Autenticazione EAP-FAST con Wireless LAN Controller e Identity Services Engine

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Premesse PAC Modalità di provisioning PAC Configurazione Esempio di rete Configurazioni Configurazione del WLC per l'autenticazione EAP-FAST Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno Configurazione della WLAN per l'autenticazione EAP-FAST Configurazione del server RADIUS per l'autenticazione EAP-FAST Creazione di un database utenti per autenticare i client EAP-FAST Aggiungere il WLC come client AAA al server RADIUS Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC inband autenticato Verifica Configurazione profilo NAM Verificare la connettività a SSID utilizzando l'autenticazione EAP-FAST. Log di autenticazione ISE Debug lato WLC sul flusso EAP-FAST completato Risoluzione dei problemi

Introduzione

In questo documento viene spiegato come configurare il controller WLC (Wireless LAN Controller) per l'autenticazione EAP (Extensible Authentication Protocol) - Autenticazione flessibile tramite autenticazione FAST (Secure Tunneling) con l'utilizzo di un server RADIUS esterno. In questo esempio di configurazione viene utilizzato Identity Services Engine (ISE) come server RADIUS esterno per autenticare il client wireless.

In questo documento viene illustrato come configurare ISE per la configurazione delle credenziali di accesso protetto (PAC) in banda anonime e autenticate per i client wireless.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC
- Conoscenze base del protocollo CAPWAP
- Informazioni su come configurare un server RADIUS esterno, ad esempio Cisco ISE
- Conoscenze funzionali del quadro generale EAP
- Conoscenze base dei protocolli di sicurezza, ad esempio MS-CHAPv2 e EAP-GTC, e conoscenze dei certificati digitali

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

 Cisco serie 5520 WLC con firmware versione 8.8.11.0Cisco serie 4800 APAnyconnect NAM.Cisco Secure ISE versione 2.3.0.298Cisco serie 3560-CX Switch con versione 15.2(4)E1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Premesse

Il protocollo EAP-FAST è un tipo EAP IEEE 802.1X accessibile al pubblico sviluppato da Cisco per supportare i clienti che non possono applicare policy per la password complesse e desiderano distribuire un tipo EAP 802.1X che non richiede certificati digitali.

Il protocollo EAP-FAST è un'architettura di sicurezza client-server che cripta le transazioni EAP con un tunnel TLS (Transport Level Security). La creazione del tunnel EAP-FAST si basa su segreti sicuri specifici degli utenti. Questi segreti si chiamano PAC, che l'ISE genera utilizzando una chiave master nota solo all'ISE.

EAP-FAST si articola in tre fasi:

 Fase zero (fase di preparazione automatica della PAC) - Fase zero di EAP-FAST, una fase opzionale è un mezzo protetto dal tunnel per fornire a un client utente finale EAP-FAST una PAC per l'utente che richiede l'accesso alla rete. L'unico scopo della fase zero è fornire una PAC al client dell'utente finale.Nota: la fase zero è facoltativa in quanto le PAC possono anche essere assegnate manualmente ai client anziché utilizzare la fase zero.Per ulteriori informazioni, vedere la sezione <u>Modalità di provisioning PAC</u> di questo documento.

- Fase 1: nella fase 1, l'ISE e il client dell'utente finale stabiliscono un tunnel TLS in base alle credenziali PAC dell'utente. Questa fase richiede che il client dell'utente finale disponga di una PAC per l'utente che sta tentando di ottenere l'accesso alla rete e che la PAC sia basata su una chiave master non scaduta. Nessun servizio di rete abilitato dalla fase uno di EAP-FAST.
- Fase due: nella fase due, le credenziali di autenticazione utente vengono passate in modo sicuro utilizzando un metodo EAP interno supportato da EAP-FAST all'interno del tunnel TLS al RADIUS creato utilizzando la PAC tra il client e il server RADIUS. EAP-GTC, TLS e MS-CHAP sono supportati come metodi EAP interni. Per EAP-FAST non sono supportati altri tipi di EAP.

Per ulteriori informazioni, fare riferimento a Come funziona EAP-FAST.

PAC

Le PAC sono importanti segreti condivisi che consentono all'ISE e al client dell'utente finale EAP-FAST di autenticarsi a vicenda e stabilire un tunnel TLS da utilizzare nella seconda fase di EAP-FAST. L'ISE genera PAC utilizzando la chiave master attiva e un nome utente.

II PAC comprende:

- PAC-Key: segreto condiviso associato a un'identità client (e di dispositivo client) e server.
- PAC opaco: campo opaco che il client memorizza nella cache e passa al server. Il server recupera la PAC-Key e l'identità del client per autenticarsi reciprocamente con il client.
- **PAC-Info**: include almeno l'identità del server per consentire al client di memorizzare nella cache PAC diverse. Facoltativamente, include altre informazioni quali l'ora di scadenza del PAC.

Modalità di provisioning PAC

Come accennato in precedenza, la fase zero è una fase facoltativa.

EAP-FAST offre due opzioni per il provisioning di un client con una PAC:

- Preparazione automatica della PAC (fase 0 di EAP-FAST o preparazione della PAC in banda)
- Preparazione manuale della PAC (fuori banda)

La preparazione automatica della PAC in banda invia una nuova PAC al client dell'utente finale tramite una connessione di rete protetta. La preparazione automatica delle credenziali di accesso protette non richiede l'intervento dell'utente di rete o di un amministratore ISE, a condizione che l'ISE e il client dell'utente finale siano configurati in modo da supportare la preparazione automatica.

L'ultima versione di EAP-FAST supporta due diverse opzioni di configurazione della preparazione della PAC in banda:

- Preparazione PAC in banda anonima
- Provisioning PAC in banda autenticato

Nota: in questo documento vengono descritti i metodi di preparazione della PAC in banda e la relativa configurazione.

La preparazione manuale/fuori banda della PAC richiede che un amministratore ISE generi i file PAC, che devono quindi essere distribuiti agli utenti della rete interessati. Gli utenti devono configurare i client degli utenti finali con i relativi file PAC.

Configurazione

Esempio di rete



Configurazioni

Configurazione del WLC per l'autenticazione EAP-FAST

Per configurare il WLC per l'autenticazione EAP-FAST, eseguire la procedura seguente:

- 1. Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno
- 2. Configurazione della WLAN per l'autenticazione EAP-FAST

Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno

Ènecessario configurare il WLC per inoltrare le credenziali dell'utente a un server RADIUS esterno. Il server RADIUS esterno convalida quindi le credenziali utente utilizzando EAP-FAST e fornisce l'accesso ai client wireless.

Per configurare il WLC per un server RADIUS esterno, completare la procedura seguente:

- 1. Scegliere **Sicurezza** e **Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Quindi, fare clic su **New** (Nuovo) per definire un server RADIUS.
- Definire i parametri del server RADIUS nella pagina Server di autenticazione RADIUS > Nuovo. Questi parametri includono:Indirizzo IP server RADIUSSegreto condivisoNumero portaStato serverNel documento viene usato il server ISE con indirizzo IP 10 48.39 128

CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serv	ers > New
T AAA	Server Index (Priority)	
General RADIUS	Server IP Address(Ipv4/Ipv6)	10.48.39.128
Authentication	Shared Secret Format	
Accounting Auth Cached Users	Shared Secret Format	ASCH
Fallback	Shared Secret	
DNS Downloaded AVP	Confirm Shared Secret	••••
▶ TACACS+	Apply Cisco ISE Default settings	
LDAP	Apply Cisco ACA Default settings	
Local Net Users MAC Filtering	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
 Disabled Clients 	Port Number	1912
User Login Policies	Port Number	
Password Policies	Server Status	Enabled \$
Local EAP	Support for CoA	Enabled \$
Advanced FAR	Server Timeout	5 seconds
Driasity Orden	Network User	Enable
Priority Order	Management	🗸 Enable
Certificate	Management Betransmit Timeout	5 seconds
Access Control Lists	Tunnel Draw	
Wireless Protection	Tunnel Proxy	
Policies	PAC Provisioning	Enable
Web Auth	IPSec	Enable
TrustSec	Cisco ACA	Enable
Local Policies		
Umbrella		
Advanced		

Configurazione della WLAN per l'autenticazione EAP-FAST

Configurare quindi la WLAN utilizzata dai client per connettersi alla rete wireless per l'autenticazione EAP-FAST e assegnarla a un'interfaccia dinamica. Il nome WLAN configurato in

questo esempio è **eap fast**. In questo esempio la WLAN viene assegnata all'interfaccia di gestione.

Completare questa procedura per configurare la WLAN eap fast e i relativi parametri:

- 1. Fare clic su **WLAN** dalla GUI del controller per visualizzare la pagina WLAN.In questa pagina vengono elencate le WLAN esistenti sul controller.
- 2. Per creare una nuova WLAN, fare clic su New (Nuovo).

WLANs > Edit 'eap fast'

ululu cisco		<u>w</u> lans <u>c</u> o	ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
WLANs	WLANs										
VLANs WLANs	Current Filter	r: None	[Change Filter]	[Clear Filter]					Create New 🗘 Go	
Advanced	U WLAN ID	Туре	Profile Nar	ne		WLAN SSID		А	dmin Status	Security Policies	
		WLAN	test			test		E	nabled	[WPA2][Auth(802.1X)]	
	2	WLAN	AndroidAP			AndroidAP		E	nabled	[WPA2][Auth(PSK)]	

3. Configurare il nome SSID della WLAN **eap_fast**, il nome del profilo e l'ID della WLAN nella pagina WLAN > Nuovo. Quindi fare clic su **Apply** (Applica).



- 4. Dopo aver creato una nuova WLAN, viene visualizzata la pagina WLAN > Modifica per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN. Sono inclusi i criteri generali, i server RADIUS, i criteri di sicurezza e i parametri 802.1x.
- Per abilitare la WLAN, selezionare la casella di controllo Admin Status (Stato amministratore) nella scheda General Policies (Criteri generali). Se si desidera che l'access point trasmetta il SSID nei frame del beacon, selezionare la casella di controllo Broadcast SSID.

Profile Nameeap_fastTypeWLANSSIDeap_fast
Profile Name eap_fast Type WLAN SSID eap_fast
Type WLAN SSID eap_fast
SSID eap_fast
Status 🕑 Enabled
(Modifications done under security tab will appear after applying the cha
Radio Policy All
Interface/Interface Group(G) vlan1477 🛟
Multicast Vlan Feature Enabled
Broadcast SSID 🖉 Enabled
NAS-ID none

6. In "WLAN -> Modifica -> Sicurezza -> Layer 2" selezionare WPA/WPA2 parameters e selezionare dot1x per AKM.

In questo esempio viene usato WPA2/AES + dot1x come protezione di layer 2 per questa WLAN. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN.

.ANs > E	dit 'eap_fa	ast'					
eneral	Security	QoS	Policy-Map	oping Ad	vanced		
Layer 2	Layer 3	AAA Se	ervers				
Layer 2	Security f	VPA+WPA2 \C Filtering≌	:				
Fast Trans	ition						
Fast Transit	tion	Disa	ble 🗘				
Protected	Management	Frame					
PMF		Disa	bled				
WPA+WP/	A2 Parameter	s					
WPA Po	licy						
WPA2 P	olicy		_				
WPA2 E	ncryption	AES	с 🗌 ткір	CCMP25	6 🗌 G0	CMP128	GCMP256
OSEN P	olicy						
Authentica	ation Key Man	agement ¹	<u>.9</u>				
802.1X		Enable					
ССКМ		Enable	_				
PSK		Enable					
ET 000	1	nabla					

7. Nella scheda "WLAN -> Modifica -> Protezione -> Server AAA" scegliere il server RADIUS appropriato dal menu a discesa in Server RADIUS.

eneral	Security	QoS	Policy-	Mapping	Advanced		
ayer 2	Layer 3	AAA 9	Servers				
elect AAA se ADIUS Serv RADIUS Se	ervers belo v ers erver Overwa	w to ove	rride use o ace 🗌 Enab	f default se	rvers on this V	VLAN	
Apply Cisco	o ISE Defaul	t Settings	Enab		Servers		FAP P
Apply Cisco	o ISE Defaul Authentica C Enabled	t Settings	Enab	Accounting	Servers		EAP P
Apply Cisco Server 1	Authentica	t Settings ation Serv 39.128, Po	ers A	Accounting Enabled None	Servers	\$	EAP P Ena
Apply Cisco Server 1 Server 2	Authentica Contempt for the second se	t Settings ation Serv 39.128, Po	Enab	Accounting Enabled None None	Servers	†	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3	Authentica Contraction Contraction Authentica Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contrac	t Settings ation Serv 39.128, Po	Enab	Accounting Enabled None None None	Servers	 	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Constraints Authentica Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constra	t Settings ation Serv 39.128, Po	Enab	Accounting Enabled None None None None	Servers	 <	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Contraction Authentica Contraction Authentica Contraction None None None None None	t Settings ation Serv 39.128, Po	Enab	Accounting Enabled None None None None None None	Servers	 <	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	Enab	Accounting Enabled None None None None None None None	Servers	 <	EAP P Ena

8. Fare clic su **Apply** (Applica).**Nota:** questa è l'unica impostazione EAP da configurare sul controller per l'autenticazione EAP. Tutte le altre configurazioni specifiche di EAP-FAST devono essere eseguite sul server RADIUS e sui client da autenticare.

Configurazione del server RADIUS per l'autenticazione EAP-FAST

Per configurare il server RADIUS per l'autenticazione EAP-FAST, attenersi alla procedura seguente:

- 1. Creazione di un database utenti per autenticare i client EAP-FAST
- 2. Aggiungere il WLC come client AAA al server RADIUS
- 3. Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo
- 4. Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC in-band autenticato

Creazione di un database utenti per autenticare i client EAP-FAST

Nell'esempio, il nome utente e la password del client EAP-FAST sono configurati rispettivamente come <*eap_fast>* e <*EAP-fast1>*.

1. Nell'interfaccia utente di ISE Web admin, selezionare "Administration -> Identity Management -> Users" e premere l'icona "Add".

dentity Services Engine	Home Context	Visibility • Open	ations +	Policy -A	dministratio	Work Cer	nters			
► System - Identity Management	Network Resources	 Device Portal Ma 	nagement	pxGrid Service	s ⊧ Feed	Service + Thr	eat Centric NAC			
▼Identities Groups External Identit	y Sources Identity S	ource Sequences	 Settings 							
G										
Users	Network Access	s Users								
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status	🛃 Import	🕞 Export 👻	X Delete	Duplicate				
	Status	Name	I	Description		First Name	Last Name	Email Address	User Identity Groups	Admin
								No da	ita available	

 Compilare i moduli obbligatori per la creazione dell'utente - "Nome" e "Password di accesso" e selezionare "Gruppo utenti" dall'elenco a discesa;[facoltativamente è possibile compilare altre informazioni per l'account utente]
 Premere "Invia"

	outor					
▶ System	Network Resources Device Portal Ma	nagement pxGrid Services	Feed Service Freat Centric NA	с		
✓Identities Groups External Iden	tity Sources Identity Source Sequences	 Settings 				
(
Users	Network Access Users					
Latest Manual Network Scan Results	/ Edit 🕂 Add 🔀 Change Status 👻	🕞 Import 🔹 Export 👻 🗙	Delete 👻 🕒 Duplicate			/ Groups Admin
	Status Name	 Description 	First Name Last Name	Email Address	User Identity Groups	Admin
	🗌 🔤 Enabled 👲 eap_fast	\oplus	Test user Test user		Employee	

Completare questa procedura per definire il controller come client AAA sul server ACS:

1. Nell'interfaccia utente di ISE Web admin, selezionare "Administration -> Network Resources -> Network Devices" e premere l'icona "Add".



 Compilare i moduli richiesti per il dispositivo da aggiungere - "Nome", "IP" e configurare la stessa password segreta condivisa, come configurato sul WLC nella sezione precedente, nel modulo "Segreto condiviso" [facoltativamente è possibile compilare altre informazioni per il dispositivo come posizione, gruppo, ecc.]. Premere "Invia"

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 WICSS20
Device Security Settings	Description
	IP Address v P IP : 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	Device Profile the Cisco •
	Model Name
	Software Version
	Network Device Group
	Location LAB 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
	COA POR 1700 Set To Default
	RADIUS DTLS Settings ()
	UILS Required Grading/dtls
	CoA Port 2003 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional)

3. La periferica viene aggiunta all'elenco delle periferiche di accesso alla rete ISE. (AND)



Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo

In genere si preferisce utilizzare questo tipo di metodo nel caso in cui non sia disponibile un'infrastruttura PKI nella distribuzione.

Questo metodo funziona all'interno di un tunnel ADHP (Authenticated Diffie-Hellman Key Agreement Protocol) prima che il peer autentichi il server ISE.

Per supportare questo metodo, è necessario abilitare "Allow Anonymous In-band PAC Provisioning" (Consenti provisioning PAC in-band anonimo) su ISE in "Authentication Allowed Protocols" (Protocolli autorizzati per l'autenticazione):

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

Nota: accertarsi di aver consentito l'autenticazione del tipo di password, come EAP-MS-CHAPv2

per il metodo interno EAP-FAST, poiché ovviamente con il provisioning in banda anonimo non è possibile utilizzare alcun certificato.

Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning della PAC in-band autenticato

Si tratta dell'opzione più sicura e consigliata. Il tunnel TLS viene creato in base al certificato del server convalidato dal richiedente e il certificato del client viene convalidato da ISE (impostazione predefinita).

Questa opzione richiede un'infrastruttura PKI per client e server, anche se può essere limitata al solo lato server o ignorata su entrambi i lati.

ISE offre due opzioni aggiuntive per il provisioning in-band autenticato:

- "Server Returns Access Accept After Authenticated Provisioning" In genere, dopo la preparazione della PAC, è necessario inviare un messaggio di rifiuto dell'accesso che impone al richiedente di rieseguire l'autenticazione utilizzando le PAC. Tuttavia, poiché la preparazione della PAC viene eseguita in un tunnel TLS autenticato, è possibile rispondere immediatamente con Access-Accept per ridurre al minimo i tempi di autenticazione. in questo caso, verificare di disporre di certificati attendibili sul lato client e server.
- 2. "Accetta certificato client per provisioning" se non si desidera fornire l'infrastruttura PKI ai dispositivi client e si dispone solo di un certificato attendibile su ISE, abilitare questa opzione, che consente di ignorare la convalida del certificato client sul lato server.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	lient Provisioning - Policy Elements
Dictionaries + Conditions - Resu	ts
G	✓ Illow EAP-FAST
▼Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	Allow EAP-MS-CHAPv2
b Drofiling	Allow Password Change Retries 3 (Valid Range 0 to 3)
• Proming	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
	Proactive PAC update will occur after 90 % of PAC Time To Live has expired
	Allow Anonymous In-Band PAC Provisioning
	Allow Authenticated In-Band PAC Provisioning
	Server Returns Access Accept After Authenticated Provisioning
	Accept Client Certificate For Provisioning
	Allow Machine Authentication
	Machine PAC Time To Live 1 Weeks *
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 1
	Enable EAP Chaining

Su ISE definiamo anche criteri di autenticazione semplici impostati per gli utenti wireless, qui di seguito esempio sta utilizzando come parametro di condizione tipo di dispositivo e posizione e tipo di autenticazione, il flusso di autenticazione corrispondente a quella condizione sarà convalidato rispetto al database degli utenti interni.

M.Clab AND P DEVICE Device Type EQUALS AIL Device Types#MLC-lab Image: DEVICE Location EQUALS AILLocations#LAB Options				Wireless_802.1X	Internal Users × v		
DEVICE-Location EQUALS All Locations#LAB Device-Location EQUALS All Locations#LAB	WLC_lab	WLC_lab	AND 🖵 DEVICE-Device Type EQUALS All Device Types#WLC-lab	College	2		
				DEVICE-Location EQUALS All Locations#LAB	 Opuons 		

Verifica

In questo esempio vengono mostrati il flusso di provisioning della PAC in banda autenticata e le impostazioni di configurazione di Network Access Manager (NAM) insieme ai rispettivi debug WLC.

Configurazione profilo NAM

Per configurare il profilo Anyconnect NAM in modo che autentichi la sessione utente con ISE usando EAP-FAST, è necessario eseguire le seguenti operazioni:

- 1. Aprire l'Editor profili di Network Access Manager e caricare il file di configurazione corrente.
- 2. Verificare che "EAP-FAST" sia abilitato in "Modalità di autenticazione consentite"



3. "Aggiungi" un nuovo profilo di rete:

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	1	
				Edit	•	
				Delete		
	* 4					
	* A network in gr	oup Global is a member of airgr	oups.			
						~
	<					>
		🕕 Help)			

4. Nella sezione di configurazione **"Tipo di supporto"** definire il profilo "**Nome**", wireless come tipo di rete multimediale e specificare il nome SSID.

🕍 AnyConnect Profile Editor - Network Access Manager	_		×
File Help			
Network Access Manager Client Policy Profile:ility Client\Network Access Manager\system\configuration.xml			
Authentication Policy Name: eap_fast Group Membership In group: In all groups (Global) Choose Your Network Media Wred (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wrifi (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Wrifi (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Wrifi (wireless) Network Select a WiFi network if the endstations will be connecting to the network with a traditional ethernet cable. Wrifi (wireless) Retwork Select a WiFi network if the endstations will be connecting to the network with a wireless radio connection to an Access Point. SSID (max 32 chars): eap_fast Hidden Network Corporate Network Common Settings Script or application on each user's machine to run when connected. Rowse Local Machine Connection Timeout Next Cancel		Medi	a Typ ∧ y Les
<			>
i) Help			

5. Nella scheda di configurazione "Livello di protezione" selezionare "Autenticazione rete" e specificare la modalità di associazione come WPA2 Enterprise (AES)

Naturals Access Manager	Natuarka		
Client Policy	Networks Brofile: ility Client/Network Appage Manager/system		nl
Authentication Policy	Secritulard	nconngulation.xi	
M Networks	Security Level		Media Type
	Open Network	ange This is	Connection Tv
	the least secure type of network.	anger molo	
	Shared Key Networks use a shared key to encrypt data between en	d 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 an	e perfect for	
	enterprise level networks. Authentication networks require radius se	ervers, and	
	other network infrastructure.		
	802.1X Settings		
	802.1X Settings authPeriod (sec.) 30 startPeriod (sec.)	30	
	802.1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) heldPeriod (sec.) 60 Association Mode WPA2 Enterprise (AES)	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) heldPeriod (sec.) 60 maxStart Association Mode	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart	30	
	802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) heldPeriod (sec.) 60 maxStart Association Mode MPA2 Enterprise (AES) v Next Cancel	30	

6. In questo esempio viene utilizzata l'autenticazione basata sul tipo di utente, quindi nella scheda successiva "Tipo di connessione" selezionare "Connessione utente"

AnyConnect Profile Editor	Network Access Manager	-		×
File Help				
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml			
Network Groups	Network Connection Type Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. 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. Next Cancel 		Media Security Connect User / Crede	Type ^ / Leve ion Ty Auth ntials
	Help			

7. Nella scheda "Autenticazione utente" specificare EAP-FAST come metodo di autenticazione consentito e disattivare la convalida dei certificati del server, poiché in questo esempio non vengono utilizzati certificati protetti.

🐴 AnyConnect Profile Editor -	Network Access Manager		- 🗆 🗙
File Help			
Network Access Manager	Networks Profile:ility Client\Net	work Access Manager\system\configuration.x	ml
	EAP Methods		Media Type \land
Network Groups	C EAP-TLS	○ PEAP	Security Leve
	C EAP-TTLS	● EAP-FAST	Connection Ty User Auth
		Ũ	Credentials
		n bevond log off	_
			_
	EAP-FAST Settings		
	Validate Server Identity	<u>X</u>	
		a Smart Card	
	Inner Methods based on Crede	entials Source	
	Authenticate using a Page	assword	
	EAP-MSCHAPv2	EAP-GTC	
	If using PACs, allow	w unauthenticated PAC provisioning	
	 Authenticate using a Comparison 	ertificate	
	 When requested set 	end the dient certificate in the dear	
	 Only send client ce 	ertificates inside the tunnel	
	Send client certification	ate using EAP-TLS in the tunnel	
	Authenticate using a To	oken and EAP-GTC	
	Use PACs		
	Ν	Next Cancel	×
	<		>
		🕕 Help	

Nota: in un ambiente di produzione reale assicurarsi di avere un certificato attendibile installato su ISE e mantenere l'opzione di convalida del certificato server abilitata nelle impostazioni NAM.

Nota: L'opzione "Se si utilizzano PAC, consenti preparazione PAC non autenticata" deve essere selezionata solo in caso di preparazione PAC in banda anonima.

8. Definire le credenziali utente come SSO se si desidera utilizzare le stesse credenziali utilizzate per l'accesso, selezionare "Richiedi credenziali" se si desidera che all'utente vengano richieste le credenziali durante la connessione alla rete oppure definire credenziali statiche per il tipo di accesso. In questo esempio vengono richieste le credenziali dell'utente al tentativo di connessione alla rete.

	×

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

	Jser Identity		M	Media Type /
	Unprotected Identity Pattern:	aponymous	Se	curity Leve
	onprotected racing (atterni		Con	nection Ty
	Protected Identity Pattern:	[username]	l	User Auth
				Credentials
	Jser Credentials			
	O Lise Single Sign On Credentials	s		
		5		
	Prompt for Credentials			
	Remember Forever			
	Remember while User	is Logged On		
	Never Remember			
	O Lise Static Credentials			
	Password:			
	Done	Cancel		,
1				

9. Salvare il profilo configurato nella cartella NAM corrispondente.

Verificare la connettività a SSID utilizzando l'autenticazione EAP-FAST.

1. Seleziona il profilo corrispondente dall'elenco delle reti Anyconnect

🕚 Cisco AnyCo	onnect Secure Mobility Client		-	L		×	
	VPN: Verify your network connection.	~		Con	nect		
No Network Co	onnectivity						
	Network: Authenticating						
_	eap_fast		8	att	\sim	≔	
	eap_fast			۵.	al j		
-				<u></u>	ull -		
					11		
				- -			
						_	

- 2. Immettere il nome utente e la password necessari per l'autenticazione
- 3. Accetta certificato server (autofirmato)



4. Fine

🕙 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	A	att 🗸 🗄	

Log di autenticazione ISE

I log di autenticazione ISE che mostrano il flusso di provisioning EAP-FAST e PAC possono essere visualizzati in "**Operations -> RADIUS -> Live Logs**" (Operazioni -> RAGGIO -> Live Logs) e consultati in maggior dettaglio usando l'icona "**Zoom**" (Zoom):

1. Il client ha avviato l'autenticazione e ISE ha proposto EAP-TLS come metodo di autenticazione, ma il client ha rifiutato e ha proposto EAP-FAST; questo è stato il metodo accettato sia dal client che da 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-FAS1 challenge-response and accepting EAP-FAST as negotiated

2. L'handshake TLS è stato avviato tra il client e il server per fornire l'ambiente protetto per lo scambio PAC ed è stato completato.

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-respo
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request (10 Step latency=13317 ms)
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-respo
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
10000	Property TLC Finished meanings
12816	TLS handshake succeeded

3. Autenticazione interna avviata e credenziali utente convalidate da ISE con MS-CHAPv2 (autenticazione basata su nome utente/password)