EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und Identity Services Engine

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen PAC PAC-Bereitstellungsmodi Konfigurieren Netzwerkdiagramm Konfigurationen Konfigurieren des WLC für die EAP-FAST-Authentifizierung Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server WLAN für die EAP-FAST-Authentifizierung konfigurieren Konfigurieren des RADIUS-Servers für die EAP-FAST-Authentifizierung Erstellen einer Benutzerdatenbank zum Authentifizieren von EAP-FAST-Clients Hinzufügen des WLC als AAA-Client zum RADIUS-Server Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit authentifizierter In-Band-PAC-Bereitstellung Überprüfen NAM-Profilkonfiguration Testen Sie die Verbindung zum SSID mithilfe der EAP-FAST-Authentifizierung. ISE-Authentifizierungsprotokolle WLC-seitiges Debugging bei erfolgreichem EAP-FAST-Flow Fehlerbehebung

Einführung

In diesem Dokument wird erläutert, wie der WLAN-Controller (WLC) für Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST)-Authentifizierung mithilfe eines externen RADIUS-Servers konfiguriert wird. In diesem Konfigurationsbeispiel wird die Identity Services Engine (ISE) als externer RADIUS-Server für die Authentifizierung des Wireless-Clients verwendet.

In diesem Dokument wird erläutert, wie Sie die ISE für die Bereitstellung der Wireless-Clients für die Bereitstellung von Anonymous and Authenticated In-Band (Automatic) Protected Access Credentials (PAC) konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Grundkenntnisse des CAPWAP-Protokolls
- Kenntnisse zum Konfigurieren eines externen RADIUS-Servers, z. B. der Cisco ISE
- Funktionale Kenntnisse des allgemeinen EAP-Frameworks
- Grundkenntnisse zu Sicherheitsprotokollen, wie MS-CHAPv2 und EAP-GTC, und Kenntnisse zu digitalen Zertifikaten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

 Cisco WLC der Serie 5520 mit Firmware-Version 8.8.111.0Cisco AP der Serie 4800AnyConnect NAMCisco Secure ISE Version 2.3.0.298Cisco Switch der Serie 3560-CX mit Version 15.2(4)E1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Das EAP-FAST-Protokoll ist ein öffentlich zugänglicher EAP-Typ nach IEEE 802.1X, den Cisco entwickelt hat, um Kunden zu unterstützen, die keine strenge Kennwortrichtlinie durchsetzen können und einen 802.1X-EAP-Typ bereitstellen möchten, für den keine digitalen Zertifikate erforderlich sind.

Das EAP-FAST-Protokoll ist eine Client-Server-Sicherheitsarchitektur, die EAP-Transaktionen mit einem Transport Level Security (TLS)-Tunnel verschlüsselt. Die Einrichtung von EAP-FAST-Tunneln basiert auf strengen Geheimnissen, die nur für Benutzer gelten. Diese sicheren Geheimnisse werden als PACs bezeichnet, die von der ISE mithilfe eines Master-Schlüssels generiert werden, der nur der ISE bekannt ist.

EAP-FAST findet in drei Phasen statt:

• Phase Null (Automatische PAC-Bereitstellungsphase) - EAP-FAST-Phase Null. Eine optionale

Phase ist ein tunnelsicheres Mittel, um einem EAP-FAST-Endbenutzer-Client eine PAC für den Benutzer bereitzustellen, der Netzwerkzugriff anfordert. **Die Bereitstellung einer PAC für den Endbenutzer-Client ist der einzige Zweck von Phase Null.Hinweis:** Phase Null ist optional, da PACs Clients auch manuell bereitgestellt werden können, anstatt Phase Null zu verwenden.Weitere Informationen finden Sie im Abschnitt <u>PAC-Bereitstellungsmodi</u> dieses Dokuments.

- Phase 1: In Phase 1 richten die ISE und der Endbenutzer-Client einen TLS-Tunnel auf der Grundlage der PAC-Anmeldeinformationen des Benutzers ein. Für diese Phase muss dem Endbenutzer-Client eine PAC für den Benutzer bereitgestellt werden, der versucht, auf das Netzwerk zuzugreifen, und die PAC basiert auf einem Master-Schlüssel, der noch nicht abgelaufen ist. In Phase 1 des EAP-FAST ist kein Netzwerkservice aktiviert.
- Phase 2 In Phase 2 werden die Anmeldeinformationen für die Benutzerauthentifizierung sicher mithilfe einer vom EAP-FAST im TLS-Tunnel unterstützten inneren EAP-Methode an den RADIUS weitergeleitet, der mithilfe der PAC zwischen dem Client und dem RADIUS-Server erstellt wurde. EAP-GTC, TLS und MS-CHAP werden als innere EAP-Methoden unterstützt. Für EAP-FAST werden keine anderen EAP-Typen unterstützt.

Weitere Informationen finden Sie unter Funktionsweise von EAP-FAST.

PAC

PACs sind sichere, gemeinsam genutzte Geheimnisse, die es der ISE und einem EAP-FAST-Endbenutzer-Client ermöglichen, sich gegenseitig zu authentifizieren und einen TLS-Tunnel für die Verwendung in Phase 2 von EAP-FAST einzurichten. Die ISE generiert PACs, indem sie den aktiven Master-Schlüssel und einen Benutzernamen verwendet.

PAC umfasst:

- PAC-Key Gemeinsam genutzter geheimer Schlüssel, der an einen Client (und Client-Gerät) und eine Serveridentität gebunden ist.
- PAC Opaque (Opak PAC): Opakes Feld, das der Client zwischenspeichert und an den Server übergibt. Der Server stellt den PAC-Schlüssel und die Client-Identität für die gegenseitige Authentifizierung mit dem Client wieder her.
- PAC-Info: Enthält mindestens die Serveridentität, um dem Client das Zwischenspeichern verschiedener PACs zu ermöglichen. Optional enthält es weitere Informationen, wie z. B. die Ablaufzeit des PAC.

PAC-Bereitstellungsmodi

Wie bereits erwähnt, ist Phase Null eine optionale Phase.

EAP-FAST bietet zwei Optionen für die Bereitstellung eines Clients mit einer PAC:

Automatische PAC-Bereitstellung (EAP-FAST Phase 0 oder In-Band-PAC-Bereitstellung)

• Manuelle (Out-of-Band) PAC-Bereitstellung

Die In-Band-/automatische PAC-Bereitstellung sendet eine neue PAC über eine gesicherte Netzwerkverbindung an einen Endbenutzer-Client. Die automatische PAC-Bereitstellung erfordert keine Eingriffe des Netzwerkbenutzers oder eines ISE-Administrators, vorausgesetzt, Sie konfigurieren die ISE und den Endbenutzer-Client, um die automatische Bereitstellung zu unterstützen. Die neueste EAP-FAST-Version unterstützt zwei verschiedene In-Band-Konfigurationsoptionen für die PAC-Bereitstellung:

Anonyme In-Band-PAC-Bereitstellung

Authentifizierte In-Band-PAC-Bereitstellung

Hinweis: In diesem Dokument werden diese In-Band-PAC-Bereitstellungsmethoden und deren Konfiguration beschrieben.

Für die Out-of-Band-/manuelle PAC-Bereitstellung muss ein ISE-Administrator PAC-Dateien generieren, die dann an die entsprechenden Netzwerkbenutzer verteilt werden müssen. Benutzer müssen Endbenutzer-Clients mit ihren PAC-Dateien konfigurieren.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Konfigurieren des WLC für die EAP-FAST-Authentifizierung

Führen Sie die folgenden Schritte aus, um den WLC für die EAP-FAST-Authentifizierung zu konfigurieren:

1. Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server 2. WLAN für die EAP-FAST-Authentifizierung konfigurieren

Konfigurieren des WLC für die RADIUS-Authentifizierung über einen externen RADIUS-Server

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server validiert die Benutzeranmeldeinformationen anschließend mithilfe von EAP-FAST und ermöglicht den Zugriff auf die Wireless-Clients.

Gehen Sie wie folgt vor, um den WLC für einen externen RADIUS-Server zu konfigurieren:

- Wählen Sie Security und RADIUS Authentication (RADIUS-Authentifizierung) in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen. Klicken Sie anschließend auf Neu, um einen RADIUS-Server zu definieren.
- Definieren Sie die RADIUS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu). Zu diesen Parametern gehören:IP-Adresse des RADIUS-ServersGemeinsamer geheimer SchlüsselPort-NummerServerstatusIn diesem Dokument wird der ISE-Server mit der IP-Adresse 10.48.39.128 verwendet

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	RADIUS A	uthenti	cation Server	s > New					
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LOCAI 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 	KADIUS A Server Inde Server IP A Shared Sec Confirm Sh Apply Cisco Apply Cisco Key Wrap Port Numbe Server Stat Support for Server Tim Network Us Managemen Tunnel Prov PAC Provisi IPSec Cisco ACA	ex (Priorit) Address(Ip cret Forma cret bared Secre- b ISE Defa b ACA Defa er tus r CoA eout ser nt nt Retrans xy ioning	() v4/Ipv6) t et ult settings ault settings	 S > New 2 ‡ 10.48.39.128 ASCII ‡ (Designed 1812 Enabled ‡ Enabled ‡ S seconds Enable 	for FIPS custor	mers and requires	a key wrap comp	liant RAD	IUS server)
Advanced									

3. Klicken Übernehmen.

WLAN für die EAP-FAST-Authentifizierung konfigurieren

Konfigurieren Sie anschließend das WLAN, das die Clients zur Verbindung mit dem Wireless-Netzwerk für die EAP-FAST-Authentifizierung verwenden, und weisen Sie es einer dynamischen Schnittstelle zu. Der in diesem Beispiel konfigurierte WLAN-Name ist **schnell**. In diesem Beispiel wird dieses WLAN der Verwaltungsschnittstelle zugewiesen. Gehen Sie wie folgt vor, um das schnelle WLAN und die zugehörigen Parameter zu konfigurieren:

- Klicken Sie in der Benutzeroberfläche des Controllers auf WLANs, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
- 2. Klicken Sie auf **Neu**, um ein neues WLAN zu erstellen.

،، ،،، ،، cısco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	M <u>a</u> nagement c <u>o</u> mmands he	₽ <u>F</u> EEDBACK		
WLANs	WLANs					
VLANS WLANS	Current Filter: Non	e [Change Filter] [Clear Filter]			Create New 🗘 Go	
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
	1 WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]	
	2 WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]	

3. Konfigurieren Sie auf der Seite WLANs > New den Namen **eap_fast** WLAN-SSID, den Profilnamen und die WLAN-ID. Klicken Sie anschließend auf **Übernehmen**.

ahaha				Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS C	CONTROLLER WIRELESS SECURITY MANA	GEMENT COMMANDS HELP FEEDBACK	🔒 Home
WLANs	WLANs > New			< Back Apply
 ▼ WLANS WLANS ▶ Advanced 	Type Profile Name SSID ID	WLAN 2 cap_fast cap_fast 3 3		

- 4. Sobald Sie ein neues WLAN erstellt haben, wird die Seite WLAN > Bearbeiten f
 ür das neue WLAN angezeigt. Auf dieser Seite k
 önnen Sie verschiedene Parameter f
 ür dieses WLAN definieren. Dies umfasst allgemeine Richtlinien, RADIUS-Server, Sicherheitsrichtlinien und 802.1x-Parameter.
- Aktivieren Sie das Kontrollkästchen Admin Status unter Allgemeine Richtlinien, um das WLAN zu aktivieren. Wenn der Access Point die SSID in seinen Beacon-Frames übertragen soll, aktivieren Sie das Kontrollkästchen Broadcast SSID (SSID senden).

LANs > E	dit 'eap_fa	ıst'			
General	Security	QoS	Policy-Mapping	Advanced	
Profile Na	me	eap	o_fast		
Туре		WL	AN		
SSID		eap	_fast		
Status			Enabled		
Radio Poli	су	(Mo	difications done under	security tab will ap	opear after applying the changes.)
Interface/	Interface Group	o(G) vla	an1477 🗘		
Multicast	Vlan Feature		Enabled		
Broadcast	SSID		Enabled		
NAS-ID		non	e		

wählen Sie dot1x für AKM aus.

In diesem Beispiel wird WPA2/AES + dot1x als Layer-2-Sicherheit für dieses WLAN verwendet. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden.

LANs > E	dit 'eap_f	ast'				
General	Security	QoS	Policy-Mappi	ing Adva	nced	
Layer 2	Layer 3	AAA Se	rvers			
Layer 2	Security 🧧 🚺	VPA+WPA2	\$			
Fast Trans	ition					
Fast Transit	ion	Disat	le 🗘			
Protected	Management	Frame				
PMF		Disab	led 🗘			
WPA+WPA	2 Parameter	S				
WPA Pol	icy					
WPA2 Po	olicy		_			
WPA2 E	ncryption	AES	🗆 ТКІР	CCMP256	GCMP128	GCMP256
OSEN Po	olicy		_			
Authentica	tion Key Mar	agement ¹	2			
802.1X		Enable				
ССКМ		Enable				
PSK		Enable				
ET 000 ·		nahla				

7. Wählen Sie unter "WLAN -> Edit -> Security -> AAA Servers" im Dropdown-Menü unter RADIUS Servers den entsprechenden RADIUS-Server aus.

neral	Security	QoS	Policy	Mapping	Advanced		
ayer 2	Layer 3		Servers				
ADIUS Serv RADIUS Se	ervers belo v ers erver Overwa	w to ove	r ride use o ce 🔲 Ena	o f default se bled	rvers on this V	VLAN	
Apply Cisco	o ISE Defaul	t Settings	🗆 Ena	bled	Comucine		
Apply Cisco	o ISE Defaul	t Settings	Ena	Accounting	Servers		EAP P
Apply Cisco Server 1	Authentica	t Settings ation Serv 39.128, Pc	Ena	Accounting Content Enabled None	Servers	\$	EAP P Ena
Apply Cisco Server 1 Server 2	Authentica Contemporation Contempora	t Settings ation Serv 39.128, Pc	Ena vers ort:1812 \$	Accounting Enabled None None	Servers	¢ ¢	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3	Authentica Control Enabled IP:10.48.2 None None	t Settings ntion Serv 39.128, Pc	Ena	Accounting Enabled None None None	Servers	 <	EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4	Authentica Contraction Authentica Contraction Authentica Contraction Contraction None None None	t Settings ntion Serv 39.128, Pc	Ena	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	t Settings ntion Serv 39.128, Pc	Ena	Accounting Enabled None None None None None	Servers		EAP P Ena
Apply Cisco Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Authentica Control Enabled IP:10.48.3 None None None None None None	t Settings ation Serv 39.128, Pc	Ena	Accounting Enabled None None None None None None None	Servers	\Rightarrow	EAP P Ena

8. Klicken Sie auf Übernehmen. Hinweis: Dies ist die einzige EAP-Einstellung, die auf dem Controller für die EAP-Authentifizierung konfiguriert werden muss. Alle anderen EAP-FASTspezifischen Konfigurationen müssen auf dem RADIUS-Server und den zu authentifizierenden Clients ausgeführt werden.

Konfigurieren des RADIUS-Servers für die EAP-FAST-Authentifizierung

Führen Sie die folgenden Schritte aus, um den RADIUS-Server für die EAP-FAST-Authentifizierung zu konfigurieren:

- 1. Erstellen einer Benutzerdatenbank zum Authentifizieren von EAP-FAST-Clients
- 2. Hinzufügen des WLC als AAA-Client zum RADIUS-Server
- 3. Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung
- 4. Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit authentifizierter In-Band-PAC-Bereitstellung

Erstellen einer Benutzerdatenbank zum Authentifizieren von EAP-FAST-Clients

In diesem Beispiel werden Benutzername und Kennwort des EAP-FAST-Clients als <*eap_fast*> bzw. <*EAP-fast1*> konfiguriert.

1. Navigieren Sie in der ISE Web-Admin-Benutzeroberfläche unter "Administration -> Identity Management -> Users" (Verwaltung -> Identitätsverwaltung -> Benutzer), und drücken Sie das Symbol "Add" (Hinzufügen).

···· , ····							
dentity Services Engine	Home ► Context Visibility ► Ope	rations ► Policy - Ad	ministration Vork Cer	nters			
► System - Identity Management	Network Resources Device Portal Ma	anagement pxGrid Services	Feed Service Three	eat Centric NAC			
▼Identities Groups External Id	Identity Sources Identity Source Sequences	▶ Settings					
	0						
Users	Network Access Users						
Latest Manual Network Scan Results	🖊 Edit 🕂 Add 🔣 Change Status	😭 Import 🛛 🚯 Export 👻	X Delete				
	Status Name	 Description 	First Name	Last Name	Email Address	User Identity Groups	Admin
					No da	ta available	

 Füllen Sie die erforderlichen Formulare für den zu erstellenden Benutzer aus: "Name" und "Anmeldekennwort" und wählen Sie "Benutzergruppe" aus der Dropdown-Liste aus.[Optional können Sie weitere Informationen für das Benutzerkonto eingeben] Drücken Sie "Sumbit".

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
► System - Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓Identities Groups External Iden	tity Sources Identity Source Sequences + Settings
(9
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Results	* Name eap_fast
	Status 🛃 Enabled 💌
	Email
	▼ Passwords
	Password Type: Internel Licence -
	Paceward Paceward Paceward
	Enable Password
	▼ User Information
	First Name Test user
	Last Name Test user
	▼ Account Options
	Description
	Change password on next login
	▼ Account Disable Policy
	Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)
	▼ User Groups
	Employee 🗢 🕂
	Submit Cancel

3. Der Benutzer wird erstellt.

System Identity Management	Network Resources Device Portal Man	agement pxGrid Services	Feed Service Fnree	eat Centric NAC			
Identities Groups External Identity Sources Identity Source Sequences + Settings							
© Users	Network Access Users						
Latest Manual Network Scan Results	🖊 Edit 🕂 Add 🔢 Change Status 👻	😭 Import 🔹 😭 🙀	Delete 👻 🕒 Duplicate				
	Status Name	 Description 	First Name	Last Name	Email Address	User Identity Groups	Admin
	🗌 🛃 Enabled 🧕 eap_fast	\oplus	Test user	Test user		Employee	

Hinzufügen des WLC als AAA-Client zum RADIUS-Server

Gehen Sie wie folgt vor, um den Controller als AAA-Client auf dem ACS-Server zu definieren:

 Navigieren Sie in der ISE Web-Admin-Benutzeroberfläche unter "Administration -> Network Resources -> Network Devices" (Verwaltung -> Netzwerkressourcen -> Netzwerkgeräte), und drücken Sie das Symbol "Add" (Hinzufügen).

dentity Services Engine	Home Context Visibility	Operations Policy	-Administration		
System Identity Management	Network Resources Pevice Pe	ortal Management pxGrid Se	ervices + Feed Service + Threat Cent	ic NAC	
▼ Network Devices Network Device G	roups Network Device Profiles	External RADIUS Servers F	RADIUS Server Sequences NAC Manage	rs External MDM	Location Services
G					
Network Devices	Network Devices				
Default Device					
Device Security Settings	/ Edi 🕂 Add 🚡 Duplicate	Export 🕞 Export	Generate PAC X Delete		
	Name 🔺 IP/Mask	Profile Name	Location	Туре	Description
					No data available

 Füllen Sie die erforderlichen Formulare für das hinzuzufügende Gerät aus: "Name", "IP" und konfigurieren Sie das gleiche gemeinsam genutzte geheime Kennwort, wie im vorherigen Abschnitt für WLC konfiguriert wurde, im Formular "Gemeinsamer geheimer Schlüssel" [optional können Sie weitere Informationen für das Gerät wie Standort, Gruppe usw. eingeben].

Drücken Sie "Sumbit".

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Manageme	nt + Network Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
Network Devices Network Devices	vice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
	0
Network Devices	
Default Device	* Name WICS520
Device Security Settings	Description
	IP Address v IP: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	1 Davias Profile dth Close D
	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
	Cox Port 1/00 Set to Default
	RADIUS DTLS Settings ()
	DILS Required
	CoA Port 2003 Set To Default
	Issuer CA of ISE Certificates for CoA Select if equived (options)
	Laster CA OF ISE Certaincates of CAA

3. Gerät wird der Liste der ISE-Netzwerkzugriffsgeräte hinzugefügt. (NAD)



Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit anonymer In-Band-PAC-Bereitstellung

Im Allgemeinen sollte dieser Methodentyp verwendet werden, falls die Bereitstellung nicht über eine PKI-Infrastruktur verfügt.

Diese Methode wird in einem Authenticated Diffie-HellmanKey Agreement Protocol (ADHP)-Tunnel ausgeführt, bevor der Peer den ISE-Server authentifiziert.

Um diese Methode zu unterstützen, müssen wir "Anonyme In-Band-PAC-Bereitstellung zulassen" auf der ISE unter "Authentifizierungs-zulässige Protokolle" aktivieren:

cisco Identity Services Engine	Home Context Visibility Operations -Policy Administration Work Centers
Policy Sets Profiling Posture C	Client Provisioning -Policy Elements
Dictionaries + Conditions • Resu	Its
	Allow EAP-FAST
▼Authentication	
Allowed Protocols	
Authorization	
▶ Profiling	
► Posture	
Client Provisioning	Allow Authorization of avaired certificates to allow certificate received in Authorization Policy
	Use PACs 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

Hinweis: Stellen Sie sicher, dass Sie die Kennworttypauthentifizierung zugelassen haben, wie z. B. EAP-MS-CHAPv2 für die innere EAP-FAST-Methode, da wir bei der anonymen In-BandBereitstellung natürlich keine Zertifikate verwenden können.

Konfigurieren der EAP-FAST-Authentifizierung auf dem RADIUS-Server mit authentifizierter In-Band-PAC-Bereitstellung

Dies ist die sicherste und empfohlene Option. Der TLS-Tunnel basiert auf dem Serverzertifikat, das vom Supplicant validiert wird, und das Client-Zertifikat wird durch die ISE validiert (Standard).

Für diese Option ist eine PKI-Infrastruktur für Client und Server erforderlich, die jedoch möglicherweise auf Serverseite beschränkt oder auf beiden Seiten übersprungen wird.

Für die ISE gibt es zwei zusätzliche Optionen für die authentifizierte In-Band-Bereitstellung:

- "Server Returns Access Accept After Authenticated Provisioning" Normalerweise sollte nach der PAC-Bereitstellung eine Access-Reject gesendet werden, die den Supplicant zur erneuten Authentifizierung mithilfe von PACs zwingt. Da die PAC-Bereitstellung jedoch im authentifizierten TLS-Tunnel erfolgt, können wir sofort mit Access-Accept reagieren, um die Authentifizierungszeit zu minimieren. (in diesem Fall sollten Sie sich vergewissern, dass Sie auf Client- und Serverseite vertrauenswürdige Zertifikate besitzen).
- "Accept Client Certificate For Provisioning" Wenn Client-Geräte keine PKI-Infrastruktur bereitstellen und nur über ein vertrauenswürdiges Zertifikat für die ISE verfügen sollen, aktivieren Sie diese Option, mit der die Validierung von Client-Zertifikaten auf Serverseite übersprungen werden kann.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	lient Provisioning - Policy Elements
Dictionaries + Conditions - Resul	15
G	✓ Allow EAP-FAST
▼Authentication	
Allowed Protocols	EAP-FAST Inner Methods
Authorization	
• Profiling	Allow Password Change Retries 3 (Valid Range 0 to 3)
, ronning	Allow EAP-GTC
Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)
➤ Client Provisioning	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy I Use PACs Ont Use PACs Use PAC Time To Live 90 Days * Proactive PAC update will occur after 90 % of PAC Time To Live has expired I Allow Anthenticated In-Band PAC Provisioning I Allow Authenticated In-Band PAC Provisioning I Allow Authenticate For Provisioning I Accept Client Certificate For Provisioning I Allow Authentication Machine PAC Time To Live 1
	Enable Stateless Session Resume
	Authorization PAC Time To Live 1 1
	Enable EAP Chaining

Auf der ISE definieren wir auch einfache Authentifizierungsrichtlinien für Wireless-Benutzer. Im folgenden Beispiel werden Gerätetyp und Standort sowie Authentifizierungstyp als Verbindungsparameter verwendet. Der Authentifizierungsfluss, der dieser Bedingung entspricht, wird anhand der internen Benutzerdatenbank validiert.

	> Ontions	802.1X	C
--	-----------	--------	---

Überprüfen

In diesem Beispiel werden die Konfigurationseinstellungen für den Authenticated In-Band PAC Provisioning Flow und den Network Access Manager (NAM) zusammen mit den entsprechenden WLC-Debuggen angezeigt.

NAM-Profilkonfiguration

Die folgenden Schritte müssen ausgeführt werden, um das AnyConnect NAM-Profil für die Authentifizierung von Benutzersitzungen mit der ISE mithilfe von EAP-FAST zu konfigurieren:

- 1. Öffnen Sie den Network Access Manager Profile Editor, und laden Sie die aktuelle Konfigurationsdatei.
- 2. Stellen Sie sicher, dass "EAP-FAST" unter "Zulässige Authentifizierungsmodi" aktiviert ist.

AnyConnect Profile Editor -	Network Access Manager	- 🗆 ×
File Help		
Network Access Manager	Authentication Policy	
	Profile: Untitled	
Networks	Allow Association Modes	Allowed Authentication Modes
wetwork Groups	Select All (Personal)	Select All Outer
	Open (no encryption)	EAP-FAST
	Open (Static WEP)	EAP-GTC
	Shared (WEP)	EAP-TLS
	WPA Personal TKIP	✓ EAP-TLS
	WPA Personal AES	☐ EAP-TTLS
	WPA2 Personal TKIP	□ EAP-MD5 □ EAP-MSCHAPv2 □ PAP (legacy) □ CHAP (legacy)
	WPA2 Personal AES	MSCHAP (legacy)
		MSCHAPv2 (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
	1 Help	

3. Neues Netzwerkprofil "hinzufügen":

work Access Manager Client Policy	Networks Profile: Untit	led			
Authentication Policy Networks	Network				
nethoric croups	Name	Media Type	Group*		
	wired	Wired	Global		
				Add	
				Edit	
				Delete	
	* A network in a	oun 'Clobal' is a member of all or	20105		
	Aneworking	oup diobar is a member of angi	oups.		

4. Im Konfigurationsabschnitt **"Medientyp"** definieren Sie das Profil "**Name**", das Wireless-Netzwerk als Ihren Mediennetzwerktyp und geben den SSID-Namen an.

Name: eap_fast Group Membership In group: 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.	Media Typ Security Lev
 Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): eap_fast Hidden Network Corporate Network Association Timeout seconds 	

5. Wählen Sie auf der Registerkarte "**Sicherheitsstufe**" die Option "Authenticating Network" (Netzwerk authentifizieren) aus, und geben Sie den Zuordnungsmodus als WPA2 Enterprise (AES) an.

Networks Access Manager Client Policy Authentication Policy Networks Scurity Level Open Network Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. Shared Key Network Shared Key Network 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 Authentication networks require radius servers, and other network infraeture tree	Media Type A Security Lew Connection Ty
Security Level Open Networks Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. Shared Key Network Shared K	Media Type A Security Lew Connection Ty
ould new ork in as dearer	
802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3	
Association Mode	
Next Cancel	×

6. In diesem Beispiel wird die Benutzertypauthentifizierung verwendet. Wählen Sie daher unter der nächsten Registerkarte "Verbindungstyp" die Option "Benutzerverbindung".

File Help Wetwork Access Manager Authentication Foldy Authentication Foldy Authentication Foldy Wetwork Groups Machine Connection Type Machine Connection Type Machine Connection This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access. Wetwork Groups Machine and User Connection This typically used for connecting to domains, to get GPO's and other updates from the network before the user has logged on. Machine and User Connection This type of connection This type of connection will make the network available after the user has logged on. This type of connection This type of connection will be back up again with different credentials when the user logs in. Next Cancel	AnyConnect Profile Editor	- Network Access Manager —			×
Network Access Manager Gruth Taily Methinoids Conception Network Sciences Network Groups Media Oper Methinoids Media Type Media Type	File Help				
Network Method Method Method Security Lew 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. Image: Connection Connection Image: Connection 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 Credentals 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. Image: Connection Machine boots. It will then be brought down, and back up again with different credentials when the user logs in. Image: Connection Image: Connection It will then be brought down, and back up again with different credentials when the user logs in. Image: Connection Image: Connection It will then be brought down, and back up again with different credentials Image: Connection Image: Connection It will then be accessed up again with different credentials Image: Connection Image: Connection It will then be accessed up again with different credentials Image: Connection Image: Connection It will then be accessed up addition Image: Connection Image: Connection<	Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml			
< >>	Authentication Policy	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. Image:	Me Sec. Conn Us Cre	dia Tr rity L ection er Au .dent	vpe ^ n Ty th ials
Helo		*			-

7. Geben Sie auf der Registerkarte "**User Auth**" (Benutzerauthentifizierung) EAP-FAST als zulässige Authentifizierungsmethode an, und deaktivieren Sie die Validierung von Serverzertifikaten, da in diesem Beispiel keine vertrauenswürdigen Zertifikate verwendet werden.

File Help	Networks Profile:ility Client\Network Access Manager\system\config	guration.xml
Networks	EAP Methods EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-TLS EAP-FAST EAP-FAST EAP-FAST Settings Validate Server Identity EAP-FAST Settings Validate Server Identity EAP-FAST Settings Validate Server Identity EAP-MSCHAPv2 EAP-GTC Inner Methods based on Credentials Source Authenticate using a Password EAP-MSCHAPv2 EAP-GTC Authenticate using a Certificate Only send client certificate in the clear Only send client certificate in the tunnel Send client certificate using EAP-TLS in the tunnel Authenticate using a Token and EAP-GTC Use PACs	Media Type ∧ Security Leve Connection Ty User Auth Credentials
	Next Cancel	~

Hinweis: Stellen Sie in der realen Produktionsumgebung sicher, dass Sie auf der ISE installiertes Zertifikat installiert haben, und lassen Sie die Option zur Validierung von Serverzertifikaten in den NAM-Einstellungen aktiviert.

Hinweis: Option "Bei Verwendung von PACs muss die nicht authentifizierte PAC-Bereitstellung zugelassen werden" nur bei anonymer In-Band-PAC-Bereitstellung ausgewählt werden.

8. Definieren Sie Benutzeranmeldeinformationen, entweder als SSO für den Fall, dass Sie dieselben Anmeldeinformationen wie für die Anmeldung verwenden möchten, oder wählen Sie "Aufforderung zur Eingabe von Anmeldeinformationen" aus, falls der Benutzer bei der Verbindung mit dem Netzwerk um Anmeldeinformationen gebeten werden soll, oder definieren Sie statische Anmeldeinformationen für diesen Zugriffstyp. In diesem Beispiel wird der Benutzer beim Verbindungsversuch mit dem Netzwerk zur Eingabe von Anmeldeinformationen aufgefordert.

Anyconnect Frome Editor - Network Access Manager
--

User Identity		Media Type
Unprotected Identity Pattern:	anonymous	Security Lev
Drotostad Identify Dattara		Connection Ty
Protected Identity Pattern:	[username]	User Auth
User Credentials Use Single Sign On Credentials Use Single Sign On Credentials C Remember Forever Remember while User is Never Remember	Logged On	
Use Static Credentials		
Password:		
Done	Cancel	

9. Speichern Sie das konfigurierte Profil im entsprechenden NAM-Ordner.

Testen Sie die Verbindung zum SSID mithilfe der EAP-FAST-Authentifizierung.

1. Wählen Sie das entsprechende Profil aus der AnyConnect-Netzwerkliste aus

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. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung ein.
- 3. Serverzertifikat akzeptieren (selbstsigniert)

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. Fertig

🕙 Cisco AnyConnect Secure Mobility Client - 🗆 🗙			×	
	VPN: Network error. Unable to lookup host	name:	s. Connect	
Limited Acces	s - DNS Failure			
	Network: Connected (192.168.77.34) eap_fast	A	atl 🗸	

ISE-Authentifizierungsprotokolle

ISE-Authentifizierungsprotokolle, die den EAP-FAST- und PAC-Bereitstellungs-Flow anzeigen, sind unter "**Operations -> RADIUS -> Live Logs**" (**Vorgänge -> RADIUS -> Live Logs**) zu sehen und können mithilfe des Symbols "**Zoom**" detaillierter dargestellt werden:

1. Der Client hat mit der Authentifizierung begonnen, und die ISE schlug EAP-TLS als Authentifizierungsmethode vor. Der Client lehnte jedoch EAP-FAST ab und schlug dies vor. Dabei handelte es sich um die vereinbarte Methode für Client und 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. Der TLS-Handshake wurde zwischen Client und Server gestartet, um eine geschützte Umgebung für den PAC-Austausch bereitzustellen, und wurde erfolgreich abgeschlossen.

12800	Extracted first TLS record: TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12811	Extracted TLS Certificate message containing client certificate
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request (g Step latency=13317 ms)
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12002	Proposed TLC Finished message
12816	TLS handshake succeeded

3. Die interne Authentifizierung wurde gestartet, und die Benutzeranmeldeinformationen wurden mithilfe von MS-CHAPv2 erfolgreich von der ISE validiert (Authentifizierung auf Basis von Benutzernamen/Kennwort).