

Compréhension de l'EAP-FAST et enchaînement des réalisations sur AnyConnect NAM et ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Théorie](#)

[Phases](#)

[PAC](#)

[Quand des PACs sont générés](#)

[Clé principale de serveur d'EAP-FAST ACS 4.x contre ACS 5x et ISE](#)

[Reprise de session](#)

[État de serveur](#)

[Sans état \(PAC basé\)](#)

[Implémentation d'AnyConnect NAM](#)

[Ravitaillement PAC \(phase 0\)](#)

[Tunnel anonyme de TLS](#)

[Tunnel authentifié de TLS](#)

[Eap-enchaînement](#)

[Là où des fichiers PAC sont enregistrés](#)

[AnyConnect NAM 3.1 contre 4.0](#)

[Exemples](#)

[Diagramme du réseau](#)

[EAP-FAST sans EAP enchaînant avec l'utilisateur et l'ordinateur PAC](#)

[L'EAP-FAST avec l'EAP enchaînant avec le PAC rapide rebranchent](#)

[EAP-FAST avec l'EAP enchaînant sans PAC](#)

[EAP-FAST avec l'EAP enchaînant l'expiration PAC d'autorisation](#)

[L'EAP-FAST avec l'EAP enchaînant le tunnel PAC a expiré](#)

[L'EAP-FAST avec l'enchaînement d'EAP et le TLS anonyme percent un tunnel le ravitaillement PAC](#)

[EAP-FAST avec l'EAP enchaînant l'authentification de l'utilisateur seulement](#)

[EAP-FAST avec l'enchaînement d'EAP et les paramètres de tunnel anonymes contradictoires de TLS](#)

[Dépannez](#)

[ISE](#)

[AnyConnect NAM](#)

[Références](#)

Introduction

Cet article explique des détails concernant des réalisations d'EAP-FAST sur le gestionnaire d'accès au réseau de Cisco

AnyConnect (NAM) et le Cisco Identity Services Engine (ISE). Il explique plus loin comment les caractéristiques spécifiques fonctionnent ensemble et fournit les cas d'utilisation et les exemples typiques.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de cadre d'EAP et de méthodes d'EAP-FAST
- Connaissance de base du Cisco Identity Services Engine (ISE)
- Connaissance de base d'AnyConnect NAM et d'éditeur de profil
- Connaissance de base de configuration de Cisco Catalyst pour des services de 802.1x

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Windows 7 avec le Client à mobilité sécurisé Cisco AnyConnect, la version 3.1 et 4.0
- Commutateur de Cisco Catalyst 3750X avec le logiciel 15.2.1 et plus tard
- Cisco ISE, version 1.4

Théorie

Phases

L'EAP-FAST est une méthode flexible d'EAP qui permet l'authentification mutuelle d'un suppliant et d'un serveur. Il est semblable à EAP-PEAP, mais typiquement n'exige pas l'utilisation des Certificats de client ou même de serveur. Un avantage d'EAP-FAST est la capacité d'enchaîner de plusieurs authentifications (suivre de plusieurs méthodes intérieures) et de les lier cryptographiquement ensemble (EAP enchaînant). Les réalisations de Cisco utilisent ceci pour l'utilisateur et les authentifications de machine.

L'EAP-FAST utilise les qualifications de Protected Access (PAC) afin d'établir rapidement le TLS percent un tunnel (reprise de session) ou autoriser l'utilisateur/ordinateur (méthode intérieure de saut pour l'authentification).

Il y a 3 phases pour l'EAP-FAST :

- phase 0 (ravitaillement PAC)
- phase 1 (établissement de tunnel de TLS)
- phase 2 (authentification)

L'EAP-FAST prend en charge la conversation PAC sans et PAC basée sur. PAC basé sur se compose du ravitaillement PAC et de l'authentification PAC basée sur. Le ravitaillement PAC peut être basé sur la session anonyme ou authentifiée de TLS.

PAC

Le PAC est des qualifications de Protected Access générées par le serveur et si au client. Il se compose :

- Clé PAC (valeur secrète aléatoire, utilisée pour dériver le maître et les clés de session de TLS)
- PAC opaque (clé + identité de l'utilisateur PAC - tout chiffrée par la clé principale de serveur d'EAP-FAST)
- Les informations PAC (identité de serveur, temporisateurs TTL)

Le serveur émettant le PAC chiffrera la clé et l'identité PAC utilisant la clé principale de serveur d'EAP-FAST (qu'est à dire PAC opaque) et envoie le PAC entier au client. Il ne fait pas garder/mémoire aucune autre informations (excepté la clé principale qui est identique pour tous les PACs).

Une fois que le PAC opaque est reçu, il est déchiffré utilisant la clé principale de serveur d'EAP-FAST et validé. La clé PAC est utilisée pour dériver le maître de TLS et les clés de session pour TLS abrégé percent un tunnel.

De nouvelles clés principales de serveur d'EAP-FAST sont générées quand la clé principale précédente expire. Dans certains cas, une clé principale peut être retirée.

Il y a quelques types de PAC étant utilisés actuellement :

- Tunnel PAC : utilisé pour l'établissement de tunnel de TLS (sans besoin de certificat de client ou de serveur). Introduit le client de TLS bonjour
- Ordinateur PAC : utilisé pour le TLS percez un tunnel l'établissement et l'autorisation immédiate d'ordinateur. Introduit le client de TLS bonjour
- Autorisation PAC d'utilisateur : utilisé pour l'authentification de l'utilisateur immédiate (méthode intérieure de saut) si autorisé du serveur. Tunnel intérieur envoyé de TLS utilisant la TLV.
- Autorisation PAC d'ordinateur : utilisé pour l'authentification de machine immédiate (méthode intérieure de saut) si autorisé du serveur. Tunnel intérieur envoyé de TLS utilisant la TLV.
- Trustsec PAC : utilisé pour l'autorisation quand exécuter ambient ou stratégie régénèrent.

Tous ces PAC sont habituellement livrés automatiquement dans la phase 0. Certains des PAC (tunnel, ordinateur, Trustsec) peuvent être également livrés manuellement.

Quand des PACs sont générés

- Tunnel PAC : provisioned après une authentification réussie (méthode intérieure) sinon l'a utilisé précédemment.
- Autorisation PAC : provisioned après l'authentification réussie (méthode intérieure) sinon l'a utilisé précédemment.
- Ordinateur PAC : provisioned après l'authentification de machine réussie (méthode intérieure) sinon l'a utilisé précédemment et quand une autorisation PAC n'est pas utilisée. Il provisioned quand le tunnel PAC expire ; cependant, pas quand l'autorisation PAC expire. Il provisioned quand l'Eap-enchaînement est activé ou désactivé.

Remarque:

Chaque ravitaillement PAC exige l'authentification réussie excepté du cas d'utilisation suivant : l'utilisateur autorisé demande l'ordinateur PAC pour un ordinateur qui n'a pas un compte d'AD.

Le tableau suivant récapitule le ravitaillement et la fonctionnalité proactive de mise à jour :

Type PAC	Tunnel v1/v1a/CTS	Ordinateur	Autorisation
Fournissez le PAC sur demande sur le ravitaillement	oui	seulement sur le ravitaillement authentifié	seulement sur le ravitaillement authentifié si le tunnel PAC est demandé également
Fournissez le PAC sur demande sur l'authentification	oui	oui	seulement s'il n'était pas utilisé dans cette authentification
Mise à jour proactive	oui	non	non
En retombant au ravitaillement PAC après l'authentification PAC basée sur défectueuse (par exemple quand le PAC est expiré)	l'anomalie et ne fournissent pas le neuf	l'anomalie et ne fournissent pas le neuf	l'anomalie et ne fournissent pas le neuf
Support ACS 4.x PACs	pour le tunnel PAC v1/v1a	oui	non

Clé principale de serveur d'EAP-FAST ACS 4.x contre ACS 5x et ISE

Il y a une légère différence dans la clé principale manipulant en comparant ACS 4.x et ISE

Caractéristique	ACS 4.1.2	ACS 5.x/ISE
Clé principale	La clé principale a le TTL, peut être en activité, retirée ou expirée	La clé principale est automatiquement générée de la graine à chaque période configurée. La clé principale spécifique est toujours accessible et alors non jamais expirée
Le PAC régénèrent	La mise à jour PAC est envoyée par le serveur quand le PAC est expiré, à moins que la clé principale utilisée pour le cryptage PAC soit expirée	La mise à jour PAC est envoyée par le serveur après la première authentification réussie qui est exécutée dans la période configurable spécifique avant le moment d'expiration PAC.

En d'autres termes, ISE gardera toutes les clés de grand maître et générera un neuf par défaut une fois par semaine. Car la clé principale ne peut pas expirer, seulement le PAC TTL sera validé.

La période de génération de clé principale ISE est configurée de la *gestion - > des configurations - > Protocol - > EAP-FAST - > des configurations d'EAP-FAST*.

Reprise de session

C'est un important composant tenant compte de l'utilisation PAC de tunnel. Il tient compte de la renégociation de tunnel de TLS sans utilisation des Certificats.

Il y a deux types de reprise de session pour l'EAP-FAST : État de serveur basé et sans état (PAC basé).

État de serveur

La méthode basée par TLS standard est basée sur le TLS SessionID caché sur le serveur. Le client envoyant le client de TLS bonjour relie le SessionID afin de reprendre la session. La session est seulement utilisée pour le ravitaillement PAC en utilisant TLS anonyme percent un tunnel :

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l= anonymous	
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l anonymous	
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=30	
10.62.148.109	10.48.17.14	RADIUS	510	Access-Request(1) (id=31, l anonymous	

Length: 138

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 127

▽ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 123

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 9a344ae351082ec6dbaafb8509cf99b4fa664574b6272f876...

Cipher Suites Length: 52

▷ Cipher Suites (26 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

Sans état (PAC basé)

L'autorisation PAC d'utilisateur/ordinateur est utilisée d'enregistrer les états précédents d'authentification et d'autorisation pour le pair.

La reprise de côté client est basée sur RFC 4507. Le serveur n'a pas besoin de ne cacher aucune donnée ; au lieu de cela le client relie le PAC dans l'extension de SessionTicket de client de TLS bonjour. Consécutivement, le PAC est validé par le serveur. Exemple basé sur le tunnel PAC livré au serveur :

	Source	Destination	Protocol	Length	Info	User-Name
23	10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=91, l=259)	anonymous
24	10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=91, l=151)	
25	10.62.148.109	10.48.17.14	RADIUS	666	Access-Request(1) (id=92, l=624)	anonymous
26	10.48.17.14	10.62.148.109	RADIUS	311	Access-Challenge(11) (id=92, l=269)	
27	10.62.148.109	10.48.17.14	RADIUS	437	Access-Request(1) (id=93, l=395)	anonymous
28	10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=93, l=184)	
29	10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=94, l=426)	anonymous
30	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=94, l=216)	
31	10.62.148.109	10.48.17.14	RADIUS	516	Access-Request(1) (id=95, l=474)	anonymous
32	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=95, l=216)	
33	10.62.148.109	10.48.17.14	RADIUS	452	Access-Request(1) (id=96, l=410)	anonymous

Secure Sockets Layer

▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 281

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 277

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 0

Cipher Suites Length: 52

▷ Cipher Suites (26 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

Extensions Length: 184

▼ Extension: SessionTicket TLS

Type: SessionTicket TLS (0x0023)

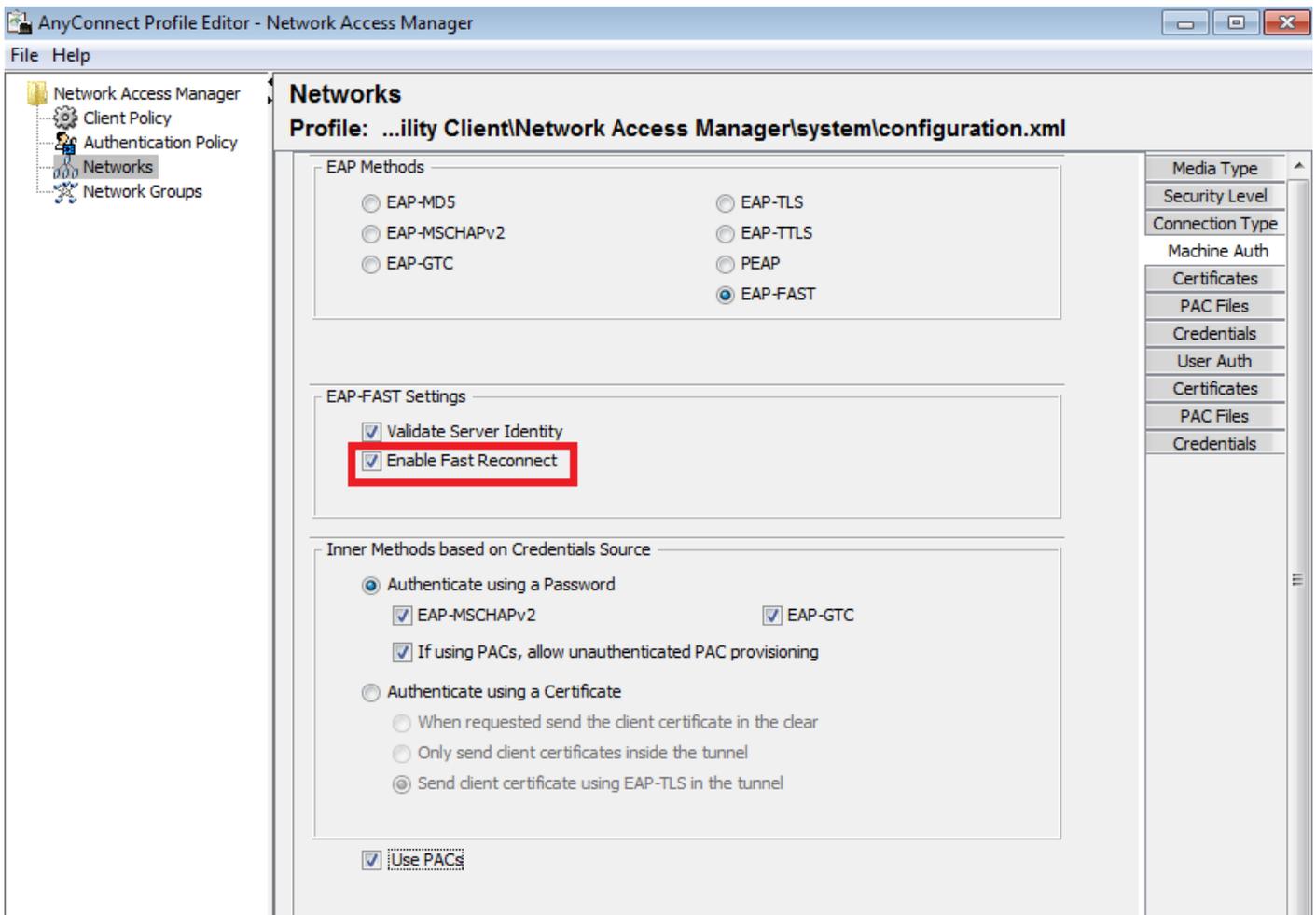
Length: 180

Data (180 bytes)

▷ AVP: l=18 t=Message-Authenticator(80): 0cb2477c076ea96d3ba150245e6291e8

Implémentation d'AnyConnect NAM

Il a activé sur le côté client (AnyConnect NAM) par l'intermédiaire de rapide rebranchent - mais il contrôlait seulement l'utilisation PAC d'autorisation.



La configuration étant désactivée, NAM utilisera toujours le tunnel PAC pour construire le tunnel de TLS (aucun Certificats requis). Cependant, ceci n'emploiera pas l'autorisation PACs afin d'exécuter l'autorisation immédiate d'utilisateur et d'ordinateur. En conséquence, la phase 2 avec la méthode intérieure sera toujours exigée.

ISE a une option d'activer la reprise sans état de session. Et comme sur NAM il est juste pour l'autorisation PAC. L'utilisation PAC de tunnel est contrôlée avec des options la « utilisation PACs ».

Allow EAP-FAST

EAP-FAST Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Use PACs Don't Use PACs

Tunnel PAC Time To Live

Proactive PAC update will occur after % 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

Enable Stateless Session Resume

Authorization PAC Time To Live

Enable EAP Chaining

Preferred EAP Protocol

NAM essaiera d'utiliser des PAC si l'option est activée. Si « n'utilisez pas les PACs » est configuré dans ISE et ISE reçoit un tunnel PAC dans l'extension de TLS que l'erreur suivante sera signalée et une panne d'EAP est retournée :

insérez ici

Dans ISE, il est également nécessaire d'activer la reprise de session basée sur le TLS SessionID (des configurations globales d'EAP-FAST). Il a désactivé par défaut :

EAP FAST Settings

* Authority Identity Info Description

* Master Key Generation Period

Revoke all master keys and PACs

PAC-less Session Resume

Enable PAC-less Session Resume

* PAC-less Session Timeout

Maintenez s'il vous plaît dans l'esprit que seulement un type de reprise de session peut être utilisé. SessionID a basé est utilisé seulement pour des déploiements PAC sans, RFC 4507 basé est utilisé seulement pour des déploiements PAC.

Ravitaillement PAC (phase 0)

Des PACs peuvent automatiquement provisioned dans phase0. La phase 0 se compose :

- Établissement de tunnel de TLS
- Authentification (méthode intérieure)

Des PACs sont livrés après une authentification réussie à l'intérieur du TLS percent un tunnel par l'intermédiaire de l'accusé de réception TLV PAC (et TLV PAC)

Tunnel anonyme de TLS

Pour des déploiements sans infrastructure de PKI, il est possible d'utiliser un tunnel anonyme de TLS. Le tunnel anonyme de TLS sera construit utilisant la suite de chiffrement de Diffie Hellman - sans besoin d'un serveur ou d'un certificat client. Cette approche est à homme enclin dans les attaques moyennes (personnification).

Pour utiliser cette option, NAM exige l'option configurée suivante :

« Si en utilisant des PACs tenez compte du ravitaillement unauthenticated PAC » (qui semble raisonnable seulement pour la méthode intérieure basée sur mot de passe parce que sans infrastructure de PKI il n'est pas possible d'utiliser la méthode intérieure basée sur certificat).

En outre, ISE aura besoin du suivant configuré sous l'authentification permise des protocoles :

« Permettez le ravitaillement anonyme PAC d'intrabande »

Le ravitaillement anonyme PAC d'intrabande est utilisé dans des déploiements NDAC de TrustSec (session d'EAP-FAST négociée entre les périphériques de réseau).

Tunnel authentifié de TLS

C'est l'option sécurisée et recommandée de la plupart. Le TLS que le tunnel est construit a basé sur le certificat de serveur qui est validé par le suppliant. Ceci exige une infrastructure de PKI sur le côté serveur seulement, qui est prié pour ISE (sur NAM qu'il est possible de désactiver l'option « validez l'identité de serveur »).

Pour ISE il y a deux options supplémentaires :

- Allow Anonymous In-Band PAC Provisioning
- Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning

Normalement, après ravitaillement PAC, une Access-anomalie devrait être envoyée forçant le suppliant pour authentifier à nouveau utilisant des PACs. Mais puisque des PACs ont été livrés dans le TLS percez un tunnel avec l'authentification, il est possible pour raccourcir le processus

entier et le retour Access-reçoivent juste après le ravitaillement PAC.

La deuxième option construit le TLS percent un tunnel basé sur le certificat client (ceci exige le déploiement de PKI sur les points finaux). Ceci permet le tunnel de TLS à construire avec l'authentification mutuelle, qui ignore la méthode intérieure et va directement à la phase de ravitaillement PAC. Il est important de faire attention ici - parfois le suppliant présentera un certificat qui n'est pas fait confiance par ISE (destiné à d'autres fins) et la session échouera.

Eap-enchaînement

Permet l'utilisateur et l'authentification de machine à moins d'une session Radius/EAP. De plusieurs méthodes d'EAP peuvent être enchaînées ensemble. Après que la première authentification (typiquement ordinateur) ait terminé avec succès, le serveur enverra une TLV d'Intermédiaire-résultat (tunnel de TLS d'intérieur) indiquant le succès. Cette TLV doit être accompagnée d'une demande Crypto-contraignante TLV. Cryptobinding est utilisé pour montrer que le serveur et le pair ont participé à l'ordre spécifique des authentifications. Le processus de Cryptobinding utilise le matériel de base de la phase 1 et de la phase 2. Supplémentaire, une plus de TLV est reliée : Eap-charge utile - ceci initie la nouvelle session (typiquement pour l'utilisateur). Une fois que le serveur de rayon (ISE) reçoit la réponse Crypto-contraignante TLV et la valide, ce qui suit sera affiché dans le log et la prochaine méthode d'EAP sera essayée (typiquement pour l'authentification de l'utilisateur) :

```
12126 EAP-FAST cryptobinding verification passed
```

Si la validation cryptobinding échoue, la session entière d'EAP échoue. Si une des authentifications dans manqué alors lui est encore bonne - en conséquence, ISE permet à un administrateur pour configurer le multiple enchaînant des résultats basés sur l'état NetworkAccess d'autorisation : EapChainingResult :

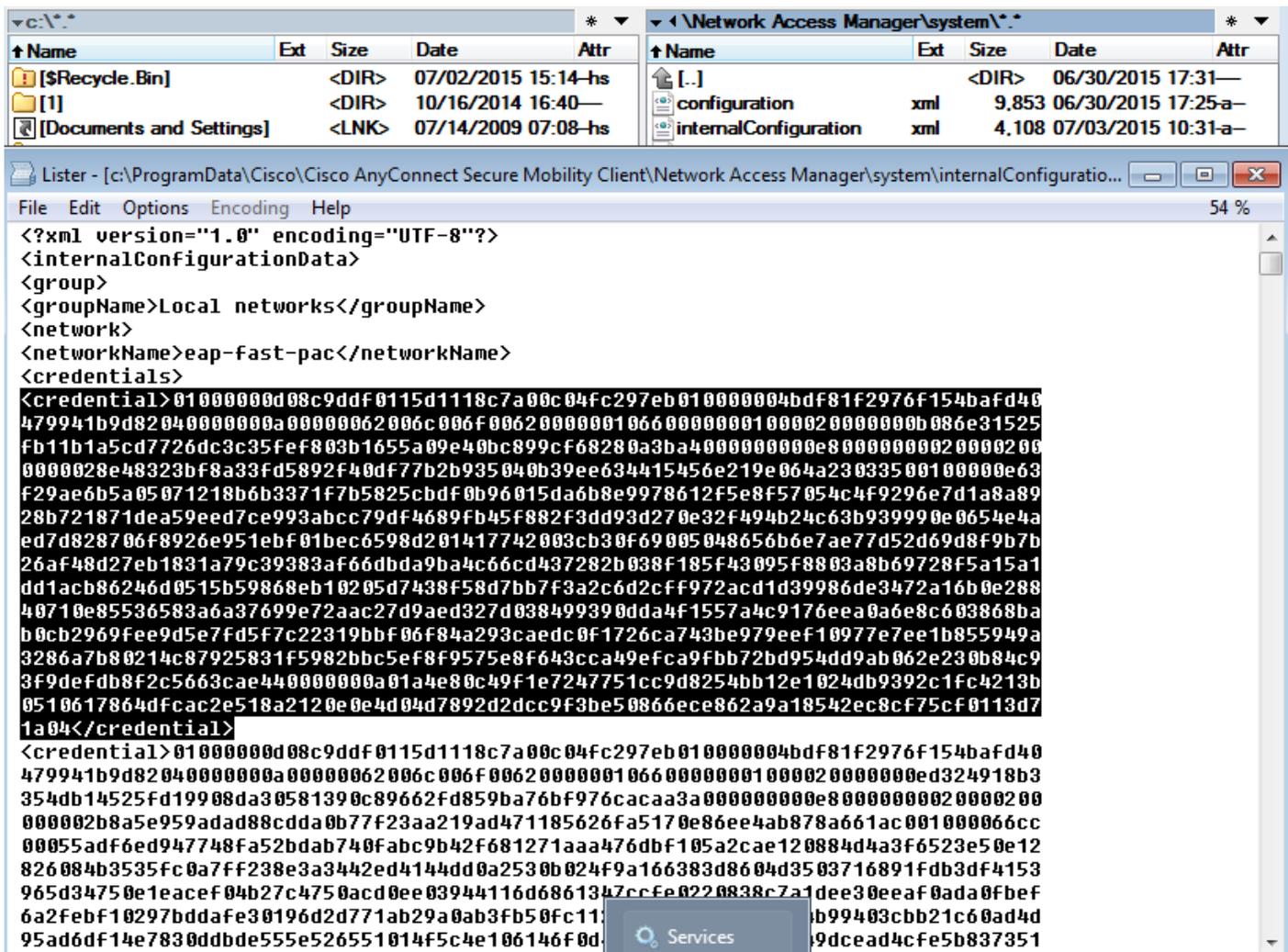
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

L'Eap-enchaînement est activé sur NAM automatiquement quand l'utilisateur et l'authentification de machine d'EAP-FAST est activé.

L'Eap-enchaînement doit être configuré dans ISE.

Là où des fichiers PAC sont enregistrés

Par défaut, le tunnel et l'ordinateur PACs sont enregistrés dans le client de mobilité de C:\ProgramData\Cisco\Cisco AnyConnect \ gestionnaire d'accès au réseau \ système sécurisés \ internalConfiguration.xml dans le <credential> de sections. Ceux sont enregistrés sous la forme chiffrée.

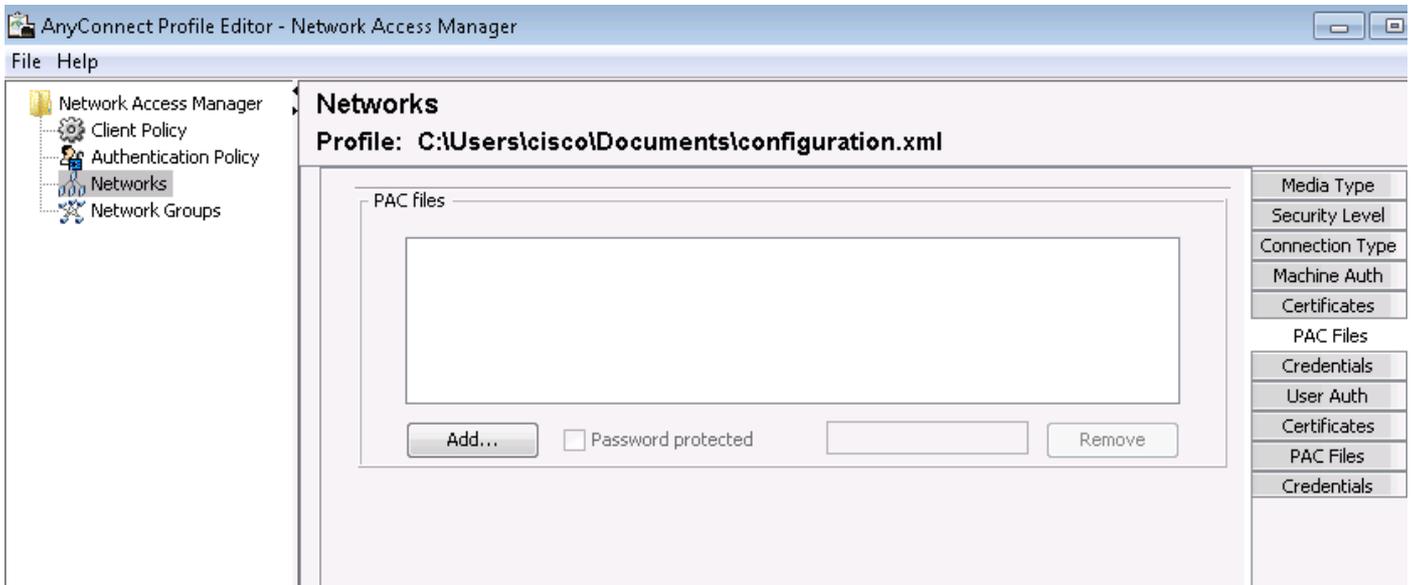


L'autorisation PACs sont enregistrées seulement dans la mémoire et sont enlevées après que réinitialisation ou reprise de service NAM.

Une reprise de service est exigée pour retirer le tunnel ou l'ordinateur PAC.

AnyConnect NAM 3.1 contre 4.0

L'éditeur de profil d'AnyConnect 3.x NAM a permis à l'administrateur pour configurer des PACs manuellement. Cette caractéristique a été retirée de l'éditeur de profil d'AnyConnect 4.x NAM.

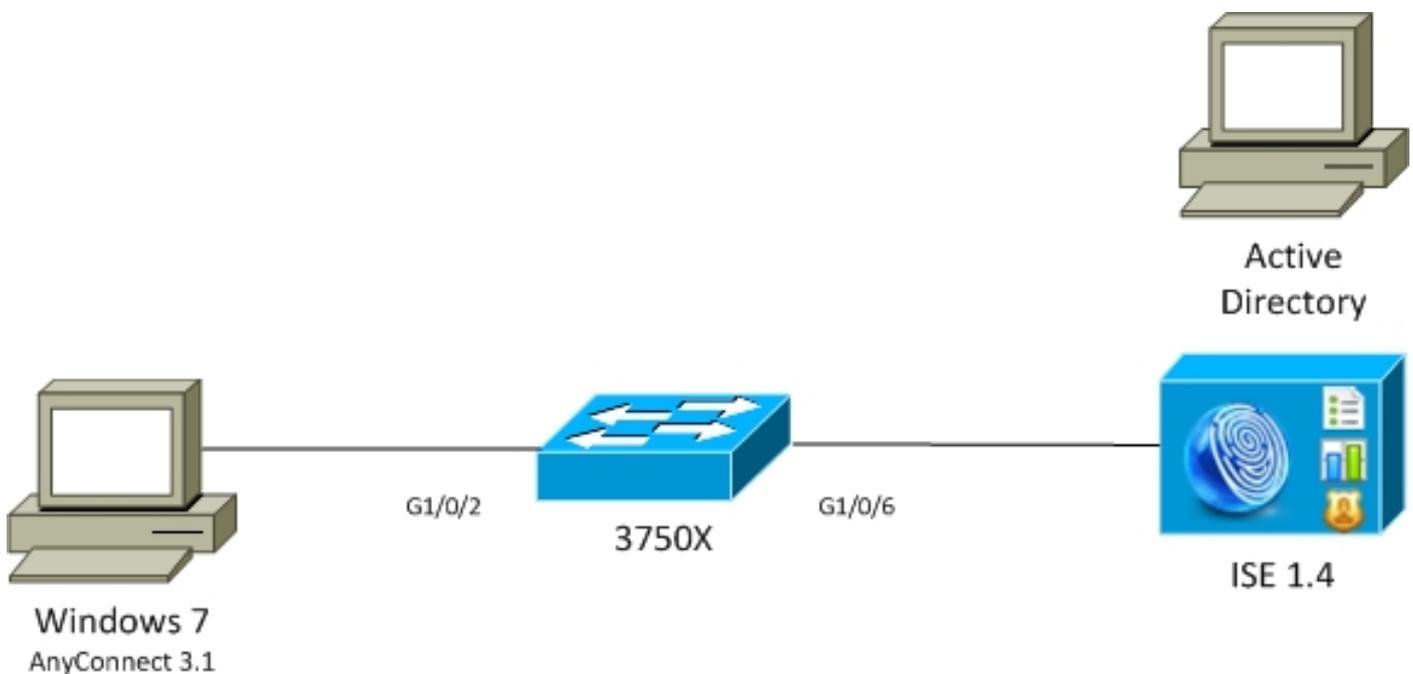


La décision de retirer que la fonctionnalité est basée sur [CSCuf31422](#) et [CSCua13140](#).

Exemples

[Diagramme du réseau](#)

Tous les exemples ont été testés utilisant la topologie du réseau suivante. Le même s'applique également à l'aide de la radio.



EAP-FAST sans EAP enchaînant avec l'utilisateur et l'ordinateur PAC

Par défaut, EAP_chaining est désactivé sur ISE. Cependant, toutes autres options sont activées comprenant l'ordinateur et l'autorisation PACs. Le supplicant a déjà un ordinateur et un tunnel valides PAC. Dans cet écoulement, il y aura deux authentifications distinctes - une pour l'ordinateur et une pour l'utilisateur - avec les logins distincts ISE. Les étapes de canalisation comme connectées par ISE. Première authentification (ordinateur) :

- Le suppliant envoie le client de TLS bonjour avec l'ordinateur PAC.
- Le serveur valide l'ordinateur PAC et construit le tunnel de TLS (aucun Certificats utilisés).
- Le serveur valide l'ordinateur PAC et exécute la consultation de compte dans le Répertoire actif et ignore la méthode intérieure.

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

12800 Extracted first TLS record; TLS handshake started

12174 Received Machine PAC

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded

12132 EAP-FAST built PAC-based tunnel for purpose of authentication

24351 Account validation succeeded

24420 User's Attributes retrieval from Active Directory succeeded - example.com

22037 Authentication Passed

12124 EAP-FAST inner method skipped

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

La deuxième authentification (utilisateur) :

- Le suppliant envoie le client de TLS bonjour avec le tunnel PAC.
- Le serveur valide le PAC et construit le tunnel de TLS (aucun Certificats utilisés).
- Car le suppliant n'a aucune autorisation PAC, la méthode intérieure (EAP-MSCHAP) est utilisée pour l'authentification.

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

12800 Extracted first TLS record; TLS handshake started

12175 Received Tunnel PAC

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded

12132 EAP-FAST built PAC-based tunnel for purpose of authentication

12125 EAP-FAST inner method started

11806 Prepared EAP-Request for inner method proposing **EAP-MSCHAP** with challenge

24402 User authentication against Active Directory succeeded - example.com

22037 Authentication Passed

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

Dans la section de « autres attributs » du rapport détaillé dans ISE, ce qui suit est noté pour l'utilisateur et les authentifications de machine :

EapChainingResult: No chaining

L'EAP-FAST avec l'EAP enchaînant avec le PAC rapide rebranchent

Dans cet écoulement, le suppliant a déjà un tunnel valide PAC avec l'autorisation PACs

d'utilisateur et d'ordinateur :

- Le suppliant envoie le client de TLS bonjour avec le tunnel PAC.
- Le serveur valide le PAC et construit le tunnel de TLS (aucun Certificats utilisés).
- ISE commence l'EAP enchaîner, l'autorisation PACs d'attachés de suppliant pour l'utilisateur et l'ordinateur utilisant la TLV à l'intérieur du TLS percent un tunnel.
- ISE valide l'autorisation PACs (aucune méthode intérieure requise), vérifie que les comptes existent dans le Répertoire actif (aucune authentification supplémentaire), succès de retours.

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
12210  Received User Authorization PAC
12211  Received Machine Authorization PAC

24420  User's Attributes retrieval from Active Directory succeeded - example.com
22037  Authentication Passed

24439  Machine Attributes retrieval from Active Directory succeeded - example.com
22037  Authentication Passed

11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept
```

Dans la section de « autres attributs » du rapport détaillé dans ISE, ce qui suit est noté :

```
EapChainingResult: EAP Chaining
```

Supplémentaire, des qualifications d'utilisateur et d'ordinateur sont incluses dans le même log que vues ci-dessous :

```
EapChainingResult: EAP Chaining
```

EAP-FAST avec l'EAP enchaînant sans PAC

Dans cet écoulement, NAM est configuré pour ne pas utiliser un PAC, ISE est également configuré pour ne pas utiliser le PAC (mais avec l'enchaînement d'EAP)

- Le suppliant envoie le client de TLS bonjour sans tunnel PAC.
- Le serveur répond avec le TLS certificat et des charges utiles de demande de certificat.
- Le suppliant doit faire confiance au certificat de serveur, n'enverra pas n'importe quel certificat client (la charge utile de certificat est zéro), TLS que le tunnel est construit.
- ISE envoient une demande TLV du certificat client à l'intérieur du tunnel de TLS, mais le suppliant ne fait pas (il n'est pas nécessaire de l'avoir afin de continuer).
- EAP de débuts enchaînant pour l'utilisateur, suivre la méthode intérieure avec l'authentification MSCHAPv2.
- Continue l'authentification de machine, suivre la méthode intérieure avec l'authentification

MSCHAPv2.

- Aucun PACs pas provisionned.

```
12102      Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800      Extracted first TLS record; TLS handshake started
12805      Extracted TLS ClientHello message
12806      Prepared TLS ServerHello message
12807      Prepared TLS Certificate message
12809      Prepared TLS CertificateRequest message
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message

12816      TLS handshake succeeded
12207      Client certificate was requested but not received during tunnel establishment. Will
renegotiate and request client certificate inside the tunnel.
12226      Started renegotiated TLS handshake

12104      Extracted EAP-Response containing EAP-FAST challenge-response
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message
12804      Extracted TLS Finished message
12801      Prepared TLS ChangeCipherSpec message
12802      Prepared TLS Finished message
12226      Started renegotiated TLS handshake
12205      Client certificate was requested but not received inside the tunnel. Will continue
with inner method.
12176      EAP-FAST PAC-less full handshake finished successfully

12209      Starting EAP chaining
12218      Selected identity type 'User'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402      User authentication against Active Directory succeeded - example.com
22037      Authentication Passed

12219      Selected identity type 'Machine'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470      Machine authentication against Active Directory is successful - example.com
22037      Authentication Passed

11503      Prepared EAP-Success
11002      Returned RADIUS Access-Accept
```

EAP-FAST avec l'EAP enchaînant l'expiration PAC d'autorisation

Dans cet écoulement, le suppliant a un tunnel valide PAC mais a l'autorisation expirée PACs :

- Le suppliant envoie le client de TLS bonjour avec le tunnel PAC.
- Le serveur valide le PAC et construit le tunnel de TLS (aucun Certificats utilisés).
- ISE commence l'EAP enchaîner, l'autorisation PACs d'attachés de suppliant pour l'utilisateur et l'ordinateur utilisant la TLV à l'intérieur du TLS percent un tunnel.
- Pendant que les PACs sont expirés, la méthode intérieure pour l'utilisateur et l'ordinateur est commencée (EAP-MSCHAP).
- Une fois que les deux authentifications sont réussies, l'utilisateur et l'autorisation PACs

d'ordinateur provisioned.

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
12227  User Authorization PAC has expired - will run inner method
12228  Machine Authorization PAC has expired - will run inner method
12218  Selected identity type 'User'

11806  Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402  User authentication against Active Directory succeeded - example.com
22037  Authentication Passed

12219  Selected identity type 'Machine'

24470  Machine authentication against Active Directory is successful - example.com
22037  Authentication Passed

12171  Successfully finished EAP-FAST user authorization PAC provisioning/update
12179  Successfully finished EAP-FAST machine authorization PAC provisioning/update

11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept
```

L'EAP-FAST avec l'EAP enchaînant le tunnel PAC a expiré

Dans cet écoulement quand aucun tunnel valide PAC n'existe, la pleine négociation de TLS avec la phase intérieure se produit.

- Le suppliant envoie le client de TLS bonjour sans tunnel PAC.
- Le serveur répond avec le TLS certificat et des charges utiles de demande de certificat.
- Le suppliant doit faire confiance au certificat de serveur, n'enverra pas le certificat client (la charge utile de certificat est zéro), tunnel de TLS construit.
- ISE envoie la demande TLV du certificat client à l'intérieur du tunnel de TLS, mais le suppliant ne fait pas (il n'est pas nécessaire de l'avoir afin de continuer).
- EAP de débuts enchaînant pour l'utilisateur, suivre la méthode intérieure avec l'authentification MSCHAPv2.
- Continue l'authentification de machine, suivre la méthode intérieure avec l'authentification MSCHAPv2.
- Provisioned avec succès tous les PACs (activés dans le config ISE).

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
```

12809 Prepared TLS CertificateRequest message
 12105 Prepared EAP-Request with another EAP-FAST challenge
 11006 Returned RADIUS Access-Challenge
 11001 Received RADIUS Access-Request

12816 TLS handshake succeeded
 12207 **Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel.**
 12226 Started renegotiated TLS handshake

 12104 Extracted EAP-Response containing EAP-FAST challenge-response
12811 Extracted TLS Certificate message containing client certificate
 12812 Extracted TLS ClientKeyExchange message
 12804 Extracted TLS Finished message
 12801 Prepared TLS ChangeCipherSpec message
 12802 Prepared TLS Finished message
 12226 Started renegotiated TLS handshake
12205 Client certificate was requested but not received inside the tunnel. Will continue with inner method.
12149 EAP-FAST built authenticated tunnel for purpose of PAC provisioning
 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
12209 Starting EAP chaining
12218 Selected identity type 'User'
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402 User authentication against Active Directory succeeded - example.com
22037 Authentication Passed

12126 EAP-FAST cryptobinding verification passed
 12200 Approved EAP-FAST client Tunnel PAC request
 12202 Approved EAP-FAST client Authorization PAC request
12219 Selected identity type 'Machine'

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470 Machine authentication against Active Directory is successful - example.com
22037 Authentication Passed

12169 Successfully finished EAP-FAST tunnel PAC provisioning/update
12171 Successfully finished EAP-FAST user authorization PAC provisioning/update
12170 Successfully finished EAP-FAST machine PAC provisioning/update
12179 Successfully finished EAP-FAST machine authorization PAC provisioning/update

 11503 Prepared EAP-Success
 11002 Returned RADIUS Access-Accept

L'EAP-FAST avec l'enchaînement d'EAP et le TLS anonyme percent un tunnel le ravitaillement PAC

Dans cet écoulement, ISE et NAM le tunnel qu'anonyme de TLS est configuré pour la demande de ravitaillement PAC de ravitaillement PAC (le TLS authentifié par ISE perce un tunnel pour le ravitaillement PAC est désactivé) ressemble à :

- Le suppliant envoie le client de TLS bonjour sans plusieurs ciphersuites.
- Le serveur répond avec le serveur de TLS bonjour et les chiffrements anonymes de Diffie

Hellman de TLS (par exemple TLS_DH_anon_WITH_AES_128_CBC_SHA).

- Le supplicant le reçoit et le tunnel anonyme de TLS est construit (aucun Certificats permutés).
- EAP de débuts enchaînant pour l'utilisateur, suivre la méthode intérieure avec l'authentification MSCHAPv2.
- Continue l'authentification de machine, suivre la méthode intérieure avec l'authentification MSCHAPv2.
- Puisque le tunnel anonyme de TLS est construit on ne permet pas l'autorisation PACs.
- L'anomalie de rayon est retournée au supplicant de force pour authentifier à nouveau (utilisant le PAC provisioned).

```
12102      Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800      Extracted first TLS record; TLS handshake started
12805      Extracted TLS ClientHello message
12806      Prepared TLS ServerHello message
12808      Prepared TLS ServerKeyExchange message
12810      Prepared TLS ServerDone message

12812      Extracted TLS ClientKeyExchange message
12804      Extracted TLS Finished message
12801      Prepared TLS ChangeCipherSpec message
12802      Prepared TLS Finished message
12816      TLS handshake succeeded
12131      EAP-FAST built anonymous tunnel for purpose of PAC provisioning

12209      Starting EAP chaining
12218      Selected identity type 'User'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402      User authentication against Active Directory succeeded - example.com
22037      Authentication Passed

12162      Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be
provisioned only on authenticated provisioning
12200      Approved EAP-FAST client Tunnel PAC request
12219      Selected identity type 'Machine'

24470      Machine authentication against Active Directory is successful - example.com
22037      Authentication Passed

12162      Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be
provisioned only on authenticated provisioning
12169      Successfully finished EAP-FAST tunnel PAC provisioning/update
12170      Successfully finished EAP-FAST machine PAC provisioning/update

11504      Prepared EAP-Failure
11003      Returned RADIUS Access-Reject
```

Les captures de paquet de Wireshark pour le TLS anonyme percent un tunnel la négociation :

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=190,	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	498	Access-Request(1) (id=191,	anonymous
10.48.17.14	10.62.148.109	RADIUS	793	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	706	Access-Request(1) (id=192,	anonymous
10.48.17.14	10.62.148.109	RADIUS	232	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=193,	anonymous
10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=194,	anonymous
10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=19	

Code: Request (1)

Id: 161

Length: 622

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 74

▽ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 70

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 41aee5db065f48165c56144aa9dccdc93f67167fbae96393...

Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA (0x0034)

Compression Method: null (0)

▽ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange

Content Type: Handshake (22)

EAP-FAST avec l'EAP enchaînant l'authentification de l'utilisateur seulement

Dans cet écoulement, AnyConnect NAM avec l'EAP-FAST et l'utilisateur (EAP-TLS) et l'authentification de machine (EAP-TLS) est configuré. Le PC Windows est amorcé mais des identifiants utilisateurs ne sont pas fournis. Le commutateur initie la session de 802.1x, NAM doit répondre cependant, des identifiants utilisateurs ne sont pas fournis, (aucun accès à la mémoire et au certificat d'utilisateur pourtant) donc. l'authentification de l'utilisateur échouera tandis que l'ordinateur sera réussi - accès au réseau d'état d'authz ISE « : L'utilisateur d'ÉGAUX d'EapChainingResult a manqué et l'ordinateur réussi » est satisfait. Plus tard, des logins d'utilisateur et une authentification différente commenceront, utilisateur et l'ordinateur réussira.

- Le suppliant envoie le client de TLS bonjour avec l'ordinateur PAC.
- Le serveur répond avec le TLS changeant la spécification de chiffrement - le tunnel de TLS est immédiatement construction basée sur ce PAC.
- ISE initie l'EAP enchaînant et demandant l'identité de l'utilisateur.

- Le suppliant fournit l'identité d'ordinateur à la place (utilisateur pas encore prêt), méthode intérieure d'EAP-TLS de finitions.
- ISE demande l'identité de l'utilisateur de nouveau, suppliant ne peut pas la fournir.
- ISE envoie la TLV avec le résultat intermédiaire = la panne (pour l'authentification de l'utilisateur).
- ISE renvoie le message de succès final d'EAP, accès au réseau d'état ISE : L'utilisateur d'ÉGAUX d'EapChainingResult a manqué et l'ordinateur réussi est satisfait.

```

12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12174  Received Machine PAC

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication

12209  Starting EAP chaining
12218  Selected identity type 'User'

12213  Identity type provided by client is not equal to requested type
12215  Client suggested 'Machine' identity type instead

12104  Extracted EAP-Response containing EAP-FAST challenge-response
12523  Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
12809  Prepared TLS CertificateRequest message

12816  TLS handshake succeeded
12509  EAP-TLS full handshake finished successfully

22070  Identity name is taken from certificate attribute
15013  Selected Identity Source - Test-AD
24323  Identity resolution detected single matching account
22037  Authentication Passed

12202  Approved EAP-FAST client Authorization PAC request
12218  Selected identity type 'User'
12213  Identity type provided by client is not equal to requested type
12216  Identity type provided by client was already used for authentication
12967  Sent EAP Intermediate Result TLV indicating failure

12179  Successfully finished EAP-FAST machine authorization PAC provisioning/update
12106  EAP-FAST authentication phase finished successfully
11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept

```

EAP-FAST avec l'enchaînement d'EAP et les paramètres de tunnel anonymes contradictoires de TLS

Dans cet écoulement, ISE est configuré pour le ravitaillement PAC seulement par l'intermédiaire du TLS anonyme perce un tunnel, mais NAM est utilisation TLS authentifié perce un tunnel, le

suivant est enregistré par ISE :

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12814  Prepared TLS Alert message
12817  TLS handshake failed
12121  Client didn't provide suitable ciphers for anonymous PAC-provisioning

11504  Prepared EAP-Failure
11003  Returned RADIUS Access-Reject
```

Ceci se produit quand NAM essaye de construire TLS authentifié parce un tunnel avec lui est des chiffrements speciphic de TLS - et ceux ne sont pas reçus par ISE qui est configuré pour le tunnel anonyme de TLS (recevant des chiffrements CAD seulement)

Dépannez

ISE

Pour les logs détaillés, le Délai d'exécution-AAA met au point devrait être activé sur le noeud correspondant RPC. Sont ci-dessous quelques logs d'exemple de prrt-server.log :

Génération PAC d'ordinateur :

```
DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Using IID from PAC request for machine,EapFastTlv.cpp:1234

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Adding PAC of type=Machine Authorization,EapFastProtocol.cpp:3610

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: Generating Pac, Issued PAC type=Machine Authorization with expiration time: Fri Jul 3 10:38:30 2015
```

Approbation de demande PAC :

```
INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,user=host/mgarcarz-pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request approved for PAC type - Requested PAC type=Machine,EapFastProtocol.cpp:955

INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,user=host/mgarcarz-pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request approved for PAC type - Requested PAC type=Machine Authorization,EapFastProtocol.cpp:955
```

Validation PAC :

```
DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-
```

```
ise14/223983918/29243,CPMSessionID=0A3E946D0000FE5131F9D26,user=anonymous,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC is valid,EapFastProtocol.cpp:3403
```

```
Eap,2015-07-03 09:34:39,208,DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-ise14/223983918/29243,CPMSessionID=0A3E946D0000FE5131F9D26,user=anonymous,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC accepted,EapFastProtocol.cpp:3430
```

Exemple de résumé réussi pour la génération PAC :

```
DEBUG,0x7fd5331fd700,cntx=0001162749,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,user=cisco,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Conversation summary: Provisioning. Authenticated. Inner method succeeded. Inner method succeeded. Generated PAC of type Tunnel V1A. Generated PAC of type User Authorization. Generated PAC of type Machine. Generated PAC of type Machine Authorization. Success
```

Exemple de résumé réussi pour la validation PAC :

```
DEBUG,0x7fd5330fc700,cntx=0001162503,sesn=mgarcarz-ise14/223983918/29243,CPMSessionID=0A3E946D0000FE5131F9D26,user=host/mgarcarz-pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Conversation summary: Authentication. PAC type Tunnel V1A. PAC is valid.Skip inner method. Skip inner method. Success
```

AnyConnect NAM

Les logs de DART de NAM fournissent les détails suivants :

L'exemple pour Eap-enchaîner non la session, authentification de machine sans rapide rebranchent :

```
EAP: Identity requested
Auth[eap-fast-pac:machine-auth]: Performing full authentication
Auth[eap-fast-pac:machine-auth]: Disabling fast reauthentication
```

Exemple de la consultation PAC d'autorisation (authentification de machine pour la session non de Eap-enchaînement) :

```
Looking for matching pac with iid: host/ADMIN-PC2
Requested machine pac was sen
```

Tous les états de méthode intérieure (pour MSCHAP) peuvent être vérifiés des logs ci-dessous :

```
EAP (0) EAP-MSCHAP-V2: State: 0 (eap_auth_mschapv2_c.c 731
EAP (0) EAP-MSCHAP-V2: State: 2 (eap_auth_mschapv2_c.c 731
EAP (0) EAP-MSCHAP-V2: State: 1 (eap_auth_mschapv2_c.c 731
EAP (0) EAP-MSCHAP-V2: State: 4 (eap_auth_mschapv2_c.c 73
```

NAM permet la configuration de la fonctionnalité de journalisation étendue qui capturera tous les paquets d'EAP et les archivera dans le fichier de pcap. C'est particulièrement utile pour la fonctionnalité de Start Before Logon (des paquets d'EAP sont capturés même pour les authentifications qui se produisent avant que connexion d'utilisateur). Pour le lancement de caractéristique demandez à votre ingénieur TAC.

Références

- [Guide de l'administrateur de Client à mobilité sécurisé Cisco AnyConnect, configuration](#)

[d'EAP-FAST de version 4.0](#)

- [Guide de l'administrateur de Logiciel Cisco Identity Services Engine, recommandations d'EAP-FAST de version 1.4](#)
- [Guides de conception de Logiciel Cisco Identity Services Engine](#)
- [Déployer l'EAP enchaînant avec AnyConnect NAM et Cisco ISE](#)
- [Support et documentation techniques - Cisco Systems](#)