Configureer statische IP-adrestoewijzing aan AnyConnect-gebruikers via RADIUS-autorisatie

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Remote Access VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren machtigingsbeleid op ISE (RADIUS-server) configureren Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u RADIUS-autorisatie met een ISE-server (Identity Services Engine) kunt configureren, zodat altijd hetzelfde IP-adres naar het Firepower Threat Defense (FTD) wordt verzonden voor een specifieke Cisco AnyConnect Secure Mobility Client-gebruiker via het RADIUS-kenmerk 8 framed-IP-adres.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FTD
- FireSIGHT Management Center (FMC)
- ISE
- Cisco AnyConnect beveiligde mobiliteit-client
- RADIUS-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- FMCv 7.0.0 (bouw 94)
- FTDv 7.0.0 (gebouwd 94)
- ISE 2.7.0.356
- AnyConnect 4.10.2086
- Windows 10 Pro

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

Configureren

Netwerkdiagram



Remote Access VPN-verificatie met AAA/RADIUS-verificatie via FMC configureren

Verwijs voor een stap voor stap naar dit document en deze video:

- AnyConnect Remote Access VPN-configuratie op FTD
- Initiële AnyConnect-configuratie voor FTD beheerde door FMC

Remote Access VPN-configuratie op de 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
```

machtigingsbeleid op ISE (RADIUS-server) configureren

tunnel-group RA_VPN webvpn-attributes

group-alias RA_VPN enable

Stap 1. Meld u aan bij de ISE-server en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**.

deate Identity Services Engine	Home	Context Visibility	Operations	Policy	- Administra	tion • Work	Centers					Licens	e Warning 🔺 🔍		5 f
Summary Endpoints	Guests	Vulnerability	Threat	+	System		Network	Resources	pxGrid Services					¢.	-
METRICS Total Endpol	ints 0	1	Active Endpo	vints Ø	Licensing Certificate: Logging Maintenan Upgrade Backup & I Admin Acc Settings Identities Groups	i ce Restore ess sagement	Network Network External RADIUS NAC Ma External Location Device P Blacklis BYOD Centrics	Cherice Groups R Device Profiles i RADIUS Servers Server Sequences anagers MDM n Senices ortal Management it ate Provisioning	Feed Service Profiler Threat Centric NAC Third Party Vendors	-	Authenticated Guests @	BYOD Endp	oints 0	- 0 0; >	
AUTHENTICATIONS	ork Device	Failure Reason		80	External Id Identity So Settings	entity Sources arce Sequences	Client P Mobile (My Devi Custom Settings	Provisioning Device Management ices 1 Portal Files 8		×	ENDPOINTS			e o x	
inter_ussens: [100%]_	(2				drivea550	D6: [100%]	0			workstations: [1				
₿ BYOD ENDPOINTS ●				0 9	×	ALARMS 0			6	дaх	# SYSTEM SUMM	ARY O		gox	
Type Profile					Seve	rity Name		Occu Last O	ccurred	^	1 node(s)			All = 24HR =	
	No dat	a available.				¥ Name					driverap-ISE-2-7	Memory Lisage	Authentics	ition Latency	
tor://10.21.124.21:6012/admin/#a	desisietesti	on/administration	naturatives	ureae (admi	nistration cot	DNS Re	esolution Failure	941 less that	n 1 min ago		010		Patricia		
short in a rule a rule relagimit a	on mon aux	on you minimise action	Chermonicesou	in coy aumi		ional esources.	previnces a lagenti	4600 loss the	0.1 min 200						×

Stap 2. Klik in het gedeelte Network Devices op **Add** zodat ISE RADIUS-toegangsaanvragen van de FTD kan verwerken.

dentity Services Engine	Home Context Visibility	 Operations 	Policy Administr	ation + Work Centers			License Warning 🔺	9 9 9 9
System Identity Management	Network Resources Device	ce Portal Manager	nent pxGrid Services + F	eed Service + Threat Centric	NAC			
·Network Devices Network Device G	roups Network Device Profile	s External RAD	IUS Servers RADIUS Serve	r Sequences NAC Managers	External MDM Location Services			
•								
Network Devices	Network Devices							
Default Device							Selecte	d 0 Total 1 🧐 🚰 🗸
Device Security Settings	/Edit -Add ChDupicate	Dimport @	Export • OGenerate PAC	X Delete *			Show AI	- 8
	Name 🔺	IP/Mask	Profile Name	Location	Type	Description		
	DRIVERAP_ASA5506	172.16.255.2	🟥 Cisco 🙂	All Locations	All Device Types			

Voer de velden Naam en IP-adres van het netwerkapparaat in en controleer vervolgens RADIUSverificatie-instellingen. Het Gedeeld Gebied moet dezelfde waarde zijn die is gebruikt toen het object RADIUS Server op FMC is gemaakt.

dentity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🍳 😐 🧿 🔿 🏠
System Identity Management	Herknerk Resources Herknerk Resource	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Servers RADIUS Servers NAC Managers External MDM + Location Services	
0		
Network Devices	Network Devices List > New Retwork Device	
Default Device		
Device Security Settings	name DRIVERAP_FTD_7.0	
	Lieschgeon	
		ŵ•
	* Device Protite (ab Cisco) • 0	
	Model Name	
	Software Version +	
	* Network Device Group	
	Location Al Locations O Set. To Default	
	IPSEC Is INSECTORY OF Sector Contract	
	In Advise 1943	
	rRADUS Authentication Settings	
	RADIUS UOP Settings	
	Protocol RADIUS Shared Secret	
	Use Second Shared Secret 🗌 🖗	
	Show	
	CoA Port 1700 Set To Default	
	RADRUS DTL.S Settings @	
	DTLS Required 🗖 🕖	~

Sla deze op met de knop aan het einde van deze pagina.

Stap 3. Navigeer naar Administratie > identiteitsbeheer > Identificatiegegevens.

dealer Identity Services Engine	Home + Context Visibility + Operations + F	licy Administration Work Cente	45		License Warning 🔺 🔍 😐 🔿 🔿
System Identity Management	Network Resources Device Portal Management	Grid E System	Network Resources	pxGrid Services	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Ser	rs Deployment	Network Devices	Feed Service	
0		Certificates	Network Device Profiles	Profiler	
Network Devices	Network Devices	Logging Maintenance	External RADIUS Servers RADIUS Server Sequences	Threat Centric NAC Third Party Vendors	
Default Device		Upgrade	NAC Managers		Salected 0 Total 2 😵 🥁 🚽
Device Security Settings	/Edit -Add LaDupicate @Import @Export	OG Backup & Restore	External MDM Location Services		Show Al 🔪
	Name - IP/Mask Profile Name	Settings	Device Portal Management		
	DRIVERAP_A. 172.16.200.2	Identity Management	Blacklist		
		Identities	BYOD Certificate Provisioning		
		External Identity Sources	Client Provisioning		
		Identity Source Sequences Settings	Mobile Device Management My Devices		
			Custom Portal Files		
			Settings		
https://10.31.124.31:6012/admin/#a	administration/administration_identitymanageme	t/administration_identitymanagement	nt_identities		

Stap 4. Klik in het gedeelte Gebruikers van netwerktoegang op **Add** om *user1* te maken in de lokale database van ISE.



Voer een gebruikersnaam en wachtwoord in in de velden **Naam** en **Wachtwoord voor aanmelding** en klik vervolgens op **Indienen**.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺		5 ⁴
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC			
·Identities Groups External Iden	atly Sources I identity Source Sequences → Settings			
0				
Users	Network Access Users List > New Network Access User			
Latest Manual Network Scan Res	Network Access User Name User Status Construction			
	Enai			
	* Passwords			
	Password Type: Internal Users +			
	Password Re-Enter Password			
	*Login Password - Generate Password ()			
	Enable Password Generate Password ()			
	▼ User Information			
	First Name			
	LastName			
	Account Options			
	Description			
	Change password on next login			- 1
	▼ Account Disable Policy			-1
	Disable account if date exceeds 2021-11-21 (yyy-mm-dd)			
	• User Groups			
	Sekct an tem O - +			
	Storel Ganal			
<				>

Stap 5. Herhaal de vorige stappen om *gebruiker2* te maken.



Stap 6. Navigeer naar **beleid > Beleidsformaten**.



Stap 7. Klik op de pijl >rechts van het scherm.

adaada cisco	identity Servic	es Engine Home + Con	text Visibility	Policy Administration Work Centers			License Warning		
Polic	r Sets Profilin	g Posture Client Provisioning	Policy Elements						
Polic	y Sets					•	eset Policyset Hitcou	nts Reset	Save
+	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server	Sequence Hits	Actions	View
Sea	ch								
					+				
	0	Default	Default policy set			Default Network Access	× * + 17	¢	>
								Reset	Save

Stap 8. Klik op de pijl *>*naast **Authorized Policy** om deze uit te vouwen. Klik nu op het *+* symbool om een nieuwe regel toe te voegen.

dentity Service	is Engine Home → Conte	ot Visibilit	y Operations	Policy Administration	n 🔹 Work Ce	enters						License Warning	▲	
Policy Sets Profiling	Posture Client Provisioning	 Policy E 	Elements											
Policy Sets + De	fault										Res	et Policyset Hitcour	nts Res	et Save
Status	Policy Set Name	Descrip	otion	Conditions							AI	lowed Protocols / Ser	ver Sequence	e Hits
Search														
0	Default	Default	policy set									Default Network Access	×* 4	17
> Authentication Po	olicy (3)													
> Authorization Poli	cy - Local Exceptions													
> Authorization Pol	cy - Global Exceptions													
 Authorization Poli 	cy.(13)													
								5	Desite					
Status	Rule Name	Condi	itions					F	Profiles		Security Groups		Hits	Actions
Search														
			Wireless_Acc	cess						_		_		
0	Wireless Black List Default	AND	4. IdentityGroup	Name EQUALS EndpointIde	intity Groups:Blac	cklist			×Blackhole_Wireless_Access	+	Select from list	* +	0	¢
Θ	Profiled Cisco IP Phones	48	IdentityGroup Name Ef	QUALS Endpoint Identity Grou	ups Profiled Cisco	co-IP-Phone			×Cisco_IP_Phones	+	Select from list	• +	0	٥
ø	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_P	Phones					×Non_Cisco_IP_Phones	+	Select from list	· +	0	٥
0	Internet Complete Particul		Network_Acce	ess_Authentication_Passed					VOICE TAMPACE Onhourd		Calart from list			
0	Unknown_Compliance_Reared	AND	Compliance_	Unknown_Devices					[A Glaco_temporal_onboard]		OTHER REAL PROPERTY.		v	*
			Network_Acce	ess_Authentication_Passed						10	(
0	NonCompliant_Devices_Redirect	AND	Non_Complia	ant_Devices					× Cisco_Temporal_Onboard	+	Select from list	· +	0	¢

Typ een naam voor de regel en selecteer het + symbool in de kolom Voorwaarden.

✓ Author	rization 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		٥

Klik in het Tekstvenster van de Lijst en klik op het pictogram **Onderwerp**. Scrolt naar beneden tot u *RADIUS User-Name* attribuut vindt en kiest deze.

ibrar	у		Editor															
Sear	rch by Name			Click to add an attribute														
♥ 🛱		. 🛛 🖁 😤	В	Select	attribu	ite for co	nditic	n										3
	BYOD_is_Registered	0		0	Ē		3	۲	₽	Ē	F	ு		₽	୯	10	ໍະ	(:-
	Catalyst_Switch_Local_Web_Authentica tion	0			Die	ctionary					Attribu	te				ID	Info	
	Compliance_Unknown_Devices	Ø		1	Mic	All Diction	ries			~	MS-HC	AP-Use	r-Name	÷		60	()	^
	Compliant_Devices			1	Мо	torola-Syr	nbol				Symbo	I-User-(Group			12	()	
	EAP-MSCHAPv2	()		1	Ne	twork Acc	ess				AD-Us	er-DNS-	Domai	n			()	
	EAP-TLS	1		1 1	Ne	twork Acc	ess				AD-Us UserN:	er-Join-I ame	Point				(i) (i)	
	Guest_Flow			1	Pa	ssiveID					Passiv	eID_Us	ername)			0	
	MAC_in_SAN	1		1	Ra	dius					User-N	lame				1	()	٩,
	Network_Access_Authentication_Passe			1	Ra	dius ckus					User-P Ruckus	asswor -User-(d Groups			2	() ()	~
	Non_Cisco_Profiled_Phones	1			-	-					-	-	-	-	-		-	-
	Non_Compliant_Devices	0																
	Switch_Local_Web_Authentication																	
	Switch Web Authentication																	

Bewaar **gelijken** als de operator en voer *user1* in het tekstvak naast deze in. Klik op **Gebruik** om de eigenschap op te slaan.

orary	Editor		
Search 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	itica 🕖		
Compliance_Unknown_Devices	0	+ New C	AND OR
Compliant_Devices	0		
EAP-MSCHAPv2	0		
EAP-TLS			
Guest_Flow			
MAC_in_SAN	0		
Network_Access_Authentication_Part d	sse 🕡		
Non_Cisco_Profiled_Phones	٢		
Non_Compliant_Devices	()		
Switch_Local_Web_Authentication	0		
Switch Web Authentication			

De voorwaarde voor deze regel is nu ingesteld.

Stap 9. In de kolom **Resultaten/profielen** klikt u op het symbool + en vervolgens kiest u **een nieuw autorisatieprofiel maken**.

✓ Author	rization Policy	y (13)					
				Results			
٠	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
1	0	Static IP Address User 1	Adus-User-Name EQUALS user1	Select from list	Select from list • +		۰
				Create a New Authorization Profile			

Geef het een **Naam op** en bewaar *ACCESS_ACCEPT* als het **Access Type**. Scrolt naar het gedeelte **Advance Attributes**.

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

Klik op de oranje pijl en kies Straal > framed-IP-Address-[8].

Add New Standard Profile				×
Track Mayamant				
Hack Movement [] ()				
Passive Identity Tracking 🔲 🕧				
	Radius			
 Common Tasks 			^	L
DACL Name	U 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]		~	
	Framed-IP-Address[8]			
	Framed-IP-Netmask[9]			
	Framed-IPv6-Address[168]			
 Advanced Attributes Setting 	B I Framed-IPv6-Pool[100]			
Radius:Framed-IP-Address				
			_	
▼ Attributes Details				
Access Type = ACCESS_ACCEPT				
Framed-IP-Address =		11		
		111.	~	
<			>	
		Sav	e Canc	el

Typ het IP-adres dat u automatisch aan deze gebruiker wilt toewijzen en klik op **Opslaan**.

Add New Standard Profile	×
Service Template	^
▼ Common Tasks	
AREspace JPV6 ACL Name ASA VPN	
AVC Profile Name	- 11
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 Cancel

Stap 10. Kies nu het nieuwe vergunningsprofiel.

Authori	ization Polic	y (13)							
•					Results				
•	Status	Rule Name	Cond	tions	Profiles		Security Groups	Hits	Actions
Search									
1	0	Static IP Address User 1	1	Radius-User-Name EQUALS user1	Belect from list	÷	Select from list • 4		¢
					CISCO_WebAbai	^			
	0	Wireless Black List Default	AND	Wireless_Access	DenyAccess		Select from list + +	• •	0
				IdentityGroup Name EQUALS Endpoint Identity Groups Blacklist	NSP_Onboard				
					Non_Cisco_IP_Phones				
	\odot	Profiled Cisco IP Phones	-22-	IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	PermilAccess		Select from list		¢
	0	Drofiled Non Cinco ID Dhones	-	Nee Piece Builled Bhance	Static/PaddressUser1		Calact from list		~
	9	Fromed non-dia/colie Priories	-	non_vievo_rioneo_rioneo	Static IP address				¥

De autorisatieregel is nu helemaal ingesteld. Klik op Opslaan.

dada ide	ntity Service	es Engine Home + Co	ontext Visibility + Operations	Policy Administration	Work Centers				License Warning 🔺	. Q ●	• •
Policy Set	ts Profiling	Posture Client Provisioning	Policy Elements								
Policy S	Sets → De	fault						Res	et Policyset Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions				A	llowed Protocols / Serve	er Sequence	Hits
Search											
	0	Default	Default policy set						Default Network Access	× * +	17
Authe	entication Po	licy (3)									
Autho	prization Poli	cy - Local Exceptions									
Autho	prization Poli	cy - Global Exceptions									
Autho	orization Poli	cy (13)									
							Results				
•	Status	Rule Name	Conditions				Profiles	Security Groups		Hits	Actions
Search											
1	0	Static IP Address User 1	Radius-User-Name	EQUALS user1			×StaticlPaddressUser1	+ Select from list	- +		۵

Verifiëren

Stap 1. Navigeer naar uw clientmachine waar Cisco AnyConnect Secure Mobility-client is geïnstalleerd. Sluit aan op uw FTD head-end (hier wordt een Windows-machine gebruikt) en voer de *user1* aanmeldingsgegevens in.



Klik op het pictogram versnelling (linker benedenhoek) en navigeer naar het tabblad **Statistieken**. Bevestig in het gedeelte **Adres Information** dat het IP-adres is toegewezen, dat is ingesteld op ISE Authorization policy voor deze gebruiker.

🕙 Cisco Any	Connect Secure Mobility Client	-		×
	VPN: Connected to 192.168.0.100. 192.168.0.100	~	Disconnect	
00:00:23		_	IP	v4
۞			-1 C	lulu Isco

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			
Butes				
DYLCS				h.d.

De debug straal straal alle opdrachtuitvoer op FTD toont:

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).....

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 De FTD-logboeken tonen: 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

02 03 00 88 0c af 1c 41 4b c4 a6 58 de f3 92 31 |AK..X...1

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

```
De RADIUS Live-logbestanden op ISE tonen:
```

Event	5200 Authentication succeeded
Isername	user!
Endpoint Id	00.50.55.95.45.57 ()
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Statio IP Address User 1
Authorization Result	StaticiPaddressUser1

2021-09-22 23:53:19:72 Source Tin 2021-09-22 23:53:19.72 driverap-ISE-2-7 Policy Serve Exant 5200 Authentica user1 User 00 50 50 90 40 07 192.168.0.101 Calling Stat Windows10-Work Internal Users Authentication Workstation (0+50004000) Audit Session Id PAP_ASCI PAP_ASCII DRIVERAP_FTD_7.0 Authentication Protocol Network Device All Device Types Location All Locations NAS IPv4 Address 0.0.0.0

Steps

- Sector 1951 Residued RADUS Access Resource 1951 Residued RADUS Access Resource 1957 RADUS greated a new section 1959 Residued greans Benefactor Relay 1959 Residued greans Benefactor Relay 1959 Residued Sector Relay 1959 Sectores Benefactor Relay 1959 Relay Sectores Relay 1950 Relay Sectores Relay Sectores Relay 1950 Relay Sectores Relay Sectores Relay 1950 Relay Sectores Relay Sectores

- 24715 ISE has not confirmed locally previous authentication for user in Active Direct
- 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal E
- 22211 Found Endpoint in Internal Endpoints IOStore 15048 Queried PIP- Radius UserName 15015 Belected Authorization Profile StatistPadre 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache 11002 Returned RADIUS Access-Accept

tives cost type	15.4
Authorization Profile 5	tatidPaddressUser1
Response Time 0	1 milliseconds
Other Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	49152
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PDC7x-Tunnel- Group Name	RA_VPN
OriginalUserName	user1
NetworkDeviceProfileId	b0099505-3150-4215-a80e-6753d45b/56o
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/P0/7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417494978/23
SelectedAuthenticationIdentityStores	Internal Users
Selected Authentication/dentity Stores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
Authentication Status	AuthenticationPassed
identityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Static IP Address Uver 1
1SEPolicySettame	Default
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

Framed-IP-Address	10.0.50.101
esult	
CiscoWPair	mdin-ti-indexica-platformain. mdin-ti-refarita-maran-26 2000-4500 mdin-ti-refarita-maran-26 2000-4500 mdin-ti-refarita-platformator/2005/98-4500 mdin-ti-refarita-platformator/2005/98-4500 mdin-ti-refarita-platformator/2002/2014/16/24 ModAlactore glates-mtdin-ti-refarita-platformator- maran-ti-refarita-platformator- glates-mtdin-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita-platformator- maran-ti-refarita- maran-ti-refarita-platformator- maran-ti-refarita- maran
CPMSessionID Called-Station-ID	dba800540000db000146c100
Device IP Address	192,168.0.100
RADIUS Username	user1
EnableFlag	Enabled

Stap 2. Sluit aan op uw FTD head-end (hier wordt een Windows-machine gebruikt) en voer de user2 aanmeldingsgegevens in.

S Cisco AnyConnect 192.168.0.100 ×	🚳 Cisco AnvConnect Secure Mobility Client — 🗆	×
Group: RA_VPN ~ Username: user2 Password: ******	VPN: Contacting 192.168.0.100. 192.168.0.100	
OK Cancel	\$ ()	uluulu cisco

Het gedeelte **Adres Informatie** laat zien dat het IP-adres dat is toegewezen inderdaad het eerste IP-adres is dat beschikbaar is in de IPv4-pool die via FMC is geconfigureerd.

Sisco AnyConnect Secure Mobil	ity Client	÷		×
cisco AnyCon	nect Secure Mobility Clien	t		()
Virtual Private Network (VF	PN)	Diagnostic	s	
Preferences Statistics Route Deta	ls 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.	

De debug straal straal alle opdrachtuitvoer op FTD toont:

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 De FTD-logboeken tonen:

<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

De RADIUS Live-logbestanden op ISE tonen:

Event	5200 Authentication succeeded
Usemame	use2
Endpoint Id	00.50.56.96.46.6F 🕀
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess
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	use2
User Type	User
User Type Endpoint Id	User 00 50 50 50 45 6F
User Type Endpoint Id Calling Station Id	Uver 00 50 56 56 46 6F 192.168.0.101
User Type Endpoint Id Calling Station Id Endpoint Profile	Uker 00 50 56 56 46 6F 192 168 0 101 Windows10-Woldstation
User Type Endpoint Id Calling Station Id Endpoint Profile Authentication Identity Store	Uter 00 50 64 69 192 108 2.101 Windows 5-Violaitation Internal Uters
User Type Endpoint M Calling Station Id Endpoint Profile Authentication Identity Store Identity Group	Uker 00 80 66 46 6F 192 168 8-00 1 Windows15 Withinsteinn Internal Ukers Wontartion
User Type Endpoint Id Calling Station Id Endpoint Profile Aothentication Identity Store Identity Group Audit Session Id	Uker 00 05 05 4-05 ⁰ 192 105 8. 101 Windows 10 Winitiation Internat Ukes Wohtsteinn ulba0004000000001 Hecto?
User Type Endpoint M Calling Station M Endpoint Profile Authentication Identify Store Identify Group Audit Bression Id Authentication Method	Uwer 00 50 feb 40 193 : 168 : 161 Windowsh's Workstation Internet Uwes Workstation Workstation Bioleanotet 400000014/ws/807
User Type Endpoint Id Calling Staton M Endpoint Profile Authentication Identity Store Identity Group Auth Session M Authentication Method Authentication Protocol	Uwer 00 50 56 64 7 1925 - 193 - 193 - Windows 10 Worksation Hitemas Uwes Workstoor Workstoor Workstoor Para_ACCI
User Type Endpoint Id Calling Station Md Endpoint Protifie Authentication Identity Store Identity Group Auth Enssion M Authentication Method Authentication Protocol Interock Device	Uwr 00 80 66 84 667 192 168 84 667 Internal Uws Worksteinn Internal Uws Worksteinn Internal Uws Worksteinn Refwy, action Refw, action Refw, action Deliver, action action action action Refw, action Deliver, action action action action action action Refw, action Deliver, action actio

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 time
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
15035	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 LogicalProfile
15048	Queried PIP - Network Access AuthenticationStatus
15016	Selected Authorization Profile - PermitAccess
22081	Max sessions policy passed
22080	New accounting session created in Session cache

NAS Port Type	Vidual
Authorization Profile	PermitAccess
Response Time	202 milliseconds
ther Attributes	
ConfigVersionId	140
DestinationPort	1812
Protocol	Radius
NAS-Port	53248
Tunnel-Client-Endpoint	(tag=0) 192.168.0.101
CVPN3000/ASA/PDC7x-Tunnel- Group Name	RA_VPN
OriginalUserName	use/2
NetworkDeviceProfileId	b0099505-3150-4215-a00e-6753d45b/56o
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PO/7x-Client-Type	2
AcsSessionID	driverap-15E-2-7/417494978/24
SelectedAuthenticationIdentityStore	es Internal Users
SelectedAuthenticationIdentityStore	es All_AD_Join_Points
SelectedAuthentication/dentityStore	es Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
1SEPolicySettame	Default
Identity SelectionMatchedRule	Default
DTL S Support	Unknown
HostidentityGroup	Endpoint Identity Groups Profiled Workstation
Network Device Profile	Cisco
Location	Location#All Locations

IPSEC	IPSEC#Is IPSEC Device#No
Name	Endpoint Identity Groups Profiled Workstation
EnableFlag	Enabled
RADIUS Username	use/2
Device IP Address	192.168.0.100
CPMSessionID	c0a800640000.d000614bc367
Called-Station-ID	192.168.0.100
CiscoM/Pair	India Bindenia (Jatamwaik, India Bindenia Imagio De Arto 404, 444, 444, 444, 444, 444, 444, 444
esult	
Class	CACS:c0a800540000d000514bc367.driverap-ISE-2-7/417454978/24
cisco-av-pair	profile-name+Windows10-Workstation
	Base lineare convent

Session Events

CACS:c0x8000640000:d000614bc367:driverap-ISE-2-7/417494978/24
profile-name=Windows10-Workstation
Base license consumed

Opmerking: U moet verschillende IP-adresbereik gebruiken voor IP-adrestoewijzing op zowel de lokale FTD-pool als het ISE-autorisatiebeleid om dubbele IP-adresconflicten tussen uw AnyConnect-clients te voorkomen. In dit configuratievoorbeeld werd FTD geconfigureerd met een IPv4 lokale pool van 10.0.50.1 tot 10.0.50.100 en de ISE server toegewezen een statisch IP-adres van 10.0.50.101.

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Op FTD:

Straal verwijderen

Op ISE:

RADIUS-live logbestanden