RADIUS 권한 부여를 통해 AnyConnect 사용자에 게 고정 IP 주소 할당 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 네트워크 다이어그램 FMC를 통해 AAA/RADIUS 인증을 사용하여 원격 액세스 VPN 구성 ISE(RADIUS 서버)에서 권한 부여 정책 구성 다음을 확인합니다. 문제 해결

소개

이 문서에서는 RADIUS Attribute 8 Framed-IP-Address를 통해 항상 특정 Cisco AnyConnect Secure Mobility Client 사용자의 FTD(Firepower Threat Defense)에 동일한 IP 주소를 전달하도록 ISE(Identity Services Engine) 서버를 사용하여 RADIUS 권한 부여를 구성하는 방법에 대해 설명합 니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMCv 7.0.0(빌드 94)
- FTDv 7.0.0(빌드 94)
- ISE 2.7.0.356
- AnyConnect 4.10.02086
- Windows 10 Pro

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램



FMC를 통해 AAA/RADIUS 인증을 사용하여 원격 액세스 VPN 구성

단계별 절차는 이 문서와 다음 비디오를 참조하십시오.

- FTD의 AnyConnect 원격 액세스 VPN 컨피그레이션
- FMC에서 관리하는 FTD의 초기 AnyConnect 컨피그레이션

FTD CLI의 원격 액세스 VPN 컨피그레이션:

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
```

authentication-server-group ISE_Server tunnel-group RA_VPN webvpn-attributes group-alias RA_VPN enable

tunnel-group RA_VPN type remote-access tunnel-group RA_VPN general-attributes

http-comp none

activex-relay disable file-entry disable file-browsing disable url-entry disable deny-message none

address-pool AC_Pool

ISE(RADIUS 서버)에서 권한 부여 정책 구성

1단계. ISE 서버에 로그인하고 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.

tiese Identity Services Engine Home + Cor	ntext Visibility + Operations + Policy	Administration Work Centers		License Warr	ing 🔺 🔍 👄 💿 🜼 🤷
Summary Endpoints Guests	Vulnerability Threat +	System Network Resources	pxGrid Services		ō -
METRICS Total Endpoints 0	Active Endpoints Ø	Lensing Netern Device Group Lensing Netern Device Group Lensing Netern Device Group Lensing Extension Lenging Extension RADUS Server Seque Upgrade NAC Managem Bacius & Restere Bacius Sefrig Device Petat Managem Bacius Sefrig Device Petat Managem Bacius Sefrig Device Petat Sefrig Device Petat Management Bacius Sefrig Proc Groups Centicate Provisioning	Feed Service Profiler Thread Centric NAC cores Third Party Vendors	Authenticated Guests 0 BYOD Endpoints	• 0 •
AUTHENTICATIONS Kientity Store Identity Group Network Device Failure	Presson	External Identity Sources Client Provisioning Identity Source Sequences Mobile Device Manager Settings My Devices Custom Portal Files Settings	ment ×	ENDPOINTS Prote	8 0 X
inter_users: [100%])	drivea5506: [100%]		workstations: [100%]	
BYOD ENDPOINTS [®]	A C A	II ALARMS [©]	a a x	SYSTEM SUMMARY 0	₽¤× ∣
Type Profile		Severity Name Occu	Last Occurred	1 node(s)	All × 24HR ×
No data ava	ailable.	✓ Name		CPU Memory Usage	Authentication Latency
https://10.31.124.31:6012/admin/#administration/a	administration networkresources/administra	DNS Resolution Failure 941 ation networkresources devices	less than 1 min ago		
		a least 4600	lose then 1 min new		

2단계. Network Devices(네트워크 디바이스) 섹션에서 Add(**추가)**를 클릭하여 ISE가 FTD에서 RADIUS 액세스 요청을 처리할 수 있도록 합니다.

dealer Identify Services Engine	Home + Context Visibility	Operations	Policy Administra	Non Work Centers			License Warning 🔺	9.00
System Identity Management	Network Resources Device	ce Portal Manager	ment pxGrid Services + F	eed Service + Threat Centric f	NAC			
Network Devices Network Device 0	Groups Network Device Profile	is External RAD	UUS Servers RADIUS Serve	r Sequences NAC Managers	External MDM + Location Services			
•								
Network Devices	Network Devices							
Default Device		1					Select	d 0 Total 1 🧐 🎡 🖕
Device Security Settings	Edt de Add	e @pimport @p	Export • OGenerate PAC	X Delete *			Show AI	• 6
	Name ·	172.16.255.2	Profile Name	Location	Type	Description		
	D DRIVEROP_ASA5506	172.10.233.2	usco 🗠	All Locations	All Device Types			

네트워크 디바이스 Name 및 IP Address 필드를 입력한 다음 RADIUS Authentication Settings 상자 를 선택합니다. 공유 **암호**는 FMC의 RADIUS 서버 객체가 생성될 때 사용된 값과 같아야 합니다.

death Identify Services Engine	Home + Context Visibility + Operations + Policy +Administration + Work Centers	License Warning 🔺 🔍	0 0	• ^
System Identity Management	Helwork Resources Device Portal Management puGrid Services Feed Service Threat Centric NAC			
Network Devices Network Device	Croups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM → Location Services			
0				
Network Devices	Notivors Dorkos Lat New Retwork Device			
Default Device	* Name DRIVERAD ETD 7.0			
Device Security Settings				
	▼ Address * ♥: 192.166.0.100 /[32	@ .		
	* Device Profile 🖾 Clisco 🔍 🕀			
	Model Name 📃 👻			
	Software Version 📃 👻			
	* Mahard Deales Grown			
	reserves unless of early			
	Location All Locations 📀 Set: To Default			
	IPSEC Is IPSEC Device 📀 Set. To Default			
	Device Type AI Device Types 🗿 Set. To Default			
	C + RADUS Authentication Settings			
	RADIUS UDP Settings			- 1
	Protocol RADNIS			
	* Shared Secret Show			
	Use Second Shared Secret 🔲 🛈			
	Show			
	CoA Port 1700 Set To Default			
	RADIUS DTL.S Settings ()			
	DTLS Required 🗖 🕡			~

이 페이지 끝에 있는 단추를 사용하여 저장합니다.

3단계. Administration(관리) > Identity Management(ID 관리) > Identities(ID)로 이동합니다.

deate Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Centers			License Warning 🔺 🔍 😐 🔿 🗢
System Identity Management	Network Resources Device Portal Management pxGrid	System	Network Resources	pxGrid Services	
Network Devices Network Device 0	Croups Network Device Profiles External RADIUS Servers	Deployment	Network Devices Network Device Groups	Feed Service	
0		Certificales	Network Device Profiles	Profiler	
Network Devices	Network Devices	Logging Maintenance	External RADIUS Servers RADIUS Server Sequences	Third Party Vendors	
Default Device	the true Destruction across low	Upgrade	NAC Managers		Selected 0 Total 2 🧐 🅁 🚽
Device Security Settings	/ Est	Admin Access	External MDM Location Services		Show Al V
	Name P/Mask Profile Name	Settings	Device Portal Management		
	□ DRMERAP_F 192.168.0.10 # Cisco ⊕	Identity Management	Blacklist		
		Groups	Certificate Provisioning		
		External Identity Sources	Client Provisioning Mobile Device Management		
		Settings	My Devices		
			Custom Portal Files Settings		
https://10.31.124.31:6012/admin/#a	idministration/administration_identitymanagement/adr	ministration_identitymanagement	_identities		

4단계. Network Access Users(네트워크 액세스 사용자) 섹션에서 **Add(추가)**를 클릭하여 ISE의 로 컬 데이터베이스에서 *user1*을 생성합니다.



Name 및 Login Password 필드에 사용자 이름과 비밀번호를 입력하고 Submit(제출)을 클릭합니다.

dentity Services Engine	Home + Context Visibility + Operations + Poky +Administration + Work Centers	License Warning 🔺	<u> २</u>	• •	^
System Identity Management	Network Resources Device Portal Management puGrid Service Feed Service Threat Centric NAC				
Identities Groups External Iden	ty Sources Identity Source Sequences + Settings				
0					
Users	Network Access Users Lul > New Retwork Access User				
Latest Manual Network Scan Res					
	* Name Luser1				
	Status 🕑 Enabled 🖌				
	Email				
	* Passwords				
	Password Type: Internal Users •				
	Password Re-Enter Password				
	*Logn Password				
	Enable Password Generate Password @				
	a they before the				
	* user anormation				
	First Name				
	LastName				
	▼ Account Options				
	Description //				
	Change password on next login				- 11
	✓ ACCOUNT UBGROUP ONCY				
	Disable account if date exceeds 2021-11-21 (0)///emm-dd)				
	▼ User Groups				
	Select an term				
	Short Contail				
				_	~
·					>

5단계. user2를 생성하려면 이전 단계를 반복합니다.



6단계. Policy(정책) > Policy Sets(정책 세트)로 이동합니다.



7단계. 화면 오른쪽에서 화살표>를 클릭합니다.

databa ide	ntity Service	es Engine Home + Con	text Visibility + Operations	Policy Administration	Work Centers License Warnin			
Policy Se	ts Profiling	Posture Client Provisioning	Policy Elements					
Policy S	Sets				Reset Policyset Hitco	nts Re	iset	Save
•	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits	Action	s	View
Search								
					+			
					•			_
	\odot	Default	Default policy set		Default Network Access * * 17	\$		>
						R	Iset	Save

8단계. 권한 부여 정책 옆*의* 화살표>를 클릭하여 확장합니다. 이제 새 규칙을 추가하려면 *+* 기호를 클릭합니다.

dentity Service	es Engine Home + Conte	xt Visibilit)	y Operations	Policy Administration	n + Work Centers				License Warning 🔺	٩,	0 0
y Sets Profiling	Posture Client Provisioning	 Policy E 	ilements								
/ Sets → De	fault							Res	et Policyset Hitcount	Res	et Sa
Status	Policy Set Name	Descrip	tion	Conditions				А	llowed Protocols / Serve	r Sequence	e Hits
ch											
0	Default	Defaults	policy set						Default Network Access	×* 4	17
uthentication Po	olicy (3)										
athorization Pol	icy - Local Exceptions										
uthorization Pol	icy - Global Exceptions										
uthorization Pol	icy (13)										
						Results					
+) Status	Rule Name	Condi	tions			Profiles	s	ecurity Groups		Hits	Actions
earch											
0	Western Brask List Cafeed		Wireless_A	ccess		v Biscibola Wirelass Arrass		Calart from list	- 4		Å
0	WIRNESS BIACK LISE D'RIADIE	AND	4 IdentityGrou	p-Name EQUALS EndpointIder	intity Groups:Blacklist						*
0	Profiled Cisco IP Phones	48-	IdentityGroup-Name	EQUALS Endpoint Identity Group	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	٥
0	Unincum Compliance Dediced		Network_Ac	cess_Authentication_Passed		x Cisco Tampural Onhoard		Select from list	- 4		
0	control of the second s	AND	Compliance	_Unknown_Devices		(, in the second s	4
				and the state of the state							
0	NonCompliant Davicas Radicad	ANID	Pretwork_Ac	cess_Aumentication_Passed		v Cisco Temporal Onhoard	+	Salart from list			*

규칙에 이름을 입력하고 Conditions(조건) 열 아래에서 + 기호를 선택합니다.

✓ Authori	zation Polic	y (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	r i	٥

속성 편집기 텍스트 상자를 클릭하고 **제목** 아이콘을 클릭합니다. RADIUS *User-Name* 특성을 찾을 때까지 아래로 스크롤하여 선택합니다.

ibrar	у		Editor														
Sea	rch by Name		L	Click to add an attribute													
Q		. 🛛 t 😤	G	Select	attribute f	or condi	tion										:
	BYOD_is_Registered			Q) 🛎	۲	₽	Ĩ	e	,	2	P	©	2	ີ ະ	((:-
	Catalyst_Switch_Local_Web_Authentica tion				Diction	ary				Attribut	e			ID		Info	
	Compliance_Unknown_Devices	0			All Di	ctionaries			~	Attribute	P-User	-Name	2	60)	Ø	^
	Compliant_Devices	0		1	Motorol	a-Symbol				Symbol-	User-G	roup		12		0	
	EAP-MSCHAPv2	0		1	Networ	k Access				AD-Use	-DNS-I	Domair	n			<i>(i)</i>	
	EAP-TLS	0		1	Networ	k Access k Access				AD-User UserNa	r-Join-P me	oint				() ()	
	Guest_Flow			1	Passiv	eID				Passive	ID_Use	ername				<i>i</i>	
	MAC_in_SAN				Radius					User-Na	ime	4		1		0	4
	Network_Access_Authentication_Passe d			1	Ruckus	\$				Ruckus-	User-G	roups		1		(i)	~
	Non_Cisco_Profiled_Phones						-	-			-	-	-		-		-
	Non_Compliant_Devices	0															
	Switch_Local_Web_Authentication																
8	Switch Web Authentication																

Equals를 연산자로 유지하고 *user1*을 연산자 옆에 입력합니다. Use in을 클릭하여 특성을 저장합니 다.

ibrary		Editor			
Search by Name			Radius-User-Nan	ne	
♥ □ ▲ ● 무 및 땀 ២ ♪ . 0	9101	1	Equals	user1	
BYOD_is_Registered	()		Set to 'Is not'		Duplicate
Catalyst_Switch_Local_Web_Auther	ntica 🕧				
Compliance_Unknown_Devices	0			+ New AND OR	
Compliant_Devices	0				
EAP-MSCHAPv2	0				
EAP-TLS	()				
Guest_Flow	0				
MAC_in_SAN	0				
Network_Access_Authentication_Pa	isse (j)				
Non_Cisco_Profiled_Phones	0				
Non_Compliant_Devices	()				
Switch_Local_Web_Authentication					
Switch Web Authentication	()				

이 규칙에 대한 조건이 설정되었습니다.

9단계. **Results/Profiles**(결과/프로파일) 열에서 + 기호를 클릭하고 Create a **New Authorization Profile(새 권한 부여 프로파일 생성)을 선택합니다**.

✓ Author	ization Policy	y (13)					
				Results			
٠	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
/	0	Static IP Address User 1	2 Radius UserName EQUALS user1	Select from list	Select from list 🔹 🕈		¢
				Create a New Authorization Profile			

이름을 지정하고 ACCESS_*ACCEPT*를 **액세스 유형**으로 **유지합니다**. 아래로 스크롤하여 Advance Attributes Settings 섹션**으로** 이동합니다.

Add New Standard Profile		×
Authorization Profile		^
* Name	StaticIPaddressUser1	
Description		
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	344 CSC0 + 10	
Service Template		
Track Movement		
Passive Identity Tracking		
 Common Tasks 		
DACL Name		î
IPv6 DACL Name		
ACL (Filter-ID)		
ACL IPv6 (Filter-ID)		~
 Advanced Attributes 	Settings	~
<		Ze Cancel
		- Sunter

주황색 화살표를 클릭하고 Radius > Framed-IP-Address—[8]를 선택합니다.

Add New Standard Profile Service Template				2
Track Movement				1
Dacsive Identity Tracking				
Passive menocy macking [] (
	Radius			
 Common Tasks 				4
			^	
DACL Name	Egress-VLANID(56)			
	Error-Cause[101]			
IPv6 DACL Name	Filter-ID[11]			
	Framed-AppleTalk-Link[37]			
	Framed-AppleTalk-Network[38]			
ACL (Fitter-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]			
- advanced antillutes conti	Framed-IPv6-Address[168]			
 Advanced Attributes Setting 	9 u Framed-IPv6-Pool[100]			
Radius:Framed-IP-Address				
 Attributes Details 				
Access Type = ACCESS_ACCEPT				
Framed-IP-Address =		11	- 1	٩.
		///.		1
(>	1
		Save	Can	cel

이 사용자에게 항상 정적으로 할당할 IP 주소를 입력하고 Save(저장)를 **클릭합니다**.

Add New Standard Profile		×
Service Template		
Passive submicky mackang ()		
▼ Common Tasks		
Arespace IPv6 ACL Name	^	
ASA VPN		
AVC Profie 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 Car	ncel

10단계. 이제 새로 생성된 권한 부여 프로파일을 선택합니다.

• Author	ization Policy	y (13)							
					Results				
Ŧ	Status	Rule Name	Cond	tions	Profiles		Security Groups	Hits	Actions
Search									
/	0	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	+	Select from list • +		٥
				Window Array	CIDCO_W40ADEI	^			
	\odot	Wireless Black List Default	AND	Interies_nuces	NSP Onboard		Select from list • +	0	٥
				Identifycroup warte Eduwa's Endoom identify Groups Blackist	Non Cisco IP Phones				
	\odot	Profiled Cisco IP Phones	48-	IdentityGroup Name EQUALS Endpoint Identity Groups Profiled Cisco-IP-Phone	PermitAccess		Select from list - +	0	¢
	Ø	Profiled Non Cisco IP Phones	8	Non Cisco Profilad Phones	StaticiPaddressUser1	1	Select from list	0	ö
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		-	undersed united units	Static_IP_address	~			*

이제 권한 부여 규칙이 모두 설정되었습니다. 저장을 클릭합니다.

dudu ident	tity Service	es Engine Home	Context Visibility	Operations	* Policy	Administration	Work Centers					License	Warning 🔺	۹ 0	•
Policy Sets	Profiling	Posture Client Pro	visioning + Policy E	ements											
Policy Se	ets → De	fault									R	eset Policyset	Hitcounts	Reset	Save
	Status	Policy Set Name	Descript	ion	Condi	tions						Allowed Protoc	ols / Server	Sequence	Hits
Search															
	0	Default	Default p	olicy set								Default Network	k Access	× * +	17
> Authen	ntication Po	icy (3)													
> Authori	ization Poli	cy - Local Exceptions													
> Authori	ization Poli	cy - Global Exception	s												
✓ Authori	ization Poli	cy (13)													
									Results						
•	Status	Rule Name	Condit	ons					Profiles	Se	curity Group	15		Hits	Actions
Search															
1	0	Static IP Address Us	er 1 🙎	Radius-User-Name	EQUALS use	er1			× StaticlPaddressUser1	+ 8	elect from list		+		¢

# 다음을 확인합니다.

1단계. Cisco AnyConnect Secure Mobility 클라이언트가 설치된 클라이언트 시스템으로 이동합니 다. FTD 헤드엔드에 연결하고(여기에 Windows 시스템이 사용됨) *user1* 자격 증명*을* 입력합니다.



기어 아이콘(왼쪽 아래 모서리)을 클릭하고 **통계** 탭으로 이동합니다. 할당된 IP 주소가 실제로 이 사 용자에 대해 ISE 권한 부여 정책에 구성된 주소임을 [**주소 정보**] 섹션에서 확인합니다.

🕙 Ci	sco AnyC	Connect Secure Mobility Client	-		×
		VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconneo	ct
00:	00:23				IPv4
Ø	<b>i</b>				uluilu cisco

Cisco AnyConnect Secure Mob	ility Client	_		
AnyCon	nect Secure Mobility Clie	nt		(
rtual Private Network (V	PN)	Diagnostic	s	
eferences Statistics Route Deta	ails Firewall Message History			
				^
Connection Information	<u></u>		- ^	
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				
DYLCS				h.d.

#### FTD의 debug radius all 명령 출력은 다음과 같습니다.

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 로그는 다음과 같습니다. 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

```
ISE의 RADIUS Live 로그에는 다음이 표시됩니다.
```

lvent	5200 Authentication succeeded
Isemame	user!
Indpoint Id	00.50.55.95.45.57 ()
Indpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Statio IP Address User 1
Authorization Result	StaticlPaddressUser1

#### 2021-09-22 23:53:19:72 Source Timestamp Received Timestamp 2021-09-22 23:53:19.72 Policy Server driverap-ISE-2-7 Event 5200 Authenticati user1 Usemame User User Type Endpoint Id 00 50 50 90 40 OF 192.168.0.101 Calling Station Id Windows10-Works Endpoint Profile ntity Store Internal Users Authentication Ide Workstation Identity Group Audit Session Id 004000040000 PAP_ASCI Authentication Method Authentication Protocol PAP_ASCI Network Device DRIVERAP_FT0_7.0 Device Type All Device Types Location All Locations NAS IPv4 Address 0.0.0.0

#### Steps

- Stopp
   Stopp

   11911
   Resided RADUS Access Reservet

   11911
   Resided RADUS Access Reservet

   11911
   Resided RADUS Access Reservet

   11911
   Resided Resord Selection Rulpy

   1091
   Evaluating Service Selection Rulpy

   1091
   Evaluating Selection Rulpy

   1091
   Evaluating Selection Rulpy

   1091
   Evaluation Rulpy

   1091
   Evaluation Rulpy

   1091
   Evaluation Rulpy

   1091
   Evaluation Rulpy

   1092
   From Operating Service Rulpy Rul

- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 24175 Juhrendräcken für uter In Adrian Directory 15035 Erstussting Auforditation Policy 2405 Looing as Dragonic in Internal Endpoints (DStars 2417): Found Endpoint in Internal Endpoints (DStars 2418): Found Endpoint in Internal Endpoints (DStars 2418): Extra Endpoint (Starsmann, Endpoint) 2418 Autor (Starsmann, Stars) 2418 Starsmann, Stars) 2418 Starsmann, Stars 2518 Max assuming passion deade in Session cache 11002 Returned RADUS Access-Accept

en internet of the office	
NAS Port Type	Vitual
Authorization Profile	Static/PaddressUser1
Response Time	51 milliseconds
Other Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Redus
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
CVPN3000/ASA/P0/7x-Tunnel- Group Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0099505-3150-4215-a80e-6753d45bf56o
Is ThirdPartyDeviceFlow	faite
CVPN3000/A SA/PDX7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417494978/23
SelectedAuthenticationIdentity Sto	res Internal Users
Selected Authentication Identity Sto	res All AD Join Points
Selected & theories stical deaths fits	as front then
Authentication Status	AdmentionEnned
Marth Pales Matched Pale	Pada di
Authorization Dalign Matched Dale	State ID Address Lines 1
AuthorizationPolicyMatchedRule	Statio IP Address Geer 1
15t Policy Settlame	Delani
Identity SelectionMatchedRule	Default
DTLS Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types

10400	IDEECAN IDEEC Device Alle
IP SEC	IPSEC#s IPSEC Device#vo
EnableFlag	Enabled
RADIUS Username	user1
Device IP Address	192.168.0.100
CPMSessionID	c0x800040000c000014bc140
Called-Station-ID	192.108.0.100
CiscoAVPair	motil-Investing additionals     motil-Investing additionals     motil-Investing and 2002 69 69 49 491     motil-Investing applicationals     motil-Investing     motil-Investing
esult	
Framed-IP-Address	10.0.50.101
Framed-IP-Address Class	10.0.50.101 CACS x0x800840000x800814bx140 driverap-ISE-2-7/417494978/23
Framed-IP-Address Class cisco-av-pair	10.0.00.101 CACS (da800040000000146);c140 (shiwesp-ISE-0-7)417454978/23 profile-name=Windows10-Workstation
Framed-IP-Address Class cisco-av-pair LicenseTypes	10.0.05.151 CACSI schedoodsdood16sc1e0.chiverap-ISE.2.7417494978-23 profile-name+Window10-Workston Base Icones consumed

2단계. FTD 헤드엔드에 연결하고(여기에 Windows 시스템이 사용됨) 사용자2 자격 증명을 입력합 니다.

S Cisco AnyConnect   192.168.0.100 ×	🚳 Cisco AnyConnect Secure Mobility Client — 🗌	×
Group: RA_VPN ~ Username: user2 Password: *****	VPN:           Contacting 192.168.0.100.           192.168.0.100           Connect	
OK Cancel	<b>\$</b> (i)	ili.ili. cisco

Address Information 섹션에는 할당된 IP 주소가 실제로 FMC를 통해 구성된 IPv4 로컬 풀에서 사용 가능한 첫 번째 IP 주소임을 보여 줍니다.

Sisco AnyConnect Secure Mobil	ity Client	-		×
cisco AnyConi	nect Secure Mobility Client			<b>(</b> )
Virtual Private Network (VF	N)	Diagnostics	s	
Preferences Statistics Route Detai	s Firewall Message History			
Connection Information			_ ^	^
State:	Connected			
Tunnel Mode (IPv4):	Tunnel All Traffic			
Tunnel Mode (IPv6):	Drop All Traffic			
Dynamic Tunnel Exclusion:	None			
Dynamic Tunnel Inclusion:	None			
Duration:	00:01:05			
Session Disconnect:	None			
Management Connection State:	Disconnected (user tunnel active)			
Address Information			- •	
Client (IPv4):	10.0.50.1			
Client (IPv6):	Not Available			
Server:	192.168.0.100			
Bytes	· · · · · · ·		^	~
	Reset	Expo	rt Stats	

FTD의 debug radius all 명령 출력은 다음과 같습니다.

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 로그는 다음과 같습니다.

<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

#### ISE의 RADIUS Live 로그에는 다음이 표시됩니다.

Event	5200 Authentication succeeded
Username	ute/2
Endpoint 1d	00.50.56.96.46.6F B
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess
thentication Details	
Source Timestamp	2021-09-23 00:00:06:488
Received Timestamp	2021-09-23 00:00:08:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
2semame	user2
Jser Type	User
Endpoint Id	00.50.56.96.46.6F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users
identity Group	Workstation
identity Group Audit Session Id	Workstation dba800540000d000614bc357
dentity Group Audit Session Id Authentication Method	Volstation cha8005400004000614bc387 PAP_ASCII
dentity Group Audit Session Id Authentication Method Authentication Protocol	Wotekation dba800064000030008146c587 PAP_ASCII PAP_ASCII
dentity Group kudit Session Id Authentication Method Authentication Protocol Setwork Device	Wotalson data0004-00000000000000000000000000000000

NAS Port Type	Vitual
Authorization Profile	PermitAccess
Response Time	202 milliseconds
ther Attributes	
ConfigWersionid	140
DestinationPort	1812
Protocol	Radius
NAS-Port	63248
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101
CVPH3000/ASA/PIX7x-Tunnel- Group Name	RA_VPN
OriginalUserName	use/2
NetworkDeviceProfileId	b0099505-3150-4215-a80e-8753d45b/55c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PDC7x-Client-Type	2
AcsSessionID	driverap-ISE-2-7/417484978/24
SelectedAuthenticationIdentityStor	res Internal Users
SelectedAuthenticationIdentityStor	res All_AD_Join_Points
SelectedAuthenticationIdentityStor	res Quest Users
Authentication Status	AuthenticationPassed
identityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
15EPolicySettame	Default
identity SelectionMatchedRule	Default
DTL5Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

1902 . 445 (K. 2008). 694 4 10 2008). 994 (K. 442) 2008 . 994 (K.
1307. 4804. 4804. 4804. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 4904. 49
1392, -46-65, 10.02086, Sons 4, 10.02086, S674BAA2AE20083, 84408586C717E370388C01 Hol857,
302. .48.05. ne Vihal Platom, 56/48A42420083. 84408598C717E37D388C01 w387.
tion

**참고:** AnyConnect 클라이언트 간의 중복 IP 주소 충돌을 방지하려면 FTD IP 로컬 풀 및 ISE 권한 부여 정책 모두에서 IP 주소 할당에 서로 다른 IP 주소 범위를 사용해야 합니다. 이 컨피 그레이션 예에서 FTD는 10.0.50.1~10.0.50.100의 IPv4 로컬 풀로 구성되었으며 ISE 서버는 10.0.50.101의 고정 IP 주소를 할당합니다.

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

FTD에서:

• 디버그 radius 모두 ISE에서:

• RADIUS 라이브 로그