Autenticación EAP-FAST con controladores de LAN inalámbrica e Identity Services Engine

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Convenciones **Antecedentes** PAC Modos de suministro de PAC Configurar Diagrama de la red Configuraciones Configuración del WLC para la Autenticación EAP-FAST Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo Configuración de la WLAN para la Autenticación EAP-FAST Configuración del Servidor RADIUS para la Autenticación EAP-FAST Crear una base de datos de usuario para autenticar clientes EAP-FAST Agregue el WLC como cliente AAA al servidor RADIUS Configure la autenticación EAP-FAST en el servidor RADIUS con aprovisionamiento PAC anónimo en banda Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con Aprovisionamiento PAC Autenticado en Banda Verificación configuración del perfil NAM Pruebe la conectividad con SSID mediante la autenticación EAP-FAST. Registros de autenticación ISE Depuración del lado WLC en el flujo EAP-FAST exitoso Troubleshoot

Introducción

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para EAP (Extensible Authentication Protocol) - autenticación FAST (Flexible Authentication via Secure Tunneling) mediante un servidor RADIUS externo. Este ejemplo de configuración utiliza Identity Services Engine (ISE) como servidor RADIUS externo para autenticar el cliente inalámbrico.

Este documento se centra en cómo configurar el aprovisionamiento de ISE para las credenciales de acceso protegido (PAC) anónimas y autenticadas en banda (Automático) a los clientes inalámbricos.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los puntos de acceso ligeros (LAP) y los WLC de Cisco
- Conocimiento básico del protocolo CAPWAP
- Conocimiento de cómo configurar un servidor RADIUS externo, como Cisco ISE
- Conocimientos funcionales sobre el marco general de EAP
- Conocimientos básicos sobre protocolos de seguridad, como MS-CHAPv2 y EAP-GTC, y conocimientos sobre certificados digitales

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• WLC de la serie 5520 de Cisco que ejecuta la versión de firmware 8.8.111.0AP Cisco serie 4800Anyconnect NAM.Cisco Secure ISE versión 2.3.0.298Switch de la serie Cisco 3560-CX que ejecuta la versión 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El protocolo EAP-FAST es un tipo EAP IEEE 802.1X de acceso público desarrollado por Cisco para admitir clientes que no pueden aplicar una política de contraseña segura y desean implementar un tipo EAP 802.1X que no requiere certificados digitales.

El protocolo EAP-FAST es una arquitectura de seguridad cliente-servidor que cifra las transacciones EAP con un túnel de seguridad de nivel de transporte (TLS). El establecimiento del túnel EAP-FAST se basa en secretos seguros que son exclusivos de los usuarios. Estos secretos seguros se denominan PAC, que el ISE genera utilizando una clave maestra conocida únicamente por el ISE.

EAP-FAST se produce en tres fases:

 Fase cero (fase de aprovisionamiento automático de PAC): fase cero de EAP-FAST, una fase opcional es un medio seguro de túnel para proporcionar un cliente de usuario final EAP-FAST con una PAC para el usuario que solicita acceso a la red. Proporcionar un PAC al cliente del **usuario final es el único propósito de la fase cero**.**Nota:** La fase cero es opcional porque las PAC también se pueden aprovisionar manualmente a los clientes en lugar de utilizar la fase cero.Consulte la sección <u>Modos de aprovisionamiento PAC</u> de este documento para obtener más detalles.

- Fase uno: en la fase uno, el ISE y el cliente de usuario final establecen un túnel TLS basado en la credencial PAC del usuario. Esta fase requiere que se haya proporcionado al cliente de usuario final una PAC para el usuario que intenta obtener acceso a la red y que la PAC se base en una clave maestra que no ha caducado. No hay servicio de red habilitado por la fase uno de EAP-FAST.
- Fase dos: en la fase dos, las credenciales de autenticación de usuario se pasan de forma segura utilizando un método EAP interno compatible con EAP-FAST dentro del túnel TLS al RADIUS creado mediante el PAC entre el cliente y el servidor RADIUS. EAP-GTC, TLS y MS-CHAP se soportan como métodos EAP internos. No se soportan otros tipos EAP para EAP-FAST.

Consulte Cómo funciona EAP-FAST para obtener más información.

PAC

Los PAC son secretos compartidos sólidos que permiten que el ISE y un cliente de usuario final EAP-FAST se autentiquen mutuamente y establezcan un túnel TLS para su uso en la fase dos de EAP-FAST. El ISE genera PACs utilizando la clave maestra activa y un nombre de usuario.

PAC comprende:

- Clave PAC: secreto compartido enlazado a un cliente (y dispositivo cliente) y a la identidad del servidor.
- PAC opaco: campo opaco que el cliente almacena en caché y pasa al servidor. El servidor recupera la clave PAC y la identidad del cliente para autenticarse mutuamente con el cliente.
- Información PAC: como mínimo, incluye la identidad del servidor para permitir que el cliente almacene en caché diferentes PACs. Opcionalmente, incluye otra información como la hora de vencimiento del PAC.

Modos de suministro de PAC

Como se ha mencionado anteriormente, la fase cero es una fase opcional.

EAP-FAST ofrece dos opciones para aprovisionar un cliente con un PAC:

• Aprovisionamiento PAC automático (EAP-FAST Fase 0 o Aprovisionamiento PAC en banda)

• Aprovisionamiento manual (fuera de banda) de PAC

El aprovisionamiento PAC en banda/automático envía un nuevo PAC a un cliente de usuario final a través de una conexión de red segura. El aprovisionamiento automático de PAC no requiere la intervención del usuario de la red ni de un administrador de ISE, siempre que configure el ISE y el cliente de usuario final para que admita el aprovisionamiento automático.

La última versión de EAP-FAST admite dos opciones de configuración de aprovisionamiento PAC en banda diferentes:

Aprovisionamiento anónimo de PAC en banda

Aprovisionamiento PAC autenticado en banda

Nota: Este documento trata estos métodos de aprovisionamiento PAC en banda y cómo configurarlos.

El aprovisionamiento PAC manual/fuera de banda requiere que un administrador de ISE genere archivos PAC, que luego deben distribuirse a los usuarios de red correspondientes. Los usuarios deben configurar los clientes de usuario final con sus archivos PAC.

Configurar

Diagrama de la red



Configuraciones

Configuración del WLC para la Autenticación EAP-FAST

Realice estos pasos para configurar el WLC para la autenticación EAP-FAST:

- 1. Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo
- 2. Configuración de la WLAN para la Autenticación EAP-FAST

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario mediante EAP-FAST y proporciona acceso a los clientes inalámbricos.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

- Elija Security y RADIUS Authentication en la GUI del controlador para mostrar la página RADIUS Authentication Servers . Luego, haga clic en Nuevo para definir un servidor RADIUS.
- Defina los parámetros del servidor RADIUS en la página Servidores de autenticación RADIUS > Nuevo. Estos parámetros incluyen:Dirección IP de servidor RADIUSsecreto compartidonúmero de puertoEstado del servidorEste documento utiliza el servidor ISE con una dirección IP de 10.48.30.128

11111										
cisco	MONITOR	<u>w</u> lans	<u>CONTROLLER</u>	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	RADIUS	Authenti	cation Server	s > New						
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Server In Server IP Shared Se Confirm S Apply Cise Apply Cise Apply Cise Key Wrap Port Numi Server St Support for Server Tir Network I Managem Tunnel Pr PAC Provi IPSec Cisco ACA	dex (Priorit Address(Ip acret Forma acret ishared Secr co ISE Defa co ACA Defa ber atus or CoA meout Jser ent ent Retrans oxy sioning	() v4/Ipv6) it et ult settings ault settings	2 ¢ 10.48.39.128 ASCII ¢ (Designed 1812 Enabled ¢ Enabled ¢ Enabled ¢ Enable Enable Enable Enable Enable Enable	for FIPS custon	ners and requires a	a key wrap comp	liant RAD	IUS server)	

3. Haga clic Aplicar.

Configuración de la WLAN para la Autenticación EAP-FAST

A continuación, configure la WLAN que los clientes utilizan para conectarse a la red inalámbrica para la autenticación EAP-FAST y asignarla a una interfaz dinámica. El nombre WLAN configurado en este ejemplo es **eap fast**. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN eap fast y sus parámetros relacionados:

1. Haga clic en **WLANs** desde la GUI del controlador para mostrar la página de WLANs.Esta página enumera las WLANs que existen en el controlador.

2. Haga clic en Nuevo para crear una nueva WLAN.

cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
WLANs	WLANs										
VLANs WLANs	Current Filte	er: None	e	[Change Filter]	[Clear Filter]					Create New \$ Go	
Advanced) Type	Profile Na	me		WLAN SSID		4	dmin Status	Security Policies	
		WLAN	test			test		E	nabled	[WPA2][Auth(802.1X)]	
	□ <u>2</u>	WLAN	AndroidAP			AndroidAP		E	nabled	[WPA2][Auth(PSK)]	

3. Configure el nombre **eap_fast** WLAN SSID, el nombre del perfil y el ID de WLAN en la página WLANs > New. A continuación, haga clic en **Aplicar**.

ahaha								Sa <u>v</u> e Configuration Ping Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER WIR	ELESS SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	A Home
WLANs	WLANs > New							< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN eap_fast eap_fast 3 \$	•					

- 4. Una vez que crea una nueva WLAN, aparece la página WLAN > Edit para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, servidores RADIUS, políticas de seguridad y parámetros 802.1x.
- 5. Marque la casilla de verificación Admin Status bajo la ficha General Policies para habilitar la WLAN. Si desea que el AP transmita el SSID en sus tramas de baliza, marque la casilla de verificación Broadcast

SSID.

/LANs > Ed	it 'eap_fa	ist'			
General	Security	QoS	Policy-Mappi	ng Advanced	
Profile Nam	e	ea	p_fast		
Туре		WL	AN		
SSID		ea	p_fast		
Status			Enabled		
Security Pol	licies	[W (Mo	/PA2][Auth(802. difications done un	1X)] der security tab will a	ppear after applying the ch
Radio Policy	/	A	l 🗘		
Interface/In	nterface Group	o(G) 🔽	an1477 🗘		
Multicast VI	an Feature		Enabled		
Broadcast S	SID		Enabled		
NAS-ID		nor	ne		

 En "WLAN -> Editar -> Seguridad -> Capa 2" seleccione parámetros WPA/WPA2 y seleccione dot1x para AKM.

Este ejemplo utiliza WPA2/AES + dot1x como seguridad de Capa 2 para esta WLAN. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN.

_ANs > E	dit 'eap_f	ast'				
General	Security	QoS	Policy-Map	ping Adv	anced	
Layer 2	Layer 3	AAA Se	ervers			
Layer 2	Security <mark>6</mark> () M/	WPA+WPA2 AC Filtering	¢)		
Fast Trans	ition					
Fast Transit	tion	Disa	ble 🗘			
Protected	Management	Frame				
PMF		Disal	bled			
WPA+WPA	A2 Parameter	s				
WPA Po	licy					
WPA2 P	olicy		_			
WPA2 E	ncryption	AES	ткір	CCMP256	GCMP128	GCMP256
OSEN P	olicy					
Authentica	ation Key Mar	agement ¹	9			
802.1X		Enable				
ССКМ		Enable	_			
PSK		Enable				
LT 000	1	nahla				

7. En la ficha **"WLAN -> Edit -> Security -> AAA Servers"**, elija el servidor RADIUS apropiado del menú desplegable en 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	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 39.128, Po	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

8. Haga clic en Apply (Aplicar).Nota: Este es el único parámetro EAP que se debe configurar en el controlador para la autenticación EAP. El resto de las configuraciones específicas de EAP-FAST deben realizarse en el servidor RADIUS y en los clientes que deben autenticarse.

Configuración del Servidor RADIUS para la Autenticación EAP-FAST

Realice estos pasos para configurar el servidor RADIUS para la autenticación EAP-FAST:

- 1. Crear una base de datos de usuario para autenticar clientes EAP-FAST
- 2. Agregue el WLC como cliente AAA al servidor RADIUS
- 3. Configure la autenticación EAP-FAST en el servidor RADIUS con aprovisionamiento PAC anónimo en banda
- 4. Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con Aprovisionamiento PAC Autenticado en Banda

Crear una base de datos de usuario para autenticar clientes EAP-FAST

Este ejemplo configura el nombre de usuario y la contraseña del cliente EAP-FAST como <*eap_fast*> y <*EAP-fast1* >, respectivamente.

1. En la interfaz de usuario de ISE Web admin, navegue bajo "Administration -> Identity Management -> Users" y presione el icono "Add".

dentity Services Engine	Home	y	Policy -Administ	ration	nters			
► System - Identity Management	Network Resources De	vice Portal Management	pxGrid Services +	Feed Service + Th	reat Centric NAC			
▼Identities Groups External Ident	ity Sources Identity Source S	equences For Settings						
G								
Users	Network Access User	5						
Latest Manual Network Scan Results	/ Edit 🔒 Add 🔯 Ch	ange Status 👔 Import	t 😭 Export 👻 🗙 De	ete Duplicate				
	Status Name		Description	First Name	Last Name	Email Address	User Identity Groups	Admin
						N	lo data available	

2. Rellene los formularios necesarios para que se cree el usuario: "Nombre" y "Contraseña de inicio de sesión" y seleccione "Grupo de usuarios" en la lista desplegable;[opcionalmente puede rellenar otra información para la cuenta de usuario] Pulse "Sumbit"

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 Identit	y Sources Identity Source Sequences + Settings
0	Network Anness Lisers List > New Network Anness Liser
Users	▼ Network Access User
Latest Manual Network Scan Results	* Name eap fast
	Status Finabled -
	▼ Passwords
	Password Type: Internal Users 💌
	Password Re-Enter Password
	* Login Password Generate Password (
	Enable Password (j
	▼ liser Information
	▼ Account Options
	Description
	Change password on next login
	- Assessed Disable Deline
	Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)
	✓ User Groups
	Employee 💟 — 🕂
	Suomic Cancel
Se crea el usuario	

► System - Identity Management	Network Resources Device Portal Ma	nagement pxGrid Services	Feed Service For	eat Centric NAC			
	ty Sources Identity Source Sequences	 Settings 					
C Users	Network Access Users						
Latest Manual Network Scan Results	/ 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	

Complete estos pasos para definir el controlador como un cliente AAA en el servidor ACS:

1. En la interfaz de usuario de ISE Web admin navegue bajo "Administration -> Network Resources -> Network Devices" y presione el icono "Add".



 Rellene los formularios requeridos para que el dispositivo sea agregado - "Nombre", "IP" y configure la misma contraseña secreta compartida, como configuramos en WLC en la sección anterior, en el formulario "Secreto Compartido" [opcionalmente puede llenar otra información para el dispositivo como ubicación, grupo, etc]. Pulse "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
	Debugli Devices Lista New Network Device
Network Devices	
Default Device	• Name WII C5520
Device Security Settings	Description
	IP Address v P: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	* Davies Profile dth Cisco - P
	Model Name v
	Software Version
	Network Device Group
	Location [LAB O] Set to Default
	ISEC Device Construction Insection Set To Default
	WLC-lab Set To Default
	RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	Shared Secret Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings ()
	DTLS Required 🔲 👔
	Shared Secret radius/dtls ①
	CoA Port 2083 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional) * (i)

3. El dispositivo se agrega a la lista de dispositivos de acceso de red ISE. (NAD)



Configure la autenticación EAP-FAST en el servidor RADIUS con aprovisionamiento PAC anónimo en banda

Por lo general, uno quisiera utilizar este tipo de método en caso de que no tengan infraestructura PKI en su implementación.

Este método funciona dentro de un túnel de protocolo de acuerdo de clave Diffie-Hellman autenticado (ADHP) antes de que el par autentique el servidor ISE.

Para admitir este método, necesitamos habilitar "**"Permitir aprovisionamiento PAC anónimo en banda**" en ISE bajo los "**Protocolos permitidos de autenticación**":

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	Client Provisioning -Policy Elements
Dictionaries + Conditions - Resul	lits
G	Allow EAP-FAST
▼ Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	
▶ Profiling	Allow Password Change Retnes 3 (Valio Range U 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
	Benerice BAC unders will see un after an Alfred Table Time To Live her surgical
	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
	Enable EAP Chaining

Nota: Asegúrese de haber permitido la autenticación de tipo de contraseña, como EAP-MS-CHAPv2 para el método interno EAP-FAST, ya que obviamente con Aprovisionamiento en banda anónimo no podemos utilizar ningún certificado.

Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con Aprovisionamiento PAC Autenticado en Banda

Esta es la opción más segura y recomendada. El túnel TLS se genera basándose en el certificado del servidor que es validado por el solicitante y el certificado del cliente es validado por ISE (valor predeterminado).

Esta opción requiere disponer de infraestructura PKI para el cliente y el servidor, aunque sólo puede limitarse al lado del servidor o omitirse en ambos lados.

En ISE hay dos opciones adicionales para el aprovisionamiento en banda autenticado:

- "Server Devuelve el Acceso Aceptar después de un Aprovisionamiento Autenticado" -Normalmente, después de un Aprovisionamiento PAC, se debe enviar un Rechazo de Acceso que obliga al solicitante a volver a autenticarse mediante PAC. Sin embargo, dado que el aprovisionamiento PAC se realiza en el túnel TLS autenticado, podemos responder inmediatamente con Access-Accept para minimizar el tiempo de autenticación. (en tal caso, asegúrese de que dispone de certificados de confianza en el cliente y en el servidor).
- "Aceptar certificado de cliente para aprovisionamiento": si no se desea proporcionar infraestructura PKI a los dispositivos cliente y sólo se tiene certificado de confianza en ISE, active esa opción, que permite omitir la validación de certificados de cliente en el servidor.

cisco de la companya	
Policy Sets Profiling Posture	lient Provisioning - Policy Elements
Dictionaries + Conditions - Res	ts
(✓ ✓ Allow EAP-FAST
▼Authentication	
Allowed Protocols Allowed Protocols Authorization Profiling Posture Client Provisioning	EAP-FAST Inner Methods Allow EAP-MS-CHAPV2 Allow Password Change Retries 3 (Valid Range 0 to 3) Allow EAP-GTC Allow Password Change Retries 3 (Valid Range 0 to 3) 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 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 Accept Client Certificate For Provisioning Accept Client Certificate For Provisioning Allow Machine Authentication Machine PAC Time To Live <u>1</u> Weeks * Enable Stateless Session Resume Authorization PAC Time To Live <u>1</u> Hours *

En ISE también definimos un conjunto de políticas de autenticación simple para los usuarios inalámbricos. A continuación, el ejemplo utiliza como tipo de dispositivo de parámetro de condición y tipo de ubicación y autenticación, el flujo de autenticación que coincide con esa condición se validará en la base de datos de usuarios interna.

✓ Opuolis

Verificación

En este ejemplo se mostrarán los parámetros de configuración del flujo de aprovisionamiento PAC autenticado en banda y del administrador de acceso de red (NAM) junto con los debugs de WLC respectivos.

configuración del perfil NAM

Se deben realizar los siguientes pasos para configurar el perfil NAM de Anyconnect para autenticar la sesión de usuario con ISE mediante EAP-FAST:

- 1. Abra Network Access Manager Profile Editor y cargue el archivo de configuración actual.
- 2. Asegúrese de que "EAP-FAST" esté habilitado en "Modos de autenticación permitidos"



3. "Agregar" un nuevo perfil de red:

AnyConnect Profile Editor -	Network Access Mar	nager			- 0	×
File Help						
Network Access Manager	Networks Profile: Untitl	ed				
Networks	Network					^
	Name	Media Type	Group*			
	wired	Wired	Global	Add	٦	
				r du		
				Edit		
				Delete		
	* A network in gro	oup 'Global' is a member of <i>all</i> gr	oups.			
	<					>
		🕕 Help)			

4. En la sección de configuración **"Tipo de medios"**, defina el perfil "**Nombre**", como el tipo de red de medios y especifique el nombre SSID.

AnyConnect Profile Editor - Network Access Manager	-		×
File Help			
Network Access Manager Networks Client Policy Profile:ility Client\Network Access Manager\system\configuration.xml			
Authentication Policy Name: eap_fast 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. Image: Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Image: Wired (802.3) Network Select a wire on etwork if the endstations will be connecting to the network with a traditional ethernet cable. Image: Wired (802.3) Network Select a WFi network if the endstations will be connecting to the network with a traditional ethernet cable. Image: Wired (802.3) Network Select a WFi network if the endstations will be connecting to the network with a traditional ethernet cable. Image: Wired (802.3) Network Select a WFi network if the endstations will be connecting to the network with a traditional ethernet cable. Image: Wired (802.3) Network Select a WFi network if the endstations will be connecting to the network with a sociation Timeout Image: Size (Size (WFi network)) Corporate Network Image: Size (Size (Size (WFi network))) Size (Size (Size (WFi network))) Image: Size (Size		Media	y Ley
<			>
1 Help			

5. En la ficha de configuración **"Nivel de seguridad"**, seleccione "Autenticación de red" y especifique el modo de asociación como WPA2 Enterprise (AES)

🐴 AnyConnect Profile Editor - I	Network Access Manager -	- 🗆 X
File Help		
Network Access Manager Client Policy Authentication Policy	Networks Profile:ility Client\Network Access Manager\system\configuration.xml	
Networks	Security Level	Media Type 🔺
└─ 🔆 Network Groups	 Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. Shared Key Network Shared Key Network 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. 	Security Levi Connection Ty
	802.1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30	
	Association Mode	
	Next Cancel	~
	Help	

6. En este ejemplo estamos utilizando la autenticación de tipo de usuario, por lo tanto, en la ficha siguiente "Tipo de conexión" seleccione "Conexión de usuario"

AnyConnect Profile Editor	- Network Access Manager —]	×
File Help Network Access Manager Client Policy Authentication Policy Networks Network Groups	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Network Connection Type	Me Sec	edia T urity	ype ^ Leve
	 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. (e) <u>User Connection</u> 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. (c) 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. 	Conr U: Cr	nectio ser Al	n Ty ith ials
	<			`
	Help			

7. En la ficha "**User Auth**", especifique EAP-FAST como método de autenticación permitido e inhabilite la validación del certificado del servidor, ya que en este ejemplo no utilizamos certificados de confianza.

AnyConnect Profile Editor -	Network Access Manager		– 🗆 ×
File Help Network Access Manager Client Policy	Networks Profile:ility Client\Netw	rork Access Manager\system\configuration	on.xml
Network Groups	EAP Methods EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TS EAP-FAST Settings Validate Server Identity Eable Fast Reconnect Disable when using a Inner Methods based on Credent Authenticate using a Pas EAP-MSCHAPv2 If using PACs, allow to Only send client certificatt Send client certificatt Send client certificatt Authenticate using a Tok Use PACs	PEAP ● EAP-FAST beyond log off a Smart Card tials Source sword ✓ EAP-GTC unauthenticated PAC provisioning tificate ad the client certificate in the clear ificates inside the tunnel e using EAP-TLS in the tunnel eusing EAP-GTC	Media Type A Security Leve Connection Ty User Auth Credentials
	Ne	Cancel	, v
L	x	i) Help	,

Nota: en el entorno de producción real, asegúrese de tener instalado el certificado de confianza en ISE y mantenga la opción de validación del certificado del servidor habilitada en la configuración de NAM.

Nota: opción "Si se utilizan PACs, se debe seleccionar permitir el aprovisionamiento PAC no autenticado" sólo en caso de aprovisionamiento PAC anónimo en banda.

8. Defina las credenciales de usuario, ya sea como SSO en caso de que desee utilizar las mismas credenciales que se usaron para el inicio de sesión, o seleccione "Pedir credenciales" en caso de que desee que se pida al usuario las credenciales mientras se conecta a la red, o defina las credenciales estáticas para ese tipo de acceso. En este ejemplo, solicitamos al usuario credenciales al intentar conectarse a la red.

	×

AnyConnect Profile Editor - Network Access Mar	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		
		5	
		5	
	Prompt for Credentials		
	Remember Forever		
	Remember while User	is Logged On	
	Never Remember		
	O Use Static Credentials		
	Password:		
	Done	Cancel	
<			>

9. Guarde el perfil configurado en la carpeta NAM correspondiente.

Pruebe la conectividad con SSID mediante la autenticación EAP-FAST.

1. Seleccionar el perfil respectivo de la lista de redes de Anyconnect

real Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Verify your network connection.	~	Con	nect	
No Network C	onnectivity				
	Network: Authenticating				
_	eap_fast		llı. 🖰	~ :	
	eap_fast		8	att p	
				att 🗖	-
	(Shame			att	
				att	
				att	
			8	att	

- 2. Introduzca el nombre de usuario y la contraseña necesarios para la autenticación
- 3. Aceptar certificado de servidor (firmado automáticamente)

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. Fin

🕙 Cisco AnyC	connect Secure Mobility Client	_		\times
	VPN: Network error. Unable to lookup host	names	s. Connect	
Limited Acces	s - DNS Failure			
	Network: Connected (192.168.77.34) eap_fast	A	atl 🗸	

Registros de autenticación ISE

Los registros de autenticación ISE que muestran el flujo de aprovisionamiento de EAP-FAST y PAC se pueden ver en "**Operaciones -> RADIUS -> Registros en directo**" y se pueden ver en más detalles usando el icono "**Zoom**":

1. El cliente ha iniciado la autenticación e ISE estaba proponiendo EAP-TLS como método de autenticación, pero el cliente rechazó y propuso EAP-FAST en su lugar, ese era el método en el que el cliente y el ISE estaban de acuerdo.

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. El intercambio de señales TLS se inició entre el cliente y el servidor para proporcionar un entorno protegido para el intercambio PAC y se completó correctamente.

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	Property TLC Finished message
12816	TLS handshake succeeded

3. Se inició la autenticación interna y las credenciales de usuario fueron validadas correctamente por ISE mediante MS-CHAPv2 (autenticación basada en nombre de usuario/contraseña)