ワイヤレスLANコントローラおよびIdentity Services Engineを使用したEAP-FAST認証

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 背景説明 PAC PAC プロビジョニング モード 設定 ネットワーク図 設定 EAP-FAST 認証用の WLC の設定 外部 RADIUS サーバによる RADIUS 認証用の WLC の設定 EAP-FAST 認証用の WLAN を設定する EAP-FAST 認証のための RADIUS サーバの設定 EAP-FAST クライアント認証用のユーザ データベースの作成 AAA クライアントとしての WLC の RADIUS サーバへの追加 匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定 RADIUS サーバの EAP-FAST 認証に認証付きインバンド PAC プロビジョニングを設定する 確認 NAMプロファイルの設定 EAP-FAST認証を使用して、SSIDへの接続をテストします。 ISE認証ログ 正常なEAP-FASTフローでのWLC側のデバッグ トラブルシュート

概要

このドキュメントでは、外部 RADIUS サーバで使用する拡張認証プロトコル(EAP)Flexible Authentication via Secure Tunneling(FAST)認証のためにワイヤレス LAN コントローラ (WLC)を設定する方法について説明します。この設定例では、ワイヤレスクライアントを認証 するために、外部RADIUSサーバとしてIdentity Services Engine(ISE)を使用します。

このドキュメントでは、ワイヤレスクライアントに対する匿名および認証済みのインバンド (Automatic)保護アクセスクレデンシャル(PAC)プロビジョニング用にISEを設定する方法について 説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Lightweight アクセス ポイント(LAP)および Cisco WLC の設定に関する基礎知識
- CAPWAPプロトコルに関する基礎知識
- Cisco ISEなどの外部RADIUSサーバの設定方法に関する知識
- 一般的な EAP フレームワークに関する実践的な知識
- MS-CHAPv2 および EAP-GTC などのセキュリティ プロトコルに関する基本的な知識、デジ タル証明書に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

ファームウェア リリース 8.8.111.0 が稼働する Cisco 5520 シリーズ WLCCisco 4800 シリーズ APAnyConnect NAM.Cisco Secure ISE バージョン 2.3.0.298Cisco 2950 シリーズ スイッチバージョン 15.2(4)E1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

背景説明

EAP-FASTプロトコルは、強力なパスワードポリシーを適用できない802.1X EAPの種類をデジタ ル証明書を必要としない802.1X EAPの導入をシスコがサポートするために開発した、一般アクセ スのIEEE 802.1X EAPタイプです。

EAP-FAST プロトコルは、Transport Level Security(TLS)トンネルで EAP トランザクションを 暗号化するクライアント サーバ型のセキュリティ アーキテクチャです。EAP-FAST トンネルは 、ユーザに固有な強力なシークレットに基づいて確立されます。これらの強力な秘密はPACと呼 ばれ、ISEのみが認識するマスターキーを使用してISEが生成します。

EAP-FAST は3つのフェーズで実行されます。

- フェーズ 0(自動 PAC プロビジョニング フェーズ): EAP-FAST フェーズ 0は、オプションフェーズで、ネットワーク アクセスを要求するユーザのために EAP-FAST エンドユーザクライアントに PAC を提供するトンネル セキュア方法です。エンドユーザ クライアントに PAC を提供することが、フェーズ 0 の唯一の目的です。注:フェーズゼロはオプションです。これは、フェーズ0を使用する代わりに、PACを手動でクライアントにプロビジョニングできるためです。詳細については、このドキュメントの「PAC プロビジョニング モード」を参照してください。
- •フェーズ1:フェーズ1では、ISEとエンドユーザクライアントが、ユーザのPACクレデンシ

ャルに基づいてTLSトンネルを確立します。このフェーズでは、ネットワーク アクセスの取 得を試行するユーザ用の PAC がエンドユーザ クライアントに提供されていることと、期限 の切れていないマスター キーに PAC が基づいていることが必要です。EAP-FAST のフェー ズ 1 ではネットワーク サービスは有効になりません。

フェーズ2:フェーズ2では、ユーザ認証クレデンシャルが、TLS内で EAP-FAST によりサポートされる内部 EAP 方式を使用して、クライアントと RADIUS サーバ間の PAC を使用して作成された RADIUS に安全に渡されます。
 内部 EAP 方式として EAP-GTC、TLS およびMS-CHAP がサポートされています。
 その他の EAP タイプは EAP-FAST ではサポートされていません。

詳細は、『EAP-FAST の動作の仕組み』を参照してください。

PAC

PACは、ISEとEAP-FASTエンドユーザクライアントが相互に認証し、EAP-FASTフェーズ2で使用するTLSトンネルを確立できるようにする強力な共有秘密です。ISEは、アクティブなマスター キーとユーザ名を使用してPACを生成します。

PAC は、次のもので構成されています。

- ・PAC-Key:クライアント(およびクライアント デバイス)とサーバの ID にバインドされて いる共有秘密情報。
- PAC Opaque: クライアントがキャッシュしてサーバに渡す暗号化されたフィールド。サーバは、PAC-Key およびクライアント ID を復号化して、クライアントとの相互認証を行います。
- PAC-Info: クライアントがさまざまな PAC をキャッシュできるように、少なくともサーバの ID が含まれています。PAC の有効期限などの情報が含まれていることもあります。

PAC プロビジョニング モード

前述のように、フェーズ 0 はオプション フェーズです。

EAP-FAST は、PAC でクライアントをプロビジョニングする 2 つのオプションを提供します。

- ・自動 PAC プロビジョニング(EAP-FAST フェーズ 0 またはインバンド PAC プロビジョニン グ)
- ・手動(アウトオブバンド)PAC プロビジョニング

インバンド/自動 PAC プロビジョニングは、セキュア ネットワーク接続を介して新規 PAC をエ ンドユーザ クライアントに送信します。自動PACプロビジョニングをサポートするようにISEと エンドユーザクライアントを設定する場合、ネットワークユーザまたはISE管理者の介入は必要 ありません。

最新の EAP-FAST バージョンは、次に示す 2 種類のインバンド PAC プロビジョニング設定オプ ションをサポートします。

- ・匿名インバンド PAC プロビジョニング
- ・認証付きインバンド PAC プロビジョニング

注:このドキュメントでは、これらのインバンドPACプロビジョニング方法とその設定方法について説明します。

アウトオブバンド/手動PACプロビジョニングでは、ISE管理者がPACファイルを生成する必要が あります。生成したファイルは、該当するネットワークユーザに配布する必要があります。ユー ザは PAC ファイルでエンドユーザ クライアントを設定する必要があります。

設定

ネットワーク図



EAP-FAST 認証用の WLC の設定

WLCのEAP-FAST認証を設定するには、次の手順を実行します。

1. 外部 RADIUS サーバによる RADIUS 認証用の WLC の設定

2. EAP-FAST 認証用の WLAN を設定する

外部 RADIUS サーバによる RADIUS 認証用の WLC の設定

ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります 。そうすると、外部 RADIUS サーバは、EAP-FAST を使用してユーザのクレデンシャルを検証し 、ワイヤレス クライアントにアクセス権を付与します。

外部 RADIUS サーバ用に WLC を設定するには、次の手順を実行します。

- 1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サー バを定義します。
- 2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義しま す。次のパラメータがあります。RADIUS サーバの IP アドレス共有秘密ポート番号サーバ ステータスこのドキュメントでは、IPアドレスが10.48.39.128のISEサーバを使用します。

CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Security	RADIUS /	Authenti	cation Server	rs > 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 	Server Ind Server IP Shared Se Shared Se Confirm S Apply Cisc Apply Cisc Key Wrap Port Numb Server Sta Support fo Server Tir Network L Managemu Tunnel Prov PAC Provis IPSec Cisco ACA	dex (Priorit Address(Ip ecret Forma ecret ishared Secr to ISE Defa to ISE Defa to ACA Defa atus to COA to COA meout Jser ent ent Retrans oxy sioning	y) w4/Ipv6) at et uult settings ault settings smit Timeout	2 ¢ 10.48.39.128 ASCII \$ (Designed 1812 Enabled \$ Enabled \$ Enabled \$ Enable Enable Enable Enable Enable	3 I for FIPS custor	mers and requires	a key wrap comp	bliant RADIU	IS server)

3. クリック Apply.

EAP-FAST 認証用の WLAN を設定する

次に、EAP-FAST 認証のためにワイヤレス ネットワークに接続するときにクライアントが使用す る WLAN を設定し、ダイナミック インターフェイスに割り当てます。この例で設定される WLAN 名は eap fast です。この例では、この WLAN を管理インターフェイスに割り当てます。 eap fast WLAN およびその関連パラメータを設定するには、次の手順を実行します。

- 1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このペー ジには、コントローラに存在する WLAN の一覧が表示されます。
- 2. [New] をクリックして新規の WLAN を作成します。

WLANs > Edit 'eap_fast'

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
WLANs	WLANs										
WLANS	Current Filte	r: None	e (Change Filter]	[Clear Filter]					Create New 🛟 Go	
Advanced	WLAN ID	Туре	Profile Na	me		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. [WLANs] > [New]ページで**eap_fast WLAN SSID**名、プロファイル名、およびWLAN IDを設 定します。次に、[Apply] をクリックします。

ahaha						Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	FEEDBACK	A Home
WLANs	WLANs > New					< Back Apply
WLANS WLANS Advanced	Type Profile Name SSID ID	WLAN \$ eap_fast 3				

- 4. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されま す。このページでは、その WLAN に固有のさまざまなパラメータを定義できます。このペ ージには、[General Policies]、[RADIUS Servers]、[Security Policies]、[802.1x] パラメータ があります。
- 5. WLANを有効にする**には、[General Policies]**タブの**[Admin Status]**チェックボックスをオンに します。AP にビーコン フレームで SSID をブロードキャストさせる場合は、[Broadcast SSID] にチェックボックスをオンにします。

onoral	Cocurity	0.05	Deliev-M	onning	Advanced		
meral	Security	Q05	Policy-M	apping	Auvanced		
Profile Nam	ie	ea	p_fast				
Гуре		W	LAN				
SSID		ea	p fast				
Status			Enabled				
Security Po	licies	ΓV	PA21[Auth/	802.13)	1		
Security 10		(Mo	difications do	ne under	security tab will ap	pear after applying the	changes.
							-
Radio Policy	ý	A	11	\$			
Interface/In	nterface Group	o(G) 🔽	lan1477 🛟				
Multicast VI	lan Feature		Enabled	_			
Broadcast S	SSID		Enabled				
NAS-ID		no	ne				

6. 通常の"**[WLAN] -> [Edit] -> [Security] -> [Layer 2]** タブで[WPA/WPA2 parameters]を選択し、 AKMに[dot1x]を選択します。

この例では、このWLANのレイヤ2セキュリティとしてWPA2/AES + dot1xを使用します。

WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。

ANs > Edi	it 'eap_fa	ast'				
eneral	Security	QoS	Policy-Map	ping Adva	nced	
ayer 2	Layer 3	AAA Se	ervers			
Layer 2 Se	ecurity 🧧 🚺	VPA+WPA2	¢			
ast Transiti	MA on	C Filtering				
ast Transitio	n	Disa	ble 🗘			
Protected Ma	anagement	Frame				
PMF		Disa	bled			
VPA+WPA2	Parameter	5				
WPA Policy	4					
WPA2 Poli	су		_			
WPA2 Enc	ryption	🗹 AES	Б ТКІР	CCMP256	GCMP128	GCMP256
OSEN Poli	су					
uthenticati	on Key Man	agement ²	<u>9</u>			
802.1X		Enable				
ССКМ		Enable				
PSK		Enable				
ET 000 1V		nabla				

7. [WLAN] -> [Edit] -> [Security] -> [AAA Servers] タブで、[RADIUS Servers]のプルダウンメニ ューから適切なRADIUSサーバを選択します。

	Security	QoS	Policy-Map	oing Adv	vanced		
ayer 2	Layer 3		Servers				
elect AAA s ADIUS Serv RADIUS Se Apply Cisco	ervers belo vers erver Overwi o ISE Defaul	rite interfa t Settings	rride use of def ice Enabled	ault servers	on this W	LAN	
,		J					
	Authentica	ition Serv	vers Accou	Inting Serve	rs		EAP Pa
Server 1	Authentica	ition Serv 39.128, Pc	vers Accou Cont: 1812 \$ Non	inting Serve abled e	rs	◆]	EAP Pa
Server 1 Server 2	Authentica Enabled IP:10.48.3 None	ation Serv 39.128, Pc	vers Accou Cort:1812 \$ Non \$ Non	Inting Serve abled e e	rs	 	EAP P
Server 1 Server 2 Server 3	Authentica Enabled IP:10.48.2 None None	ation Serv	vers Accou ort:1812 Non Non Non	abled e e	rs	 	EAP P
Server 1 Server 2 Server 3 Server 4	Authentica Enabled IP:10.48.3 None None None	ation Serv	vers Accou ort:1812 Non Non Non Non	Inting Serve abled e e e	rs	 	EAP P
Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Enabled IP:10.48.3 None None None None	ation Serv	vers Accou ort:1812 Non Non Non Non Non Non	abled e e e e e e	rs	$\begin{array}{c} \bullet \\ \bullet $	EAP Pa Enal
Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Authentica Enabled IP:10.48.3 None None None None None	ation Serv	vers Accou vers Accou En Dort: 1812 Non Non Non Non Non Non Non Non	abled e e e e e e e e	rs	$\diamond \diamond \diamond \diamond \diamond \diamond \diamond$	EAP P Ena

8. [Apply] をクリックします。注:これは、EAP認証用にコントローラで設定する必要がある 唯一のEAP設定です。EAP-FAST に固有なその他すべての設定は、RADIUS サーバおよび認 証が必要なクライアントで行う必要があります。

EAP-FAST 認証のための RADIUS サーバの設定

RADIUS サーバの EAP-FAST 認証を設定するには、次の手順を実行します。

- 1. EAP-FAST クライアント認証用のユーザ データベースの作成
- 2. AAA クライアントとしての WLC の RADIUS サーバへの追加
- 3. 匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認証の設定
- 4. RADIUS サーバの EAP-FAST 認証に認証付きインバンド PAC プロビジョニングを設定する

EAP-FAST クライアント認証用のユーザ データベースの作成

この例では、EAP-FASTクライアントのユーザ名とパスワードをそれぞれ<*eap_fast*>および <*EAP-fast1*>として設定します。

1. ISE Web管理UIで、[Administration] -> [Identity Management] -> [Users]の下に移動し、 [Add]アイコンを押します。

diale Identity Services Engine	Home + Contex	t Visibility → Opera	itions	Policy -/	Administration	• Work Cer	iters			
System Identity Management	Network Resources	Device Portal Mar	nagement	pxGrid Service	es 🕨 Feed	Service + Thr	eat Centric NAC			
▼Identities Groups External Identit	y Sources Identity	Source Sequences	 Settings 							
G	Notwork Access									
Users	Network Acces	susers								
Latest Manual 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 d	ata available	

2. 作成するユーザーに必要なフォーム(「Name」および「Login password」を入力し、ドロッ プダウン・リストから「User group」を選択します。[オプションで、ユーザーアカウントの 他の情報を入力できます] 「Sumbit」を押します

dentity S	Services Engine	Home ► Context V	sibility F Operations	▶ Policy → Ad	ministration V	/ork Centers		
► System - I	dentity Management	 Network Resources 	 Device Portal Management 	t pxGrid Services	Feed Service	Threat Centric NAC		
✓Identities G	roups External Ide	entity Sources Identity So	urce Sequences + Setting	s				
		Network Access Liser	list > New Network Access	e Hear				
Users		 Network Acce 	ss User	000				
Latest Manual Net	work Scan Results	* Name ean fas	:					
		Statue Statue						
		Email						
		▼ Passwords						
		Password Type:	Internal Users	•				
			Password	Re-Ente	er Password			
		* Login Passwor	· ·····	•••••		Generate Password	(i)	
		Enable Passwor	1			Generate Password	۲	
		 User Information 	tion					
		First Name Te	t user					
		Last Name Te	t user					
		 Account Opti 	ons					
			Description					
		Change another	d en seut lacin					
		Change passwol						
		✓ Account Disa	ble Policy					
		Disable acc	ount if date exceeds 2019-	-04-23	(yyyy-mm-	dd)		
		 User Groups 		_				
		Employee	○ — ○	t				
		Submit Cance						
. <u>ユーザが</u>	<u>`作成され</u>	.ます。						
► System - Iden	tity Management	Network Resources + Devic	e Portal Management pxGrid	Services + Feed S	ervice + Threat Cent	tric NAC		
Identities Grou	ps External Identity	Sources Identity Source Sec	uences					
	G	Network Access Users						
Users	rk Soon Resulte							
Latest Manual Netwo	K OCAN RESULTS	/ Edit 🕂 Add 🔃 Chang	e Status 👻 💽 Import 🔹 Ex	port 👻 🗙 Delete 👻	Duplicate			
		Status Name	▲ Descrip st ⊕	tion F	rst Name Last N est user Test us	Name Email Address	User Identity Groups Employee	Admin
			- <u></u>				<i>p1</i>	

AAA クライアントとしての WLC の RADIUS サーバへの追加

ACS サーバでコントローラを AAA クライアントとして定義するには、次の手順を実行します。

1. ISE Web管理UIで、[管理(Administration)] -> [ネットワークリソース(Network Resources)] -> [ネットワークデバイス(Network Devices)]の下に移動し、[追加(Add)]アイコンを押します。

dudu Identity Services Engine		/-		/-	
cisco lucitaty del vices Englite	Home Context Visibility	Operations Policy	Administration Work Centers		
System Hentity Management	Network Resources Device	Portal Management pxGrid	Services + Feed Service + Threat Cent	ric NAC	
▼ Network Devices Network Device Gr	roups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences NAC Manage	ers External MDM + Locat	ion Services
0					
Network Devices	Network Devices				
Default Device					
Device Security Settings	🥖 Edi 🕂 🕂 Add 🖒 Duplica	ate 😭 Import 🚯 Export	Generate PAC X Delete		
	Name 🔺 IP/Ma	sk Profile Name	Location	Туре	Description
					No data available

 追加するデバイスに必要なフォーム(「Name」、「IP」)に入力し、前のセクションで WLCで設定した共有秘密パスワードと同じ共有秘密パスワードを設定します。[オプション で、場所、グループなどの情報を入力できます。 「Sumbit」を押します

dentity Services Engine	Home → Context Visibility → Operations → Policy - Administration → Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
G	
Network Devices	Network Devices List > New Network Device
Default Device	* Name WI (75520
Device Security Settings	Description
	IP Address VIP: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	t Device Dealls
	Davide Provide 1982 Criscol +
	Model Name v
	Software Version
	* Network Device Group
	Location LAB Set To Default
	IPSEC Is IPSEC Device Set To Default
	Device Type WLC-lab Set. To Default
	RADIUS Authentication Settings
	DADIUS UDD Sattings
	Protocol RADIUS
	Shared Secret Shared Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (2)
	DTLS Required 1
	Shared Secret radius/dtls
	CoA Port 2083 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional)
	DNS Name

3. デバイスがISEネットワークアクセスデバイスリストに追加されます。(NAD)



匿名インバンド PAC プロビジョニングによる RADIUS サーバへの EAP-FAST 認 証の設定

一般的には、このタイプの方法を使用して、導入にPKIインフラストラクチャがない場合を想定 します。

この方式は、ピアがISEサーバを認証する前に、Authenticated Diffie-HellmanKey Agreement Protocol(ADHP)トンネル内で動作します。

この方法をサポートするには、[Authentication Allowed Protocols] でISEの[Allow Anonymous Inband PAC Provisioning]を有効にする必要があります。

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 (Valid Range 0 to 3)
▶ Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)
Client Provisioning	Allow Authorization of expired certificates to allow certificate renewal in Authorization Policy
	Use PACs O Don't Use PACs
	Tunnel PAC Time To Live 90 Days *
	Proactive PAC update will occur after 90 % of PAC Time To Live has expired
	Allow Anonymous In-Band PAC Provisioning
	Allow Authenticated In-Band PAC Provisioning
	Server Returns Access Accept After Authenticated Provisioning
	Accept Client Certificate For Provisioning
	Allow Machine Authentication
	Machine PAC Time To Live 1 Weeks *
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 (i)
	Enable EAP Chaining

注:EAP-FAST内部方式に対してEAP-MS-CHAPv2などのパスワードタイプの認証を許可していることを確認してください。これは、明らかに匿名インバンドプロビジョニングでは証明書を使

RADIUS サーバの EAP-FAST 認証に認証付きインバンド PAC プロビジョニングを 設定する

これは最もセキュアで推奨されるオプションです。TLSトンネルは、サプリカントによって検証 されるサーバ証明書に基づいて構築され、クライアント証明書はISE(デフォルト)によって検 証されます。

このオプションでは、クライアントとサーバのPKIインフラストラクチャが必要ですが、サーバ 側だけに限定されるか、両側でスキップされる場合があります。

ISEでは、認証済みインバンドプロビジョニングに2つの追加オプションがあります。

- 「Server Returns Access Accept After Authenticated Provisioning」:通常、PACプロビジョ ニング後に、PACを使用してサプリカントを再認証するようにAccess-Rejectを送信する必 要があります。ただし、PACプロビジョニングは認証されたTLSトンネルで実行されるため 、認証時間を最小限に抑えるために、Access-Acceptで即座に応答できます。(このような 場合は、クライアント側とサーバ側に信頼できる証明書があることを確認してください)。
 「プロビジョニング用クライアント証明書の受け入れ」:クライアントデバイスにPKIイン
- フラストラクチャを提供せず、ISE上に信頼できる証明書のみを持つ場合は、そのオプショ ンを有効にします。これにより、サーバ側のクライアント証明書の検証をスキップできます

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ient Provisioning -Policy Elements
Dictionaries + Conditions - Result	S
G	- Illow EAP-FAST
▼Authentication	
Allowed Protocols	
Authorization	
▶ Profiling	Allow Password Change Retries 3 (Valid Range 0 to 5)
▶ Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)
Client Provisioning	C Allow EAP-ILS
	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
	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 Accent After Authenticated Provisioning
	Accept Client Certificate For Provisioning
	Machine PAC Time To Live 1 Weeks
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 Hours T
	Enable EAP Chaining

ISEでは、無線ユーザに対する単純な認証ポリシーセットも定義します。次の例では、接続パラ メータのデバイスタイプと場所と認証タイプとして、その条件に一致する認証フローが内部ユー ザデータベースに対して検証されます。

確認

この例では、それぞれのWLCデバッグとともに、認証済みインバンドPACプロビジョニングフローとNetwork Access Manager(NAM)の設定値を示します。

NAMプロファイルの設定

EAP-FASTを使用してISEに対してユーザセッションを認証するようにAnyconnect NAMプロファ イルを設定するには、次の手順を実行する必要があります。

- 1. Network Access Manager Profile Editorを開き、現在の設定ファイルをロードします。
- 2. [Allowed Authentication Modes]の下で[EAP-FAST]が有効になっていることを確認します。

🐴 AnyConnect Profile Editor -	Network Access Manager	- 🗆 X					
File Help							
Network Access Manager	Authentication Policy						
Client Policy	Profile: Untitled						
and Networks	Allow Association Modes	Allowed Authentication Modes					
	Select All (Personal)	Select All Outer					
	Open (no encryption)	EAP-FAST					
	Open (Static WEP)						
	Shared (WEP)	EAP-TLS					
	WPA Personal TKIP	EAP-TLS					
	WPA Personal AES	EAP-TTLS					
	WPA2 Personal TKIP	EAP-MD5 EAP-MSCHAPv2 PAP (legacy) CHAP (legacv)					
	WPA2 Personal AES	MSCHAP (legacy)					
	Select All (Enterprise)	LEAP					
	🗹 Open (Dynamic (802.1X) WEP)						
	WPA Enterprise TKIP	EAP-MSCHAPv2					
	WPA Enterprise AES	EAP-TLS					
	WPA2 Enterprise TKIP	Allowed Wired Security					
	WPA2 Enterprise AES						
	CCKM Enterprise TKIP						
	CCKM Enterprise AES	✓ 802.1x with MacSec					
		E Stera marmace					
	🕕 Help						

3. 新しいネ**ットワーク**プロファイルを「追加」します。

ork Access Manager , Networks				
uthentication Policy etworks	luted			
etwork Groups	Media Type	Group*		
wired	Wired	Global		
		CICC CI	Add	
			Edit	
			Delete	
* A network i	n group 'Global' is a member of <i>all</i> gro	oups.		

4. [Media type] 設定セクションで、プロファイル「**Name**」を定義し、メディアネットワーク タイプとしてwirelessを定義し、SSID名を指定します。

AnyConnect Profile Editor - File Help Network Access Manager	Network Access Manager –	
Authentication Policy	Promie: inity Clientivetwork Access Managersystem:configuration.xmi Name: eap_fast Group Membership in group: In group: Local networks In all groups (Global) in group: Choose Your Network Media in group: Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Image:	Media Typ A Security Let
	Next Cancel	~
	<	>

5. [Security Level] 設定タブで[Authenticating Network]を選択し、アソシエーションモードを [WPA2 Enterprise (AES)]に指定します

, Networks Profile:ility Client\Network Access Manager\system\configuration	on.xml
Security Level	Media Type
Open Network Open networks have no security, and are open to anybody within range. This is the least secure time of activation.	Security Lev Connection Ty
Shared Key Network Shared Key Network Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium sequrity level is suitable for	
small/home offices.	
Authenticating Network Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and	
other network infrastructure.	
- 802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30	
802.1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES)	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 60 maxStart 3	

6. この例では、ユーザーの種類の認証を使用しています。次のタブの[Connection type]で[User Connection]を選択します。

AnyConnect Profile Editor	Network Access Manager -		×
File Help			
File Help Network Access Manager Clent Policy Clent Policy Metworks Network Groups	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Network Connection Type O 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.	Media Security Connecti User / Creder	Type ^ / Leve on Ty Auth ntials
	A user connection will have 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		>
	Help		

7. この例では信頼できる証明書を使用していないため、[User Auth] タブで、許可される認証 方式としてEAP-FASTを指定し、サーバ証明書の検証を無効にします。

🐴 AnyConnect Profile Editor - Ne	twork Access Manager		– 🗆 ×
File Help			
Network Access Manager	letworks Profile:ility Client\Networ	k Access Manager\system\configuration	on.xml
Networks	EAP Methods		Media Type 🔨
	C EAP-TLS	O PEAP	Security Leve
			Connection Ty
	O EAP-TTLS	EAP-FAST	User Auth
	◯ LEAP		Credentials
	Extend user connection bey	ond log off	
	EAP-FAST Settings		
	Validate Server Identity		
	Enable Fast Reconnect		
	Disable when using a Sn	nart Card	
	- Inner Methods based on Credentials	Source	
	✓ EAR-MISCHARV2		
	I I using PACs, allow una	surrenucated FAC provisioning	
	 Authenticate using a Certific 	cate	
	O When requested send t	he client certificate in the clear	
	Only send client certifica	ates inside the tunnel	
	 Send client certificate us 	sing EAP-TLS in the tunnel	
	O Authenticate using a Token	and EAP-GIC	
	Use PACs		
	Next	Cancel	
<			¥
		🕕 Help	

注:実際の実稼働環境では、信頼できる証明書がISEにインストールされていることを確認 し、NAM設定でサーバ証明書の検証オプションを有効にしておいてください。

注:オプション「PACを使用している場合、非認証PACプロビジョニングを許可する」は、 匿名インバンドPACプロビジョニングの場合にのみ選択する必要があります。

8. ユーザのクレデンシャルをSSOとして定義します。ログイン時と同じクレデンシャルを使用 する場合は、[クレデンシャルの入力を求める]を選択し、ネットワークへの接続中にクレデ ンシャルを求める場合は[クレデンシャルの入力]を選択します。この例では、ユーザに対し て、ネットワークへの接続の試行時にクレデンシャルを要求します。

– 🗆 🗙

AnyConnect Profile Editor - Network Access Manag	ger
--	-----

User Identity			Media Type
Unprotected Identity Pa	anonymous		Security Leve
			Connection Ty
Protected Identity Patte	ern: [username]		User Auth
		•	Credentials
User Credentials			
Use Single Sign O	n Credentials		
Prompt for Crede	ntials		
O Remember	er Forever		
Remember	er while User is Logged On		
O Never Re	member		
O Use Static Creder	ntials		
Password:			
, abbridter			
Г	Dana		
	Done Cancer		

9. 設定されたプロファイルを各NAMフォルダに保存します。

EAP-FAST認証を使用して、SSIDへの接続をテストします。

1. Anyconnectネットワークリストからそれぞれのプロファイルを選択します

🕚 Cisco AnyCo	onnect Secure Mobility Client		—		~
	VPN: Verify your network connection.	~	Cc	onnect	
No Network C	onnectivity				
F	Network: Authenticating				
	eap_fast		llı. 🖰	\sim	
	eap_fast		8	all	
			8	all	
	(Standard		_	all	
			8	all	
			8	all	
		_	<u> </u>	alli	

- 2. 認証に必要なユーザ名とパスワードを入力します
- 3. サーバ証明書の承認(自己署名)

Cisco AnyConnect					
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?					
Certificate Name:	Certificate Name: rmanchur-ise.wlaaan.com@				
Issued To:	ssued 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	onnect Secure Mobility Client	—		×
	VPN: Network error. Unable to lookup host n	ames	s. Connect	
Limited Acces	s - DNS Failure			
	Network: Connected (192.168.77.34) eap_fast	8	atl 🗸 🗄	=

ISE認証ログ

EAP-FASTおよびPACプロビジョニングフローを示すISE認証ログは、[Operations] -> [RADIUS] -> [Live Logs] の下に表示され、[Zoom] アイコンを使用して詳細を確認できます。

1. クライアントが認証を開始し、ISEが認証方式としてEAP-TLSを提案していましたが、クラ イアントが拒否し、代わりにEAP-FASTを提案しました。これは、クライアントとISEの両 方が合意した方式でした。

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. クライアントとサーバの間でPAC交換のために提供された保護環境へのTLSハンドシェイク が開始され、正常に完了しました。

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
40000	Propered TLC Finished message
12816	TLS handshake succeeded

3. 内部認証が開始され、ユーザクレデンシャルがMS-CHAPv2を使用してISEによって正常に 検証されました(ユーザ名/パスワードベースの認証)