AnyConnect NAM と ISE での EAP-FAST およびチェーンの実装について

目次

概要

この記事では、Cisco AnyConnect Network Access Manager（NAM）および Identity Services Engine（ISE）での EAP-FAST 実装に関する詳細を説明します。 さらに、特定の機能がどのように連動するかを説明し、一般的な使用法および例を記載します。

前提条件

要件

次の項目に関する知識が推奨されます。

- EAP フレームワークおよび EAP-FAST 手法の基礎知識
- Identity Services Engine（ISE）の基礎知識
- AnyConnect NAM およびプロファイル エディタの基礎知識
- 802.1x サービス向け Cisco Catalyst 設定の基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco AnyConnect Secure Mobility Client リリース 3.1 および 4.0 がインストールされた Windows 7
- Cisco Catalyst 3750X スイッチ、ソフトウェア 15.2.1 以降
- Cisco ISE、リリース 1.4

理論

フェーズ

EAP-FAST とは、サプリカントとサーバの相互認証を可能にする柔軟な EAP 方式です。 これは EAP-PEAP と似ていますが、通常はクライアントを使用する必要がなく、サーバ証明書さえも不要です。 EAP-FAST の利点の 1 つは、複数の内部方式を使用して複数の認証を連鎖させ、暗号法によって 1 つにバインドできることです（EAP チェーン）。 シスコの実装では、ユーザ認証とマシン認証にこれを使用します。

EAP-FAST は、Protected Access Credential（PAC）を利用することによって、迅速に TLS トンネルを確立したり（セッション再開）、短時間でユーザ/マシンを認証したり（認証で内部方式をスキップ）することができます。

EAP-FAST には以下の 3 つのフェーズがあります。

- フェーズ 0（PAC プロビジョニング）
- フェーズ 1（TLS トンネルの確立）
- フェーズ 2（認証）

EAP-FAST では、PAC なしメッセージ交換と PAC ベースのメッセージ交換の両方をサポートしています。 PAC ベースのメッセージ交換では、PAC プロビジョニングと PAC ベースの認証が行われます。 PAC プロビジョニングは、匿名 TLS セッションまたは認証済み TLS セッションに基づいて行うことができます。

PAC

PAC（Protected Access Credential）は、サーバによって生成されてクライアントに提供されます。 この構成は次のとおりです。

- PAC キー（TLS マスター キーとセッション キーを派生させるために使用する、ランダム シークレット値）
- PAC opaque（PAC キー とユーザ ID の組み合わせ。すべて EAP-FAST サーバ マスター キーで暗号化されます）
- PAC 情報（サーバ ID、TTL タイマー）

PAC を発行するサーバが、EAP-FAST サーバ マスター キーを使用して PAC キーと ID を暗号化し（つまり、PAC opaque）、PAC 全体をクライアントに送信します。 その他の情報（すべての PAC で同一のマスター キーを除く）は一切、保持/保管しません。

受信された PAC opaque は、EAP-FAST サーバ マスター キーを使用して復号化され、検証されます。 簡易 TLS トンネルの TLS マスター キーとセッション キーを派生させるには、PAC キーが使用されます。

前の EAP-FAST サーバ マスター キーの有効期限が切れると、新しいマスター キーが生成されます。 場合によっては、マスター キーを失効させることもできます。

現在使用されている PAC には、次のタイプがあります。

- トンネル PAC： TLS トンネルを確立するために使用されます（クライアント証明書やサーバ証明書は必要ありません）。 TLS Client Hello に含めて送信されます。
- マシン PAC： TLS トンネルを確立して即時にマシン認証を行うために使用されます。 TLS Client Hello に含めて送信されます。
- ユーザ認証 PAC： サーバが許可する場合、内部方式をスキップして即時にユーザ認証を行うために使用されます。 TLV を使用して TLS トンネル内で送信されます。
- マシン認証 PAC： サーバが許可する場合、内部方式をスキップして即時にマシン認証を行うために使用されます。 TLV を使用して TLS トンネル内で送信されます。
- TrustSec PAC： 環境またはポリシーを更新する際の認証に使用されます。

通常、上記の PAC はすべて、フェーズ 0 で自動的に配信されます。 一部の PAC（トンネル、マシン、Trustsec）は、手動で配信することもできます。

PAC の生成時の動作

- トンネル PAC： 前に使用されていない場合、認証（内部方式）の成功後にプロビジョニングされます。
- 認証 PAC： 前に使用されていない場合、認証（内部方式）の成功後にプロビジョニングされます。
- マシン PAC： 前に使用されていない場合、認証 PAC が使用されていなければ、マシンの認証（内部方式）の成功後にプロビジョニングされます。 これは、トンネル PAC が有効期限切れになった時点でプロビジョニングされます。 認証 PAC が有効期限切れになった時点ではありません。 また、EAP チェーンが有効または無効になると、プロビジョニングされます。

注：

各 PAC をプロビジョニングするには認証が成功しなければなりませんが、例外として、 認可されたユーザが AD アカウントを持たないマシンのマシン PAC を要求する場合は認証が必要ありません。

以下の表に、プロビジョニングおよび予防的更新機能を要約します。

PAC のタイプ	トンネル v1/v1a/CTS	マシン	許可

プロビジョニング時に要求に応じて PAC を提供	yes	認証されたプロビジョニング時にのみ提供	認証されたプロビジョニング時に、トンネル PAC が要求されている場合に提供
認証時に要求に応じて PAC を提供	yes	yes	この認証で使用された場合にのみ提供
予防的更新	yes	いいえ	いいえ
PAC ベースの認証が失敗した後（PAC の有効期限が切れている場合など）、PAC プロビジョニングにフォールバックした場合の処置	拒否して新しい PAC を提供しない	拒否して新しい PAC を提供しない	拒否して新しい PAC を提供しない
ACS 4.x PAC のサポート	トンネル PAC v1/v1a でサポート	yes	いいえ

EAP-FAST サーバ マスター キー ACS 4.x と ACS 5x + ISE の相違点

ACS 4.x と ISE を比較すると、マスター キーの処理で若干の違いがあります。

機能	ACS 4.1.2	ACS 5.x / ISE
マスター キー	マスター キーには TTL があり、アクティブ、廃止、または期限切れの状態があります	設定された間隔で、マスター キーがシードから自動的に生成されます。 特定のマスター キーが常時アクセス可能になり、その有効期限が切れることはありません。
PAC 更新	PAC の暗号化に使用されたマスター キーが失効していない限り、PAC の有効期限が切れると、サーバから PAC 更新が送信されます。	PAC の期限が切れる前に、設定された特定の期間中に行われた最初の認証が成功すると、サーバから PAC 更新が送信されます。

つまり、ISE はすべての古いマスタ キーを保持し、デフォルトで 1 週間ごとに新しいマスター キーを生成します。 マスター キーの有効期限は切れることがないため、PAC の TTL のみが検証されます。

ISE のマスター キー生成期間は、[Administration] -> [Settings] -> [Protocol] -> [EAP-FAST] -> [EAP-FAST Settings] で設定されます。

セッション再開

これは、トンネル PAC を使用可能にする重要なコンポーネントです。 セッション再開により、証明書を使用せずに TLS トンネルの再ネゴシエーションをすることが可能になります。

EAP-FAST には、2 つのタイプのセッション再開があります。 それは、サーバの状態に基づくセッション再開とステートレス (PAC ベースの) セッション再開です。

サーバの状態

標準的な TLS ベースの方式は、サーバ上でキャッシュされた TLS SessionID に基づきます。 クライアントはセッションを再開するために、SessionID を追加した TLS Client Hello を送信します。 匿名 TLS トンネルを使用する場合、セッションは PAC のプロビジョニングにのみ使用されます。

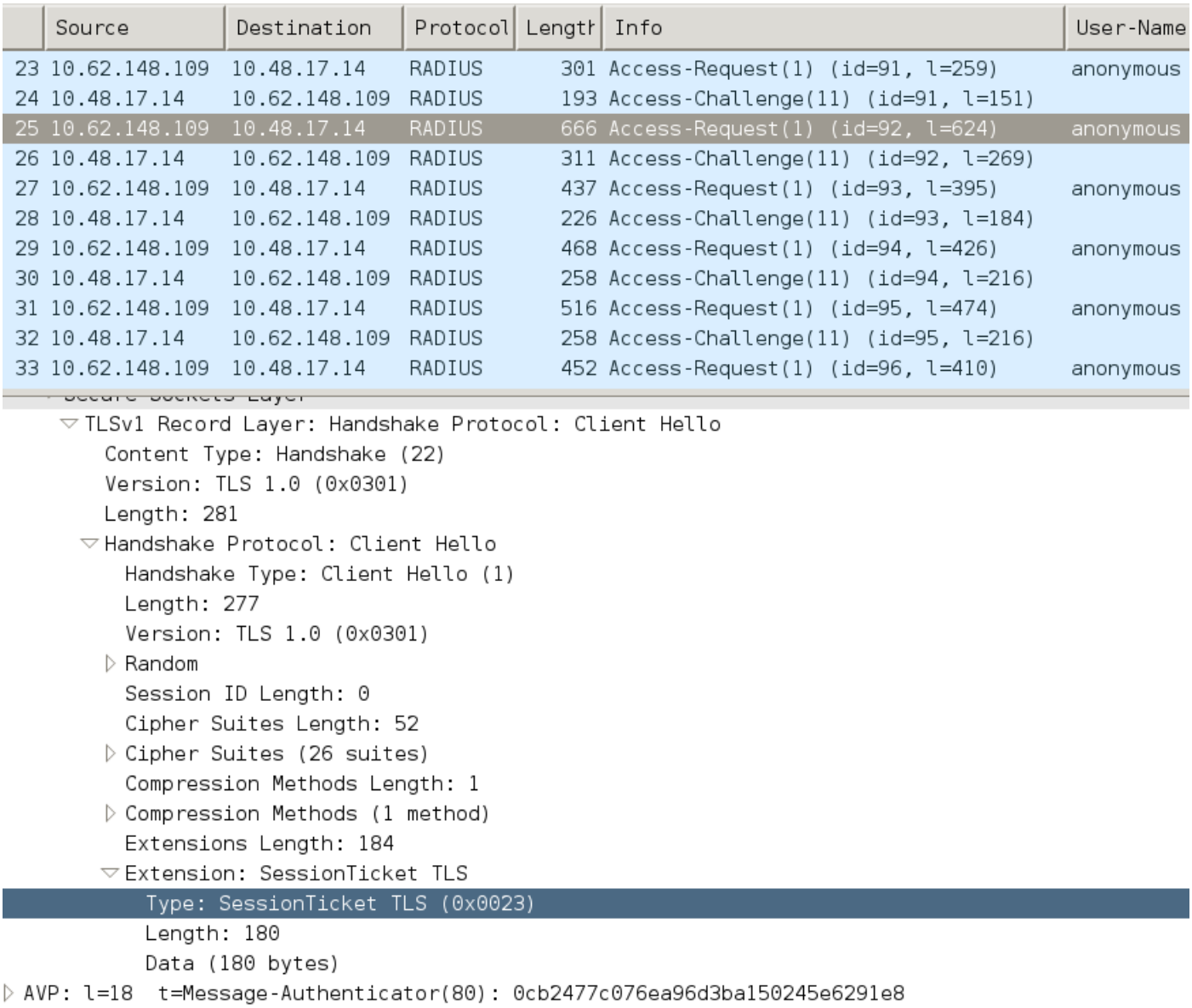
Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l=	anonymous
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	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: 9a344ae351082ec6dbafb8509cf99b4fa664574b6272f876...
        Cipher Suites Length: 52
      ▷ Cipher Suites (26 suites)
        Compression Methods Length: 1
      ▷ Compression Methods (1 method)
```

ステートレス (PAC ベース)

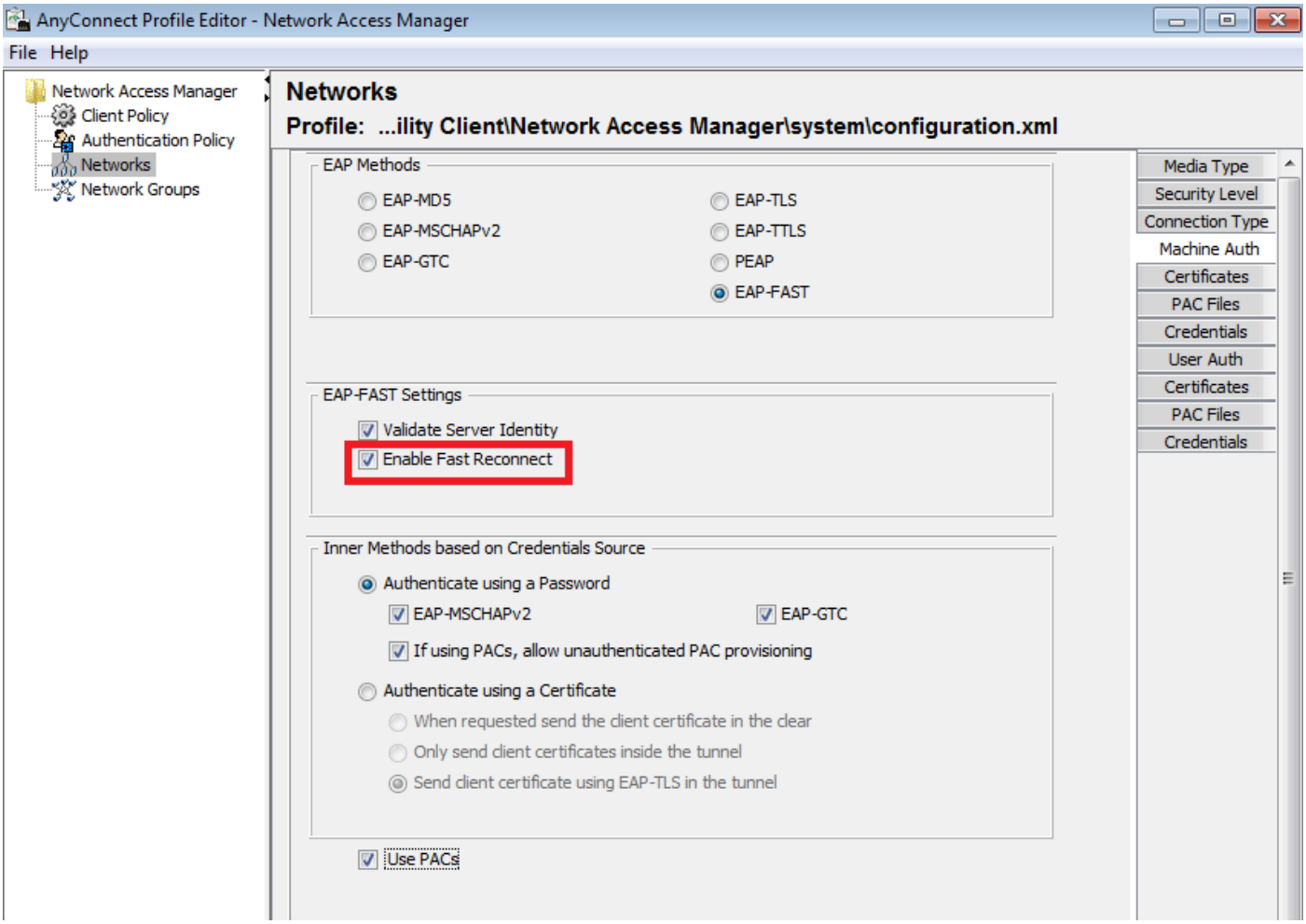
ユーザ/マシン認証 PAC を使用して、ピアの前の認証および許可の状態が保管されます。

クライアント側の再開は、RFC 4507 に基づいています。 サーバがデータをキャッシュする必要はありません。 代わりに、クライアントは TLS Client Hello SessionTicket 拡張に PAC を追加します。 その PAC が、サーバによって検証されます。 サーバに配信されるトンネル PAC に基づく例を示します。



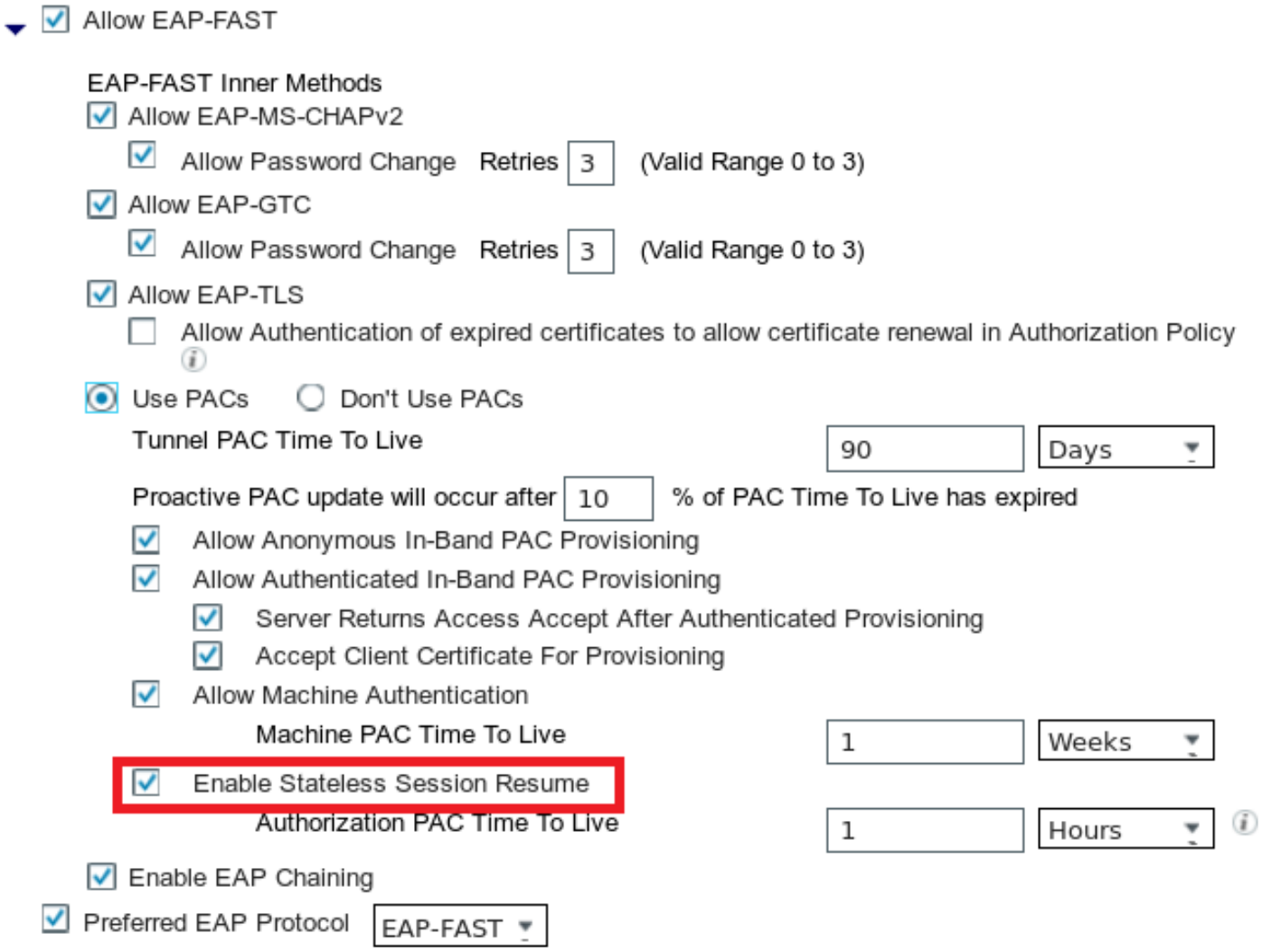
AnyConnect NAM の実装

これは Fast Reconnect によってクライアント側（AnyConnect NAM）で有効化されますが、認証 PAC の使用を制御するためだけに使用されます。



この設定が無効になっていても、NAM はトンネル PAC を使用して TLS トンネルを確立します（証明書は必要ありません）。 ただし、認証 PAC を使用した即時のユーザ認証およびマシン認証は行われません。 そのため、常にフェーズ 2 で内部方式が必要になります。

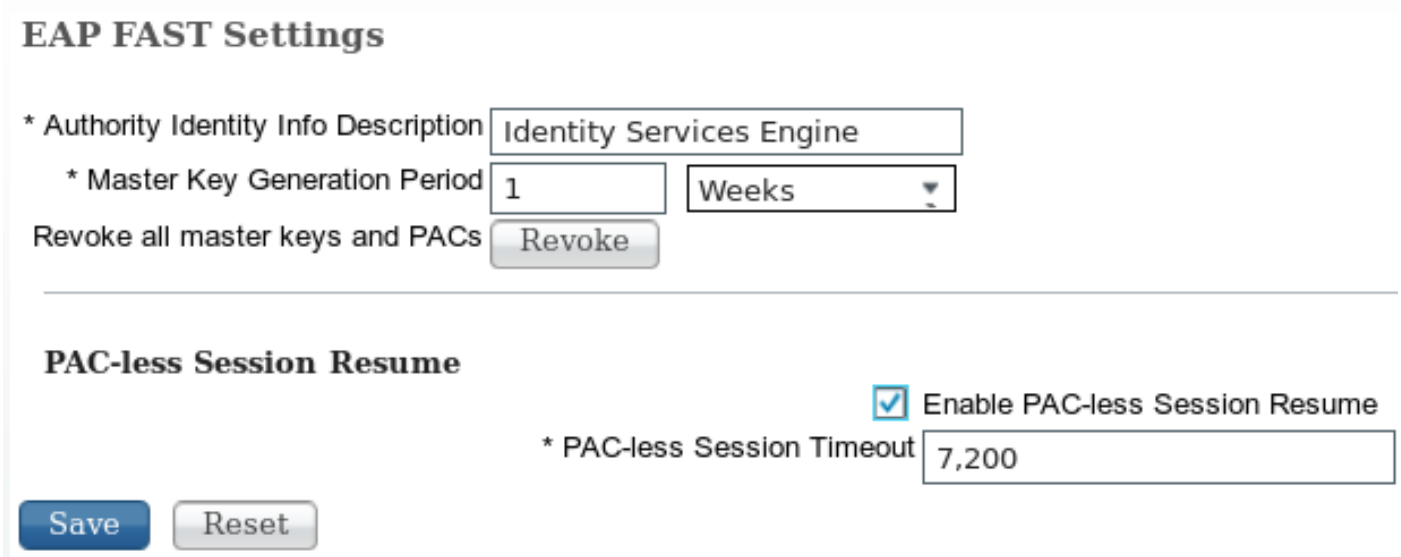
ISE には、ステートレス セッション再開を有効にするオプションがあります。 NAM での場合と同じく、このオプションは認証 PAC 用です。 トンネル PAC の使用は、[Use PACs] のオプションで制御されます。



このオプションが有効になっている場合、NAM は PAC の試用を試みます。 ISE に [Don't Use PACs] が設定されている場合、ISE が TLS 拡張でトンネル PAC を受信すると、以下のエラーが報告されて、EAP 失敗が返されます。

ここに挿入

ISE では、TLS SessionID に基づくセッション再開を有効にする必要もあります（グローバル EAP-FAST 設定を使用）。 これは、デフォルトでは無効になっています。



使用できるセッション再開は 1 つのタイプに限られることに注意してください。 SessionID ベースのセッション再開は、PAC を使用しない導入のみに使用され、RFC 4507 ベースのセッション再開は PAC 導入のみに使用されます。

PAC プロビジョニング (フェーズ 0)

PAC は、フェーズ 0 で自動的にプロビジョニングできます。 フェーズ 0 では以下の処理が行われます。

- TLS トンネルの確立
- 認証 (内部方式)

PAC は、TLS トンネル内での PAC TLV (および PAC TLV 確認応答) による認証成功後に配信されます。

匿名 TLS トンネル

PKI インフラストラクチャを使用しいない配置では、匿名 TLS トンネルを使用することができます。 匿名 TLS トンネルは、Diffie Hellman 暗号スイートを使用して確立されます (サーバ証明書やクライアント証明書は必要ありません)。 このアプローチは中間者攻撃 (偽装) にさらされやすい傾向があります。

このオプションを使用する場合、NAM には以下のオプションの設定が必要です。

[If using PACs allow for unauthenticated PAC provisioning] (PKI インフラストラクチャを使用しない場合、証明書ベースの内部方式を使用することは不可能であるため、このオプションはパスワード ベースの内部方式にのみ意味があります)。

また、ISE には認証許可プロトコルで以下の設定も必要になります。

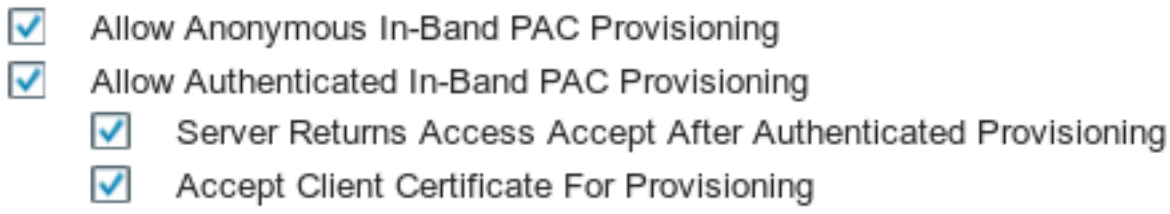
[Allow Anonymous In-band PAC Provisioning]

TrustSec NDAC 導入環境で匿名インバンド PAC プロビジョニングが使用されます (ネットワーク デバイス間で EAP-FAST セッションがネゴシエートされます)。

認証済み TLS トンネル

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たサーバ証明書に基づいて確立されます。 このオプションでは、ISE に必要な PKI インフラストラクチャはサーバ側にのみ必要です (NAM では、オプション [Validate Server Identity] を無効にできます)。

ISE には、以下のようにさらに 2 つのオプションがあります。



通常、PAC プロビジョニングの完了後は、Access-Reject を送信してサプリカントに PAC を使用して強制的に認証させる必要があります。 とはいえ、PAC は認証によって TLS トンネルで配

信されているため、このプロセス全体を短縮して、PAC プロビジョニング直後に Access-Accept を返すことができます。

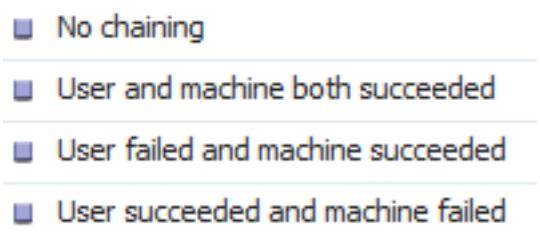
2 つ目のオプションは、クライアント証明書に基づいて TLS トンネルを確立します（この場合、エンドポイントに PKI を導入する必要があります）。 このオプションを使用すると、相互認証で TLS トンネルを確立できるため、内部方式を省略して直接 PAC プロビジョニング フェーズに進むことができます。 ここで注意しなければならない点として、サプリカントが ISE で信頼されていない（他の目的のために用意された）証明書を提示する場合があります。その場合、セッションは失敗します。

EAP チェーン

1 回の Radius/EAP セッションでユーザとマシンの認証が可能になります。 複数の EAP 方式をつなげることができます。 最初の認証（通常はマシン）が正常に完了すると、サーバは成功を示す中間結果 TLV を送信します（TLS トンネル内）。 この TLV には暗号バインディング TLS 要求が伴っている必要があります。 暗号バインディングは、特定の認証シーケンスにサーバとピアの両方が参加していることを証明するために使用されます。 暗号バインディング プロセスでは、フェーズ 1 とフェーズ 2 でキーを生成した要素が使用されます。 さらに、もう 1 つの TLV が追加されます。 それは、新しいセッション（通常はユーザ用）を開始する EAP ペイロードです。 RADIUS サーバ（ISE）が暗号バインディングの TLV 応答を受信してそれを検証すると、以下のメッセージがログに記録され、次の EAP 方式（通常はユーザ認証が対象）が試行されます。

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

暗号バインディング検証が失敗すると、EAP セッション全体が失敗します。 認証のうちの 1 つが失敗した場合でも、その認証は有効です。したがって、ISE では、管理者が複数のチェーン結果を設定できます。これは、認証状態 [NetworkAccess: EapChainingResult] に基づいて設定できます。

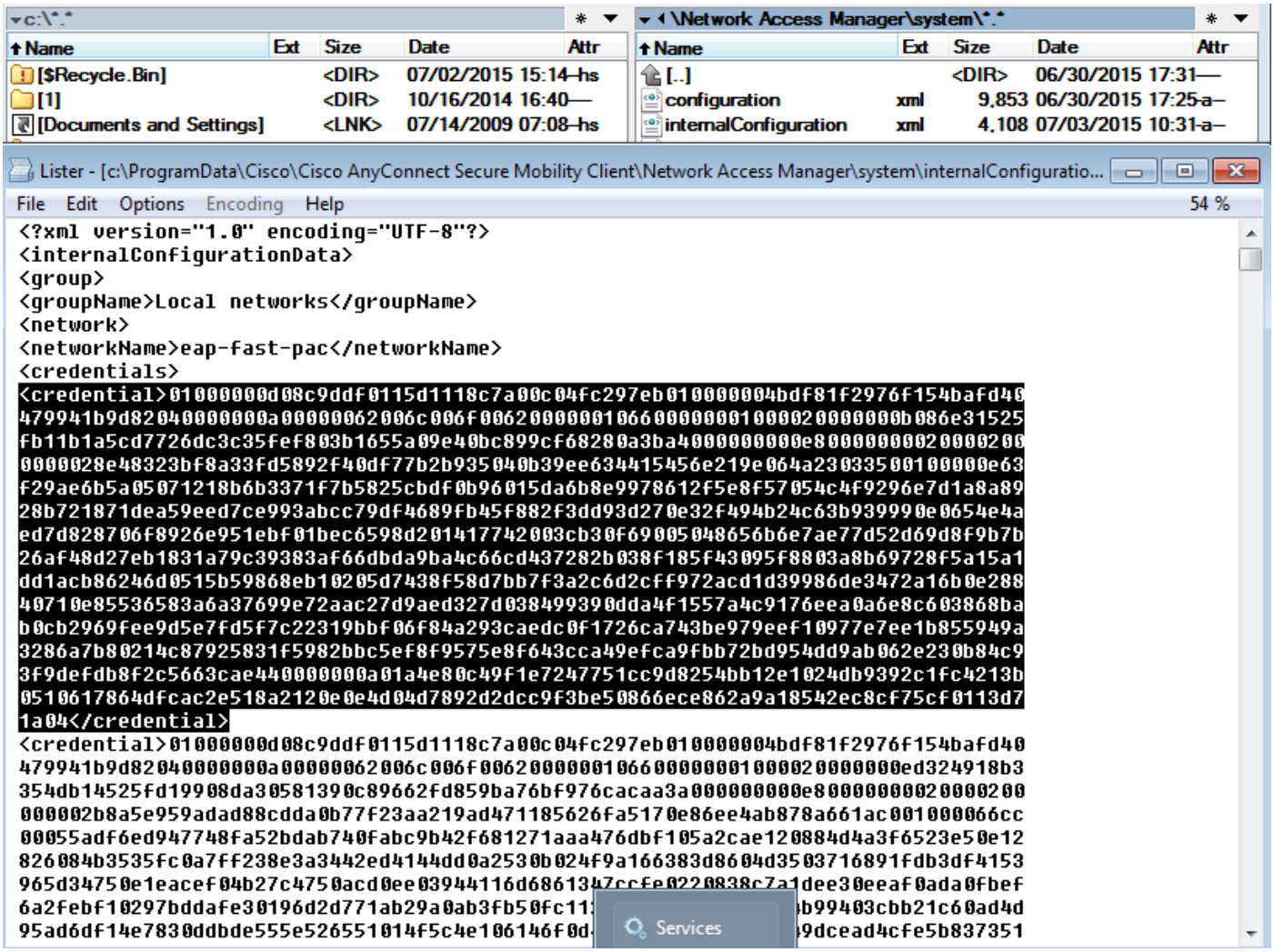


EAP チェーンは、EAP-FAST ユーザおよびマシンの認証が有効になると、NAM で自動的に有効になります。

EAP チェーンは ISE で設定する必要があります。

PAC ファイルの格納場所

トンネルとマシンの PAC が格納されるデフォルトの場所は、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml の <credential> セクションです。 これらは暗号化形式で保管されます。

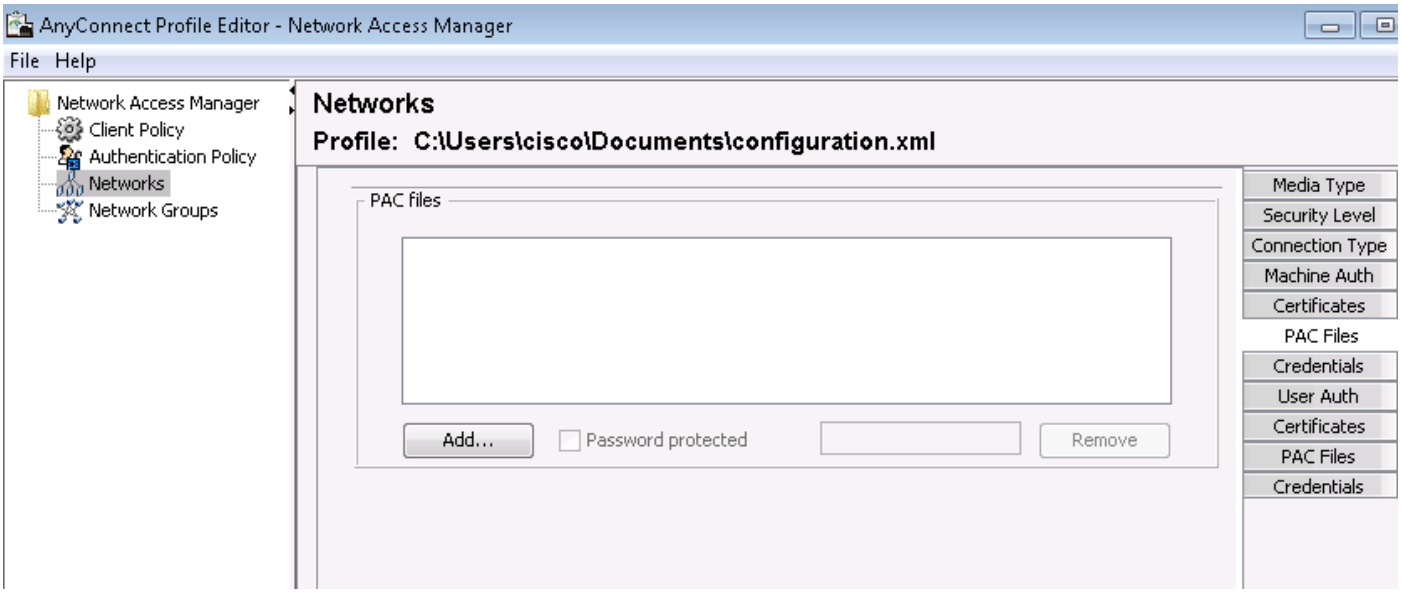


認証 PAC はメモリにのみ保管され、リブートまたは NAM サービスの再起動が行われると削除されます。

トンネルまたはマシンの PAC を削除するには、サービスを再起動する必要があります。

AnyConnect NAM 3.1 と 4.0 の相違点

AnyConnect 3.x NAM プロファイル エディタでは、管理者が PAC を手動で設定できます。 この機能は、AnyConnect 4.x NAM プロファイル エディタからは削除されています。

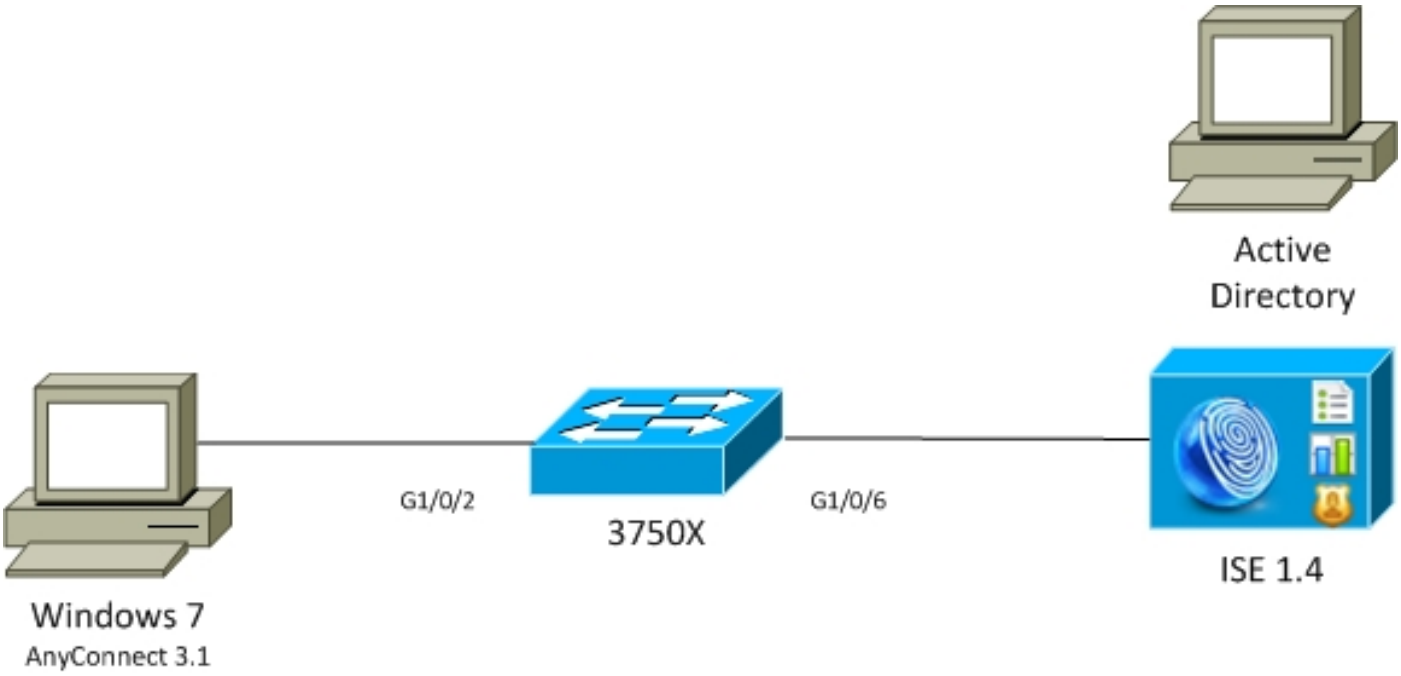


この機能を削除するかどうかの決定は、CSCuf31422 および CSCua13140 に基づきます。

例

ネットワーク図

すべての例は、次のネットワーク トポロジを使用してテストされました。 これはワイヤレスを使用する場合にも適用されます。



ユーザおよびマシン PAC を使用した EAP チェーンなしの EAP-Fast

デフォルトでは、EAP チェーンは ISE で無効になっています。 ただし、マシン PAC と認証 PAC を含め、他のすべてのオプションは有効になっています。 サプリカントには、すでに有効なマシン PAC とトンネル PAC があります。 このフローでは、マシン認証とユーザ認証の 2 つの認証が個別に行われ、ISE 上のそれぞれ異なるログに記録されます。 ISE がログに記録する主なステップは以下のとおりです。 最初の認証（マシン）：

- サプリカントがマシン PAC を含めた TLS Client Hello を送信します。
- サーバがマシン PAC を検証し、TLS トンネルを確立します（証明書は使用されません）。
- サーバがマシン PAC を検証し、Active Directory でアカウント ルックアップを行い、内部方式をスキップします。

```
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
```

2 回目の認証（ユーザ）：

- サプリカントがトンネル PAC を含めた TLS Client Hello を送信します。
- サーバが PAC を検証し、TLS トンネルを確立します（証明書は使用されません）。
- サプリカントには認証 PAC がないため、内部方式（EAP-MSCHAP）が認証に使用されます。

```
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
```

ISE の詳細レポートの [Other Attributes] セクションに、ユーザ認証とマシン認証に共通して以下の結果が示されます。

```
EapChainingResult: No chaining
```

PAC 高速再接続を使用した EAP チェーンによる EAP-Fast

このフローでは、サプリカントにはすでに有効なトンネル PAC に加え、ユーザとマシンの認証

PAC があります。

- サプリカントがトンネル PAC を含めた TLS Client Hello を送信します。
- サーバが PAC を検証し、TLS トンネルを確立します（証明書は使用されません）。
- ISE が EAP チェーンを開始し、サプリカントが TLS トンネル内で TLV を使用してユーザおよびマシンの認証 PAC を追加します。
- ISE が認証 PAC を検証し（内部方式は不要）、アカウントが Active Directory 内に存在することを確認して（追加の認証なし）、成功メッセージを返します。

```
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
```

ISE の詳細レポートの [Other Attributes] セクションに、以下の結果が示されます。

```
EapChainingResult: EAP Chaining
```

さらに、ユーザ クレデンシャルとマシン クレデンシャルの両方が、以下のように同じログ内に記録されます。

```
EapChainingResult: EAP Chaining
```

PAC を使用しない EAP チェーンによる EAP-Fast

このフローでは、NAM が PAC を使用しないように設定され、ISE も PAC を使用しないように設定されます（ただし、EAP チェーンは使用します）。

- サプリカントがトンネル PAC なしで TLS Client Hello を送信します。
- サーバが TLS 証明書および証明書要求のペイロードで応答します。
- サプリカントはサーバ証明書を信頼する必要があります。サプリカントがクライアント証明書を送信することなく（証明書ペイロードがゼロ）、TLS トンネルが確立されます。
- ISE がクライアント証明書の ＴＬＶ 要求を ＴＬＳ トンネル内で送信しますが、サプリカントはその要求を送信しません（これは続行するために必要ではありません）。
- MSCHAPv2 認証で内部方式を使用して、ユーザに対して EAP チェーンを開始します。
- MSCHAPv2 認証で内部方式を使用してマシン認証を続行します。
- PAC はプロビジョニングされません。

```
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
```

認証 PAC が失効している場合の EAP チェーンによる EAP-Fast

このフローでは、サプリカントに有効なトンネル PAC がありますが、認証 PAC の有効期限は切れています。

- サプリカントがトンネル PAC を含めた TLS Client Hello を送信します。
- サーバが PAC を検証し、TLS トンネルを確立します（証明書は使用されません）。
- ISE が EAP チェーンを開始し、サプリカントが TLS トンネル内で TLV を使用してユーザおよびマシンの認証 PAC を追加します。
- PAC は失効しているため、ユーザとマシンの両方に対して内部方式（EAP-MSCHAP）が開始されます。
- 両方の認証が成功すると、ユーザとマシン両方の認証 PAC がプロビジョニングされます。

```
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
```

トンネル PAC が失効している場合の EAP チェーンによる EAP-Fast

このフローでは、有効なトンネル PAC がないため、内部方式を使用した完全な TLS ネゴシエーション フェーズが発生します。

- サプリカントがトンネル PAC なしで TLS Client Hello を送信します。
- サーバが TLS 証明書および証明書要求のペイロードで応答します。
- サプリカントはサーバ証明書を信頼する必要があります。サプリカントがクライアント証明書を送信することなく（証明書ペイロードがゼロ）、TLS トンネルが確立されます。
- ISE がクライアント証明書の ＴＬＶ 要求を ＴＬＳ トンネル内で送信しますが、サプリカントはその要求を送信しません（これは続行するために必要ではありません）。
- MSCHAPv2 認証で内部方式を使用して、ユーザに対して EAP チェーンを開始します。
- MSCHAPv2 認証で内部方式を使用してマシン認証を続行します。
- すべての PAC が正常にプロビジョニングされます（ISE 設定で有効になっています）。

```
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
```

EAP チェーンおよび匿名 TLS トンネル PAC プロビジョニングによる EAP-Fast

このフローでは、ISE と NAM の匿名 TLS トンネルが PAC プロビジョニング用に設定されます（PAC プロビジョニングに対して、ISE の認証済み TLS トンネルは無効になります）。PAC プロビジョニング要求は、次のようになります。

- サプリカントが複数の暗号スイートなしで TLS Client Hello を送信します。
- サーバが TLS Server Hello および TLS 匿名 Diffie Hellman 暗号スイート（たとえば、TLS_DH_anon_WITH_AES_128_CBC_SHA）で応答します。
- サプリカントがそれを受け入れ、匿名 TLS トンネルが確立されます（証明書は交換されません）。
- MSCHAPv2 認証で内部方式を使用して、ユーザに対して EAP チェーンを開始します。
- MSCHAPv2 認証で内部方式を使用してマシン認証を続行します。
- 匿名 TLS トンネルが確立されているため、認証 PAC は許可されません。
- サプリカントに再認証（プロビジョニング済み PAC を使用）を強制するために、Radius

Reject が返されます。

```
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
```

匿名 TLS トンネル ネゴシエーションの Wireshark パケット キャプチャは以下のとおりです。

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)
```

ユーザ認証のみの EAP チェーンによる EAP-Fast

このフローでは、AnyConnect NAM に EAP-FAST とユーザ認証（EAP-TLS）およびマシン認証（EAP-TLS）が設定されています。 Windows PC は起動されますが、ユーザ クレデンシャルは提供されません。 スイッチが 802.1x セッションを開始し、NAM が応答しなければなりませんが、ユーザ クレデンシャルが提供されていないため（ユーザ ストアおよび証明書にはまだアクセスできません）、 ユーザ認証は失敗する一方、マシン認証は成功します。つまり、ISE 認証状態 [Network Access: EapChainingResult EQUALS User failed and machine succeeded] に該当します。 その後、ユーザがログインして別の認証が開始すると、ユーザとマシンの両方の認証が成功します。

- サプリカントがマシン PAC を含めた TLS Client Hello を送信します。
- サーバが TLS Change Cipher Spec で応答します。その PAC に基づいて、即時に TLS トンネルが確立されます。
- ISE が EAP チェーンを開始し、ユーザ ID を尋ねます。

- サプリカントは代わりにマシン ID を提供し（ユーザはまだ準備ができていないので）、EAP-TLS 内部方式を終了します。
- ISE がユーザ ID を再度尋ねますが、サプリカントはそれを提供できません。
- ISE が中間結果を失敗（ユーザ認証が失敗）とした TVL を送信します。
- ISE が最終的に EAP 成功メッセージを返します。つまり、ISE 状態 [Network Access: EapChainingResult EQUALS User failed and machine succeeded] に該当します。

```
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 チェーンおよび一貫性のない匿名 TLS トンネル設定による EAP-Fast

このフローでは、ISE は PAC プロビジョニングに匿名 TLS トンネルだけを使用するように設定されている一方、NAM は認証済み TLS トンネルを使用しています。この場合、ISE は以下のように口グに記録します。

```
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
```

この事態が発生するのは、NAM が特定の TLS 暗号を使用して認証済み TLS トンネルを確立しようとする場合です。匿名 TLS トンネルを使用するように設定されている ISE は、これらの TLS 暗号を受け入れません（受け入れるのは DH 暗号のみです）。

トラブルシューティング

ISE

詳細な口グを記録するには、対応する PSN ノードで Runtime-AAA デバッグを有効にする必要があります。 以下に、prrt-server.log に記録される内容の例を示します。

マシン PAC の生成：

```
DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,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=0A3E946D00000FE5131F9D26,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=0A3E946D00000FE5131F9D26,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
```

PAC 要求の承認：

```
INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,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=0A3E946D00000FE5131F9D26,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
```

PAC の検証：

```
DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-
ise14/223983918/29243,CPMSessionID=0A3E946D00000FE5131F9D26,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=0A3E946D00000FE5131F9D26,user=anonymous,CallingStationID=00-
50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC accepted,EapFastProtocol.cpp:3430
```

PAC 生成が成功した場合の要約情報の例：

```
DEBUG,0x7fd5331fd700,cntx=0001162749,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,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
```

PAC 検証が成功した場合の要約情報の例：

```
DEBUG,0x7fd5330fc700,cntx=0001162503,sesn=mgarcarz-
ise14/223983918/29243,CPMSessionID=0A3E946D00000FE5131F9D26,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

NAM による DART ログに、以下の詳細が記録されます。

非 EAP チェーン セッションにおける、高速再接続を使用しないマシン認証の例：

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

承認 PAC ルックアップの例（非 EAP チェーン セッションでのマシン認証）：

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

内部方式（MSCHAP）のすべての状態は、以下のログで検証できます。

```
 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 では、拡張ロギング機能を設定して、すべての EAP パケットをキャプチャし、pcap ファイルに保存することができます。 この機能は、特にログイン前の起動機能に役立ちます（ユーザ ログイン前に行われる認証でも、EAP パケットがキャプチャされます）。 この機能をアクティブにするには、TAC エンジニアに連絡してください。

参考資料

- Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 4.0 の EAP-FAST の設定
- Cisco Identity Services Engine 管理者ガイド リリース 1.4 の EAP-FAST に関する推奨事項
- Cisco Identity Services Engine 設計ガイド
- AnyConnect NAM と Cisco ISE を使用した EAP の連結の導入
- テクニカル サポートとドキュメント – Cisco Systems