Autenticação EAP-FAST com Wireless LAN Controllers e Identity Services Engine

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Informações de Apoio PAC Modos de provisionamento de PAC Configurar Diagrama de Rede **Configurações** Configurar a WLC para a autenticação EAP-FAST Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo Configurar a WLAN para a autenticação EAP-FAST Configurar o servidor RADIUS para autenticação EAP-FAST Criar um banco de dados de usuário para autenticar clientes EAP-FAST Adicione a WLC como cliente AAA ao servidor RADIUS Configurar a autenticação EAP-FAST no servidor RADIUS com provisionamento PAC em banda anônima Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento PAC em banda autenticado Verificar configuração de perfil NAM Teste a conectividade com o SSID usando a autenticação EAP-FAST. Logs de autenticação do ISE Depuração lateral de WLC no fluxo EAP-FAST completo Troubleshoot

Introduction

Este documento explica como configurar o Controller de LAN Wireless (WLC) para uma autenticação Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST) com o uso de um servidor RADIUS externo. Este exemplo de configuração usa o Identity Services Engine (ISE) como o servidor RADIUS externo para autenticar o cliente sem fio.

Este documento enfatiza como configurar o ISE para o provisionamento de PACs (Credenciais de Acesso Protegido) Anônimas e Autenticadas em Banda (Automáticas) para os clientes sem fio.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração de pontos de acesso leves (LAPs) e Cisco WLCs
- Conhecimento básico do protocolo CAPWAP
- Conhecimento de como configurar um servidor RADIUS externo, como o Cisco ISE
- Conhecimentos funcionais sobre o quadro geral de PEA
- Conhecimento básico sobre protocolos de segurança, como MS-CHAPv2 e EAP-GTC, e conhecimento sobre certificados digitais

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

 Cisco 5520 Series WLC que executa o firmware versão 8.8.111.0AP Cisco 4800 SeriesAnyconnect NAM.Cisco Secure ISE versão 2.3.0.298Switch Cisco 3560-CX Series que executa a versão 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

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Informações de Apoio

O protocolo EAP-FAST é um tipo de EAP IEEE 802.1X acessível ao público que a Cisco desenvolveu para suportar clientes que não podem aplicar uma política de senha forte e querem implantar um tipo de EAP 802.1X que não requer certificados digitais.

O protocolo EAP-FAST é uma arquitetura de segurança cliente-servidor que criptografa transações EAP com um túnel TLS (Transport Level Security). O estabelecimento do túnel EAP-FAST baseia-se em segredos fortes que são exclusivos dos usuários. Esses segredos fortes são chamados de PACs, que o ISE gera usando uma chave mestra conhecida apenas pelo ISE.

O EAP-FAST ocorre em três fases:

• Fase zero (fase de provisionamento automático da PAC) — fase zero do EAP-FAST, uma fase opcional é um meio protegido por túnel para fornecer uma PAC ao usuário final do EAP-FAST com uma PAC para o usuário que solicita acesso à rede. Fornecer uma PAC ao cliente do usuário final é a única finalidade da fase zero.Observação: a fase zero é opcional porque as PACs também podem ser provisionadas manualmente para os clientes em vez de usar a fase zero.Consulte a seção Modos de Provisionamento PAC deste documento para obter

detalhes.

- Fase um Na fase um, o ISE e o cliente de usuário final estabelecem um túnel TLS com base na credencial PAC do usuário. Essa fase exige que o cliente do usuário final tenha recebido uma PAC para o usuário que está tentando obter acesso à rede e que a PAC seja baseada em uma chave mestre que não expirou. Nenhum serviço de rede é ativado pela fase um do EAP-FAST.
- Fase dois Na fase dois, as credenciais de autenticação de usuário são passadas com segurança usando um método EAP interno suportado pelo EAP-FAST dentro do túnel TLS para o RADIUS criado usando a PAC entre o cliente e o servidor RADIUS. EAP-GTC, TLS e MS-CHAP são suportados como métodos EAP internos. Nenhum outro tipo de EAP é suportado para EAP-FAST.

Consulte Como o EAP-FAST funciona para obter mais informações.

PAC

As PACs são fortes segredos compartilhados que permitem que o ISE e um cliente de usuário final EAP-FAST se autentiquem e estabeleçam um túnel TLS para uso na fase dois EAP-FAST. O ISE gera PACs usando a chave mestra ativa e um nome de usuário.

A PAC inclui:

- **PAC-Key** Segredo compartilhado associado a um cliente (e dispositivo cliente) e identidade do servidor.
- PAC opaco Campo opaco que o cliente armazena em cache e passa para o servidor. O servidor recupera a chave PAC e a identidade do cliente para se autenticar mutuamente com o cliente.
- PAC-Info No mínimo, inclui a identidade do servidor para permitir que o cliente armazene em cache diferentes PACs. Opcionalmente, ele inclui outras informações, como a hora de expiração da PAC.

Modos de provisionamento de PAC

Como mencionado anteriormente, a fase zero é uma fase opcional.

O EAP-FAST oferece duas opções para provisionar um cliente com uma PAC:

- Provisionamento automático de PAC (fase 0 EAP-FAST ou aprovisionamento de PAC em banda)
- Provisionamento de PAC manual (fora da banda)

O provisionamento PAC em banda/automático envia uma nova PAC a um cliente de usuário final através de uma conexão de rede segura. O provisionamento automático de PAC não requer intervenção do usuário da rede ou de um administrador do ISE, desde que você configure o ISE e o cliente do usuário final para suportar o provisionamento automático.

A versão EAP-FAST mais recente suporta duas opções diferentes de configuração de provisionamento PAC na banda:

- Provisionamento de PAC em banda anônima
- Provisionamento de PAC em banda autenticado

Observação: este documento discute esses métodos de provisionamento de PAC em banda e como configurá-los.

O **provisionamento de PAC fora da banda/manual** exige que um administrador do ISE gere arquivos PAC, que devem ser distribuídos para os usuários de rede aplicáveis. Os usuários devem configurar clientes de usuário final com seus arquivos PAC.

Configurar

Diagrama de Rede



Configurações

Configurar a WLC para a autenticação EAP-FAST

Execute estas etapas para configurar a WLC para autenticação EAP-FAST:

- 1. Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo
- 2. Configurar a WLAN para a autenticação EAP-FAST

Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário usando EAP-FAST e fornece acesso aos clientes sem fio.

Conclua estes passos para configurar a WLC para um servidor RADIUS externo:

- Escolha Segurança e Autenticação RADIUS na GUI do controlador para exibir a página Servidores de Autenticação RADIUS. Em seguida, clique em New para definir um servidor RADIUS.
- Defina os parâmetros do servidor RADIUS na página Servidores de Autenticação RADIUS > Novo. Esses parâmetros incluem:Endereço IP do servidor RADIUSshared secretnúmero da portaStatus do servidorEste documento usa o servidor ISE com um endereço IP 10.48.39.128.

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLEF	R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serve	vers > 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 AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	2 \$ 10.48.39.128 ASCII \$ ASCII \$ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) 1812 Enabled \$ Enabled \$ S seconds Enable S seconds Enable Enable Enable Enable Enable Enable Enable Enable

3. Clique em Aplicar.

Configurar a WLAN para a autenticação EAP-FAST

Em seguida, configure a WLAN que os clientes usam para se conectar à rede sem fio para autenticação EAP-FAST e atribua a uma interface dinâmica. O nome da WLAN configurado neste exemplo é **muito rápido**. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN eap fast e seus parâmetros relacionados:

- 1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs.Esta página lista as WLANs que existem na controladora.
- 2. Clique em New para criar uma nova WLAN.

l.ı.lı. cısco		Ns <u>C</u> ONTROL	ER WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	<	
WLANs	WLANs								
VLANs WLANs	Current Filter:	None	[Change Filter]	[Clear Filter]				Create New Go	
Advanced	WLAN ID Ty	pe Profi	e Name		WLAN SSID		Admin Statu	s Security Policies	
	□ <u>1</u> WL	AN test			test		Enabled	[WPA2][Auth(802.1X)]	
	2 WL	AN Andro	idAP		AndroidAP		Enabled	[WPA2][Auth(PSK)]	

 Configure o nome SSID da WLAN eap_fast, o nome do perfil e a ID da WLAN na página WLANs > Nova. Em seguida, clique em Aplicar.

ahaha				Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS COM	NTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP FEEDBACK	🔒 <u>H</u> ome
WLANs	WLANs > New			< Back Apply
 ✓ WLANS WLANS ▶ Advanced 	Type Profile Name SSID ID	WLAN cop_fost cop_fost 3 ¢		

- 4. Depois de criar uma nova WLAN, a página WLAN > Edit para a nova WLAN é exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, servidores RADIUS, políticas de segurança e parâmetros 802.1x.
- Marque a caixa de seleção Admin Status na guia General Policies para habilitar a WLAN. Se você quiser que o AP transmita o SSID em seus quadros de beacon, marque a caixa de seleção Transmitir SSID.

WLANs > E	dit 'eap_fa	st'								
General	Security	QoS	Policy-M	apping	Advanced					
Profile Na	me	eap	o_fast							
Туре		WL	AN							
SSID		eap	o_fast							
Status			Enabled							
Security F	Security Policies		PA2][Auth(difications do	802.1X)] ne under s	ecurity tab will a	ppear	after apply	ying the o	changes.)	
Radio Pol	icy	A	I	\$						
Interface,	Interface Group	(G) Vla	an1477 🗘]						
Multicast	Vlan Feature		Enabled	L						
Broadcast	t SSID		Enabled							
NAS-ID		non	ne							

6. Sob "WLAN -> Editar -> Segurança -> Camada 2" escolha os parâmetros WPA/WPA2 e selecione dot1x para AKM. Este exemplo usa WPA2/AES + dot1x como segurança da camada 2 para esta WLAN. Os

outros parâmetros podem ser modificados com base no requisito da rede WLAN.

ANs > E	dit 'eap_	fast'				
General	Security	QoS	Policy-Map	ping Adv	vanced	
Layer 2	Layer 3	AAA S	ervers			
Layer 2	Security 🧧	WPA+WPA2 MAC Filtering	2)		
Fast Trans	ition					
Fast Transit	tion	Disa	able 🗘			
Protected	Manageme	nt Frame				
PMF		Disa	abled			
WPA+WPA	A2 Paramet	ers				
WPA Po	licy					
WPA2 P	olicy		_			
WPA2 E	ncryption	AE	S TKIP	CCMP256	GCMP128	GCMP256
OSEN P	olicy					
Authentica	ation Key M	anagement	<u>19</u>			
802.1X	·	Enable				
ССКМ		Enable				
PSK		Enable				
ET 902	1	Enable				

7. Na guia "WLAN -> Edit -> Security -> AAA Servers", escolha o servidor RADIUS apropriado no menu suspenso em RADIUS Servers.

neral	Security	QoS	Policy-M	apping	Advanced		
ayer 2	Layer 3		Servers				
ADIUS Serv RADIUS Se	ervers belo v ers erver Overwi	w to ove	rride use of	default ser ed	vers on this W	/LAN	
Apply Cisco	o ISE Defaul	t Settings	🗆 Enable	ed			
Apply Cisco	o ISE Defaul	t Settings	Enable	ccounting S	Servers		EAP P
Apply Cisco Server 1	Authentica	t Settings ation Serv 39.128, Pc	Enable	ccounting S Enabled None	Servers	•	EAP P Ena
Apply Cisco Server 1 Server 2	Authentica Contempt for the second se	t Settings ation Serv 39.128, Pc	Enable	ccounting S Enabled None None	Servers	¢ \$	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3	Authentica Contraction Authentica Contraction Authentica Contraction Contract	t Settings ation Serv 39.128, Pc	Enable	ed CCOUNTING S Enabled None None None	Servers	 	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Contraction Authentica Contraction Contraction Authentica Contraction Contraction Authentica Contraction Contracti	t Settings ntion Serv 39.128, Pc	Enable /ers Ac ort:1812	ed ccounting S Enabled None None None None	Servers	 <	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Control Enabled IP:10.48.3 None None None None	t Settings ation Serv 39.128, Pc	Cers Ac	ed ccounting S Enabled None None None None None	Servers	$\Rightarrow \Rightarrow $	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Authentica Authentica Enabled IP:10.48.3 None None None None None	t Settings	Enable	ed ccounting S Enabled None None None None None None	Servers	$\Rightarrow \Rightarrow \Rightarrow \Rightarrow \Rightarrow \Rightarrow$	EAP P Ena

8. Clique em Apply. Observação: esta é a única configuração de EAP que precisa ser configurada no controlador para autenticação de EAP. Todas as outras configurações específicas do EAP-FAST precisam ser feitas no servidor RADIUS e nos clientes que precisam ser autenticados.

Configurar o servidor RADIUS para autenticação EAP-FAST

Execute estas etapas para configurar o servidor RADIUS para autenticação EAP-FAST:

- 1. Criar um banco de dados de usuário para autenticar clientes EAP-FAST
- 2. Adicione a WLC como cliente AAA ao servidor RADIUS
- 3. Configurar a autenticação EAP-FAST no servidor RADIUS com provisionamento PAC em banda anônima
- 4. Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento PAC em banda autenticado

Criar um banco de dados de usuário para autenticar clientes EAP-FAST

Este exemplo configura o nome de usuário e a senha do cliente EAP-FAST como <*eap_fast*> e <*EAP-fast1*>, respectivamente.

1. Na IU do administrador da Web do ISE, navegue em "Administration -> Identity Management -> Users" e pressione o ícone "Add".

diale Ident	ity Services Engine	Home Contex	kt Visibility → Ope	arations)	Policy -A	dministratio	Work Cer	nters			
System	- Identity Management	 Network Resources 	Device Portal N	lanagement	pxGrid Service	es 🕨 Feed	Service + Thr	eat Centric NAC			
▼ Identities	Groups External Identi	ty Sources Identity	Source Sequences	 Settings 							
	0										
Users		Network Acces	ss Users								
Latest Manua	Network Scan Results	/ Edit 🔒 Add	🔀 Change Status	💽 Import	🕞 Export 👻	XDelete	Duplicate				
		Status	Name	•	Description		First Name	Last Name	Email Address	User Identity Groups	Admin
										No data available	

2. Preencha os formulários necessários para que o usuário seja criado - "Nome" e "Senha de login" e selecione "Grupo de usuários" na lista suspensa;[opcionalmente, você pode preencher outras informações para a conta de usuário] Prima "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
	ty Sources Identity Source Sequences + Settings
0	Network Access Lines Lint S New Network Access Lines
Users	▼ Network Access User
Latest Manual Network Scan Results	* Name eao fast
	Status Replied *
	Email
	▼ Passwords
	Password Type: Internal Users 💌
	Password Re-Enter Password
	* Login Password Generate Password (i)
	Enable Password (i)
	V liser Information
	▼ Account Options
	Description
	Change password on next login
	✓ Account Disable Policy
	Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)
	▼ User Groups
	Submit Cancel
O usuário é criado.	

► System - Identity Management	Network Resources Device Performance	ortal Management pxGrid Service	es + Feed Service + Th	reat Centric NAC				
▼Identities Groups External Identity Sources Identity Source Sequences → Settings								
() Users	sers Network Access Users							
Latest Manual Network Scan Results	🖊 Edit 🕂 Add 🔣 Change St	atus 👻 🎲 Import 🔹 Export 👻	🗙 Delete 👻 🕒 Duplicate					
	Status Name	 Description 	First Name	Last Name En	nail Address User Identity Grou	os Admin		
	🗌 🔄 Enabled 🙎 eap_fast	\oplus	Test user	Test user	Employee			

Conclua estes passos para definir o controlador como um cliente AAA no servidor ACS:

1. Na IU do administrador da Web do ISE, navegue em "Administração -> Recursos de rede -> Dispositivos de rede" e pressione o ícone "Adicionar".



Preencha os formulários necessários para que o dispositivo seja adicionado - "Nome", "IP" e configure a mesma senha secreta compartilhada, como configuramos na WLC na seção anterior, no formulário "Segredo compartilhado" [opcionalmente, você pode preencher outras informações para o dispositivo, como localização, grupo, etc].
 Prima "Sumbit"

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
	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
Network Devices	Network Devices List > New Network Device
Default Device	* Name Un CESO
Device Security Settings	Description
	IP Address + IP: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	Davise Profile dtt Cisco -
	Model Name 🔹 👻
	Software Version
	Network Device Group
	Location LAB C Set To Default
	IPSEC Is IPSEC Device O Set To Default
	Device Type WLC-lab O 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
	CoA Port 2083 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional) *
	DNP Name

3. O dispositivo é adicionado à lista de dispositivos de acesso à rede ISE. (NAD)



Configurar a autenticação EAP-FAST no servidor RADIUS com provisionamento PAC em banda anônima

Em geral, gostaríamos de usar esse tipo de método caso eles não tenham infraestrutura de PKI em sua implantação.

Esse método opera dentro de um túnel Authenticated Diffie-HellmanKey Agreement Protocol (ADHP) antes que o peer autentique o servidor ISE.

Para suportar este método, precisamos habilitar "**Allow Anonymous In-band PAC Provisioning**" no ISE sob **"Authentication Allowed Protocols**":

cisco	Ident	ity Service	es Engine	Home	Contex	t Visibility	Operations	+ Policy	Administration	Work Centers
Policy	Sets	Profiling	Posture	Client Provis	sioning -P	olicy Elements				
Dictio	naries	In Condition	ions 🔻 F	Results						
				0	Allov	V EAP-FAST				
▼ Author	nticati	on								
Allov	ved Pro	tocols			EA	P-FAST Inner I	Methods			
• Autho	orizatio	n						Detrice D	0/alid Dagas 0 to	2)
▶ Profil	ina						rassword Chang	je Retnes 3	(valid Range 0 to	3)
							310	Detter D	04-114 B 04	
▶ Postu	Ire					- Allow P	assword Chang	ge Retries 3	(valid Range 0 to	3)
► Client	Provi	sioning				Allow EAP-T	LS			
						Allow A	Authentication of	expired certific	ates to allow certifica	ate renewal in Authorization Policy
					۲	Use PACs	O Don't Use F	ACs		
						Tunnel PA	C Time To Live		90	Davs *
						Proactive F	PAC update will	occur after 90	% of PAC Time	e To Live has expired
						Allow	Anonymous In-	Band PAC Pro	visioning	
						Allow	Authenticated	In-Band PAC Pr	ovisioning	
						✓	Server Returns	Access Accept	After Authenticated	Provisioning
							Accept Client C	ertificate For Pr	ovisioning	
						Allow	Machine Authe	entication		
							Machine PAC T	ime To Live	1	Weeks *
						Enab	le Stateless Ser	ssion Resume		
							Authorization P/	AC Time To Live	1	Hours v 🕡
						Fachla FAD	Chaisian			
						Enable EAP	Chaining			

Observação: certifique-se de que você tenha permitido a autenticação de tipo de senha, como EAP-MS-CHAPv2 para o método interno EAP-FAST, já que obviamente com o provisionamento

em banda anônima não podemos usar nenhum certificado.

Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento PAC em banda autenticado

Essa é a opção mais segura e recomendada. O túnel TLS é construído com base no certificado do servidor que é validado pelo requerente e o certificado do cliente é validado pelo ISE (padrão).

Essa opção exige uma infraestrutura de PKI para cliente e servidor, embora possa ser limitada apenas ao lado do servidor ou ignorada em ambos os lados.

No ISE, há duas opções adicionais para o provisionamento Autenticado em banda:

- "Server Devolve Access Accept After Authenticated Provisioning" Normalmente, após o provisionamento PAC, um Access-Reject deve ser enviado forçando o requerente a reautenticar usando PACs. No entanto, como o provisionamento de PAC é feito em túnel TLS autenticado, podemos responder imediatamente com Access-Accept para minimizar o tempo de autenticação. (nesse caso, verifique se você tem certificados confiáveis no lado cliente e servidor).
- "Aceitar Certificado do Cliente para Provisionamento" se não se quiser fornecer infraestrutura de PKI para dispositivos do cliente e apenas se tiver um certificado confiável no ISE, ative essa opção, que permite ignorar a validação do certificado do cliente no lado do servidor.

cisco Identity Services Engine	Home + Context Visibility + Operations - Policy + Administration + Work Centers
Policy Sets Profiling Posture C	ient Provisioning -Policy Elements
Dictionaries + Conditions - Result	IS CONTRACTOR OF CONT
0	✓ Allow EAP-FAST
▼Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	Allow EAP-MS-CHAPv2
- Desfilie -	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 Provisioning	Allow EAP-TLS
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
	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 Hours *
	Enable FAP Chaining

No ISE, também definimos uma política de autenticação simples para usuários sem fio, abaixo, por exemplo, está usando como parâmetro de condição o tipo de dispositivo e o local e o tipo de autenticação, o fluxo de autenticação correspondente a essa condição será validado no banco de dados de usuário interno.

Wreless_602.1X

Verificar

Este exemplo mostrará as configurações de fluxo de Provisionamento de PAC Autenticado em Banda e de NAM (Network Access Manager) juntamente com as respectivas depurações de WLC.

configuração de perfil NAM

As etapas a seguir precisam ser feitas para configurar o perfil do AnyConnect NAM para autenticar a sessão do usuário em relação ao ISE usando EAP-FAST:

- 1. Abra o Editor de perfis do Network Access Manager e carregue o arquivo de configuração atual.
- 2. Certifique-se de que "EAP-FAST" está ativado em "Modos de Autenticação Permitidos"

AnyConnect Profile Editor -	Network Access Manager	- L ×
Network Access Manager Client Policy	Authentication Policy Profile: Untitled	
Authentication Policy	Allow Association Modes 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 TKIP WPA2 Personal AES Open (Dynamic (802.1X) WEP) WPA Enterprise TKIP WPA2 Enterprise AES WPA2 Enterprise TKIP WPA2 Enterprise TKIP CCKM Enterprise TKIP CCKM Enterprise AES CCKM Enterprise AES	Allowed Authentication Modes Select All Outer EAP-FAST EAP-GTC EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-MDS EAP-MSCHAPv2 PAP (legacy) CHAP (legacy) MSCHAP (legacy) MSCHAPv2 (legacy) EAP- EAP- EAP- EAP- Select All Open (no encryption) 802. 1x with MacSec
	Help	

3. "Adicionar" um novo perfil de rede:

🕍 AnyConnect Profile Editor	- Network Access Ma	nager		_		×
File Help						
Network Access Manager	Networks Profile: Untit	led				
Networks	Network					^
55	Name	Media Type	Group*		_	
	WIEG	Wired	Giobai	Add		
				Edit		
				Delete		
	* A network in gr	oup 'Global' is a member of <i>all</i> gro	oups.			
						v
	<					>
		() Help				

4. Na seção de configuração **"Tipo de mídia", defina o perfil "Nome**", sem fio como o tipo de rede de mídia e especifique o nome SSID.

🚵 AnyConnect Profile Editor - N	etwork Access Manager	-		×
File Help				
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml			
Authentication Policy	Profile: lity Client\Network Access Manager\system\configuration.xml 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. WirFi (wireless) Network Select a WFi 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 Corporate Network Association Timeout seconds Connection Timeout seconds Next Cancel 		Media	y Les
	() Help			

5. Na guia de configuração "**Nível de segurança"** selecione "Autenticando rede" e especifique o modo de associação como WPA2 Enterprise (AES)

File Help				
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml			
Networks	Security Level	1	Media Type	~
K Network Groups	Open Network		Security Leve	
	Open networks have no security, and are open to anybody within range. This is	C	onnection Ty	
	the least secure type of network.			
	◯ 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			
	-Association Mode	-		
	Next Cancel			
I	N Help		,	

6. Neste exemplo, estamos usando a autenticação de tipo de usuário, portanto, na próxima guia **"Tipo de conexão"**, selecione **"Conexão do usuário"**

File Help	-		×
Network Access Manager Client Policy Profile:ility Client\Network Access Manager\system\configuration.xml			
Network Groups Network Groups Machine Connection Machine Connection This is 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: 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. Next Cancel		Media Security Connecti User / Creder	Type ^ / Leve on Ty Auth ntials
< Heb			>

7. Na guia "**User Auth**", especifique EAP-FAST como método de autenticação permitido e desative a validação do certificado do servidor, já que não estamos usando certificados confiáveis neste exemplo.

AnyConnect Profile Editor -	Network Access Manager		- 🗆 ×
Network Access Manager	Networks Profile:ility Client\Netwo	ork Access Manager\system\configuration	ı.xml
	EAP Methods		Media Type 🔨
	◯ EAP-TLS	○ PEAP	Security Leve
	⊖ EAP-TTLS	EAP-FAST	Connection Ty User Auth
	OLEAP		Credentials
	Extend user connection b	eyond log off	
	EAP-FAST Settings		
	Validate Server Identity		
	Enable Fast Reconnect		
	Disable when using a	Smart Card	
	□ Inner Methods based on Credent	ials Source	
	 Authenticate using a Pass 	sword	
	EAP-MSCHAPv2	EAP-GTC	
	If using PACs, allow u	unauthenticated PAC provisioning	
	O Authenticate using a Cert	tificate	
	 When requested sen 	d the client certificate in the clear	
	 Only send client certi 	ficates inside the tunnel	
	 Send client certificate 	e using EAP-TLS in the tunnel	
	 Authenticate using a Toke 	en and EAP-GTC	
	Use PACs		
	Ne	xt Cancel	¥
	<		>
		🕕 Help	

Nota: no ambiente de produção real, certifique-se de que tem um certificado fidedigno instalado no ISE e mantenha a opção de validação do certificado do servidor ativada nas definições do NAM.

Note: a opção "Se estiver usando PACs, permitir provisionamento de PAC não autenticado" deve ser selecionada somente no caso do provisionamento de PAC em banda anônima.

8. Defina as credenciais do usuário, como SSO, caso deseje usar as mesmas credenciais usadas para login, ou selecione "Solicitar credenciais", caso queira que o usuário seja solicitado a fornecer credenciais durante a conexão com a rede, ou defina credenciais estáticas para esse tipo de acesso. Neste exemplo, solicitamos credenciais ao usuário na tentativa de conexão à rede.

	×

AnyConnect Profile Editor - Network Access Mar	ager
--	------

User Ide	ntity			Media Type /
oups	ected Identity Pattern:	apopymous	S	Security Leve
Chiprot		anonymous	Co	onnection Ty
Protect	ed Identity Pattern:	[username]		User Auth
				Credentials
- User Cre	dentials			
	las Single Sign On Cradentials	_		
	use single sign on credenuals	5		
۲	Prompt for Credentials			
	O Remember Forever			
	Remember while User	is Logged On		
	O Never Remember			
	In Chatta Condentiale			
	Use Static Credentials			
F	assword:			
	Done	Cancel		

9. Salve o perfil configurado na respectiva pasta NAM.

Teste a conectividade com o SSID usando a autenticação EAP-FAST.

1. Selecione o perfil respectivo na lista de redes do Anyconnect

real Cisco AnyCo	onnect Secure Mobility Client		—		×
	VPN: Verify your network connection.	~	C	onnect	
No Network Co	onnectivity				
	Network: Authenticating eap fast		الر, 8		
_	eap_fast		8	atl	
			8		

- 2. Insira o nome de usuário e a senha necessários para a autenticação
- 3. Aceitar certificado do servidor (autoassinado)

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. done

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

Logs de autenticação do ISE

Os registros de autenticação do ISE que mostram o fluxo de provisionamento EAP-FAST e PAC podem ser vistos em "**Operations -> RADIUS -> Live Logs**" e podem ser consultados em mais detalhes usando o ícone **"Zoom**":

 O cliente iniciou a autenticação e o ISE estava propondo EAP-TLS como método de autenticação, mas o cliente rejeitou e propôs o EAP-FAST, que foi o método acordado entre o cliente e o 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. O handshake TLS foi iniciado entre o cliente e o servidor para fornecer um ambiente protegido para troca de PAC e foi concluído com êxito.

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 (O 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		
40000	Deepend TLC Finished monopas		
12816	TLS handshake succeeded		

3. A autenticação interna foi iniciada e as credenciais de usuário foram validadas com êxito pelo ISE usando MS-CHAPv2 (autenticação baseada em nome de usuário/senha)