SSL AnyConnect met ISE-verificatie en -klasse configureren voor het toewijzen van groepsbeleid

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren ASA ISE Problemen oplossen Werkscenario Niet-functionerend scenario 1 Niet-functionerend scenario 2 Niet-functionerend scenario 3 Video

Inleiding

Dit document beschrijft hoe u Secure Socket Layer (SSL) AnyConnect met Cisco Identity Services Engine (ISE) kunt configureren voor gebruikerstoewijzing naar specifiek Group-beleid.

Bijgedragen door Amanda Nava, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect Secure Mobility Client versie 4.7
- Cisco ISE 2.4
- Cisco ASA versie 9.8 of hoger.

Gebruikte componenten

De inhoud van dit document is gebaseerd op deze software en hardwareversies.

- Adaptieve security applicatie (ASA) 5506 met software versie 9.8.1
- AnyConnect Secure Mobility Client 4.2.0096 op Microsoft Windows 10 64-bits.
- ISE versie 2.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

In het voorbeeld verbinden gebruikers direct zonder de optie om tunnel-groep van het vervolgkeuzemenu te selecteren aangezien zij door Cisco ISE aan specifiek Groep-Beleid in overeenstemming met hun eigenschappen worden toegewezen.

ASA

AAA-server

split-tunnel-network-list none

```
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
```

Opmerking: Met dit configuratievoorbeeld kunt u het groepsbeleid aan elke willekeurige gebruiker toewijzen door de ISE-configuratie. Omdat de gebruikers niet de optie hebben om de tunnelgroep te selecteren, worden ze aangesloten op de DefaultWEBVPNgroepstunnelgroep en de DfltGrpPolicy. Nadat verificatie plaatsvindt en de Class-attributie (Group-policy) terugkeert in de ISE-authenticatierespons, wordt de gebruiker toegewezen aan de corresponderende groep. In het geval, heeft de gebruiker geen Class Attribution toegepast, blijft deze gebruiker in DfltGrpPolicy. U kunt de **VPN-simultaan-logins 0** configureren onder de DfltGrpPolicy-groep om gebruikers te voorkomen zonder groepsbeleid om verbinding door VPN te maken.

ISE

Stap 1. Voeg de ASA toe aan ISE.

navigeren bij deze stap naar Beheer>Netwerkbronnen>Netwerkapparaten.

dentity 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	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
6	Network Devices Lists ARAM
Network Devices	Network Devices
Default Device	* Name ASAv
Device Security Settings	Description
	IP Address • IP : 10.31.124.85 / 32
	* Device Profile ditto Cisco 🔻 🕀
	Model Name ASAv T
	Software Version 9,9
	* Natwork Device Group
	Network Device Gloup
	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 ()

Stap 2. Maak identiteitsgroepen.

Defineert identiteitsgroepen om elke gebruiker in de volgende stappen aan de juiste te koppelen. Navigeren in **beheer>Groepen>Gebruikersidentiteitsgroepen**.

cisco	Identi	ity Servic	es Engine		Home	Contex	t Visibilit	y ▶ Oper	ations	Policy	▼ Ad	Iministration	1	Work Center	s								
+ Sj	/stem	◄ Identity	Manageme	nt 🔸	Network R	esources	► Dev	ice Portal Ma	nagement	pxGrid	Services	Feed Se	rvice	▶ Threat C	entric NAC								
► Id	entities	Groups	External	Identity	Sources	Identity	Source S	Sequences	 Setting 	s													
	entity	Groups	titly Groups Groups]	<u>م</u> هر	User Ide Dr Us Us	Identity G * Name escription mber L ers Add ~ Status 2 Enal	Groups > RAI roup RADIUS_A Reset Jsers X Delete + Delete	Er	rconnect_ ct mail		Userna 2 user	me 1		First Name	9	Last Name		S	how All	Selected 0	Total 1 🔮	

Stap 3. Verbonden gebruikers aan identiteitsgroepen.

Gebruikers associëren met de juiste identiteitsgroep. Navigeren in **op** beheer>ldentificaties>Gebruikers.

dentity Services Engine	Home + Contex	kt Visibility	► Policy	on Vork Centers			
System Identity Management	Network Resources	Device Portal Management	pxGrid Services Feed	Service + Threat Centric NA	с		
◄ Identities Groups External Identity	/ Sources Identity	Source Sequences . Settings					
Users	Network Acces	ss Users					
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Import	🔂 Export 👻 🗙 Delete 👻	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					

Stap 4. Maak beleidsset.

Defineer een nieuwe beleidsset zoals in voorbeeld (alle soorten apparaten) onder omstandigheden. Navigeren in op **Beleidsinstellingen.**

ahaha Id	entity Se	ervices Engine Home +	Context Visibility	Policy: Administration Work Centers	License Warning 🔺	Q	0	o 0
Policy S	ets Pro	ofiling Posture Client Provisionin	g Policy Elements					
Policy	Sets					F	Reset	Save
Œ	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	>
								Savo

Stap 5. Maak een autorisatiebeleid.

Maak een nieuw vergunningsbeleid met de juiste voorwaarde om de identiteitsgroep aan te passen.

cisco Id	entity Sei	rvices Engine Home	 Context V 	isibility	 Operations 	* Policy	 Administration 	•	 Work Centers 							License Warning	A 9	L 😐	• •
Policy S	ets Pro	filing Posture Client Provi	sioning + Po	licy Elem	ents														
Policy	Sets →	New Policy Set 1																Reset	Save
	Status	Policy Set Name	Descrip	otion		Condition	5									Allowed Protocols	/ Server	Sequenc	e Hits
Search																			
	0	New Policy Set 1				₽ DE	VICE Device Type EC	QUALS	S All Device Types	S						Default Network Ad	cess	x • 4	27
> Auth	entication	n Policy (1)																	
> Auth	orization	Policy - Local Exceptions																	
•																			
Auth	orization	Policy - Global Exceptions																	
✓ Auth	orization	Policy (3)																	
0												Results	5						
Ð	Status	Rule Name	Cond	itions								Profiles	5		Security G	roups		Hits	Actions
Search	n																		
	0		AND	묘	DEVICE-Device 1	ype EQUAL	S All Device Types						from Set	*	Salact from	. Let			~
	•	ISE_CLASS_ADMIN	AND	盘	IdentityGroup Na	me EQUALS	User Identity Group:	ps:RAD	DIUS_ANYCONNEC	CT		Genetic			Select Iron	1 1131		, ,	¥
					DEVICE-Device 1	VDE EQUAL	S All Device Types					_							
1	Ø	ISE_CLASS_USER	AND	盡	IdentityGroup Na	me EQUALS	User Identity Group	ps:RAD	DIUS_ANYCONNEC	CT_USER		Select	from list	+	Select from	n list	* +	9	¢
											 	-							
	Ø	Default										- Den	yAccess	+	Select from	n list	* +	8	¢

Reset Save

ØΧ

Search by Name Boolsis_Registered Oroblance_Unknown_Devices Oroplant_Devices Oroplant_Devices Octatives Oroplant_Devices Octatives Oroplant_Devices Octatives Oroplant_Devices Oroplant_Dev	Librar	Ŷ		Editor					
 BYOD_s_Registered BYOD_s_Registered Catalyst_Switch_Local_Web_Authentication on Compliance_Unknown_Devices Compliant_Devices AND OR Equals V Lser Identity Groups:RADIUS_ANYCONNECT Set to 'Is not' Duplication Set to 'Is not' Duplication MacLin_SAN <l< th=""><th>Sear</th><th>ch by Name</th><th>0 t ?</th><th></th><th>₽</th><th>DEVICE-Device Equals ~</th><th>Type</th><th>evice Types</th><th></th></l<>	Sear	ch by Name	0 t ?		₽	DEVICE-Device Equals ~	Type	evice Types	
 Compliance_Unknown_Devices Compliant_Devices EAP-MSCHAPv2 EAP-TLS Guest_Flow AC_in_SAN AC_in_SAN Attention_Passed Non_Cisco_Profiled_Phones Non_Compliant_Devices Attention Attention		BYOD_is_Registered Catalyst_Switch_Local_Web_Authenticati on	0	AND ~	48.	IdentityGroup N Equals v	lame ×Us	er Identity Groups:RADIUS_A	NYCONNECT
EAP-MSCHAPv2 0 EAP-TLS 0 Guest_Flow 0 MAC_in_SAN 0 Non_Clsco_Profiled_Phones 0 Non_Compliant_Devices 0		Compliance_Unknown_Devices Compliant_Devices	© 0				+	New AND OR	
 a cuest_Flow a MAC_in_SAN b Network_Access_Authentication_Passed b Non_Clisco_Profiled_Phones c Non_Compliant_Devices c Non_Compliant_Devices 		EAP-MSCHAPv2 EAP-TLS	0		Set to 'Is n	ot'			Duplicat
Network_Access_Authentication_Passed Image: Complex Comp		Guest_Flow MAC_in_SAN	0 0						
Non_Compliant_Devices Image: Compliant_Devices	2	Network_Access_Authentication_Passed	0						
		Non_Cisco_Profiled_Priories	0						
									Close

Stap 6. Maak een vergunningsprofiel.

Conditions Studio

Een nieuw autorisatieprofiel met RADIUS maken: Class<Group-policy-ASA> Eigenschappen en *Access Type: ACCESS_ACCEPT.

State Note Control State Note State State State State <								Results				
text · · · · · · · · · · · · · · · · · · ·	J	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 [] ()									
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	> [×]		

Stap 7. Controleer de configuratie van het vergunningsprofiel.

altalta cisco	Identit	y Services	s Engine	Home	▸ Context Visibilit	y ⊧o	perations	✓ Policy	Administration	► Work Centers
Polic	y Sets	Profiling	Posture	Client Provis	ioning Policy El	ements				
Dictio	onaries	 Condition 	ons v Re	sults						
				G						
► Auth	enticati	on		Autho	orization Profile				_	
▼ Auth	orizatio	n			* Name	CLASS_2	25_RADIUS_	ADMIN		
A		- Drefler	_		Description					
Aut	voloadab	In Profiles			* Access Type	ACCESS	_ACCEPT	*		
► Prof	iling			Netwo	ork Device Profile	ditte Cisco	0 🕶 🕀			
▶ Post	ure				Service Template					
					Track Movement	1				
I Clier	nt Provi	sioning		Pass	ive Identity Tracking	i				
				► Co	ommon Tasks					
				▼ Ac	Ivanced Attribute	s Setting	js			
				Ra	dius:Class		e RAD	IUS-ADMIN	Ť	÷
				_						
				▼ At	tributes Details					
				Class	ss Type = ACCESS_/ s = RADIUS-ADMIN	ACCEPT]			
				Save	Reset					

Opmerking: Volg de configuratie zoals deze op de vorige afbeelding wordt weergegeven, Access_Accept, Class—[25], is RADIUS-ADMIN de naam van uw groepsbeleid (kan worden gewijzigd).

Het beeld toont hoe de configuratie eruit moet zien. Op dezelfde beleidsset hebt u een vergunningsbeleid. Elk beleid komt overeen met de identiteitsgroep noodzakelijk in de **voorwaarden** sectie en gebruikt het groepsbeleid dat u hebt op de ASA In de profielsectie.

cisco Id	entity Se	rvices Engine Home	 Context Vi 	sibility	 Operations 	✓ Policy	 Administration 		 Work Centers 							License	Warning 🔺	Q,	0	• •
Policy S	ets Pro	filing Posture Client Provis	ioning + Pol	icy Elem	ents															
Policy	Sets →	New Policy Set 1																	Reset	Save
	Status	Policy Set Name	Descrip	tion		Conditions	;									Allowed P	Protocols / S	erver S	equence	Hits
Search																				
	0	New Policy Set 1				DE DE	VICE-Device Type E	QUAL	LS All Device Types							Default Ne	etwork Acces	is	× • +	27
> Auth	entication	n Policy (1)																		
> Auth	orization	Policy - Local Exceptions																		
> Auth	orization	Policy - Global Exceptions																		
✓ Auth	orization	Policy (3)																		
												D								
+	Status	Rulo Namo	Condi	tions								Profiles			Security	Groups			Lite	Actions
Search	Status	Nule Name	Cond	00115								Trones			occurry	oroups			Filts	Actions
1	Ø	ISE_CLASS_ADMIN	AND		DEVICE-Device	Type EQUAL	S All Device Types					× CLASS_	25_RADIUS_ADMI	N] +	Select fr	om list		+	7	٥
				424	IdentityGroup Na	ame EQUALS	User Identity Group	ps:RAI	DIUS_ANYCONNECT	Т								_		
				₽	DEVICE-Device	Type EQUAL	S All Device Types													
	0	ISE_CLASS_USER	AND	424	IdentityGroup N	ame EQUALS	User Identity Group	ps:RAI	DIUS_ANYCONNECT	T_USER		× CLASS_	25_RADIUS_USER	1	Select fr	om list		+	9	¢
	0	Default										× DenvAcc	ess	+	Select fr	rom list		+	8	ø
	Ŭ	CHOR																		Ŧ
																			Reset	Save

Met dit configuratievoorbeeld, kunt u het groep-beleid aan elke willekeurige gebruiker toewijzen door configuratie ISE gebaseerd op de class eigenschap.

Problemen oplossen

Een van de meest bruikbare insecten is **de debug straal**. Het toont details van het proces van de authenticatie van de straal en de authenticatie respons tussen AAA en ASA.

debug radius

Een ander bruikbaar gereedschap is de opdrachttest op een server. U ziet nu of de echtheidscontrole wordt AANVAARD of geweigerd en de eigenschappen (' class' attributie in dit voorbeeld) worden uitgewisseld in het authenticatieproces.

test aaa-server authentication

Werkscenario

In het hierboven genoemde configuratievoorbeeld **user1** behoort tot het groepsbeleid **RADIUS-ADMIN** in overeenstemming met de ISE-configuratie, kan dit worden geverifieerd als u de testserver en de bug straal gebruikt. Markeer de regels die gecontroleerd moeten worden.

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 06 3d 06 00 00 00 51 a
 ...Luser1....

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)

Rav	Raw packet data (length = 188)															
02	1e	00	bc	9e	5f	7c	db	ad	63	87	d8	c1	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

Een andere manier om te verifiëren of het werkt wanneer user1 door AnyConnect aansluit, gebruik de **show vpn-sessiondb om het** groepsbeleid te kennen dat door de ISE class attribuut wordt toegewezen.

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

Niet-functionerend scenario 1

Als de verificatie niet werkt bij AnyConnect en ISE antwoordt met een REJECT. U moet controleren of de gebruiker een **gebruikersgroep** heeft **of** het wachtwoord niet correct is. Navigeren in op **bewerkingen>Live loggen > Details.**

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 (0x0014)
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
cisco la dentity Services Engine

Overview			Steps	
Event	E400 Authentication failed		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 Doliny	New Deline Cat 1 >> Default		22072	Selected identity source sequence - All_User_ID_Stores
Autionzation Policy	New Policy Set 1 >> Delaut		15013	Selected Identity Source - Internal Users
Authorization Result	DenyAccess		24210	Looking up User in Internal Users IDStore - user1
	L.		24212	Found User in Internal Users IDStore
			22037	Authentication Passed
			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
Lion	and Authentication lared		L	
Failure Reason	15039 Rejected per authorization pro	e		

Opmerking: In dit voorbeeld is **user1** niet geassocieerd met een **gebruikersgroep.** Om deze reden slaat het de beleidsvormen voor standaardverificatie en -autorisatie onder **Nieuwe beleidsset 1** aan met de actie **Toegang** weigeren. U kunt deze actie wijzigen om **toegang** te verlenen in het beleid voor standaard autorisatie om gebruikers toe te staan zonder de gebruikersgroep die met de gebruikersidentiteit is geassocieerd, echt te maken.

Niet-functionerend scenario 2

Als de verificatie geen verbinding maakt en het standaard autorisatiebeleid een toegangsvergunning is, wordt de verificatie geaccepteerd. De class-eigenschap wordt echter niet weergegeven in de Radius-respons, daarom bevindt de gebruiker zich in de DfltGrpPolicy en heeft geen verbinding dankzij **VPN-simultane 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
                                               lP93BlJo: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#
```

Als de **Vpn-simultane logins 0** is veranderd in '1', sluit de gebruiker de verbinding aan zoals in de uitvoer:

:

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 — 🗆 🗙
	VPNC VPNC
	Please respond to banner.
	10.100.1.1 Connect
Q (
Cisco Ai	nyConnect
NOU DO	NUT HAVE AUTHORIZATION TO ACCECC ANY INTERNAL
RESOU	RCES
	×
	Accest Disconnect
	nucla Disconneu

Niet-functionerend scenario 3

Als de Verificatie passeert maar de gebruiker niet het juiste beleid toegepast heeft, bijvoorbeeld, als het groepsbeleid verbonden heeft de gesplitste tunnel in plaats van de volledige tunnel zoals het moet zijn. De gebruiker kan in de verkeerde gebruikersgroep zitten.

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

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

Video

Deze video bevat de stappen om SSL AnyConnect met ISE-verificatie en -klasse te configureren voor het toewijzen van groepsbeleid.