Authentification EAP-FAST avec contrôleurs de réseau local sans fil et moteur Identity Services Engine

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Conventions Informations générales APC Modes de provisionnement PAC Configuration Diagramme du réseau Configurations Configurer le WLC pour l'authentification EAP-FAST Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe Configurer le WLAN pour l'authentification EAP-FAST Configurer le serveur RADIUS pour l'authentification EAP-FAST Créer une base de données utilisateur pour authentifier les clients EAP-FAST Ajouter le WLC en tant que client AAA au serveur RADIUS Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement en bande PAC anonyme Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC inband authentifié **Vérification** Configuration du profil NAM Testez la connectivité au SSID à l'aide de l'authentification EAP-FAST. Journaux d'authentification ISE Débogage côté WLC sur le flux EAP-FAST réussi Dépannage

Introduction

Ce document explique comment configurer le contrôleur de réseau local sans fil (WLC) pour l'Extensible Authentication Protocol (EAP) - authentification flexible par l'intermédiaire de l'authentification de Secure Tunneling (FAST) avec l'utilisation d'un serveur RADIUS externe. Cet exemple de configuration utilise ISE (Identity Services Engine) comme serveur RADIUS externe pour authentifier le client sans fil.

Ce document se concentre sur la façon de configurer l'ISE pour le provisionnement des informations d'identification et de connexion protégées (PAC) anonymes et authentifiées sur les

clients sans fil.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de base de la configuration des points d'accès légers (LAP) et des WLC Cisco
- Connaissances de base du protocole CAPWAP
- Connaissance de la configuration d'un serveur RADIUS externe, tel que Cisco ISE
- Connaissances fonctionnelles sur le cadre général du PAE
- Connaissances de base sur les protocoles de sécurité, tels que MS-CHAPv2 et EAP-GTC, et connaissances sur les certificats numériques

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• WLC de la gamme Cisco 5520 qui exécute la version 8.8.111.0 du micrologicielPoint d'accès de la gamme Cisco 4800Anyconnect NAM.Cisco Secure ISE version 2.3.0.298Commutateur de la gamme Cisco 3560-CX qui exécute la version 15.2(4)E1

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, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Informations générales

Le protocole EAP-FAST est un type EAP IEEE 802.1X accessible au public que Cisco a développé pour prendre en charge les clients qui ne peuvent pas appliquer une politique de mot de passe forte et qui veulent déployer un type EAP 802.1X qui ne nécessite pas de certificats numériques.

Le protocole EAP-FAST est une architecture de sécurité client-serveur qui chiffre les transactions EAP avec un tunnel TLS (Transport Level Security). L'établissement du tunnel EAP-FAST repose sur des secrets forts propres aux utilisateurs. Ces secrets forts sont appelés PAC, que l'ISE génère en utilisant une clé principale connue uniquement de l'ISE.

EAP-FAST se déroule en trois phases :

 Phase zéro (phase de provisionnement automatique PAC) - EAP-FAST Phase zero, une phase facultative est un moyen sécurisé par tunnel de fournir à un client utilisateur final EAP- FAST un PAC pour l'utilisateur demandant l'accès au réseau. **Fournir un PAC au client de l'utilisateur final est le seul objectif de la phase zéro.Remarque :** la phase zéro est facultative car les PAC peuvent également être provisionnés manuellement aux clients au lieu d'utiliser la phase zéro.Consultez la section <u>Modes de provisionnement PAC</u> de ce document pour plus de détails.

- Phase 1 Au cours de la phase 1, ISE et le client de l'utilisateur final établissent un tunnel TLS basé sur les informations d'identification PAC de l'utilisateur. Cette phase nécessite que le client de l'utilisateur final dispose d'un PAC pour l'utilisateur qui tente d'accéder au réseau et que le PAC soit basé sur une clé principale qui n'a pas expiré. Aucun service réseau n'est activé par la phase 1 d'EAP-FAST.
- Phase deux Dans la phase deux, les informations d'identification d'authentification utilisateur sont transmises de manière sécurisée à l'aide d'une méthode EAP interne prise en charge par EAP-FAST dans le tunnel TLS vers le RADIUS créé à l'aide du PAC entre le client et le serveur RADIUS. EAP-GTC, TLS et MS-CHAP sont pris en charge en tant que méthodes EAP internes. Aucun autre type EAP n'est pris en charge pour EAP-FAST.

Référez-vous à Fonctionnement d'EAP-FAST pour plus d'informations.

APC

Les PAC sont de puissants secrets partagés qui permettent à l'ISE et à un client d'utilisateur final EAP-FAST de s'authentifier mutuellement et d'établir un tunnel TLS pour une utilisation dans la phase 2 EAP-FAST. L'ISE génère des PAC à l'aide de la clé principale active et d'un nom d'utilisateur.

Le PAC comprend :

- Clé PAC : secret partagé lié à un client (et à un périphérique client) et à l'identité du serveur.
- PAC Opaque : champ opaque que le client met en cache et transmet au serveur. Le serveur récupère la clé PAC et l'identité du client pour s'authentifier mutuellement avec le client.
- Info-PAC Inclut au minimum l'identité du serveur pour permettre au client de mettre en cache différents PAC. Le cas échéant, il inclut d'autres informations telles que la date d'expiration du PAC.

Modes de provisionnement PAC

Comme mentionné précédemment, la phase zéro est une phase facultative.

EAP-FAST offre deux options pour provisionner un client avec un PAC :

- Approvisionnement PAC automatique (EAP-FAST Phase 0 ou Approvisionnement PAC intrabande)
- Provisionnement manuel (hors bande) PAC

Le provisionnement en bande/PAC automatique envoie un nouveau PAC à un client utilisateur final via une connexion réseau sécurisée. Le provisionnement automatique PAC ne nécessite aucune intervention de l'utilisateur réseau ou d'un administrateur ISE, à condition que vous configuriez l'ISE et le client de l'utilisateur final pour prendre en charge le provisionnement automatique.

La dernière version EAP-FAST prend en charge deux options de configuration de mise en service

PAC intrabande :

- Provisionnement PAC intrabande anonyme
- Provisionnement PAC intrabande authentifié

Remarque : Ce document traite de ces méthodes de provisionnement PAC intrabande et de la façon de les configurer.

Le **provisionnement manuel/hors bande des PAC** nécessite qu'un administrateur ISE génère des fichiers PAC, qui doivent ensuite être distribués aux utilisateurs réseau concernés. Les utilisateurs doivent configurer les clients des utilisateurs finaux avec leurs fichiers PAC.

Configuration

Diagramme du réseau



Configurations

Configurer le WLC pour l'authentification EAP-FAST

Effectuez ces étapes afin de configurer le WLC pour l'authentification EAP-FAST :

- 1. Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe
- 2. Configurer le WLAN pour l'authentification EAP-FAST

Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe

WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide ensuite les informations d'identification de l'utilisateur à l'aide du protocole EAP-FAST et fournit l'accès aux clients sans fil.

Complétez ces étapes pour configurer le WLC pour un serveur RADIUS externe :

- 1. Sélectionnez Security et RADIUS Authentication depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Ensuite, cliquez sur Nouveau afin de définir un serveur RADIUS.
- Définissez les paramètres du serveur RADIUS sur la page RADIUS Authentication Servers > New. Ces paramètres incluent :Adresse IP du serveur RADIUSSecret partagéPort number (numéro de port) État du serveurCe document utilise le serveur ISE avec l'adresse IP 10.48.39.128.

cisco	MONITOR WLANS	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	RADIUS Authentic	cation Server	s > New					
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 Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies	RADIUS Authentic Server Index (Priority Server IP Address(Ipv Shared Secret Format Shared Secret Confirm Shared Secre Apply Cisco ISE Defau Apply Cisco ACA Defa Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransu Tunnel Proxy PAC Provisioning IPSec Cisco ACA	cation Server	 > New 2 ÷ 10.48.39.128 ASCII ÷ (Designed 1812 Enabled ÷ Enabled ‡ S seconds Enable 	for FIPS custon	ners and requires a	a key wrap comp	liant RADI	IUS server)
 Advanced 								

3. Cliquez sur Appliquer.

Configurer le WLAN pour l'authentification EAP-FAST

Ensuite, configurez le WLAN que les clients utilisent pour se connecter au réseau sans fil pour l'authentification EAP-FAST et l'affecter à une interface dynamique. Le nom WLAN configuré dans cet exemple est **rapide**. Cet exemple attribue ce WLAN à l'interface de gestion.

Complétez ces étapes afin de configurer le WLAN rapide d'ap et ses paramètres associés :

- 1. Cliquez sur les WLAN de la GUI du contrôleur afin d'afficher la page des WLAN.Cette page énumère les WLAN qui existent sur le contrôleur.
- 2. Cliquez sur New [nouveau] pour créer un autre WLAN.

uluulu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS H	E <u>L</u> P <u>F</u> EEDBACK		
WLANs	WLANs					
VLANs	Current Filter: None	[Change Filter] [Clear Filter]			Create New	
Advanced	UWLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
	1 WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]	i
	2 WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]	i i

 Configurez le nom SSID eap_fast WLAN, le nom de profil et l'ID WLAN sur la page WLANs > New. Cliquez ensuite sur Apply.

alada	MONITOR WI ANS			FEEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
WLANs	WLANs > New	CONTROLLER WARELEDD	SECONTL MENADEMENT	TERDBACK	< Back Apply
VLANs					
WLANs	Type Profile Name	eap_fast			
P Advanced	SSID	eap_fast			
	ID	3 \$			

- 4. Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir différents paramètres spécifiques à ce WLAN. Cela inclut les stratégies générales, les serveurs RADIUS, les stratégies de sécurité et les paramètres 802.1x.
- 5. Cochez la case **Admin Status** sous l'onglet **General Policies** afin d'activer le WLAN. Si vous voulez que l'AP diffuse le SSID dans ses trames de balise, cochez la case **Broadcast SSID**.

/LANs > E	dit 'eap_fa	st'					
General	Security	QoS	Policy-Map	oping	Advanced		
Profile Na	me	ear	o fast				
Туре		WL	AN				
SSID		eap	_fast				
Status			Enabled				
Security F	Policies	[W	PA2][Auth(80)2.1X)]			
		(Mo	difications done	under s	ecurity tab will ap	opear	after applying the changes.)
Radio Poli	су		\$	J			
Interface/	Interface Group		an1477 🗘				
Multicast	Vlan Feature		Enabled				
Broadcast	SSID		Enabled				_
NAS-ID		nor	e				
							- -

 Sous "WLAN -> Edit -> Security -> Layer 2 » choisissez les paramètres WPA/WPA2 et sélectionnez dot1x pour AKM.

Cet exemple utilise WPA2/AES + dot1x comme sécurité de couche 2 pour ce WLAN. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN.

_ANs > E	dit 'eap_f	ast'				
General	Security	QoS	Policy-Map	ping Adva	inced	
Layer 2	Layer 3	AAA Se	ervers			
Layer 2	Security 🧧 🗌	WPA+WPA2 AC Filtering ^g	¢			
Fast Trans	ition					
Fast Transit	tion	Disa	ble 🗘			
Protected	Management	Frame				
PMF		Disal	oled			
WPA+WPA	A2 Parameter	's				
WPA Po	licy					
WPA2 P	olicy		_			
WPA2 E	ncryption	🗹 AES	П ТКІР	CCMP256	GCMP128	GCMP256
OSEN P	olicy					
Authentica	ation Key Ma	nagement ¹	9			
802.1X		Enable				
ССКМ		Enable				
PSK		Enable				
-						

7. Sous l'onglet "WLAN -> Edit -> Security -> AAA Servers », sélectionnez le serveur RADIUS approprié dans le menu déroulant sous RADIUS Servers.

eneral	Security	QoS	Policy-N	lapping	Advanced		
Layer 2	Layer 3	AAA S	Servers				
elect AAA s ADIUS Serv RADIUS Se	ervers belo vers erver Overwr	rite interfa	rride use of	ed	rvers on this W	VLAN	
Apply Cisc	o ISE Defaul	t Settings	U Enabl	ed			
Apply Cisc	o ISE Defaul	t Settings	ers A	ea ccounting s	Servers		EAP Pa
Apply Cisco Server 1	o ISE Defaul Authentica ✓ Enabled IP:10.48.3	t Settings Ition Serv 39.128, Po	ers A ort:1812 \$	ed ccounting s Enabled None	Servers	•	EAP Pa
Apply Cisco Server 1 Server 2	Authentica C Enabled IP:10.48.3	t Settings Ition Serv 39.128, Po	ers A ort:1812 \$	ed ccounting s Enabled None None	Servers	 	EAP Pa
Apply Cisco Server 1 Server 2 Server 3	Authentica Contemption Authentica Contemption Authentica Contemption Contempti Contemption	t Settings Ition Serv	ers A ort:1812 \$	ed ccounting S Enabled None None None	Servers	 	EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Contempt Contemp	t Settings	ers A ort:1812	ed ccounting S Enabled None None None None	Servers	 <	EAP Pa Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	o ISE Defaul Authentica ✓ Enabled IP:10.48.3 None None None None	t Settings Ition Serv	ers A ort:1812	ed ccounting S Enabled None None None None None	Servers		EAP Pa Enal
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	o ISE Defaul Authentica ✓ Enabled IP:10.48.3 None None None None None	t Settings	ers A ort:1812	ed ccounting s Enabled None None None None None None	Servers		EAP Pa

 Cliquez sur Apply. Remarque : Il s'agit du seul paramètre EAP qui doit être configuré sur le contrôleur pour l'authentification EAP. Toutes les autres configurations spécifiques à EAP-FAST doivent être effectuées sur le serveur RADIUS et les clients qui doivent être authentifiés.

Configurer le serveur RADIUS pour l'authentification EAP-FAST

Procédez comme suit afin de configurer le serveur RADIUS pour l'authentification EAP-FAST :

- 1. Créer une base de données utilisateur pour authentifier les clients EAP-FAST
- 2. Ajouter le WLC en tant que client AAA au serveur RADIUS
- 3. Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement en bande PAC anonyme
- 4. Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC in-band authentifié

Créer une base de données utilisateur pour authentifier les clients EAP-FAST

Cet exemple configure le nom d'utilisateur et le mot de passe du client EAP-FAST comme *<eap_fast>* et *<EAP-fast1>*, respectivement.

1. Dans l'interface utilisateur de l'administrateur Web ISE, naviguez sous « Administration -> Gestion des identités -> Utilisateurs » et appuyez sur l'icône Ajouter.

dentity Services Engine	Home ► Context Visibility ► Op	arations ► Policy -Ad	ministration Vork Cer	iters			
► System - Identity Management	Network Resources Device Portal N	anagement pxGrid Services	Feed Service Three	eat Centric NAC			
▼Identities Groups External Ident	tity Sources Identity Source Sequences	 Settings 					
G							
Users	Network Access Users						
Latest Manual 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 dat	ta available	

2. Remplissez les formulaires requis pour la création de l'utilisateur - "Nom" et "Mot de passe de connexion » et sélectionnez « Groupe d'utilisateurs » dans la liste déroulante ; [Vous pouvez éventuellement remplir d'autres informations pour le compte d'utilisateur] Appuyez sur "Sumbit"

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
► System - Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
▼Identities Groups External Ident	ity Sources Identity Source Sequences
G	
Users	
Latest Manual Network Scan Results	
	Name eap_rast
	Status Zenabled -
	Email
	▼ Passwords
	Password Type: Internal Users 🔹
	Password Re-Enter Password
	* Login Password ••••••• Generate Password (
	Enable Password Generate Password
	▼ User Information
	First Name Test user
	Last Name Test user
	▼ Account Options
	Description
	Change password on peyt login
	✓ Account Disable Policy
	Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)
	* Hear Groune
	Employee
	Submit Cancel
	<i>4</i>
L utilisateur est cre	е
F System ✓ Identity Management F Ne	twork Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Identities Groups External Identity Sc	urces Identity Source Sequences + Settings
N	etwork Access Users

Name

Status

🗌 👩 Enabled 🙎 eap_fast

🖊 Edit 🕂 Add 🛛 Change Status 🗸 🕼 Import 🔐 Export 👻 🗙 Delete 👻 🖓 Duplicate

Description

First Name Last Name

Email Addre

User Identity Gro

Latest Manual Network Scan Results

Complétez ces étapes afin de définir le contrôleur en tant que client AAA sur le serveur ACS :

1. Dans l'interface utilisateur de l'administrateur Web ISE, naviguez sous « Administration -> Network Resources -> Network Devices » et appuyez sur l'icône Ajouter.



2. Remplissez les formulaires requis pour que le périphérique soit ajouté - "Name«, "IP » et configurez le même mot de passe secret partagé, comme nous l'avons configuré sur le WLC dans la section précédente, dans le formulaire Secret partagé" [vous pouvez éventuellement remplir d'autres informations pour le périphérique telles que l'emplacement, le groupe, etc]. Appuyez sur "Sumbit"

cisco	Identity S	ervices Engine	Home	Context	Visibility	 Operations 	Policy	- Adm	ninistration	Work Cen	ters			
► Syst	em ⊧ld	entity Management	- Netwo	rk Resources	Device	Portal Management	pxGrid S	Services	Feed Ser	rvice + Thre	at Centric N	AAC		
▼Netv	vork Device	s Network Devic	e Groups	Network Devi	ce Profiles	External RADIUS	Servers	RADIUS	Server Seque	ences NAC	Managers	External MDM	Location Services	
			O	ark Daviesa Li	at a Manuella	aturals Davies								
Network	Devices		Net	work Devices La	es interview no	etwork Device			_					
Default (Device					• Name WLC5	520							
Device S	Security Se	ttings				Description								
				IP Address	· ·	IP: 10.48.71.20				/ 32				
			0	IPv6 is support	ed only for	TACACS, At least on	e IPv4 mus	t be define	ed when RAD	IUS is selected	1			
					• D	avice Profile det Cis	- A							
						aste Oli	w + w							
					N	Model Name	٣]						
					Softw	vare Version	٣]						
				Network Dev	vice Group									
				Location										
				Location	LAB		Set To Defa	ult						
				IPSEC	Is IPSEC D	evice 📀 📗	Set To Defa	ult						
				Device Type	WLC-lab		Set To Defa	ult						
				- RADIUS	Authenticati	ion Settings								
				RADIUS	UDP Setti	nas								
								Protocol	RADIUS					
							Shar	ed Secret	•••••		Sh	ow		
								CoA Port	1700		Se	t To Default		
				RADIUS	DTLS Sett	ings (j)								
							DTLS	Required						
							Shar	red Secret	radius/dtls		Ð			
								CoA Port	2083		Se	t To Default		
						Issuer CA of ISI	E Certificate	s for CoA	Select if re	quired (optiona	il)	• (i)		

3. Le périphérique est ajouté à la liste des périphériques d'accès au réseau ISE. (NAD)



Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement en bande PAC anonyme

Généralement, on aimerait utiliser ce type de méthode au cas où il n'y aurait pas d'infrastructure d'ICP dans leur déploiement.

Cette méthode fonctionne à l'intérieur d'un tunnel ADHP (Authenticated Diffie-HellmanKey Agreement Protocol) avant que l'homologue n'authentifie le serveur ISE.

Pour prendre en charge cette méthode, nous devons activer "Allow Anonymous In-band PAC Provisioning" sur ISE sous "Authentication Allowed Protocols" :

dentity Services Engine	Home	Operations - Policy	Administration	Work Centers
Policy Sets Profiling Posture C	Client Provisioning - Policy Elements			
Dictionaries + Conditions - Resul	Its			
G	Allow EAP-FAST			
▼Authentication				
Allowed Protocols	EAP-FAST Inner N	ethods		
Authorization		S-CHAPVZ	04-114 Dense 04-0	
▶ Profiling		ssword Change Retries 3	(Valid Range U to 3)
	Allow EAP-G			
▶ Posture	Allow Pa	ssword Change Retries 3	(Valid Range 0 to 3))
Client Provisioning	Allow EAP-TL	.S		
	I Allow Au	thentication of expired certification	ates to allow certificat	te renewal in Authorization Policy
	Use PACs () Don't Use PACs		
	Tunnel PAC	Time To Live	90	Dave
	Proactive P	AC update will occur after 90	% of PAC Time	To Live has expired
		Anonymous In-Band PAC Prov	visioning	
		Authenticated In-Band PAC Pr	ovisioning	
		Conver Returns Access Access	After Authenticated E	travisioning
		erver Returns Access Accept		Tovisioning
	بر <u>ت</u>	Mashina Authoritation	ovisioning	
	Allow	Machine PAC Time To Live		Maria
		Statalogo Sossian Resume	1	weeks *
	Enable	Uthorization PAC Time To Live		u
	, 	anonzatori i no fille lo cive	, T	Hours V
	Enable EAP (Chaining		

Remarque : assurez-vous que vous avez autorisé l'authentification de type de mot de passe, comme EAP-MS-CHAPv2 pour la méthode interne EAP-FAST, car, évidemment, avec le

provisionnement intrabande anonyme, nous ne pouvons utiliser aucun certificat.

Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC in-band authentifié

Il s'agit de l'option la plus sécurisée et recommandée. Le tunnel TLS est construit sur la base du certificat serveur validé par le demandeur et le certificat client validé par ISE (par défaut).

Cette option nécessite une infrastructure PKI pour le client et le serveur, bien qu'elle puisse être limitée au côté serveur uniquement ou ignorée des deux côtés.

Sur ISE, il existe deux options supplémentaires pour le provisionnement intrabande authentifié :

- « Server Retourne Access Accept After Authenticated Provisioning" Normalement, après le provisionnement PAC, un Access-Reject doit être envoyé, obligeant le demandeur à se réauthentifier à l'aide de PAC. Cependant, comme le provisionnement PAC est effectué dans un tunnel TLS authentifié, nous pouvons répondre immédiatement avec Access-Accepcept pour minimiser le temps d'authentification. (dans ce cas, assurez-vous que vous avez des certificats de confiance côté client et côté serveur).
- « Accepter le certificat client pour provisionnement » si vous ne voulez pas fournir l'infrastructure PKI aux périphériques clients et que vous avez uniquement un certificat de confiance sur ISE, activez cette option, qui permet d'ignorer la validation du certificat client côté serveur.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cli	ent Provisioning -Policy Elements
Dictionaries + Conditions - Results	
0	- Illow EAP-FAST
▼Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	
▶ Profiling	Allow Password Unange Retnes 3 (Valid Range 0 to 3)
	Allow EAP-GTC
▶ Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)
Client Provisioning	✓ Allow EAP-TLS
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
	Use PACs O Don't Use PACs
	Days *
	Proactive PAC update will occur atter 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 (i)
	Enable EAP Chaining

Sur ISE, nous définissons également un ensemble de stratégies d'authentification simple pour les utilisateurs sans fil. L'exemple ci-dessous utilise comme paramètre de condition le type de périphérique et l'emplacement et le type d'authentification, le flux d'authentification correspondant à cette condition sera validé par rapport à la base de données utilisateur interne.

Internal Users

Vérification

Cet exemple montre les paramètres de configuration du flux de provisionnement PAC intrabande authentifié et du NAM (Network Access Manager), ainsi que les débogages WLC respectifs.

Configuration du profil NAM

Les étapes suivantes doivent être effectuées afin de configurer le profil Anyconnect NAM pour authentifier la session utilisateur contre ISE en utilisant EAP-FAST :

- 1. Ouvrez Network Access Manager Profile Editor et chargez le fichier de configuration actuel.
- 2. Assurez-vous que "EAP-FAST" est activé sous « Modes d'authentification autorisés »

File Help	Authentication Policy Profile: Untitled	
Authentication Policy Networks	Allow Association Modes Select All (Personal) Open (no encryption) Open (Static WEP) Shared (WEP) WPA Personal TKIP WPA Personal AES WPA2 Personal TKIP WPA2 Personal AES WPA2 Personal TKIP WPA2 Personal AES WPA2 Personal AES WPA2 Personal TKIP WPA2 Personal TKIP WPA2 Personal TKIP WPA2 Personal TKIP WPA2 Personal AES WPA2 Personal AES WPA2 Enterprise) WPA Enterprise TKIP WPA2 Enterprise AES WPA2 Enterprise AES WPA2 Enterprise TKIP WPA2 Enterprise AES CCKM Enterprise TKIP CCKM Enterprise AES	Allowed Authentication Modes Select All Outer EAP-FAST EAP-GTC EAP-MSCHAPV2 EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-MSCHAPV2 PAP (legacy) CHAP (legacy) MSCHAP (legacy) MSCHAPV2 (legacy) EAP-AP EAP-GTC EAP-MSCHAPV2 EAP-TLS Allowed Wired Security Select All Open (no encryption) S02. 1x with MacSec
	🚺 Help	

3. "Ajouter » un nouveau profil réseau :

AnyConnect Profile Editor	- Network Access Ma	nager			- 🗆	×
File Help						
Network Access Manager	Networks Profile: Untit	led				
Networks	Network					^
2 2 · · · · · · · · · · · ·	Name	Media Type	Group*			
	wired	Wired	Global	Add		
				Edit		
				Delete		
	* A mehunduin mu					
	* A network in gr	oup Global is a member of airgr	oups.			
						~
		A Helr				,
		U Help				

4. Sous **« Type de support »** section de configuration définir le profil **"Nom**« , sans fil comme type de réseau de support et spécifier le nom SSID.

File Help Network Access Manager Client Policy Authentication Policy	Networks Profile:ility Client\Network Access Manager\system\configuration.xml		
Network Groups	Name: eap_fast Group Membership In group: Local networks In all 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. Wir-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): eap_fast Hidden Network Seconds Common Settings Script or application on each user's machine to run when connected. Connection Timeout 40 Next Cancel	Medi	a Typ ∧ y Lev
	i Help		

5. Sous l'onglet Configuration **du niveau de sécurité**, sélectionnez Authentification du réseau et spécifiez le mode d'association WPA2 Enterprise (AES)

Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.x	cml	
	Security Level		Media Type
🔆 🏋 Network Groups	Open Network		Security Leve
	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		
	heldPeriod (sec.) 60 maxStart 3		
	heldPeriod (sec.) 60 maxStart 3		
	heldPeriod (sec.) 60 maxStart 3 -Association Mode		
	heldPeriod (sec.) 60 maxStart 3 -Association Mode		
	heldPeriod (sec.) 60 maxStart 3 Association Mode		
	heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) v		
	heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) V		
	heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) v		
	heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) >		
	heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) >		
	Association Mode WPA2 Enterprise (AES) Next		>

6. Dans cet exemple, nous utilisons l'authentification de type utilisateur, donc sous l'onglet suivant **"Type de connexion"** sélectionnez **"Connexion utilisateur »**

AnyConnect Profile Editor -	Network Access Manager	-		×
File Help	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Network Connection Type		Media	Type ^
Network Groups	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. User Connection The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in. 		Securit Connect User Crede	/Leve ion Ty Auth ntials
	Help			

7. Sous l'onglet **Authentification utilisateur**, spécifiez EAP-FAST comme méthode d'authentification autorisée et désactivez la validation du certificat du serveur, car nous n'utilisons pas de certificats de confiance dans cet exemple.

AnyConnect Profile Editor - Ne	twork Access Manager		– 🗆 ×
Network Access Manager	Vetworks Profile:ility Client\Netwo	ork Access Manager\system\configuration	on.xml
Network Groups	EAP Methods EAP-TLS EAP-TLS EAP-TLS EAP-TTLS EXtend user connection bo EAP-FAST Settings Validate Server Identity Enable Fast Reconnect Disable when using a 1 Inner Methods based on Credentia Authenticate using a Pass EAP-MSCHAPv2 If using PACs, allow u Authenticate using a Certi Only send client certificate Authenticate using a Toke Use PACs	PEAP ● EAP-FAST eyond log off Smart Card als Source word EAP-GTC inauthenticated PAC provisioning ificate d the client certificate in the clear ficates inside the tunnel using EAP-TLS in the tunnel en and EAP-GTC	Media Type A Security Leve Connection Ty User Auth Credentials
	Nex	ct Cancel	~
		👔 Help	

Remarque : dans un environnement de production réel, assurez-vous que le certificat de confiance est installé sur ISE et conservez l'option de validation du certificat de serveur activée dans les paramètres NAM.

Note: l'option « Si vous utilisez des PAC, autorisez le provisionnement PAC non authentifié » doit être sélectionnée uniquement en cas de provisionnement PAC intrabande anonyme.

8. Définissez les informations d'identification de l'utilisateur, soit en tant qu'authentification unique au cas où vous accepteriez d'utiliser les mêmes informations d'identification que celles utilisées pour la connexion, soit en sélectionnant « Demander des informations d'identification à l'identification » au cas où vous voudriez demander des informations d'identification à l'utilisateur lors de la connexion au réseau, ou définissez des informations d'identification statiques pour ce type d'accès. Dans cet exemple, nous invitons l'utilisateur à entrer des informations d'identification lors de la tentative de connexion au réseau.

	×

AnyConnect Profile Editor - Network Access Man	ager
--	------

- Use	er Identity		Media Type /
	nprotected Identity Pattern:	aponymous	Security Leve
	nprotected racing raterin		 Connection Ty
P	rotected Identity Pattern:	[username]	User Auth
			Credentials
_ Use	er Credentials		
		s	
		5	
	Prompt for Credentials		
	Remember Forever		
	Remember while User	is Logged On	
	Never Remember		
	O Use Static Credentials		
	Password:		
	Done	Cancel	
<			>

9. Enregistrez le profil configuré dans le dossier NAM correspondant.

Testez la connectivité au SSID à l'aide de l'authentification EAP-FAST.

1. Sélectionnez le profil correspondant dans la liste Anyconnect network

S Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Verify your network connection.	~	Cc	onnect	
No Network C	onnectivity				
	Network: Authenticating				
_	eap_fast		llı. 🖰	\sim	≔
	eap_fast		8	att	
				att	_
	(Standa		_	all	
			8	all	
				alli	
		_	Ë	an	_

- 2. Entrez le nom d'utilisateur et le mot de passe requis pour l'authentification
- 3. Accepter le certificat du serveur (auto-signé)

Cisco AnyConnect	×			
The server certificate failed validation. Do y	e for the network 'office_hq' has 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. done

🕙 Cisco AnyC	connect Secure Mobility Client	—		\times
	VPN: Network error. Unable to lookup host	name:	s. Connect	
Limited Acces	s - DNS Failure			
	Network: Connected (192.168.77.34) eap_fast	8	att 🗸 🗄	

Journaux d'authentification ISE

Les journaux d'authentification ISE affichant le flux de provisionnement EAP-FAST et PAC peuvent être affichés sous "**Opérations -> RADIUS -> Journaux en direct**" et peuvent être consultés plus en détail à l'aide de l'icône "**Zoom**" :

1. Le client a démarré l'authentification et ISE proposait EAP-TLS comme méthode d'authentification, mais le client a rejeté et proposé EAP-FAST à la place, c'était la méthode convenue à la fois par le client et ISE.

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. La connexion TLS a démarré entre le client et le serveur pour fournir un environnement protégé pour l'échange PAC et a été effectuée avec succès.

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	e-response
12105	Prepared EAP-Request with another EAP-FAST challenge	е
11006	Returned RADIUS Access-Challenge	
11001	Received RADIUS Access-Request (10 Step latency=133	317 ms)
11018	RADIUS is re-using an existing session	
12104	Extracted EAP-Response containing EAP-FAST challenge	e-response
12812	Extracted TLS ClientKeyExchange message	
12813	Extracted TLS CertificateVerify message	
12804	Extracted TLS Finished message	
12801	Prepared TLS ChangeCipherSpec message	
12002	Propered TLC Finished message	
12816	TLS handshake succeeded	

3. L'authentification interne a démarré et les informations d'identification des utilisateurs ont été validées avec succès par ISE à l'aide de MS-CHAPv2 (authentification basée sur le nom d'utilisateur/mot de passe)