** o si la contraseña es incorrecta. Vaya a **Operaciones>Registros en directo > Detalles**.

RADIUS packet decode (response)
Raw packet data (length = 20)
03 21 00 14 dd 74 bb 43 8f 0a 40 fe d8 92 de 7a 🛛 🗍 .!t.C@z
27 66 15 be 'f
Parsed packet data
Radius: Code = $3 (0x03)$
Radius: Identifier = 33 (0x21)
Radius: Length = $20 (0 \times 0014)$
Radius: Vector: DD74BB438F0A40FED892DE7A276615BE
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000009 id 33
free_rip 0x00007f03b419fb08
radius: send queue empty
ERROR: Authentication Rejected: AAA failure
-thulh Identity Services Engine

Overview			Steps	
Fuent	5400 Authentiontion foiled		11001	Received RADIUS Access-Request
Event	5400 Authentication failed		11017	RADIUS created a new session
Username	user1		11117	Generated a new session ID
Endpoint Id			15049	Evaluating Policy Group
			15008	Evaluating Service Selection Policy
Endpoint Profile			15048	Queried PIP - DEVICE.Device Type
Authentication Policy	New Policy Set 1 >> Default		15041	Evaluating Identity Policy
Authorization Policy	New Policy Set 1 >> Default		22072	Selected identity source sequence - All_User_ID_Stores
Autionzation Foncy	New Folley Get 122 Delaut		15013	Selected Identity Source - Internal Users
Authorization Result	DenyAccess		24210	Looking up User in Internal Users IDStore - user1
			24212	Found User in Internal Users IDStore
			22037	Authentication Passed
Authorities Details			15036	Evaluating Authorization Policy
Authentication Details			15048	Queried PIP - DEVICE.Device Type
Source Timestamp	2020-06-02 23:22:53.577		15048	Queried PIP - Network Access.UserName
			15048	Queried PIP - IdentityGroup.Name
Received Timestamp	2020-06-02 23:22:53.577		15016	Selected Authorization Profile - DenyAccess
Policy Server	iseamy24		15039	Rejected per authorization profile
Event	5400 Authentication failed		11003	Returned RADIUS Access-Reject
LYSIN	area numerication railed		L	
Failure Reason	15039 Rejected per authorization pro	file		

Nota: En este ejemplo, **user1** no está asociado a ningún **grupo de identidad de usuario.** Por lo tanto, llega a las políticas de Autenticación y Autorización Predeterminadas bajo el **Nuevo Conjunto de Políticas 1** con la **acción DenyAccess**. Puede modificar esta acción para que **PermitAccess** en la Política de autorización predeterminada permita que los usuarios sin el grupo de identidad de usuario asociado se autentiquen.

Situación no operativa 2

Si la autenticación falla en Anyconnect y la política de autorización predeterminada es PermitAccess, se acepta la autenticación. Sin embargo, el atributo class no se presenta en la respuesta Radius, por lo tanto el usuario se encuentra en DfltGrpPolicy y no se conectará debido a **vpn-simultáneos-logins 0.**

RADIUS packet decode (response)

```
_____
Raw packet data (length = 174).....
02 24 00 ae 5f 0f bc b1 65 53 64 71 1a a3 bd 88
                                              | .$.._..eSdq....
7c fe 44 eb 01 07 75 73 65 72 31 18 43 52 65 61 | .D...user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37 | uthSession:0a1f7
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71 | c5229Th3GhmDTI5q
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b | 7HFE0zote4j7Pvik
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50 | Z5wqkxlP93BlJo.P
                                              CACS:0a1f7c5229T
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a
                                              h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78
                                             ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32 | 1P93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37
                                               4/379556745/37
Parsed packet data....
Radius: Code = 2 (0x02)
Radius: Identifier = 36 (0x24)
Radius: Length = 174 (0x00AE)
Radius: Vector: 5F0FBCB1655364711AA3BD887CFE44EB
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31
                                                user1
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 ReauthSession:0a
31 66 37 63 35 32 32 39 54 68 33 47 68 6d 44 54
                                               | 1f7c5229Th3GhmDT
49 35 71 37 48 46 45 30 7a 6f 74 65 34 6a 37 50
                                               I5q7HFE0zote4j7P
76 69 4b 5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a | viKZ5wqkxlP93BlJ
6f
                                                0
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54 CACS:0alf7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a | h3GhmDTI5g7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78
                                               ote4j7PviKZ5wqkx
                                               | 1P93BlJo:iseamy2
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37
                                               4/379556745/37
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x800000b id 36
free_rip 0x00007f03b419fb08
radius: send queue empty
INFO: Authentication Successful
ASAv#
```

Si el **vpn-simultáneamente-logins 0** se cambia a '1', el usuario se conecta como se muestra en el resultado:

41	
Assigned IP	: 10.100.2.1 Public IP : 10.100.1.3
Protocol	: AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License	: AnyConnect Premium
Encryption	: AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing	: AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx	: 15448 Bytes Rx : 15528
Group Policy	: DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup
Login Time	: 18:43:39 UTC Wed Jun 3 2020
Duration	: 0h:01m:40s
Inactivity	: 0h:00m:00s
VLAN Mapping	: N/A VLAN : none
Audt Sess ID	: 0a640101000290005ed7ef5b
Security Grp	: none
😗 Cisco	o AnyConnect Secure Mobility Client — 🗆 🗙
6	T VPIE
	Please respond to banner.
	10.100.1.1 V Connect
A (
40	<i>y</i>
Cisco A	nyConnect
YOU DO	ONT HAVE AUTHORIZATION TO ACCESS ANY INTERNAL
RESOU	ACES
	×
	Accest Disconnect

Situación no operativa 3

Si la autenticación pasa pero el usuario no tiene las políticas correctas aplicadas, por ejemplo, si la política de grupo conectada tiene el túnel dividido en lugar del túnel completo como debe ser. El usuario puede estar en el grupo de identidad de usuario incorrecto.

ASAv# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

 Username
 i user1
 Index
 : 29

 Assigned IP
 : 10.100.2.1
 Public IP
 : 10.100.1.3

 Protocol
 : AnyConnect-Parent SSL-Turnel
 : 10.100.1.3

 License
 : AnyConnect Premium
 : 10.100.2.1

 Encryption
 : AnyConnect-Parent: (1)-ver SSL-Turnel: (1)AES-GCM-256

 Hashing
 : AnyConnect-Parent: (1)-ver SSL-Turnel: (1)SHA384

 Bytes Tx
 : 15592
 Bytes Rx
 : 0

 Group Policy
 : RADIUS-USERS
 Tunnel Group
 : DefaultWEBVPNGroup

 Login Time
 : 04:36:50 UTC Wed Jun 3 2020
 : 10
 : 10

Duration: 0h:00m:20sInactivity: 0h:00m:00sVLAN Mapping: N/AAudt Sess ID: 0a6401010001d0005ed728e2Security Grp: none

Video

Este vídeo proporciona los pasos para configurar SSL Anyconnect con autenticación ISE y atributo de clase para asignación de políticas de grupo.