為組策略對映配置SSL Anyconnect的ISE身份驗 證和類屬性

目錄

簡介

本文檔介紹如何使用思科身份服務引擎(ISE)配置安全套接字層(SSL)Anyconnect,以便使用者對映 到特定組策略。

作者:思科TAC工程師Amanda Nava。

必要條件

需求

思科建議您瞭解以下主題:

- AnyConnect安全行動化使用者端版本4.7
- Cisco ISE 2.4
- Cisco ASA 9.8或更高版本。

採用元件

本文檔的內容基於這些軟體和硬體版本。

- •採用軟體版本9.8.1的調適型安全裝置(ASA)5506
- Microsoft Windows 10 64位版上的AnyConnect安全移動客戶端4.2.00096。
- ISE版本2.4。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

在示例中,Anyconnect使用者直接連線,而無需從下拉選單中選擇隧道組的選項,因為思科ISE會 根據他們的屬性將它們分配給特定組策略。

ASA

AAA伺服器

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

附註:在此配置示例中,您可以通過ISE配置將組策略分配給每個Anyconnect使用者。由於使 用者沒有選擇隧道組的選項,因此他們連線到DefaultWEBVPNGroup tunnel-group和 DfltGrpPolicy。身份驗證發生後,Class屬性(Group-policy)在ISE身份驗證響應中返回後,將 使用者分配到相應的組。如果使用者沒有應用Class屬性,則此使用者仍保留在 DfltGrpPolicy中。您可以在DfltGrpPolicy組下配置**vpn-simultaneous-logins 0**,以避免沒有組 策略的使用者通過VPN進行連線。 步驟1.將ASA新增到ISE。

在此步驟中,導覽至**管理>網路資源>網路裝置。**

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	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	
Network Devices	Network Devices
Default Device	
Device Security Settings	Name ASAV
	Description
	IP Address • * IP : 10.31.124.85 / 32
	* Device Profile data Cisco 💌 🕀
	Model Name ASAv T
	Software Version 9,9
	* Natural 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 ()

步驟2.建立身份組。

定義身份組,以便在後續步驟中將每個使用者與正確的使用者相關聯。導航到**管理>組>使用者身份 組。**

cisco	Ident	tity Service	s Engine	Home	Contex	t Visibility	 Operations 	▶ Policy	→ Admi	inistration	Work Center	S				
۰s	ystem	▼ Identity N	Aanagement	 Network R 	esources	▶ Device	e Portal Manageme	nt pxGrid S	Services	Feed Service	► Threat C	entric NAC				
► Id	lentities	Groups	External Iden	tity Sources	Identity	Source Seq	uences 🔸 Settin	gs								
, (, , ,	(dentity	Groups	ity Groups roups	<u>م</u>	User Ide: Dr Us Us Us	Identity Gro * Name [esscription] we Res mber Use ers Add • X Status Enabled	Dups > RADIUS_AI up RADIUS_ANYCONN set ers (Delete + d	ECT Email		Username Quser1		First Name	Last Name	Show All	Selected 0 Total 1 🥹	- 3

步驟3.將使用者與身份組關聯。

將使用者關聯到正確的身份組。導航到管理>身份>使用者。

dentity Services Engine	Home	erations Policy Administrati	on Vork Centers		
System Identity Management	Network Resources Device Portal N	fanagement pxGrid Services + Feed	Service		
✓ Identities Groups External Identit	y Sources Identity Source Sequences	▶ Settings			
•					
Users	Network Access 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				

步驟4.建立策略集。

在條件下定義新的策略集,如示例(所有裝置型別)所示。導航到Policy>Policy sets。

ahaha lo cisco	fentity Se	ervices Engine Home	Context Visibility	▼Policy	Administration	Work Centers						Licen	se Warning	<mark>ه</mark> م	0	•	ø
Policy \$	Sets Pro	ofiling Posture Client Provisionin	g Policy Elements														
Policy	Sets														Reset	Sav	ve
Ð	Status	Policy Set Name	Description	Conditions						Allowed	Protocols	/ Server	Sequence	Hits	Actions	s Vi	ew
Search							_										
	0	New Policy Set 1		🖵 DEV	ICE-Device Type EQL	UALS All Device Typ	es			Default	Network Acc	ess	×* +	27	٥	:	>
	Ø	Default	Default policy set							Default	Network Acc	ess	× • +	0	٥	:	>
															Reset	Sav	ve

步驟5.建立授權策略。

建立具有適當條件的新授權策略以匹配身份組。

cisco Ide	ntity Sen	vices Engine Home	 Context Vis 	ibility • Operations		 Administration 	 Work Cent 	ters				L	cense Warning 🔺	Q,	۲	• •
Policy Se	ts Profi	ling Posture Client Provisi	ioning + Polic	cy Elements												
Policy S	iets → I	New Policy Set 1												R	leset	Save
	Status	Policy Set Name	Descript	ion	Conditions	5						Allov	ved Protocols / S	erver Se	equence	e Hits
Search																
	0	New Policy Set 1			₽ DE	VICE-Device Type EQ	UALS All Device	e Types				Def	ault Network Acces	S 1	× •	27
> Authe	ntication	Policy (1)														
> Autho	rization F	Policy - Local Exceptions														
Authorized Authoriz	rization F	Policy - Global Exceptions														
✓ Author	rization F	Policy (3)														
										Results						
Θ	Status	Rule Name	Condit	ions						Profiles		Security Groups			Hits	Actions
Search																
	0	ISE CLASS ADMIN		DEVICE-Devic	Type EQUAL	S All Device Types				Select from list	+	Select from list		+	7	ö
	Ŭ	102_00/00_70/11/	AND	A IdentityGroup-I	lame EQUALS	User Identity Groups	RADIUS_ANYC	CONNECT							1	~
				DEVICE-Devic	Type EQUAL	S All Device Types										
1	\odot	ISE_CLASS_USER	AND	A IdentityGroup I	lame EQUALS	User Identity Groups	RADIUS_ANYC	CONNECT_USER		Select from list	+	Select from list		+	9	¢
	Ø	Default								(×DenyAccess)	+	Select from list		+	8	٥

Reset Save

0×

Library Editor Search by Name DEVICE Device Type ♀ ◻ ◢ ๏ ▣ ₽ ▣ ዸ ፟ . © 1 ♥ ఓ ♥ 무 ~ All Device Types - 11 Equals BYOD_is_Registered 0 IdentityGroup-Name Catalyst_Switch_Local_Web_Authenticati 123 ND . on ~ Equals × User Identity Groups: RADIUS_ANYCONNECT . Compliance_Unknown_Devices *(i)* AND OR New Compliant_Devices (EAP-MSCHAPv2 0 Set to 'Is not' Duplicate Save EAP-TLS 0 Guest_Flow 1 MAC_in_SAN *(i)* Network_Access_Authentication_Passed () Non_Cisco_Profiled_Phones Ø Non_Compliant_Devices 0 Switch_Local_Web_Authentication 0 Close Use

步驟6.建立授權配置檔案。

Conditions Studio

使用RADIUS建立新授權設定檔:Class<Group-policy-ASA>屬性和*Access Type:ACCESS_ACCEPT。

+							Results					
	Status	Rule Name	Condit	ions			Profiles		Security Groups		Hits	Actions
Search												
	0	ISE CLASS ADMIN		DEVICE Device Type EQUAL	LS All Device Types		Select from list	+	Select from list	· +	7	ö
ĺ.			7440	LidentityGroup-Name EQUALS	LS User Identity Groups:RADIUS_ANYCONNECT		Create a New Authori:	zation Profile				+
				DEVICE-Device Type EQUAL	LS All Device Types							
1	0	ISE_CLASS_USER	AND	A IdentityGroup Name EQUALS	S User Identity Groups:RADIUS_ANYCONNECT_	USER	Select from list	+	Select from list	* +	9	¢
	Ø	Default					× DenyAccess	+	Select from list	- +	8	٥
Add N Autho Netw Passi	ew Stan orizatio ank Devic Service Track we Identit	adard Profile In Profile INAME CLAS_25_RADD Description Costs Type ACCESS_ACCEF e Profile Interplate Movement Interplate	US_ADMIN PT D							*		×
-	Annio	14585		This shoul	ld be the Group-po	licy name						
+ A	fvanced	Attributes Settings			-					_ 1		
Ra	dius:Clas	is 📀 :	RADIUS-A	MIN + +	+							
▼ A1	tributes	s Details										
Acce	ss Type : s = RAD3	= ACCESS_ACCEPT US-ADMIN										
<										~		
											Save	Cancel

步驟7.檢查授權配置檔案配置。

altalta cisco	Identit	y Services	s Engine	Home	 Context Visibility 	► Op	erations	✓ Policy	Administration	Work Centers
Polic	y Sets	Profiling	Posture	Client Provision	ing Policy Ele	ments				
Dictio	onaries	 Condition 	ons v Re	sults						
				C						
 Auth 	enticati	on		Author	zation Profile				_	
▼ Auth	orizatio	n			* Name	CLASS_25	5_RADIUS_	ADMIN		
Aut	horizatio	n Drofiloo	_		Description					
Dov	voloadab		_		* Access Type	ACCESS_A	ACCEPT	*		
Prof	iling			Networ	Device Profile	🎎 Cisco	•			
In Post	ure				Service Template					
					Track Movement	(i)				
I Clie	nt Provi	sioning		Passive	Identity Tracking	1				
				► Con	nmon Tasks					
				▼ Adv	anced Attributes	Settings	;			_
				Radi	us:Class		C = RAD	IUS-ADMIN	÷	÷
				▼ Attr	ibutes Details					
				Access Class :	Type = ACCESS_A RADIUS-ADMIN	CCEPT				
				Save	Reset					

附註:請按照上一個映像Access_Accept, Class—[25]中所示的配置進行操作,RADIUS-ADMIN是組策略的名稱(可以更改)。

該圖顯示了配置必須達到的外觀。在同一策略集上,您有n個授權策略,每個策略都與*conditions*部 分中所需的身份組匹配,並使用您在ASA上的*profile*部分中的組策略*。*

cisco Ide	ntity Ser	vices Engine Home	Context Vis	sibility	 Operations 		 Administration 	1	 Work Centers 						License Warning	A (२ 💿	• •
Policy Se	s Prof	iling Posture Client Provision	ing 🔸 Poli	icy Elemer	nts													
Policy S	ets →	New Policy Set 1														(Reset	Save
1	Status	Policy Set Name	Descript	tion		Conditions	5								Allowed Protocols	/ Serve	r Sequenc	e Hits
Search																		
	0	New Policy Set 1				🖵 DE	VICE-Device Type E	QUAL	S All Device Types						Default Network Act	ess	× • •	27
> Authe	ntication	Policy (1)																
> Autho	rization	Policy - Local Exceptions																
> Autho	rization	Policy - Global Exceptions																
✓ Author	rization	Policy (3)																
												Results						
+	Status	Rule Name	Condit	tions								Profiles		Security G	roups		Hits	Actions
Search																		
	0			₽.	DEVICE-Device	Type EQUAL	S All Device Types					CLASS OF DADELS ADME		Salact from	o Est			Å
	0	ISE_CLASS_ADMIN	AND	48.	IdentityGroup Na	ime EQUALS	User Identity Group	ps:RAE	DIUS_ANYCONNECT	r		*CD435_25_14D105_4DMI		Select nor			l '	*
	0			P	DEVICE-Device	Type EQUAL	S All Device Types							Coloritor				~
	U	ISE_CLASS_USER	AND	趣	IdentityGroup Na	ime EQUALS	User Identity Group	ps:RAE	DIUS_ANYCONNECT	LUSER		×CLASS_25_RADIUS_USER		Select Ifor	n iist		9	v
	0	Default										× DenyAccess	+	Select from	n list	• +	8	٥
																	Parat	Save

在此配置示例中,您可以根據類屬性通過ISE配置將組策略分配給每個Anyconnect使用者。

疑難排解

最有用的偵錯功能之一是**debug radius。**它顯示了AAA和ASA進程之間的radius身份驗證請求和身份 驗證響應的詳細資訊**。**

debug radius

另一個有用的工具是命令test aaa-server。現在您可以看到身份驗證是ACCEPTED還是 REFLECTED,以及身份驗證過程中交換的屬性(在本示例中為'class'屬性)。

test aaa-server authentication

工作場景

在上述**user1**配置示例中,根據ISE配置,屬於**RADIUS-ADMIN**組策略,如果運行測試aaa-server並 調試radius,則可以驗證該配置。突出顯示需要驗證的線路。

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)..... | ...T..|.X"5^.|Hs 01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73 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 05 1a | .|U....=.... 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 (0x0054) 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 : regauth: ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74 : info 0x00007f03b419fc48 session_id 0x8000007 request_id 0x1e user 'user1' response '***' app 0 reason 0 skey 'cisco123' sip 10.31.124.82

RADIUS packet decode (response)

type 1

_____ Raw packet data (length = 188).... 02 1e 00 bc 9e 5f 7c db ad 63 87 d8 c1 bb 03 41 ||..c....A 37 3d 7a 35 01 07 75 73 65 72 31 18 43 52 65 61 7=z5..user1.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 eJ9vLTjsXueY5Jpu 65 4a 39 76 4c 54 6a 73 58 75 65 59 35 4a 70 75 pDEa564fRODWx4.. 70 44 45 61 35 36 34 66 52 4f 44 57 78 34 19 0e 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 XueY5JpupDEa564f 58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66 | RODWx4:iseamy24/ 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f

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 | 1f7c52RqQGRrp6Z5 31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35 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 34 4 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:0alf7c52RgQ 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 另一種驗證在user1通過Anyconnect連線時是否工作的方法,使用show vpn-sessiondb

anyconnect命令瞭解由ISE類屬性分配的組策略。

```
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
          : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Hashing
Bytes Tx : 15604
                                   Bytes Rx : 28706
Group Policy : RADIUS-ADMIN
                                   Tunnel Group : DefaultWEBVPNGroup
Login Time : 04:14:45 UTC Wed Jun 3 2020
          : 0h:01m:29s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                   VLAN
                                              : none
Audt Sess ID : 0a6401010001c0005ed723b5
Security Grp : none
```

非工作場景1

如果Anyconnect上的身份驗證失敗,並且ISE使用REJECT回覆。您需要驗證使用者是否與使用者

身份組關聯,或者密碼是否不正確。 導航到操作>即時日誌>詳細資訊。

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

dentity Services Engin

ERROR: Authentication Rejected: AAA failure

		Steps
Overview		
Event	5400 Authentication failed	11001 Received RADIUS Access-Request
LVOIR	5466 Addientication 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
		22072 Selected identity source sequence - All_User_ID_Str
Authorization Policy	New Policy Set 1 >> Default	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
		15036 Evaluating Authorization Policy
uthentication Details		15048 Queried PIP - DEVICE.Device Type
Source Timestamp	2020-06-02 23-22-63 677	15048 Queried PIP - Network Access.UserName
Source Timestamp	2020-06-02 23.22.33.577	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
Failure Reason	15039 Rejected per authorization profile	

附註:在本示例中,user1未與任何使用者身份組相關聯。因此,它會使用DenyAccess操作在 New Policy Set 1下觸發預設身份驗證和授權策略。可以在預設授權策略中將此操作修改為 PermitAccess,以允許沒有關聯使用者身份組的使用者進行身份驗證。

非工作場景2

如果Anyconnect上的身份驗證失敗且預設授權策略為PermitAccess,則接受身份驗證。但是 ,Radius響應中未顯示class屬性,因此使用者位於DfltGrpPolicy中,並且由於**vpn-simultaneouslogins 0而無法連線。**

RADIUS packet decode (response)

```
Raw packet data (length = 174)....
02 24 00 ae 5f 0f bc bl 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
                                                c5229Th3GhmDTI5q
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71
                                                7HFE0zote4j7PviK
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b
                                                 Z5wqkx1P93BlJo.P
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54
                                                CACS:0a1f7c5229T
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:0a1f7c5229T
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
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x8000000b id 36
free_rip 0x00007f03b419fb08
radius: send queue empty
INFO: Authentication Successful
ASAv#
```

如果vpn-simultaneous-logins 0更改為'1',則使用者連線如下輸出所示:

ASAv# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : user1 Index 41 Assigned IP : 10.100.2.1 Public IP : 10.100.1.3 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol : AnyConnect Premium License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1 Hashing : 15448 Bytes Tx 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

C	VPN: Please respond to bank	ner.	Connect	
	AU- 200- 21 A		Connect	
\$ ()				
YOU DON'T H	AVE AUTHORIZATION T	0 ACCESS ANY IN	TERNAL A	

非工作場景3

如果身份驗證通過,但使用者沒有應用正確的策略,例如,如果連線的組策略有拆分隧道,而不是 必須的全隧道。使用者可能位於錯誤的使用者身份組中。

ASAv# sh vpn-sessiondb anyconnect Session Type: AnyConnect Username Index : 29 Public IP : 10.100.1.3 : user1 Assigned IP : 10.100.2.1 Protocol : AnyConnect-Parent SSL-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 15592 Bytes Rx : 0 Bytes Tx : 15592 Bytes Rx : 0 Group Policy : RADIUS-USERS Tunnel Group : DefaultWEBVPNGroup Login Time : 04:36:50 UTC Wed Jun 3 2020 : 0h:00m:20s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6401010001d0005ed728e2 Security Grp : none

影片

此影片提供了為組策略對映配置帶ISE身份驗證和類屬性的SSL Anyconnect的步驟。