EAP-FAST-verificatie met draadloze LANcontrollers en Identity Services Engine

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten **Conventies** Achtergrondinformatie PAC PAC-provisioningmodules Configureren Netwerkdiagram Configuraties De WLC configureren voor EAP-FAST-verificatie Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server De WLAN-verificatie configureren voor EAP-FAST De RADIUS-server configureren voor EAP-FAST-verificatie Een gebruikersdatabase maken om EAP-FAST-clients te certificeren Voeg WLC als AAA-client toe aan de RADIUS-server EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PAC-provisioning EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde in-band PACprovisioning Verifiëren NAM-profielconfiguratie Test connectiviteit op SSID met behulp van EAP-FAST-verificatie. **ISE-authenticatielogs** WLC-zijde debug in succesvolle EAP-FAST-stroom Problemen oplossen

Inleiding

Dit document legt uit hoe u de draadloze LAN-controller (WLC) voor Extensible Authentication Protocol (EAP) kunt configureren - Flexibele verificatie via Secure Tunneling (FAST)-verificatie met behulp van een externe RADIUS-server. Dit configuratievoorbeeld gebruikt de Identity Services Engine (ISE) als de externe RADIUS-server om de draadloze client te authenticeren.

Dit document concentreert zich op de manier om de ISE voor Anonymous en Geautomatiseerde In-Band (Automatic) Protected Access Credentials (PAC) voorziening aan de draadloze klanten te configureren.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basiskennis van de configuratie van lichtgewicht access points (LAP's) en Cisco WLC's
- Basiskennis van het CAPWAP-protocol
- Kennis van het configureren van een externe RADIUS-server, zoals Cisco ISE
- Functionele kennis van het algemene MAP-kader
- Basiskennis over veiligheidsprotocollen, zoals MS-CHAPv2 en EAP-GTC, en kennis over digitale certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

 Cisco 5520 Series WLC-software met firmware release 8.8.11.0Cisco 4800 Series APswitchesAnyConnect NAM.Cisco Secure ISE versie 2.3.0.29Cisco Catalyst 3560-CX Series switch met versie 15.2(4)E1

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 live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Het EAP-FAST-protocol is een voor het publiek toegankelijk type IEEE 802.1X MAP dat Cisco ontwikkelde om klanten te ondersteunen die geen sterk wachtwoordbeleid kunnen afdwingen en een MAP 802.1X willen inzetten dat geen digitale certificaten vereist.

Het EAP-FAST-protocol is een client-server security architectuur die EAP-transacties versleutelt met een TLS-tunnel (Transport Level Security). De totstandbrenging van de EAP-FAST-tunnel is gebaseerd op sterke geheimen die uniek zijn voor de gebruikers. Deze sterke geheimen worden PAC's genoemd, die de ISE genereert door gebruik te maken van een hoofdtoets die alleen bekend staat bij de ISE.

EAP-FAST vindt in drie fasen plaats:

- Fase nul (automatische PAC-provisioningfase)—EAP-FAST fase nul, een optionele fase is een tunnelveilig middel om een EAP-FAST eindgebruikerclient een PAC te bieden voor de gebruiker die netwerktoegang wenst. Het verstrekken van een PAC aan de eindgebruikercliënt is het enige doel van fase nul.Opmerking: Fase nul is optioneel omdat PAC's ook handmatig aan klanten kunnen worden geleverd in plaats van fase nul.Zie het gedeelte <u>PAC-</u>provisioningmodellen van dit document voor meer informatie.
- Fase één—In fase één zetten de ISE en de eindgebruiker client een TLS-tunnel op basis van de PAC-gecrediteerd van de gebruiker. Deze fase vereist dat de eindgebruiker client een PAC

is verstrekt voor de gebruiker die probeert toegang tot het netwerk te verkrijgen, en dat de PAC gebaseerd is op een hoofdtoets die niet is verlopen. Geen netwerkservice is mogelijk door fase één van EAP-FAST.

• Fase twee—In fase twee worden gebruikersverificatiegeloofsbrieven veilig doorgegeven met behulp van een interne MAP-methode die wordt ondersteund door EAP-FAST binnen de TLS-tunnel naar de RADIUS die wordt gecreëerd met behulp van de PAC tussen de client en de RADIUS-server. EAP-GTC, TLS en MS-CHAP worden ondersteund als innerlijke MAP-methoden. Voor EAP-FAST worden geen andere MAP-typen ondersteund.

Raadpleeg <u>Hoe EAP-FAST werkt</u> voor meer informatie.

PAC

PAC's zijn sterke gedeelde geheimen die de ISE en een MAP-FAST eindgebruiker-cliënt in staat stellen elkaar te authenticeren en een TLS-tunnel op te zetten voor gebruik in EAP-FAST fase twee. ISE genereert PAC's met behulp van de actieve hoofdtoets en een gebruikersnaam.

PAC omvat:

- PAC-Key-Gedeeld geheim gebonden aan een client (en client-apparaat) en server-identiteit.
- PAC ondoorzichtig-ondoorzichtig veld dat de client caches geeft en naar de server doorgeeft. De server herstelt de PAC-Key en de client-identiteit om deze wederzijds te bevestigen met de client.
- **PAC-Info** Op z'n minst omvat de identiteit van de server om de client in staat te stellen om verschillende PAC's te casten. Optioneel bevat het andere informatie zoals de vervaltijd van de PAC.

PAC-provisioningmodules

Zoals eerder vermeld is fase nul een optionele fase.

EAP-FAST biedt twee opties om een klant een PAC te verschaffen:

- Automatische PAC-provisioning (EAP-FAST fase 0 of Inband PAC-provisioning)
- Handmatige (out-of-band) PAC-provisioning

In-band/automatische PAC-voorziening verstuurt een nieuwe PAC naar een eindgebruiker-client via een beveiligde netwerkverbinding. Automatische PAC-provisioning vereist geen interventie van de netwerkgebruiker of een ISE-beheerder, mits u de ISE en de eindgebruiker client configureren ter ondersteuning van automatische provisioning.

De nieuwste EAP-FAST-versie ondersteunt twee verschillende in-band PAC-provisioningopties:

Anoniem in-band PAC-provisioning

Geautomatiseerde in-band PAC-provisioning

Opmerking: Dit document behandelt deze in-band PAC-provisioningmethoden en de manier waarop u deze kunt configureren.

Voor out-of-band/handmatige PAC-provisioning is een ISE-beheerder nodig om PAC-bestanden te genereren, die dan moeten worden gedistribueerd naar de toepasbare netwerkgebruikers. De gebruikers moeten de eindgebruikerscliënten met hun PAC-bestanden configureren.

Configureren

Netwerkdiagram



Configuraties

De WLC configureren voor EAP-FAST-verificatie

Voer deze stappen uit om de WLC voor EAP-FAST-verificatie te configureren:

- 1. Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server
- 2. De WLAN-verificatie configureren voor EAP-FAST

Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server

De WLC moet worden geconfigureerd om de gebruikersreferenties naar een externe RADIUSserver te kunnen doorsturen. De externe RADIUS-server bevestigt vervolgens de gebruikersreferenties met EAP-FAST en geeft toegang tot de draadloze klanten.

Voltooi deze stappen om de WLC te configureren voor een externe RADIUS-server:

- 1. Kies **Security** en **RADIUS-verificatie** van de controller GUI om de pagina RADIUSverificatieservers weer te geven. Klik vervolgens op **New** om een RADIUS-server te definiëren.
- Defineert de parameters van de RADIUS-server op de RADIUS-verificatieservers > Nieuwe pagina. Deze parameters omvatten:IP-adres voor RADIUS-serversGedeeld geheimPoortnummerServerstatusDit document gebruikt de ISE-server met een IP-adres van 10.48.39.128.

Security RADIUS Authentication Servers > New AAA General RADIUS Authentication Accounting Authentication Shared Secret Confirm Shared Secret Confirm Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Cocal Net Users Apply Cisco ACA Default settings Cocal Net Users Key Wrap Desbied Clients User Login Policies Server Status Enabled ‡ Server Status Server Status Seconds Advanced EAP Periority Order Periority Order Network User Enable Enable Enable Enable 	cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
AAA Server Index (Priority) 2 ÷ General Server IP Address(Ipv4/Ipv6) 10.48.39.128 Authentication Shared Secret Format ASCII ‡ Auth Cached Users Shared Secret Image: Confirm Shared Secret Downloaded AVP Confirm Shared Secret Image: Confirm Shared Secret Downloaded AVP Apply Cisco ISE Default settings Image: Confirm Shared Secret Downloaded AVP Apply Cisco ACA Default settings Image: Confirm Shared Secret DAP Apply Cisco ACA Default settings Image: Confirm Shared Secret DAP Apply Cisco ACA Default settings Image: Confirm Shared Secret DAP Apply Cisco ACA Default settings Image: Confirm Shared Secret DAP Apply Cisco ACA Default settings Image: Confirm Shared Secret DAP Apply Cisco ACA Default settings Image: Confirm Shared Secret Disabled Clients Server Status Enabled ‡ Password Policies Server Status Enabled ‡ Advanced EAP Network User S seconds Priority Order Management Enable	Security	RADIUS	Authenti	ication Server	rs > New						
Access Control Lists Management Retransmit Timeout 5 seconds Wireless Protection Policies Tunnel Proxy Enable PAC Provisioning Enable Web Auth IPSec Enable TrustSec Cisco ACA Enable Local Policies Umbrella	Security AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies ACVANCED EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Wieless Protection Policies Web Auth TrustSec Local Policies Umbrella	RADIUS . Server In Server IP Shared S Shared S Confirm S Apply Cis Apply Cis Key Wrap Port Num Server St Support f Server Ti Network I Managem Tunnel Pr PAC Prov IPSec Cisco ACJ	Authenti Address(Ip ecret Forma ecret Forma ecret Shared Seco ico ISE Defa ico ACA Def o aber tatus for CoA meout User nent nent Retran roxy isioning A	smit Timeout	 > New 2 \$ 10.48.39.126 ASCII \$ (Designed 1812 Enabled \$ Enabled \$ Seconds Enable 	3 I for FIPS custor	mers and requires	a key wrap comp	liant RAD	IUS server)	

3. Klik Toepassen.

De WLAN-verificatie configureren voor EAP-FAST

Daarna moet u de WLAN-functie configureren die de clients gebruiken om verbinding te maken met het draadloze netwerk voor EAP-FAST-verificatie en een dynamische interface toewijzen. De WLAN-naam die in dit voorbeeld wordt ingesteld, is **eenvoudig**. Dit voorbeeld wijst dit WLAN aan de beheerinterface toe.

Voltooi deze stappen om de snelle WLAN-functie en de bijbehorende parameters te configureren:

- 1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN's pagina weer te geven.Deze pagina toont de WLAN's die op de controller bestaan.
- 2. Klik op **Nieuw** om een nieuw WLAN te maken.

iiliiilii cisco		<u>W</u> LANs <u>C</u>	ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
WLANs	WLANs										
WLANS	Current Filter	r: None	ſ	Change Filter]	[Clear Filter]					Create New 🗘 Go	
Advanced	U WLAN ID	Туре	Profile Na	me		WLAN SSID		Ad	min Status	Security Policies	
		WLAN	test			test		En	abled	[WPA2][Auth(802.1X)]	
	□ <u>2</u>	WLAN	AndroidAP			AndroidAP		En	abled	[WPA2][Auth(PSK)]	

3. Configureer de naam **eap_fast** WLAN SSID, profielnaam en WLAN-id op de WLAN's > Nieuwe pagina. Klik vervolgens op **Toepassen**.

սիսիս				Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP	FEEDBACK . Home
WLANs	WLANs > New			< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN eap_fast eap_fast 3		

- 4. Zodra u een nieuw WLAN hebt gemaakt, wordt de WLAN > pagina bewerken voor de nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat algemeen beleid, RADIUS-servers, beveiligingsbeleid en 802.1x-parameters.
- Controleer het aanvinkvakje Admin Status onder het tabblad Algemeen beleid om het WLAN in te schakelen. Als u wilt dat AP de SSID in zijn beacon kaders uitzendt, controleer het aanvinkvakje Broadcast SSID.

Profile Name eap_fast Type WLAN SSID eap_fast Status Image: Comparison of the security of the security represented of the security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group() vlan1477 \$ Multicast Vlan Feature Enabled Broadcast SSID Imabled NAS-ID None	Profile Name eap_fast Type WLAN SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group() vian1477 \$ Multicast Vlan Feature Enabled Broadcast SSID Enabled NAS-ID none	sheral Se	curity	QoS	Policy-Mappi	ng Advand	ed	
Type WLAN SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vian1477 + Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	Type WLAN SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vlan1477 + Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	Profile Name		eap	_fast			
SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vlan1477 ‡ Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	SSID eap_fast Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vian1477 + Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	Туре		WL	AN			
Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vlan1477 \$ Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	Status Image: Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vlan1477 + Multicast Vlan Feature Enabled Broadcast SSID Image: Enabled NAS-ID none	SSID		eap	_fast			
Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All + Interface/Interface Group(G) Interface/Interface Group(G) vlan1477 + Enabled Broadcast SSID Image: Enabled NAS-ID none	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) vlan1477 Multicast Vlan Feature Enabled Broadcast SSID Radio Policy All Interface/Interface Group(G) vlan1477 Multicast Vlan Feature Interface Complexity tab will appear after applying the changes.)	Status			Enabled			
Interface/Interface Group(G) vlan1477 \$ Multicast Vlan Feature Enabled Broadcast SSID Image: Comparison of the sector of the sec	Interface/Interface Group(G) vlan1477 \$ Multicast Vlan Feature Enabled Broadcast SSID Image: Comparison of the second sec	Radio Policy		All	\$			
Multicast Vlan Feature Enabled Broadcast SSID Image: Comparison of the sector of the	Multicast Vlan Feature Enabled Broadcast SSID Image: Comparison of the sector of the	Interface/Inter	face Group	(G) vla	an1477 🗘			
Broadcast SSID C Enabled NAS-ID none	Broadcast SSID Image: Comparison of the second se	Multicast Vlan	Feature	🗆 E	Enabled			
NAS-ID none	NAS-ID none	Broadcast SSI	D	🖉 E	Enabled			
		NAS-ID		non	e			

6. Onder "WLAN -> Bewerken -> Beveiliging -> Layer 2" Kies het tabblad WAP/WAP2parameters en selecteer de optie punt1x voor AKM. Dit voorbeeld gebruikt WAP2/AES + dot1x als Layer 2 beveiliging voor dit WLAN. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk.

ANs > E	dit 'eap_f	ast'				
General	Security	QoS	Policy-Map	ping Adva	inced	
Layer 2	Layer 3	AAA S	ervers			
Layer 2	Security ⁶	WPA+WPA2 AC Filtering	• • •)		
ast Trans	ition					
ast Transit	ion	Disa	able 🗘			
Protected	Managemen	t Frame				
PMF		Disa	abled \$			
WPA+WPA	2 Paramete	rs				
WPA Pol	icy					
WPA2 Po	olicy					
WPA2 E	ncryption	🖉 AE	S TKIP	CCMP256	GCMP128	GCMP256
OSEN Po	olicy					
Authentica	ition Key Ma	nagement	<u>19</u>			
802.1X		Enable				
ССКМ		Enable				
PSK		Enable				
ET 002 -		Enable				

7. Onder "WLAN -> Bewerken -> Beveiliging -> AAA-servers" kiest u de juiste RADIUS-server uit het keuzemenu onder RADIUS-servers.

eneral	Security	QoS	Policy-	Mapping	Advanced		
ayer 2	Layer 3	AAA S	Servers				
elect AAA s ADIUS Serv RADIUS Se	ervers belo vers erver Overwr	w to over	r ride use o ce 🗌 Enab	f default se	rvers on this V	VLAN	
Apply Cisco	o ISE Defaul	t Settings	🗆 Enab	led			
Apply Cisco	o ISE Defaul	t Settings	ers /	Accounting	Servers		EAP Pa
Apply Cisco Server 1	Authentica	t Settings tion Serv 39.128, Po	ers	Accounting Enabled None	Servers	\$	EAP Pa Enal
Apply Cisco Server 1 Server 2	Authentica Contempt for the second se	t Settings I tion Serv 39.128, Po	ers vers vers vrt:1812 \$	Accounting Enabled None None	Servers	¢	EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3	Authentica Contemption Authentica Contemption Authentica Contemption Contempti Contemption	t Settings Ition Serv 39.128, Po	ers pers prt:1812 \$ \$	Accounting Enabled None None None	Servers	 	EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Contempt Contemp Contem	t Settings Ition Serv	Enab	Accounting Enabled None None None None None	Servers	 <	EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Contemporation Contemporation Contemporatico Contemporatico Contemporatico Contemporatico Contempor	t Settings Ition Serv	Enab	Ccounting Enabled None None None None None None	Servers	 <	EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Authentica Authentica C Enabled IP:10.48.3 None None None None None None	t Settings	Enab	Accounting Enabled None None None None None None None	Servers	 <	EAP Pa

 Klik op Toepassen. Toelichting: Dit is de enige MAP-instelling die op de controller moet worden ingesteld voor MAP-verificatie. Alle andere configuraties die specifiek zijn voor EAP-FAST moeten worden uitgevoerd op de RADIUS-server en de klanten die geauthentiseerd moeten worden.

De RADIUS-server configureren voor EAP-FAST-verificatie

Voer deze stappen uit om de RADIUS-server voor EAP-FAST-verificatie te configureren:

- 1. Een gebruikersdatabase maken om EAP-FAST-clients te certificeren
- 2. Voeg WLC als AAA-client toe aan de RADIUS-server
- 3. EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PACprovisioning
- 4. EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde in-band PACprovisioning

Een gebruikersdatabase maken om EAP-FAST-clients te certificeren

In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de EAP-FAST-client ingesteld als respectievelijk <*eap_fast*> en <*EAP-fast1*>.

1. In ISE Web admin UI navigeren onder "Beheer -> Identity Management -> Gebruikers" en druk op het pictogram "Add".

diale Ident	ity Services Engine	Home Context	Visibility > Operation	ations >	Policy -A	dministratio	n 🔶 Work Cer	iters			
System	- Identity Management	Network Resources	Device Portal Ma	nagement	pxGrid Service	is 🕨 Feed	Service + Three	eat Centric NAC			
▼ Identities	Groups External Identi	y Sources Identity S	ource Sequences	 Settings 							
	G										
Users		Network Access	Users								
Latest Manua	Network Scan Results	/ Edit 🕂 Add	🔀 Change Status	💽 Import	🔂 Export 👻	X Delete	Duplicate				
		Status	Name	•	Description		First Name	Last Name	Email Address	User Identity Groups	Admin
									No da	ta available	

2. Vul vereiste formulieren in zodat de gebruiker kan worden gemaakt - "Naam" en "Wachtwoord voor loggen" en selecteer "Gebruikersgroep" uit de vervolgkeuzelijst.[Opties dat u andere informatie voor de gebruikersaccount kunt invullen] Druk op "Sumbit"

duale Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
► System - Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓Identities Groups External Iden	tity Sources Identity Source Sequences + Settings
System Identity Management Identities Groups External Iden Users Latest Manual Network Scan Results	 Network Resources Device Portal Management pxGrid Service Threat Centric NAC tity Sources Identity Source Sequences Settings Network Access Users List > New Network Access User Network Access Users List > New Network Access User Name eap_fast Status Enabled Enabled • Email Passwords Password Re-Enter Password Cenerate Password • User Information First Name Test user Last Name Test user
	Account Options Description Change password on next login Account Disable Policy Disable account if date exceeds 2019-04-23 (yyyy-mm-dd) Viser Groups Employee Submit Cancel

3. Gebruiker is gemaakt.

				6									
 System 	✓ Identity M	anagement	Netw	ork Resource	s + Device Portal N	lanagement	pxGrid Servic	es ⊧Fee	d Service + Th	eat Centric NAC			
✓ Identities	Groups	External Ident	ity Sour	ces Identity	y Source Sequences	Settings							
		G	Not	huark Acor									
Users			Ne	WORK ACCE	ss users								
Latest Manual	I Network Sca	an Results	1	Edit 🕂 Add	Change Status	Import	🚯 Export 👻	🗙 Delete	Duplicate				
				Status	Name		Description		First Name	Last Name	Email Address	User Identity Groups	Admin
				Enabled	👤 eap_fast	\oplus			Test user	Test user		Employee	

Voltooi deze stappen om de controller te definiëren als een AAA-client op de ACS-server:

1. In ISE Web admin UI navigeer onder "Beheer -> Netwerkbronnen -> Netwerkapparaten" en druk op het pictogram "Toevoegen".



2. Vul vereiste formulieren in zodat een apparaat kan worden toegevoegd - "Naam", "IP" en stel hetzelfde gedeelde geheime wachtwoord in zoals we in eerder vak op WLC hebben ingesteld in het formulier "Gedeeld geheim" [optioneel: u kunt andere informatie voor het apparaat invullen zoals locatie, groep, enzovoort]. Druk op "Sumbit"

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
G	
Network Devices	Network Devices List > New Network Device
Default Device	* Name WILCS20
Device Security Settings	Description
	IP Address VIP: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	t Device Destile dd Class
	Model Name 👻
	Software Version
	* Network Device Group
	Location LAB Set To Default
	IPSEC Is IPSEC Device Set To Default
	Device Type WLC-lab Set To Default
	RADIUS Authentication Settings
	RADIUS UUP Settings
	Shared Secret
	CoA Port [1700 Cot To Default]
	DTI S Required
	Shared Secret radius/dtls
	CoA Port 2083 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional)
	DNS Name

3. Het apparaat wordt toegevoegd aan de lijst met ISE-toegangsapparaat. (NAD)



EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PAC-provisioning

Over het algemeen wil je dit type methode gebruiken voor het geval dat ze geen PKI-infrastructuur hebben in hun implementatie.

Deze methode werkt binnen een Authenticated Diffie-Hellman Key Agreement Protocol (ADHP)tunnel voordat de peer de ISE-server authentiek verklaart.

Om deze methode te ondersteunen moeten we "Laat anonieme In-band PAC Provisioning" op ISE mogelijk maken onder de "Verificatie toegestaan protocollen":

dentity Services Engine	Home Context Visibility Operations -Policy Administration Work Centers
Policy Sets Profiling Posture C	Client Provisioning - Policy Elements
Dictionaries ► Conditions	ts
G	- Allow EAP-FAST
▼Authentication	
Allowed Protocols	
Authorization	Allow Password Channe Retries 3 (Valid Ranne 0 to 3)
► Profiling	
h Bastura	Allow Password Change Retries 3 (Valid Range 0 to 3)
Prosture	Allow EAP-TLS
Client Provisioning	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
	Use PACs O Don't Use PACs
	Tunnel PAC Time To Live 90 Days *
	Proactive PAC update will occur after 90 % of PAC Time To Live has expired
	Allow Anonymous In-Band PAC Provisioning
	Allow Authenticated In-Band PAC Provisioning
	Server Returns Access Accept After Authenticated Provisioning
	Accept Client Certificate For Provisioning
	Allow Machine Authentication
	Machine PAC Time To Live 1 Weeks *
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 (1)
	Enable EAP Chaining

Opmerking: Zorg ervoor dat u een wachtwoord type autorisatie hebt toegestaan, zoals EAP-MS-CHAPv2 voor EAP-FAST binnenmethode, omdat we natuurlijk met Anonymous In-band

Provisioning geen certificaten kunnen gebruiken.

EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde inband PAC-provisioning

Dit is de best beveiligde en aanbevolen optie. De TLS-tunnel is gebouwd op basis van het servercertificaat dat is gevalideerd door het leveringscertificaat en het certificaat van scheiding is gevalideerd door ISE (standaard).

Voor die optie is een PKI-infrastructuur nodig voor client en server, hoewel de PKI-infrastructuur alleen aan serverkant is toegestaan of aan beide kanten is overgeslagen.

Op ISE zijn er twee extra opties voor Voor Verifieerde In-band provisioning:

- "Server Retourenaccess accepteren na geauthentiseerde provisioning" Normaal gesproken, na PAC-provisioning, dient een toegangsverwerp te worden verzonden, waarbij de aanvrager wordt gedwongen om het gebruik van PAC's te reauthentiseren. Maar omdat PAC-provisioning wordt uitgevoerd in geauthenticeerde TLS-tunnels kunnen we onmiddellijk reageren met Access-Accept om de authenticatietijd te minimaliseren. (in dat geval moet u ervoor zorgen dat u de certificaten aan de kant plint en de server hebt vertrouwd).
- "Accept Client certificaatcertificaat for Provisioning" indien men geen PKI-infrastructuur aan clientapparaten wil leveren en alleen een betrouwbaar certificaat op ISE heeft, schakelt u deze optie in, zodat de validatie van het clientcertificaat aan serverzijde overslaat.

CISCO		Linginio	nome / C	Context visionity Coperations Context of Violation Contexts
Policy Sets	Profiling P	osture	Client Provisioning	✓ Policy Elements
Dictionaries	Conditions	- ▼ Res	ults	
		(9 🗸 🗹	Allow EAP-FAST
▼Authentication	on			
Allowed Prot	tocols			EAP-FAST Inner Methods
Authorization	n			✓ Allow EAP-MS-CHAPv2
				Allow Password Change Retries 3 (Valid Range 0 to 3)
Profiling				Allow EAP-GTC
Posture				Allow Password Change Retries 3 (Valid Range 0 to 3)
Client Provis	sioning			✓ Allow EAP-TLS
				Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
				Use PACs O Don't Use PACs
				Tunnel PAC Time To Live 90 Davs *
				Proactive PAC update will occur after 90 % of PAC Time To Live has expired
				Allow Anonymous In-Band PAC Provisioning
				✓ Allow Authenticated In-Band PAC Provisioning
				Source Returns Access Access After Authenticated Provisioning
				Allow Machine Authentication
				Enable Stateless Session Resume
				Enable EAP Chaining

Op ISE definiëren we ook eenvoudig authentificatiebeleid dat voor draadloze gebruikers is ingesteld. Hieronder wordt bijvoorbeeld gebruikt als parameter van het type en locatie en authenticatie type, dan wordt authenticatie flow matching die voorwaarde gevalideerd aan de hand van interne gebruikersdatabase.

ł

Verifiëren

Dit voorbeeld zal de geauthentiseerde In-band PAC Provisioning Flow en de configuratie van het Netwerk Access Manager (NAM) samen met respectieve WLC-debugs tonen.

NAM-profielconfiguratie

Er moeten de volgende stappen worden gezet om het NAM-profiel van AnyConnect te configureren om gebruikerssessie tegen ISE te bevestigen met behulp van EAP-FAST:

- 1. Profieleditor van Open Network Access Manager en laadt het huidige configuratiebestand.
- 2. Zorg ervoor dat "EAP-FAST" is ingeschakeld onder "Toegestaan verificatiemodi"

AnyConnect Profile Editor	- Network Access Manager	- 🗆 X				
File Help						
Network Access Manager	Authentication Policy					
	Profile: Untitled					
	Allow Association Modes	Allowed Authentication Modes				
Setwork Groups	Select All (Personal)	Select All Outer				
	Open (no encryption)	☑ EAP-FAST				
	Open (Static WEP)	EAP-GTC				
	Shared (WEP)	EAP-TLS				
	WPA Personal TKIP	EAP-TLS				
	WPA Personal AES	EAP-TTLS				
	WPA2 Personal TKIP	EAP-MD5 ZEAP-MSCHAPv2				
		MSCHAP (legacy)				
	Select All (Enterprise)	⊡ LEAP				
	Open (Dynamic (802.1X) WEP)					
	WPA Enterprise TKIP	EAP-MSCHAPv2				
	WPA Enterprise AES	EAP-TLS				
	WPA2 Enterprise TKIP					
	WPA2 Enterprise AES					
	CCKM Enterprise TKIP					
	CCKM Enterprise AES	2 802 1x with MarSer				
	1 Help					

3. "Voeg" een nieuw netwerkprofiel toe:

AnyConnect Profile Editor -	Network Access Mar	nager			-	×
Network Access Manager	Networks Profile: Untitl	ed				
Networks	Network					^
34 Network Groups	Name	Media Type	Group*			
	wired	Wired	Global	Add		
				Edit		
				Delete		
	* A network in gro	oup 'Global' is a member of <i>all</i> gro	oups.			
	<					`

4. Onder **"Mediatype"** definieert de configuratie sectie profiel **"Naam**", draadloze verbinding als uw medianetype en specificeer de naam SSID.

🕍 AnyConnect Profile Editor - Network Access Manager	-		×
File Help			
Network Access Manager Client Policy Profile:ility Client\Network Access Manager\system\configuration.xml			
Profile:ility Client/Network Access Manager/system/configuration.xml Profile:ility Client/Network Access Manager/system/configuration.xml Name: eap_fast Group Membership I nal groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wirfl (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Wirfl (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Wirfl (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Common Settings Script or application on each user's machine to run when connected. Commection Timeout 40 seconds		Media	y Les
			>
🕕 Help			

5. Selecteer onder **het** tabblad "**Security Level"** het optie "Veriating Network" en specificeer de associatiemodus als WAP2 Enterprise (AES)

Networks Profile:ility Client\Network Access Manager\system\configuration.	xml	
Security Level		Media Type
Open Network		Security Lev
Open networks have no security, and are open to anybody within range. This is		Connection Ty
the least secure type of network.		
O Shared Key Network		
Shared Key Networks use a shared key to encrypt data between end stations and		
network access points. This medium security level is suitable for		
small/home offices.		
Authenticating Network		
Authenticating networks provide the highest level of security and are perfect for		
enterprise level networks. Authentication networks require radius servers, and		
other network infrastructure.		
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30		
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 MPA2 Enterprise (AES)		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3		
802. 1X Settings authPeriod (sec.) 30 heldPeriod (sec.) 60 MaxStart 3		

6. In dit voorbeeld gebruiken we gebruikerstype authenticatie, daarom onder volgende tab "Connection type" selecteert u "User Connection"

AnyConnect Profile Editor	- Network Access Manager —			×
File Help	Networks Profile:ility Client\Network Access Manager\system\configuration.xml			
Network Groups	Network Connection Type Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. Image:	S	Media [*] Security User A Creder	ype ^ Leve n Ty uth tials
	Help			,

7. Specificeer onder "**User Auth**"-tabblad EAP-FAST als toegestane authenticatiemethode en verlaag de validatie van servercertificaten omdat we in dit voorbeeld geen vertrouwde certificaten gebruiken.

AnyConnect Profile Editor -	Network Access Manager		– 🗆 ×
Network Access Manager Office Client Policy Active Statistics Policy	Networks Profile:ility Client\Ne	twork Access Manager\system\configuratio	n.xml
Authentication Policy Networks	EAP Methods C EAP-TLS EAP-TLS EAP-TLS EAP-TTLS EAP-FAST Settings Validate Server Identi EAP-FAST Settings Validate Server Identi EAP-FAST Settings Validate Server Identi EAP-FAST Settings Validate Server Identi EAP-FAST Settings Validate Server Identi Authenticate using a Validate Using a Validat	O PEAP	Media Type ^ Security Leve Connection Ty User Auth Credentials
	<	🚺 Help	>

Opmerking: in de reële productieomgeving zorgt ervoor dat u het certificaat dat op ISE is geïnstalleerd, hebt vertrouwd en houdt u de optie voor de validering van het servercertificaat ingeschakeld in de NAM-instellingen.

Opmerking: optie "Als u PAC's gebruikt, mag u niet-gewaarmerkte PAC-provisioning" alleen toestaan in het geval van Anoniem In-band PAC-provisioning.

8. Defineer gebruikersreferenties, of als SSO voor het geval u dezelfde aanmeldingsgegevens wilt gebruiken als die voor inloggen worden gebruikt, of selecteer "Wachtwoord voor referenties" voor het geval u wilt dat een gebruiker om aanmeldingsgegevens wordt gevraagd tijdens het aansluiten op een netwerk, of definieer statische aanmeldingsgegevens voor dat toegangstype. In dit voorbeeld vragen we gebruikers om aanmeldingsgegevens bij een verbinding naar een netwerk.

	×

AnyConnect Profile Editor - Network A	ccess Manager	r
---------------------------------------	---------------	---

User Identity			 Media Type /
Unprotected Identity Pat	tern:	anonymous	Security Leve
onprotected Identity Fut		anonymous	Connection Ty
Protected Identity Patter	n: [[username]	User Auth
			Credentials
Lines Condentials			
Use Single Sign On	Credentials		
Prompt for Creden	tials		
	Forever		
Remember	while User is Less	and On	
Remember	while Oser is Logg		
O Never Rer	hember		
O Use Static Credent	ials		
Demonstra			
Password:			
	Dene	Canad	
	Done	Cancel	
1			

9. Opslaan van ingesteld profiel onder de desbetreffende NAM-map.

Test connectiviteit op SSID met behulp van EAP-FAST-verificatie.

1. Selecteer respectieve profiel van AnyConnect-netwerklijst

nnect Secure Mobility Client		_		×
VPN: Verify your network connection.	~		Connect	:
nnectivity				
Network: Authenticating eap_fast		A .	all 🗸	
eap_fast		ť	an e	
		t t t		
	vPN: /erify your network connection. nnectivity Network: Authenticating eap_fast eap_fast	Annect Secure Mobility Client VPN: /erify your network connection.	VPN: /erify your network connection. verify your network connection. verify nectivity Network: Authenticating eap_fast eap_fast	VPN: /erify your network connection. Connect Innectivity Network: Authenticating eap_fast Infact Infact

- 2. Voer een gebruikersnaam en wachtwoord in dat voor verificatie vereist is
- 3. Server certificaat accepteren (zelf ondertekend)

Cisco AnyConnect	×		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?			
Certificate Name:	rmanchur-ise.wlaaan.com@		
Issued To:	rmanchur-ise.wlaaan.com		
Issued By:	rmanchur-ise.wlaaan.com		
Expiration Date:	2020-02-13 15:03:40 UTC		
	Trust Do Not Trust		

4. Gereed

🕙 Cisco AnyC	connect Secure Mobility Client	_		×
	VPN: Network error. Unable to lookup host	names	s. Connect	
Limited Acces	s - DNS Failure			
E	Network: Connected (192.168.77.34) eap_fast	8	all 🗸 🗉	

ISE-authenticatielogs

ISE-authenticatiebestanden die EAP-FAST en PAC-voorzieningsstroom tonen, kunnen worden gezien onder "**Operations -> RADIUS -> Live Logs**" en kunnen in meer details worden bekeken met behulp van het pictogram **Zoom**:

1. De cliënt is begonnen met authenticatie en ISE stelde EAP-TLS voor als authenticatiemethode, maar client verworpen en voorgesteld EAP-FAST, dat was de methode waarover zowel cliënt als ISE het eens waren.

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 11507 Extracted EAP-Response/Identity

12500 Prepared EAP-Request proposing EAP-TLS with challenge

- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session

12101 Extracted EAP-Response/NAK requesting to use EAP-FAST instead

- 12100 Prepared EAP-Request proposing EAP-FAST with challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. De TLS-handdruk is tussen client en server gestart om een beschermde omgeving te bieden voor PAC-uitwisseling en is met succes voltooid.

12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12811	Extracted TLS Certificate message containing client certificate
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request (g Step latency=13317 ms)
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12002	Proposed TLC Finished message
12816	TLS handshake succeeded

3. Inner authenticatie gestart en gebruikersreferenties werden gevalideerd door ISE met behulp van MS-CHAPv2 (op gebruikersnaam/wachtwoord gebaseerde verificatie)