Configure Static IP Address Assignment to AnyConnect Users via RADIUS Authorization

Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Configure Remote Access VPN with AAA/RADIUS Authentication via FMC Configure Authorization Policy on ISE (RADIUS Server) Verify Troubleshoot

Introduction

This document describes how to configure RADIUS Authorization with an Identity Services Engine (ISE) server so it always forwards the same IP address to the Firepower Threat Defense (FTD) for a specific Cisco AnyConnect Secure Mobility Client user via the RADIUS Attribute 8 Framed-IP-Address.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configure Remote Access VPN with AAA/RADIUS Authentication via FMC

For a step-by-step procedure, refer to this document and this video:

- AnyConnect Remote Access VPN Configuration on FTD
- Initial AnyConnect Configuration for FTD Managed by FMC

Remote Access VPN configuration on the FTD CLI is:

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
```

Configure Authorization Policy on ISE (RADIUS Server)

Step 1. Log in to the ISE server and navigate to **Administration > Network Resources > Network Devices**.

dealer Identity Services Engine	Home	 Context Visibility 	Operations	Policy	•/	Administration > Work Cent	ers				License Warning 🔺	۹ . ا	o o
Summary Endpol	nts Gues	ts Vulnerability	Threat	+	S	iystem	Network Resources	pxGrid Services					φ.
METRICS Total E	ndpoints 0	1	Active Endpo	oints O	lo	Urgsofmen Licensing Centificates Looping Maintenance Upgrade Backup & Restere Admin Access Settings Settings Settings Settings Settings Settings	Network Device Groups Network Device Profiles Entremi RADUS Servers RADIUS Server Sequences NAC Managers Externi MDM Location Services Device Portal Management Blackist BYOD Certificate Provisioning	Feed Service Profiler Threat Centric NAC Third Party Vendors	-	Authenticated Guests 0	BYOD Endpoints 0	0	0 - 0 ,
AUTHENTICATIO Identity Store Identity Group	NS Ø Network Device	Failure Reason		0 0)	External Identity Sources Identity Source Sequences Settings	Client Provisioning Mobile Device Management My Devices Custom Portal Files Settings		×	ENDPOINTS Prote		Ø	ΩX
interusen:: [10	9%]	C				drivea5506: (00%]			workstations: [100%]	2		
# BYOD ENDPOINT	S 0			øø	×	# ALARMS ⁰		0 9	x	# SYSTEM SUMMARY 0		ø	øх
Type Profile						Severity Name	Occu Last Oc	curred	^	1 node(s)		All -	24HR -
	No d	ata available.				✓ Name				driverap-ISE-2-7	man linna Ar	abantication I a	
						DNS Resolu	tion Failure 941 less than	n 1 min ago		CPU Me	nuny unage AL	And the care of La	noney.
ntps://10.31.124.31:6012/adm	n/#administra	ationyadministratio	n_networkresou	urces/admi	inistrat	tion_netwoncresources_dev	ICES a least 4600 loss that	1 min 200					

Step 2. In the Network Devices section, click **Add** so ISE can process RADIUS Access Requests from the FTD.

System + Methods: Resource + Deckor Portal Management + Network: Deckor Bortal Management Beckor B Tass + Deckor Bortal Management + Network: Deckor Bortal Management Beckor B Tass + Deckor Bortal Management + Network: Deckor Bortal Management + Network: Deckor Bortal Management Beckor B Tass + Deckor Bortal Management + Network: Deckor Bortal Management Beckor B Tass + Deckor Bortal Management + Network: Deckor Bortal Management + Deckor Bortal Manage	
Hotron Devices Network Devices N	
Intervices Network Devices Selected 2 [street PAC Selected 2 [street P	
Instruct Selected 0 [Total 1 @ @ Device Security Settings / Esting 20-backale @ those 1 @ Deport @ Depo	
Delaut Device <pre></pre>	
Device Security Settings / Lot / Lot / Doubles/ Definent RAC Xolete * Show / M * Name * Profile Name Location Type Description CRNVERNP_ADA5506 172.16.255.2	
Name IP/Mask Profile Name Location Type Description DRV/ERVP_ABA5506 172.16.255.2 #2 Occo ® All Locations All Device Types	5
CRIVERAP_A64556 172.16.255.2 db Cloro 19 Al Locations Al Device Types	

Enter the network device **Name** and **IP Address** fields and then check **RADIUS Authentication Settings** box. The **Shared Secret** must be the same value that was used when the RADIUS Server object on FMC was created.

dentity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🔍	0 0	• ^
System Identity Management	Hotwork Resources Device Portal Management psGrid Service Feed Service Threat Centric NAC			
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM → Location Services			
0				
Network Devices	Network Devices Lists New Network Device			
Default Device	* News ORDERS TO TO			
Device Security Settings	Particles Control - Contro			
	[₽ Address • * * P: 192.168.0.100 / 32	ŵ•		
	* Device Profile 🗰 Ciscol 👻 🕀			
	Model Name v			
	Software Version 📃 👻			
	* Network Device Group			
	Location Al Locations O Set. To Default			
	IPSEC Is IPSEC Device 📀 Set. To Default			
	Device Type 🛛 Al Device Types 🕐 🔰 Set. To Default			
	PADIUS Authentication Settings			
	RADIUS UDP Settings			- 1
	Protocol RADRUS			
	Shared Secret Show			
	Use Second Shared Secret 🗌 🕢			
	Show			
	CoA Port 1700 Set.To.Default			
	RADIUS DTLS Settings (2)			
	DILS Required a			~

Save it with the button at the end of this page.

Step 3. Navigate to Administration > Identity Management > Identities.

dealer Identity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Center	15		License Warring 🔺 🔍 😐 🔿 🗘
System Identity Management	Network Resources Device Portal Management pxGrid	System	Network Resources	pxGrid Services	
Network Devices Network Device C	Groups Network Device Profiles External RADIUS Servers	Deployment	Network Devices Network Device Groups	Feed Service	
0		Certificates	Network Device Profiles	Profiler	
Network Devices	Network Devices	Logging Maintenance	External RADIUS Servers RADIUS Server Seguences	Third Party Vendors	
Default Device		Upgrade	NAC Managers		Selected 0 Total 2 😻 🚭 🖬
Device Security Settings	/ Edit	Admin Access	External MDM Location Services		Show AI * 16
	Name P/Mask Profile Name	Settings	Device Portal Management		
	DRMERAP.F. 192.168.0.10 # Osco @	Identity Management	Blacklist		
		Groups	Certificate Provisioning		
		External Identity Sources	Client Provisioning		
		Settings	My Devices		
			Custom Portal Files		
			otterige		
https://10.31.124.31:6012/admin/#a	idministration/administration_identitymanagement/adi	ministration_identitymanagemen	t_identities		

Step 4. In the Network Access Users section, click **Add** in order to create *user1* in ISE's local database.



Enter username and password in the Name and Login Password fields, and then click Submit.

deather 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 NAC		
Identities Groups External Identity	Sources I dentity Source Sequences + Settings		
0			
Users	Vertorst Access User Luis > new network Access User		
Latest Manual Network Scan Res	*Name useri		
	Status 💟 Enabled +		
	Emai		
	▼ Passwords		
	Pássword Type: Internal Users •		
	Password Re-Enter Password		
	*Login Password		
	Enable Password 0		
	* User Information		
	FirstName		
	Latitiane		
	▼ Account Options		
	Description		
	Change password on next login		11
	▼ Account Disable Policy		•
	Disable account date exceeds 2021-11-21 (vyy-mm-dd)		
			. •
	▼ User Groups		
	Select an tem 📀 — +		
	Subwr Cancel		
<			>

Step 5. Repeat the previous steps in order to create *user2*.



Step 6. Navigate to **Policy > Policy Sets**.



Step 7. Click the arrow > on the right side of the screen.

-thu CIS	tder	ntity Service	es Engine Home + Con	text Visibility + Operations	Policy Administration	Work Centers License Warning A			
P	olicy Set	s Profiling	Posture Client Provisioning	Policy Elements					
Po	olicy S	ets				Reset Policyset Hitcounts	Reset	Save	Ð
	+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits A	ctions	View	
1	earch								
						+			
								_	-
		\odot	Default	Default policy set		Default Network Access * * 🕈 17	¢	>	1
									-
							Reset	Save	

Step 8. Click the arrow > next to **Authorization Policy** to expand it. Now, Click the + symbol in order to add a new rule.

dente ident	tity Services	Engine Home + Contex	d Visibilit)	y Operations	* Policy	Administration	• Work C	Centers												Licens	e Warning	<u>s</u>		o o	
Policy Sets	Profiling	Posture Client Provisioning	 Policy E 	Elements																					
Policy Se	ets → Defa	ault																	Reset	Policyse	rt Hitcoun	s Re	set	Save	
	Status	Policy Set Name	Descrip	tion	Cond	tions													Allow	ved Proto	ocols / Sen	er Sequen	ce	Hits	
Search																									
	0	Default	Default p	policy set															Def	lault Netwo	ork Access	**	+	17	
> Authen	tication Poli	icy (3)																							
> Author	ization Polic	y - Local Exceptions																							
> Author	zation Polic	y - Global Exceptions																							
¥ Author	ization Police	v (13)																							
. Autor	CONVERT ONLY	1.151																							
•													Re	esults											1
	Status	Rule Name	Condi	tions									Pr	rofiles				Security Gr	oups			Hits	A	ctions	
Search																									
	0	Wireless Black List Default		Wireless_A	ccess									× Blackhole	Wireless A	ccess	+	Select from	list		- +			ö	
	Ŭ		AND	at IdentityGrou	p-Name EQ	UALS Endpoint Iden	tity Groups:Bl	acklist					G									Ť		*	
	0	Profiled Cisco IP Phones	44	IdentityGroup-Name	EQUALS Er	idpoint Identity Group	is Profiled Cis	co-IP-Pho	hone					× Cisco_IP_	hones		+	Select from	list		• +	0		٥	i
	0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled	Phones									× Non_Ciso	_IP_Phone	5	+	Select from	list		• +	0		٥	I
	0			Network_Ac	cess_Authe	ntication_Passed								- Oi				Palasthan						~	I
	Ø	Unknown_Compliance_Redired	AND	Compliance	_Unknown_	Devices								- Grad0_1er	poral_Unot	var u		Jeneral Intern	1125			0		¥	
	0			Network_Ac	cess_Authe	ntication_Passed												Contract							
	0	NonCompliant_Devices_Redirect	AND	Non_Comp	iant_Device	5								× Cisco_Ter	iporal_Onbi	oard	+	Serect from	nst		• +	0		¢	

Provide a name to the rule an select the + symbol under **Conditions** column.

✓ Authori	zation Polic	y (13)						
					Results			
٠	Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Search								
1	ø	Static IP Address User 1		+	Select from list	Select from list	+	٥

Click in the Attribute Editor textbox and click the **Subject** icon. Scroll down until you find *RADIUS User-Name* attribute and choose it.

Library			Editor														
Searc	h by Name		0	Clic	k to ad	d an attribu	te										
♥ 🛱		0 t 😤	B	Select	attribut	e for condi	ion										
	BYOD_is_Registered	0		0	Ē	□ &	۲	<u> </u>	Ţ	F	ு	2	Ē	© ,	1 C	ີ່ຮ	(;
	Catalyst_Switch_Local_Web_Authentica tion	1			Dict	ionary				Attribut	e)	Info	
	Compliance_Unknown_Devices	0		1	Al	l Dictionaries osoft			~	Attribut	e \P-Use	r-Name)	6	0	()	^
	Compliant_Devices			1	Moto	orola-Symbol				Symbol	User-G	Group		1	2	()	
	EAP-MSCHAPv2	<i>(</i>)		1	Netv	vork Access				AD-Use	r-DNS-	Domair	n			(i)	
	EAP-TLS	0		1	Netv	vork Access				AD-Use UserNa	r-Join-F me	Point				(i) (i)	
	Guest_Flow	1		1	Pas	siveID				Passive	ID_Us	ername				()	
	MAC_in_SAN	()		1	Rad	ius				User-Na	ame			1		0	٩,
	Network_Access_Authentication_Passe d	0		1	Rad	ius kus				User-Pa Ruckus	usswor	d Groups		2		(j) (j)	~
	Non_Cisco_Profiled_Phones	1			-		-	-		-	-	-	-	-	-	-	-
	Non_Compliant_Devices																
	Switch_Local_Web_Authentication	<i>i</i>															
	Switch Web Authentication																

Keep **Equals** as the operator and enter *user1* in the text box next to it. Click **Use** in order to save the attribute.

rary	Editor		
earch by Name		Radius-User-Name	
) 1 O b 🖘 🔟	Equals V user1	
BYOD_is_Registered	0	Set to 'Is not'	Duplicate
Catalyst_Switch_Local_Web_Authen tion	tica 🥡		
Compliance_Unknown_Devices	0	+ New A	AND OR
Compliant_Devices	0		
EAP-MSCHAPv2	0		
EAP-TLS	0		
Guest_Flow	0		
MAC_in_SAN	0		
Network_Access_Authentication_Pas d	sse ()		
Non_Cisco_Profiled_Phones	0		
Non_Compliant_Devices			
Switch_Local_Web_Authentication	0		
Switch Web Authentication			

The condition for this rule is now set.

Step 9. In the **Results/Profiles** column, click the + symbol and choose **Create a New Authorization Profile**.

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

Give it a **Name** and keep *ACCESS_ACCEPT* as the **Access Type**. Scroll down to the **Advance Attributes Settings** section.

Add New Standard Profile		2
Authorization Profile		^
* Name	StaticIPaddressUser1	
Description		
* Access Type	ACCESS_ACCEPT *	
Network Device Profile	And Cisco v t	
Service Template		
Track Movement		
Passive Identity Tracking		
▼ Common Tasks		^
DACL Name		
IPv6 DACL Name		
ACL (Filter-ID)		
ACL IPv6 (Filter-ID)		~
 Advanced Attributes 	Settings	~
<	Sav	e Cancel

Click the orange arrow and choose **Radius > Framed-IP-Address--[8]**.

Add New Standard Profile Service Template			^	×
Track Movement				
Passive Identity Tracking				
	Dadies			
	Kadus			
 Common Tasks 				
		· · · · · · · · · · · · · · · · · · ·	^	
DACL Name	Egress-VLANID[56]			
	Error-Cause[101]			
IPv6 DACL Name	Filter-ID-[11]			
	Framed-AppleTalk-Link[37]			
	Framed-AppleTalk-Network[38]			
ACL (Fifter-ID)	Framed-AppleTalk-Zone[39]			
	Framed-Compression[13]			
ACL IPv6 (Filter-ID)	Framed-Interface-Id[96]		~	
	# Framed-IP-Address[8]			
	Framed-IP-Netmask[9]			
	Framed-IPv6-Address[168]			
 Advanced Attributes Settin 	9 🗉 Framed-IPv6-Pool[100]			
Radius:Framed-IP-Address				
 Attributes Details 				
Access Tune - ACCESS ACCEDT				
Framed-IP-Address =				
		11.	~	
<			>	
		Save	Cance	n
				-

Type the IP address that you want to statically assign always to this user and click **Save**.

Add New Standard Profile		×
Service Template		^
Common Tasks Aresoace 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	▼ Incel

Step 10. Now, choose the newly created Authorization Profile.

 Autho 	ization Polic	y (13)							
					Results				
T	Status	Rule Name	Cond	itions	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
				Hindare Armer	CIPCO_W40ADEI	^			
	0	Wireless Black List Default	AND	Interess_nucless	NSP Onhoused		Select from list 🔹 🕈	0	Ф
				identifycolop warne Estowel's Euclopic identify Groups Brackist	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	٥
	0	Profiled Non Cisco IP Phones	E	Non Cisco Profiled Phones	StaticlPaddressUser1	1	Select from list +	0	ò
			-		Static_IP_address			1	*

The Authorization rule is now all set. Click **Save**.

dada ide	ntity Service	es Engine Home	Context Visibility	Operations	* Policy	+ Administration	Work Centers	s			License Warning 🤞	<u> </u>	• •
Policy Set	ts Profiling	Posture Client Pr	ovisioning + Policy E	lements									
Policy S	lets → De	fault								•	Reset Policyset Hitcount	s Rese	Save
	Status	Policy Set Name	Descrip	tion	Condi	tions					Allowed Protocols / Serve	er Sequence	Hits
Search													
	0	Default	Default p	olicy set							Default Network Access	x * +	17
> Authe	entication Po	blicy (3)											
> Autho	vization Poli	icy - Local Exception											
> Autho	vrization Poli	icy - Global Exception	15										
✓ Author	vrization Poli	icy (13)											
									Results				
•	Status	Rule Name	Condi	ions					Profiles	Security Grou	ips	Hits	Actions
Search													
1	0	Static IP Address U	ier 1 🚨	Radius-User-Name	EQUALS use	er1			× StaticlPaddressUser1	+ Select from lis	• • •		\$

Verify

Step 1. Navigate to your client machine where the Cisco AnyConnect Secure Mobility client is installed. Connect to your FTD headend (a Windows machine is used here) and enter the *user1* credentials.



Click the gear icon (lower left corner) and navigate to the **Statistics** tab. Confirm in the **Address Information** section that the IP address assigned is indeed the one configured on ISE Authorization policy for this user.

🕙 Cisco AnyC	onnect Secure Mobility Client	-		×
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:23		_	IPv	4
۞			alı cı	ulu sco

Cisco AnyConnect Secure Mobi	ility Client	_		
AnyCon	nect Secure Mobility Client			(
rtual Private Network (V	PN)	Diagnostic	s	
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			- •	
-				Υ.

The debug radius all command output on FTD shows:

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) <omitted output> 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 The FTD logs show: 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 <DfltGrpPolicy> User <user1> IP <192.168.0.101> IPv4 Address <10.0.50.101> IPv6 address <::> assigned to session The RADIUS Live logs on ISE show:

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00.50.56.96.46.6F (0
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Static IP Address User 1
Authorization Result	StaticIPaddressUser1

2021-09-22 23:63:19.72 Source Timestamp 2021-09-22 23:53:19.72 Received Tin Policy Serve driverap-ISE-2-7 Event 5200 Authenticat user1 User 00 50 50 90 40 OF 192.168.0.101 Calling Static Windows10-Workst Internal Users Authentication I Workstation Audit Session Id 04800840000 PAP_ASCI Authentication Method PAP_ASCII DRIVERAP_FTD_7.0 Authentication Protocol Network Device All Device Types Device Type Location All Locations 0.0.0.0 NAS IPv4 Address

Steps

- Stopp
 Stopp

 11011
 Resided RADUS Access Respect

 11011
 Resided RADUS Access Respect

 10010
 Evaluating Revise StateMonth

 10010
 Evaluating Servise StateMonth

 10011
 Evaluating Servise StateMonth

 10012
 Evaluating Servise StateMonth

 10013
 Evaluating Servise StateMonth

 10014
 Durates Revise StateMonth

 10015
 Evaluating Servise StateMonth

 10015
 Evaluating Servise StateMonth

 10015
 Evaluating Servise StateMonth

 10015
 Evaluating Servise StateMonth

 10016
 Evaluating Servise StateMonth

 10016
 Evaluating Servise StateMonth

 10017
 Evaluating Servise StateMonth

 10018
 Evaluating Servise StateMonth

 10018
 Evaluation Pased

 10018
 Evaluation Pased

 10018
 Evaluation Pased

 10018
 Evaluation Pased

- 24715 ISE has not confirmed locally previous su authentication for user in Active Directory
- 2415 auchentication for use in Advis Denotiny 1908: Evaluating Authentication Philos 2009: Looing as Endpaint in Internal Endpaint DStare 2421: Found Endpaint in Internal Endpaints DStare 2420: Found Endpaint in Internal Endpaints DStare 2420: Found Endpaint in Internal Endpaints DStare 2420: Statuset Authorization Philis StatistPedevacub 2020: Statuset Authorization Philis StatistPedevacub 2020: New accumpting seals on testis in Sealson cache 11002: Returned RADUS Access-Accept

NAS Port Type	Vitual	
Authorization Profile	StatidPaddressUser1	
Response Time	51 milliseconds	
		_
her Attributes		
ConfigWersionId	140	
DestinationPort	1812	
Protocol	Radius	
NA5-Port	49152	
Tunnel-Client-Endpoint	(tag=0) 192.108.0.101	
CVPN3000/ASA/PDC7x-3unnel- Group Name	RA_VPN	
OriginalUserflame	user1	
NetworkDeviceProfileId	b0099505-3150-4215-a80e-6753d45b/50c	
IsThirdPartyDeviceFlow	false	
CVPN3000/ASA/PO/7x-Client-Type	2	
AcsSessionID	driverap-15E-2-7/417494978/23	
SelectedAuthenticationIdentityStor	es Internal Users	
SelectedAuthenticationIdentityStor	es All_AD_Join_Points	
SelectedAuthenticationIdentityStor	es Guest Users	
Authentication Status	AuthenticationPassed	
IdentityPolicyMatchedRule	Default	
AuthorizationPolicyMatchedRule	Statio IP Address User 1	
1SEPolicySetName	Default	
Identity Selection Matched Rule	Default	
DTL S Support	Unknown	
HostidentityGroup	Endpoint Identity Groups Profiled Workstation	
Network Device Profile	Cisco	
Location	Location#All Locations	
Device Type	Device Tune#All Device Tunes	

Class cisco-av-pair LicenseTypes	profile-name*Windows10-Workstation Base license consumed
Class cisco-av-pair	profile-name=Windows10-Workstation
Class	
	CACS: dba500540000.d00814bc1d0 driverap-ISE-2-7/417494978/23
soult	10 0.00.101
Called-Station-ID	112:168.0.100 mdb III-location g/stafformenit, mdb III-location march ¹⁰ :05:05:06.4.0.0; mdb III-location march ¹⁰ :05:05:06.4.0.0; mdb III-location march ¹⁰ :05:05:06.00; mdb III-location march ¹⁰ :05:05:06.00; mdb III-location march ¹⁰ :05:06:06; mdb III-location march ¹⁰ :05:06:06; mdb III-location march ¹⁰ :05:06; mdb III-location march ¹⁰ :06:06; md III-location march ¹⁰ :06; md II
CPMSessionID	c0a800040000c000014bc1d0
RADIUS Username	user1 192 148 0 100
Endoreriag	Enabled

Step 2. Connect to your FTD headend (a Windows machine is used here) and enter the user2 credentials.

	Greater and connect occure mobility energy of the
Group: RA_VPN ~ Username: user2	VPN: Contacting 192.168.0.100.
Password: ******	

The **Address Information** section shows that the IP address assigned is indeed the first IP address available in the IPv4 local pool configured via FMC.

🚳 Cisco AnyConnect Secure Mobi	lity Client	—		×
cisco AnyCon	nect Secure Mobility Clien	t		()
Virtual Private Network (V	PN)	Diagnosti	cs	
Preferences Statistics Route Deta	ails Firewall Message History		24	
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	Exp	ort Stats.	

The debug radius all command output on FTD shows:

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)
<omitted output>

RADIUS packet decode (response)

The FTD logs show:

_____ 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

<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 <DfltGrpPolicy> User <user2> IP <192.168.0.101> IPv4 Address <10.0.50.1> IPv6 address <::> assigned to session

The RADIUS Live logs on ISE show:

Event	5200 Authentication succeeded
Usemane	uer2
Endpoint Id	00.50.56.96.40.6F 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 00:00:08:488
Received Timestamp	2021-09-23 00:00:08:488
Policy Server	driverap-ISE-2-7
Event	5200 Authentication succeeded
Usemanie	use/2
User Type	User
Endpoint Id	00.50.50.90.45.0F
Calling Station Id	192.168.0.101
Endpoint Profile	Windows10-Workstation
Authentication identity Store	Internal Users
identity Group	Workstation
	d3a800540000d000514bc387
Audit Session Id	PAR 4878
Audit Session Id Authentication Method	PAP JADA
Audit Session Id Authentication Method Authentication Protocol	PAP_ASCI
Audit Session Id Authentication Method Authentication Protocol Network Device	PAP_ASCI DRIVERAP_FTD_7.0

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS greated a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType (4 times
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - user2
24212	Found User in Internal Users IDStore
22037	Authentication Passed
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - user2
24211	Found Endpoint in Internal Endpoints IDStore
15048	Queried PIP - Radius User-Name
15048	Queried PIP - Radius NAS-Port-Type
15048	Queried PIP - EndPoints LogicalPhofile
15048	Queried PIP - Network Access AuthenticationStatus
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache

Vitual	
PermitAccess 202 milliseconds	
140	
1812	
Radius	
53248	
(tag=0) 192.168.0.101	
RA_VPN	
use2	
b0899505-3150-4215-a00e-8753d45b/56o	
false	
2	
driverap-158-2-7/417494978/24	
es Internal Users	
es All_AD_Join_Points	
es Quest Users	
AuthenticationPassed	
Default	
Basic_Authenticated_Access	
Default	
Default	
Unknown	
Endpoint Identity Groups Profiled Workstation	
Cisco	
Location#All Locations	
Device Type#All Device Types	
IPSEC#6 IPSEC Device#No	
Endpoint Identity Groups Profiled Workstation	

EnableFtag	Enabled
RADIUS Username	use2
Device IP Address	192.168.0.100
CPMSessionID	dba800540000d000514bc357
Called-Station-ID	192.168.0.100
Liscoff/Pair	Indo Bindeolog Jattimovals, moto Hindeolog Jattimovals, moto Hindeolog Jattimovals, moto Hindeolog Jattimovals, Bit 1302 moto Hindeolog Jattimovals, Bit 1302 moto Hindeolog Jattimovals, Bit 1302 moto Hindeolog Jattimovals, Bit 1302 moto Hindeolog Jattimovals, Bit 1302 paralest Hindeolog Para Jattimoval Hondeologi paralest Hindeolog Para Jattimoval Hondeologi Makada Bit 100, 100, 101, 102, 101, Bit Handeologi, Bit 101, Bit 101,
sult	
Class	CACS:c0a800840000d000814bc387.driverap-ISE-2-7/417484978/24
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

Note: You must use different IP address ranges for IP address assignment on both FTD ip local pool and ISE Authorization policies in order to avoid duplicate IP address conflicts

among your AnyConnect Clients. In this configuration example, FTD was configured with an IPv4 local pool from 10.0.50.1 through 10.0.50.100 and ISE server assigns static IP address of 10.0.50.101.

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

On FTD:

• debug radius all On ISE:

• RADIUS live logs