通過RADIUS授權為AnyConnect使用者配置靜態 IP地址分配

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>網路圖表</u> <u>通過FMC使用AAA/RADIUS身份驗證配置遠端訪問VPN</u> <u>在ISE上配置授權策略(RADIUS伺服器)</u> <u>驗證</u> 疑難排解

簡介

本文說明如何使用身分識別服務引擎(ISE)伺服器設定RADIUS授權,以便其透過RADIUS屬性8 Framed-IP-Address將同一IP位址轉送到特定Cisco AnyConnect安全行動化使用者端的Firepower威 脅防禦(FTD)。

必要條件

需求

思科建議您瞭解以下主題:

- FTD
- Firepower Management Center (FMC)
- ISE
- Cisco AnyConnect Security Mobility Solution 遠端存取
- RADIUS通訊協定

採用元件

本檔案中的資訊是根據以下軟體版本:

- FMCv 7.0.0(內部版本94)
- •FTDv-7.0.0(內部版本94)
- ISE 2.7.0.356
- AnyConnect 4.10.02086
- Windows 10 Pro

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

網路圖表



通過FMC使用AAA/RADIUS身份驗證配置遠端訪問VPN

如需逐步程式,請參閱本檔案及以下影片:

- FTD上的AnyConnect遠端存取VPN組態
- FMC管理的FTD的初始AnyConnect配置

FTD CLI上的遠端存取VPN組態為:

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
```

在ISE上配置授權策略(RADIUS伺服器)

步驟1.登入到ISE伺服器並導航到管理>網路資源>網路裝置。

	A charactering a characterine	 Policy 	 Administration Work Cen 	ters			Junite maning A 1 V U
Summary Endpoints Guests	Vulnerability Threat	+	System	Network Resources	pxGrid Services		0
TRICS Total Endpoints Ø	Active Endpoint	ints 0	Literating Centicates Logging Maintenance Upprade Backup & Restere Admin Access Settings (Mentity Management Identities	Network Device Groups Network Device Profiles Edemail RADIUS Servers RADIUS Server Sequences NAC Manapers Eleternal MDM Location Services Device Portal Manapement Blackist BYCD Cuefficiel Provisionion	Feed Service Profiler Threat Centric MAC Third Party Vendors	Authenticated Guests • BYOD I	Endpoints 0 0 0
AUTHENTICATIONS [©]	ure Reason	80,	External identity Sources identity Source Sequences Settings	Client Provisioning Mobile Device Management My Devices Custom Portal Files	×	ENDPOINTS	a o x
interusers: [100%]			drive85806;	(100%)		workstations: [100%]	
interusers: [100%])	e o x	drivea5506:	[1005]	e o x	workstations: [100%]) S G X
interusers: [100%]		5 0 X	drivea5506: II ALARMS Ø Severity Name	[100%]	arred A	workstations: [100%]	중 전 X Ali- 24/8-
interusers: [100%] BYOD ENDPOINTS ® ge Profile No data a	vallablo.	5 0 X	drivea5506: II ALARMS 0 Severity Name V Name	(100%)	arred	workstations: [100%]	Altertrate Larger

步驟2.在「網路裝置」區段中,按一下Add,以便ISE可以處理來自FTD的RADIUS存取要求。

dealer Identity Services Engine	Home + Context Visibility	Operations Policy Admin	stration • Work Centers			ι	icense Warning 🔺 🔍 👘	0 0 0
System Identity Management	Network Resources Device	e Portal Management pxGrid Services	Feed Service Threat Centric NAG	5				
Network Devices Network Device G	roups Network Device Profiles	External RADIUS Servers RADIUS S	inver Sequences NAC Managers I	External MDM + Location Services				
•								
Network Devices	Network Devices							
Default Device	And And Designed	Advent Altered - Advention	Modula -				Selected 0 Total	- 197
Device Security Settings	Cor	Bintort Benfort + Overersterver	A Deele +	R	Barrelation .		Show [Al	• 10
	DRIVERAP ASA5506	172.16.255.2 dd Osco (1)	Al Locations	All Device Types	Description			

輸入網路裝置**名稱**和**IP地址**欄位,然後選中**RADIUS身份驗證設定**框。**Shared Secret**的值必須與建 立FMC上的RADIUS伺服器對象時使用的值相同。

deate Identify Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🔍 🔍 💿 🔿 🔷
System Identity Management	Herkvork Resources + Device Portal Management puGrid Service + Feed Service + Threat Centric NAC	
Network Devices Network Device	cocups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
(1	
Network Devices	Network Devices List > men Hetwerk Device	
Default Device	* Name DRVFRAP FTD 7.0	
Device Security Settings	Description	
	▶ Address ▼ *₽: 192.168.0.100 7/ 32	@ -
	* Device Profile Att Cisco v 🕀	
	Model Name	
	* Network Device Group	
	Location attractions Cat. To Default	
	PECC UN UNCER PARKA	
	and the state of t	
	• RACIUS Authentication Settings	
	RADUS UOP Settings	
	Protocol RADIUS	
	* Shared Secret Shared	
	Use Second Shared Secret 🔲 🕡	
	Show	
	CoA Port 1200 Set. To Default.	
	RADUS DTLS Settings (2)	

使用此頁面結尾的按鈕儲存。

步驟3.導航到管理>身份管理>身份。

dealer Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Center	MS		License Warning 🔺 🔍 🐵 🔿 🔿
etcelley Services Engine > System - Kdentky Management - Network Devices Metwork Device Default Device Device Device Security Settings Settings	Homa • Context Visibility • Operations • Pelopy • Network Resources • Directe Portal Management priority • Oreview External RADIUS Servers • Network Devices priority • Methods Periods priority priority • Network Devices priority priority • Network Devices priority priority • Network Devices priority priority priority • Devices priority priority priority priority • Devices priority priority priority priority • Devices priority priority priority priority priority • Devices priority priority priority priority • Devices priority priority priority priory priority prio	Administration Vour Center System Destoyment Licensing Centicutes Loging Maintenance Upgrade Bacturg & Retaine Admin Access Seting VourOs Licensis Licen	rs Network Resources Network Device Interwork Device Groups Network Device Groups Network Device Froless External RADUS Servers RADUS Server Researces External RADUS External RADUS	putind Services Feed Service Profiler Thereal Centric NAC Third Party Vendors	License Wanning 🔥 Q Selected 3 Total 2 Show д v V
1ttps://10.31.124.31:6012/admin/#a	administration/administration_identitymanagement/ad	ministration_identitymanageme	nt_identities		

步驟4.在Network Access Users部分,按一下**Add**以便在ISE的本地資料庫中建立*user1*。



在Name和Login Password欄位中輸入使用者名稱和密碼,然後按一下Submit。

deate- cisco- identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺 🔍	o ^
System Identity Management	Network Resources Device Portal Management puGrid Services Feed Service Threat Centric N4C		
· Identities Groups External Identity	Sources Identity Source Sequences + Settings		
0			
Users	Network Access Users List > New Network Access User		
Latest Manual Network Scan Res	*Name UserI Status C Enabled +		
	Emai		
	* Passwords		
	Pässword Type: Internal Users +		
	Password Re-Enter Password		
	*Login Password Generate Password ()		
	Enable Password Generate Password		
	• User Information		
	FirstName		
	LastName		
	▼ Account Options		
	Description		
	Change password on next login		- 4
	Account Disable Policy		- 1
	Disable account if date exceeds 2021-11-21 (vyy+mm-dd)		
			- 1
	▼ User Groups		
	Select an Rem O - +		
	Submet Cancel		
<			>

步驟5.重複上述步驟以建立user2。



步驟6.導覽至Policy > Policy Sets。



步驟7.按一下*屏*幕右側的箭頭>。

-thethe lide	ntity Service	es Engine Home + Con	text Visibility + Operations	Policy Administration	Work Centers			License	Warning 🔺	 ≤ ● 	•	٥
Policy Se	ts Profiling	Posture Client Provisioning	Policy Elements									
Policy S	Sets						Ret	et Policyset	Hitcounts	Reset		ve
+	Status	Policy Set Name	Description	Conditions			Allowed Protocols / Server Se	quence	Hits	Actions	Vie	w
Search												
					+							
	0	Default	Default policy set				Default Network Access *	- +	17	٥	>	
										Reset	\$1	ive

步驟8.按一下Authorization Policy旁邊的箭頭>將其展開。現在,按一下+符號以新增新規則。

Identity Servic	es Engine Home	ext Visibili	y Operations	Policy Administration	n				License Warning	Q (0 0
icy Sets Profiling	g Posture Client Provisioning	 Policy 	Elements								
cy Sets → De	efault							Reset P	olicyset Hitcount	Res	et Sa
Status	Policy Set Name	Descrip	notion	Conditions				Allowe	ed Protocols / Serve	er Sequence	e Hits
arch											
0	Default	Default	policy set					Defa	ult Network Access	×* +	17
Authentication P	olicy (3)										
Authorization Po	licy - Local Exceptions										
Authorization Po	licy - Global Exceptions										
Authorization Po	iry (13)										
	51.4.51										
•						Results					
Status	Rule Name	Cond	itions			Profiles		Security Groups		Hits	Actions
Narch											
Ø	Wireless Black List Default	AND	Wireless_A	locess		×Blackhole Wireless Access	+	Select from list	· +	0	ø
		1010	AL IdentityGrou	up-Name EQUALS EndpointIde	intity Groups:Blacklist						
ø	Profiled Cisco IP Phones	击	IdentityGroup-Name	EQUALS Endpoint Identity Grou	ups:Profiled.Cisco-IP-Phone	×Cisco_IP_Phones	+	Select from list	• +	0	٥
0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled	_Phones		×Non_Cisco_IP_Phones	+	Select from list	- +	0	¢
0			Network_Ac	ccess_Authentication_Passed		(Oliver Temperal Onbergel		Relation list			
0	Unknown_Compliance_Redired	AND	E Compliance	e_Unknown_Devices		[~ Gaco_remporal_Onocard]		Other and the	· •		¥
			Network_Ac	ccess_Authentication_Passed			-				

為規則提供名稱,並在**條件**列下選擇+符號。

✓ Authori	Authorization Policy (13)									
	(*)				Results					
٠	Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions		
Search										
1	0	Static IP Address User 1		+	Select from list	Select from list 👻 🛨		٥		

在「屬性編輯器」(Attribute Editor)文本框中按一下,然後按一下**「主題」(Subject**)圖示。向下滾動 ,直到找到*RADIUS User-Name*屬性並選擇它。

ibrary		Editor														
Search by Name			Clic	k to add	l an attribu	te										
♀ іі □ ▲ ⊕ 早 9 10	P 🖪 O 1 O 2 ?	, E	Select	attribute	e for condit	ion										
BYOD_is_Registered	(i)		Q	Ēġ	•	۲	<u> </u>	Ē	f		2	<u></u>	Ե 📘	C	٤	(î•
Catalyst_Switch_Local_We tion	eb_Authentica			Dicti	onary				Attribut	te			ID		Info	
Compliance_Unknown_Dev	ices 🕡		1	All	Dictionaries			~	Attribut	e AP-Use	r-Name		60		<i>(</i> i)	^
Compliant_Devices	(i)		1	Moto	rola-Symbol				Symbol	-User-0	Group		12		<i>i</i>	
EAP-MSCHAPv2	٢		1	Netw	ork Access				AD-Use	r-DNS-	Domair	ı			<i>(i</i>)	
EAP-TLS	٦		1	Netw	ork Access				AD-Use	r-Join-F me	Point				(i) (i)	
Guest_Flow			1	Pass	iveID				Passive	ID_Us	ername				<i>i</i>	
MAC_in_SAN			1	Radi	us				User-N	ame			1		() ()	4
Network_Access_Authenti	cation_Passe 🕧		1	Ruck	us :us				Ruckus	usswor-User-(a Groups		1		() ()	~
Non_Cisco_Profiled_Phone	es ()			-			-			-			-	-		
Non_Compliant_Devices	٦															
Switch_Local_Web_Auther	ntication															
Switch Web Authenticatio	in (i)															

保留Equals作為運算子,並在其旁邊的文本框中輸入*user1*。按一下「Use」以儲存屬性。

Con	ditions Studio							
.ibraı	у		Editor					
Sea	rch by Name			Radius-User-Nan	ne			
•		8 g	1	Equals	v user1			
	BYOD_is_Registered			Set to 'Is not'			Duplicate	
	Catalyst_Switch_Local_Web_Authentica tion	٦						
	Compliance_Unknown_Devices	()			+ New	AND OR		
	Compliant_Devices							
	EAP-MSCHAPv2	٢						
	EAP-TLS	٢						
	Guest_Flow							
	MAC_in_SAN	0						
	Network_Access_Authentication_Passe d	٢						
	Non_Cisco_Profiled_Phones							
	Non_Compliant_Devices							
	Switch_Local_Web_Authentication							
8	Switch Web Authentication	()						

現在已設定此規則的條件。

步驟9.在Results/Profiles列中,按一下+號並選擇Create a New Authorization Profile。

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

為其指定**名稱**,並保留ACCESS_ACCEPT作為存取型別。向下滾動至高級屬性設定部分。

Add New Standard Profile			×
Authorization Profile		^	
* Name	StaticIPaddressUser1		
Description			
* Access Type	ACCESS_ACCEPT *		
Network Device Profile	And Cisco + D		
Service Template			
Track Movement			
Passive Identity Tracking			
▼ Common Tasks			
DACL Name		î	
IPv6 DACL Name			
ACL (Filter-ID)		L.	
ACL IPv6 (Filter-ID)		~	
 Advanced Attributes 	Settings	~	1
<	Save	Cance	1

按一下橙色箭頭並選擇Radius > Framed-IP-Address - [8]。

Add New Standard Profile Service Template			-	×
Track Movement 🔲 🕧				
Passive Identity Tracking				
	Radius			
 Common Tasks 			- 1	ł.
			^	
DACL Name	Egress-VLANID[56]			
	Error-Cause(101)			
IPv6 DACL Name	Fiter-ID[11]			
	Framed-AppleTalk-Link[37]			
	Framed-AppleTalk-Network[38]			
ACL (Filter-ID)	Framed-AppleTalk-Zone(39)			
	Framed-Compression[13]			
ACL IPv6 (Filter-ID)	Framed-Interface-Id(96)		\sim	
	Framed-IP-Address[8]			
	Framed-IP-Netmask[9]			
· · · · · · · · · · · · · · · · · · ·	Framed-IPv6-Address[168]			
 Advanced Attributes Settin 	9 Framed-IPv6-Pool[100]			
Radius:Framed-IP-Address				
			- 1	
Access Type = ACCESS_ACCEPT				
Framed-IP-Address =		4		٩.
		111.	~	1
<			>	
		Save	Can	cel

鍵入要始終為此使用者靜態分配的IP地址,然後按一下**Save**。

Add New Standard Profile		×
Service Template		
Track Movement		
Passive Identity Tracking 🔲 (j)		
▼ Common Tasks		
Airespace IPv6 ACL Name	^	
ASA VPN		
AVC Profile Name		
UPN Lookup		
	~	
✓ Advanced Attributes Settings		
Radus:Framed-IP-Address 💽 = 10.0.50.101 💽 = +		
▼ Attributes Details		
Access Type = ACCESS_ACCEPT Framed-IP-Address = 10.0.50.101		
	Save	ncel

步驟10.現在,選擇新建立的授權配置檔案。

Author	zation Polic	y (13)							
					Results				
•	Status	Rule Name	Cond	tions	Profiles		Security Groups	Hits	Actions
earch									
/	0	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	+	Select from list • +		٥
				Wireless_Access	DenyAccess	^			
	Ø	Wireless Black List Default	AND	IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	NSP_Onboard		Select from list	0	\$
	0	Profiled Cisco IP Phones	4	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco-IP-Phone	Non_Cisco_IP_Phones PermiNAccess	ľ	Select from list	0	٥
	0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_Phones	StaticiPaddressUser1		Select from list +	0	¢
					Static_IP_address	\sim			

現在已設定授權規則。按一下「Save」。

dudu iden	tity Service	es Engine	Home + Co	nteid Visibilit	y Operations	* Policy	Administration	Work Centers								Lio	nse Warning	۹ م	0	• •
Policy Sets	Profiling	Posture	Client Provisioning	 Policy E 	Elements															
Policy Se	<u>ets</u> → De	fault													R	eset Policy	set Hitcour	ts Re:	set	Save
	Status	Policy Se	t Name	Descrip	tion	Condi	tions									Allowed Pr	otocols / Ser	ver Sequent	e	Hits
Search																				
	0	Default		Default	policy set											Default Ne	twork Access	** *	٠	17
> Authen	ntication Po	olicy (3)																		
> Author	ization Poli	icy - Local I	Exceptions																	
> Author	ization Poli	icy - Global	Exceptions																	
✓ Author	ization Poli	icy (13)																		
												Results								
•	Status	Rule Na	me	Cond	tions							Profiles			Security Group	15		Hits	Ac	tions
Search																				
1	0	Static IP	Address User 1	1	Radius-User-Name	EQUALS use	er1					× StaticlPaddress	sUser1	+	Select from list		- +			٥

驗證

步驟1.導航到安裝了Cisco AnyConnect Security Mobility客戶端的客戶端電腦。連線到FTD頭端(此 處使用Windows機器),並輸入*user1*憑證。



按一下齒輪圖示(左下角)並導航到Statistics頁籤。在Address Information部分中確認分配的IP地 址確實是為該使用者在ISE授權策略中配置的地址。

3	Cisco Ang	yConnect Secure Mobility Client	-		×
		VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
0	00:00:23			1	Pv4
K	ن 🕻				uluilu cisco

Cisco AnyConnect Secure Mobi	lity Client			
AnyCon	nect Secure Mobility Clie	nt		(
rtual Private Network (V	PN)	Diagnost	ics	
eferences Statistics Route Deta	ails Firewall Message History			
Connection Information			•	^
State:	Connected			
Tunnel Mode (IPv4):	Tunnel All Traffic			
Tunnel Mode (IPv6):	Drop All Traffic			
Dynamic Tunnel Exclusion:	None			
Dynamic Tunnel Inclusion:	None			
Duration:	00:01:49			
Session Disconnect:	None			
Management Connection State:	Disconnected (user tunnel active)			
Address Information			- •	
Client (IPv4):	10.0.50.101			
Client (IPv6):	Not Available			
Server:	192.168.0.100			
Bytes			- ^	~
		Free	art Ctata	
	Reset	Exp	ort stats.	••

FTD上的debug radius all命令輸出顯示:

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 FTD 記錄顯示: 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

```
ISE上的RADIUS Live日誌顯示:
```

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00.50.55.56.46.57 ()
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Statio IP Address User 1
Authorization Result	StaticIPaddressUser1

1 tication Details

Source Timestamp	2021-09-22 23:53:19.72
Received Timestamp	2021-09-22 23:53:19.72
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Usemame	user1
User Type	User
Endpoint Id	00.50.56.96.46.6F
Calling Station Id	192.108.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Identity Group	Workstation
Audit Session Id	c0x8000140000.000014bc140
Authentication Method	PAP_ASCI
Authentication Protocol	PAP_ASCI
Network Device	DRIVERAP_FTD_7.0
Device Type	All Device Types
Location	All Locations
NAS IPut Address	0000

Steps

- Skeps

 111
 MacK/DS Assess Results

 112
 MacK/DS Assess Results

NAS Port Type	Vitual
Authorization Profile	StatidPaddressUser1
Response Time	51 milliseoprids
Other Attributes	
ConfigWersionId	140
DestinationPort	1812
Protocol	Redus
NAS-Port	49152
Tunnel-Client-Endpoint	(lag=0) 192.168.0.101
CVPN3000/ASA/PUX7x-Tunnel-	RA VPN
Group Name	
OriginalUserName	user1
NetworkDeviceProfileId	b0099505-3150-4215-a00e-6753d45b856c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PO(7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417454978/23
SelectedAuthenticationIdentityStore	es Internal Users
SelectedAuthenticationIdentityStore	es All_AD_Join_Points
SelectedAuthenticationIdentityStore	es Quest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address User 1
ISEPolicySettame	Default
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Ciam
Location	Location#All Locations
Device type	Device Typeman Device Types

ExaMPlay Enable MADUS Stansame user1 Onvice IP Address 192.180.190 Calad-Status D 193.1	PSEC	IPSECHI IPSEC Device#No
Disability Disability Disability Control MARCH Si Username vier1 March Si Username vier1 Critical III Address 192, 158,0,150 Critical Estatus 193,0,150,150 Critical Estatus 193,0,150,150,150,150,150,150,150,150,150,1		
MADEU Forwarder set1 Device IP Address 50 100 Device IP Address de30040000000014:0:100 Called Status de30040000000014:0:100 Called Status 102 10 0.100 Called Status 102 10 0.100 Called Status moth-th-relative pathometers Caseod/Par moth-th-relative pathometers Caseod/Par moth-th-relative pathometers Discourse appending/Constant Works v1 (100 call Pathometers moth-th-relative pathometers Caseod/Par guidant Follower (100 call Pathometers) moth-th-relative pathometers Caseod/Par guidant Follower (100 cal	EnableFtag	Enabled
Device IP Address 192.180.180 CHM Section ID dial000400000000140140100 CARREN BRIDNING 192.180.180 Carled States Address 192.180.180 Consult Park mith On-Inducing Information, mith On-Inducing Information	RADIUS Username	user1
CHR BestionED adult006400002000143c160 Called Station ID 192,193,0,190 Called Station ID 192,193,0,190 Called Station ID 192,193,0,190 Called Station ID 192,193,0,190 Called Station ID 193,00,190 Called Station ID 193,0	Device IP Address	192.168.0.100
Called Statum 0 192.160.100 mdm.0rdesize platformasis, mdm.0rdesize platformasis, mdm.0rdesize platformasis, mdm.0rdesize platformasis, mdm.0rdesize platformasis, mdm.0rdesize platformasis, mdm.0rdesize platformasis, pla	CPMSessionID	c0a8000640000c0000514bc1d0
mich-th-relative participants. mich-th-relative mand/20 50 50 54 54 56 mich-th-relative participants. mich-th-relative participants. mich-th-relative participants. mich-th-relative participants. Cissue40/Park participant 51850007 537 1002201 4006 4104.2420208, un-accident 317 178120241 4007 4104.2420208, un-accident 317 178120241 4017 4124.212464.2008, un-accident 317 178120241 4017 4124.21246.4008027 1782170806200 un-accident 317 178120241 4017 4124.21246.4008027 1782170806200 un-accident 317 178120241 4017 4124.21246.4008027 1782170806200 un-accident 317 1782 415 4124.2124 446408027 1782170806200 un-accident 317 1782 415 4124.2124 446408027 1782170806200 un-accident 317 1782 415 4124.2124 446408027 1782170806200 un-accident 318 4124.2124 un-accident 318 4124.2124 un-acciden	Called-Station-ID	192.108.0.100
	CiscoRVPair	Indio Transmissi (a Statistimunis), Indio Transmissi Indio Statisti (Statisti (Statis
	Class	CACS.dba500540000.d000514bc1d0.driverap-ISE-2-7/417454978/23
Class CACS:dba500540000;d000014bc1d0;driverap-ISE-2-7/417454978/23	cisco-av-pair	profile-name=Windows10-Workstation
Class CACS x0x800064000x000114bc1d0.driverap.ISE-0.7/417494978/23 ciscolary pair profile namer/Windows10-Worklasion		Base license consumed
Cleas CACS deblood400004000146c140 driverp.155.2741749497523 drisen ar pair politie namer/101des151/1004850n Licensetypes Base Itomse comumed	LicenseTypes	

步驟2.連線到FTD頭端(此處使用Windows電腦)並輸入user2憑證。

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
OK Cancel	

Address Information部分顯示,分配的IP地址實際上是通過FMC配置的IPv4本地池中的第一個IP地址。

🚳 Cisco AnyConnect Secure Mobi	lity Client	— [Х
cisco AnyCon	nect Secure Mobility Client			()
Virtual Private Network (VF	PN) Diag	gnostics		
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	Export S	stats	

FTD上的debug radius all命令輸出顯示:

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 FTD 記錄顯示:

<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

ISE上的RADIUS Live日誌顯示:

Event	5200 Authentication succeeded
Usemane	U882
Endpoint Id	00:50:56:96:46:6F (B)
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess
athentication 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
Usemame	use/2
User Type	User
Endpoint Id	00.50.50.90.40.0F
Calling Station Id	192.108.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
Authentication identity Store	Internal Users Workstation
Authentication identity Store Identity Group Audit Session Id	Internal Users Workstation cba800540000-000814bc367
Authentication Identity Store Identity Group Audit Session Id Authentication Method	Internal Users Workstation db800040000000014bc387 PAP_ASCII
Authentication identity Store Identity Group Audit Session id Authentication Method Authentication Protocol	Internal Dates Workstoon disb000400000000001464d87 PMP_A500 PMP_A500
Authentication Identity Store Identity Group Audit Session Id Authentication Method Authentication Protocol Network Device	Internal Dates Workston stability stability PAP_ASCI DRV/ENAP_STID_7 5
Authentication Identity Store Identity Group Audit Session Id Authentication Method Authentication Protocol Network Device Device Type	Internal Dates Wonstation disation disation Advanced Web_ABCRI PAP_ABCRI Device Types All Device Types
Authentication Identify Store Identify Group Autit Session Id Authentication Protocol Authentication Protocol Itelevork Device Device Type Location	Internet Uses Workstein Subal0646000000014-buckt? PAPAGCI PAPAGCI Deliver/AACH Deliver/AACH All Desicer Types All Loadons

Steps

 Steps:

 111
 Attal Steaded a result

 112
 Building Stricks Exteaders Attal Steaders

 112
 Building Stricks Exteaders Attal Attal Steaders

 112
 Building Attal Steaders

NAS Port Type	(itual
Authorization Profile	PermitAccess
Response Time	102 milliseconds
ther Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PIX7x-Tunnel- Group Name	RA_VPN
OriginalUserName	use/2
NetworkDeviceProfileId	b0099505-3150-4215-a00e-0753d45b/56o
Is ThirdPartyDeviceFlow	false
CVPN3000/ASA/PDX7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417494978/24
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Quest Users
Authentication Status	AuthenticationPassed
identityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
15EPolicySetName	Default
Identity SelectionMatchedRule	Default
DTLSSupport	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

Name	Endpoint Identity Groups Profiled Workstation	
EnableFlag	Enabled	
RADIUS Username	uter2	
Device IP Address	192.108.0.100	
CPMSessionID	c0a800640000d000614bc387	
Called-Station-ID	192.165.0.100	
CiscoWPair	India Pundesia platformania. India Pundesia platforma ensoranti 20.11502. India Pundesia platforma ensoranti 20.11502. India Pundesia platforma ensoranti 20.11502. India Pundesia agenti MyConsen Michael A.10.0008, India Pundesia Secondari 20.0002.20.1004 (SALA 20.0008, India Pundesia). India Pundesia India Pundesia. India Pundesia. In	
isult		
Class	CACS:x0a800540000.d000514bc367.driverap-ISE-2-7/417484978/24	
cisco-av-pair	profile-name=Windows10-Woxlatation	
LicenseTypes	Base license consumed	

附註:您必須在FTD IP本地池和ISE授權策略上對IP地址分配使用不同的IP地址範圍,以避免 您的AnyConnectClients之間的重複IP地址衝突。在此組態範例中,FTD設定為從10.0.50.1 到 10.0.50.100的IPv4本機池,而ISE伺服器指派靜態IP位址10.0.50.101。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在FTD上:

• debug radius all 在ISE上:

• RADIUS即時日誌