瞭解AnyConnect NAM和ISE上的EAP-FAST和連結實施

目錄

簡介

本文解釋有關在Cisco AnyConnect網路訪問管理器(NAM)和身份服務引擎(ISE)上實施EAP-FAST的詳細資訊。 它進一步說明了特定功能如何協同工作，並提供了典型的使用案例和示例。

必要條件

需求

思科建議您瞭解以下主題：

- EAP框架和EAP-FAST方法的基本知識
- 身份服務引擎(ISE)基礎知識
- AnyConnect NAM和配置檔案編輯器基礎知識
- 適用於802.1x服務的Cisco Catalyst配置基礎知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- Windows 7，帶Cisco AnyConnect安全移動客戶端，版本3.1和4.0
- Cisco Catalyst 3750X交換器（含軟體15.2.1及更新版本）
- Cisco ISE版本1.4

理論

階段

EAP-FAST是一種靈活的EAP方法，允許請求方和伺服器的相互身份驗證。它類似於EAP-PEAP，但通常不需要使用客戶端甚至伺服器證書。EAP-FAST的一個優勢是能夠連結多個身份驗證（使用多個內部方法）並以密碼方式將其繫結在一起（EAP連結）。 Cisco實現將此用於使用者和電腦身份驗證。

EAP-FAST利用受保護訪問憑證(PAC)來快速建立TLS通道（作業階段恢復）或授權使用者/機器（跳過內部驗證方法）。

EAP-FAST有三個階段：

- 第0階段（PAC調配）
- 第1階段（建立TLS隧道）
- 第2階段（身份驗證）

EAP-FAST支援無PAC和基於PAC的會話。基於PAC的身份驗證包括PAC調配和PAC身份驗證。PAC設定可以基於匿名或已驗證的TLS會話。

PAC

PAC是由伺服器生成的受保護訪問憑據提供給客戶端。它包括：

- PAC金鑰（隨機金鑰值，用於派生TLS主金鑰和會話金鑰）
- PAC不透明（PAC金鑰+使用者身份 — 全部由EAP-FAST伺服器主金鑰加密）
- PAC資訊（伺服器標識、TTL計時器）

發出PAC的伺服器將使用EAP-FAST伺服器主金鑰（即PAC不透明）加密PAC金鑰和身份，並將整個PAC傳送到客戶端。它不會保留/儲存任何其他資訊（除了所有PAC相同的主金鑰）。

收到PAC不透明後，使用EAP-FAST伺服器主金鑰解密並驗證。PAC金鑰用於派生精簡型TLS隧道的TLS主金鑰和會話金鑰。

當以前的主金鑰過期時，將生成新的EAP-FAST伺服器主金鑰。 在某些情況下，可以撤銷主金鑰。

目前使用幾種型別的PAC:

- 隧道PAC：用於TLS隧道建立（無需客戶端或伺服器證書）。 在TLS客戶端Hello中傳送
- 電腦PAC:用於TLS隧道建立和即時電腦授權。在TLS客戶端Hello中傳送
- 使用者授權PAC:用於即時使用者身份驗證（跳過內部方法）（如果伺服器允許）。使用TLV在TLS隧道內傳送。
- 電腦授權PAC:用於立即機器身份驗證（跳過內部方法）（如果伺服器允許）。使用TLV在TLS隧道內傳送。
- Trustsec PAC:用於執行環境或策略刷新時的授權。

所有PAC通常在0階段自動交付。某些PAC（隧道、電腦、Trustsec）也可以手動交付。

生成PAC時

- 通道PAC:在成功進行身份驗證（內部方法）之後調配（如果以前未使用）。
- 授權PAC:如果以前未使用過成功身份驗證（內部方法），則會在身份驗證成功後進行調配。
- 電腦PAC:如果以前未使用過並且未使用授權PAC，則在電腦身份驗證成功後調配（內部方法）。將在隧道PAC到期時進行設定；但是，不會在授權PAC到期時進行設定。當啟用或禁用EAP連結時，將調配該資源。

附註：

每個PAC調配都需要成功身份驗證，以下使用情形除外：授權使用者為沒有AD帳戶的電腦請求電腦PAC。

下表彙總了預配和主動更新功能：

PAC型別	通道v1/v1a/CTS	機器	Authorization
在調配時根據請求提供PAC	是	僅在經過身份驗證的調配上	僅在經過身份驗證的調，並且如果也請求隧道
在身份驗證時根據請求提供PAC	是	是	僅當未在此身份驗證中它時
主動更新	是	否	否
在基於PAC的身份驗證失敗後回到PAC調配時（例如PAC過期時）	拒絕且不提供新版本	拒絕且不提供新版本	拒絕且不提供新版本
支援ACS 4.x PAC	適用於通道PAC v1/v1a	是	否

EAP-FAST伺服器主金鑰ACS 4.x與ACS 5x和ISE

比較ACS 4.x和ISE時，主金鑰處理略有不同

功能	ACS 4.1.2	ACS 5.x/ISE
主金鑰	主金鑰具有TTL，可以處於活動狀態、已停用或已過期	主金鑰會在每個配置的時間段從種子自動生成。特定主金鑰始終可訪問，並且永不過期
PAC刷新	當PAC過期時，伺服器會	PAC更新由伺服器在PAC到

傳送PAC更新，除非用於PAC加密的主金鑰已過期	期之前的特定可配置時間段內第一次成功進行身份驗證後傳送。

換句話說，ISE將保留所有舊主金鑰，並預設每週生成一個新主金鑰。由於主金鑰無法過期，因此將僅驗證PAC TTL。

ISE主金鑰生成期通過*管理 — >設定 — >協定 — > EAP-FAST -> EAP-FAST設定進行配置。*

會話恢復

這是允許使用隧道PAC的一個重要元件。它允許在不使用證書的情況下進行TLS隧道重新協商。

EAP-FAST有兩種會話恢復型別：基於伺服器狀態和無狀態（基於PAC）。

伺服器狀態

基於標準TLS的方法基於伺服器上快取的TLS SessionID。傳送TLS客戶端Hello的客戶端將附加SessionID以恢復會話。該會話僅在使用匿名TLS隧道時用於PAC調配：

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)
```

無狀態（基於PAC）

使用者/機器授權PAC用於儲存對等體的先前身份驗證和授權狀態。

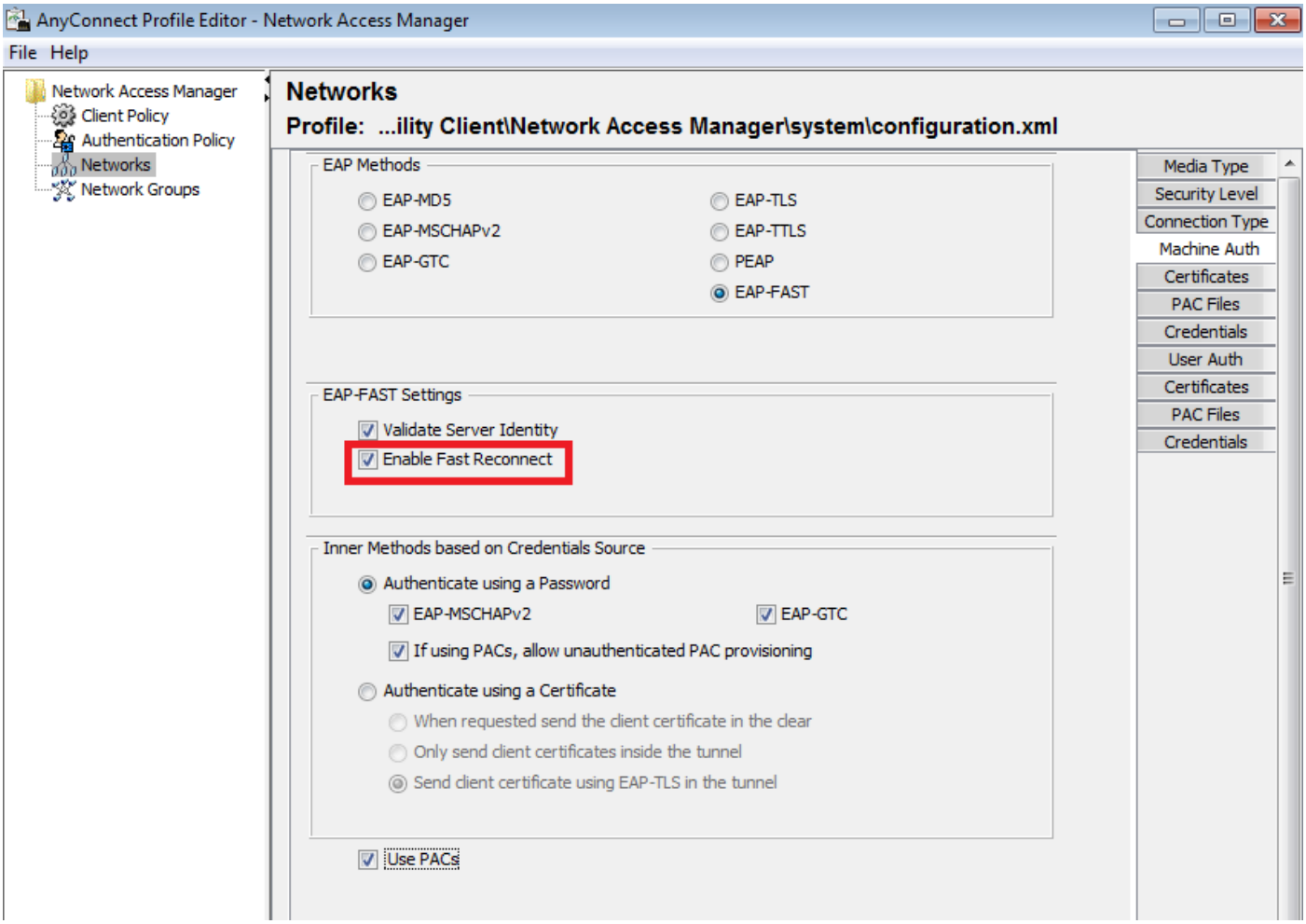
客戶端恢復基於RFC 4507。伺服器不需要快取任何資料；相反，客戶端在TLS客戶端Hello會話票證擴展中附加PAC。然後，伺服器會驗證PAC。 基於傳送到伺服器的隧道PAC的示例：

	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

```
▽ 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
```

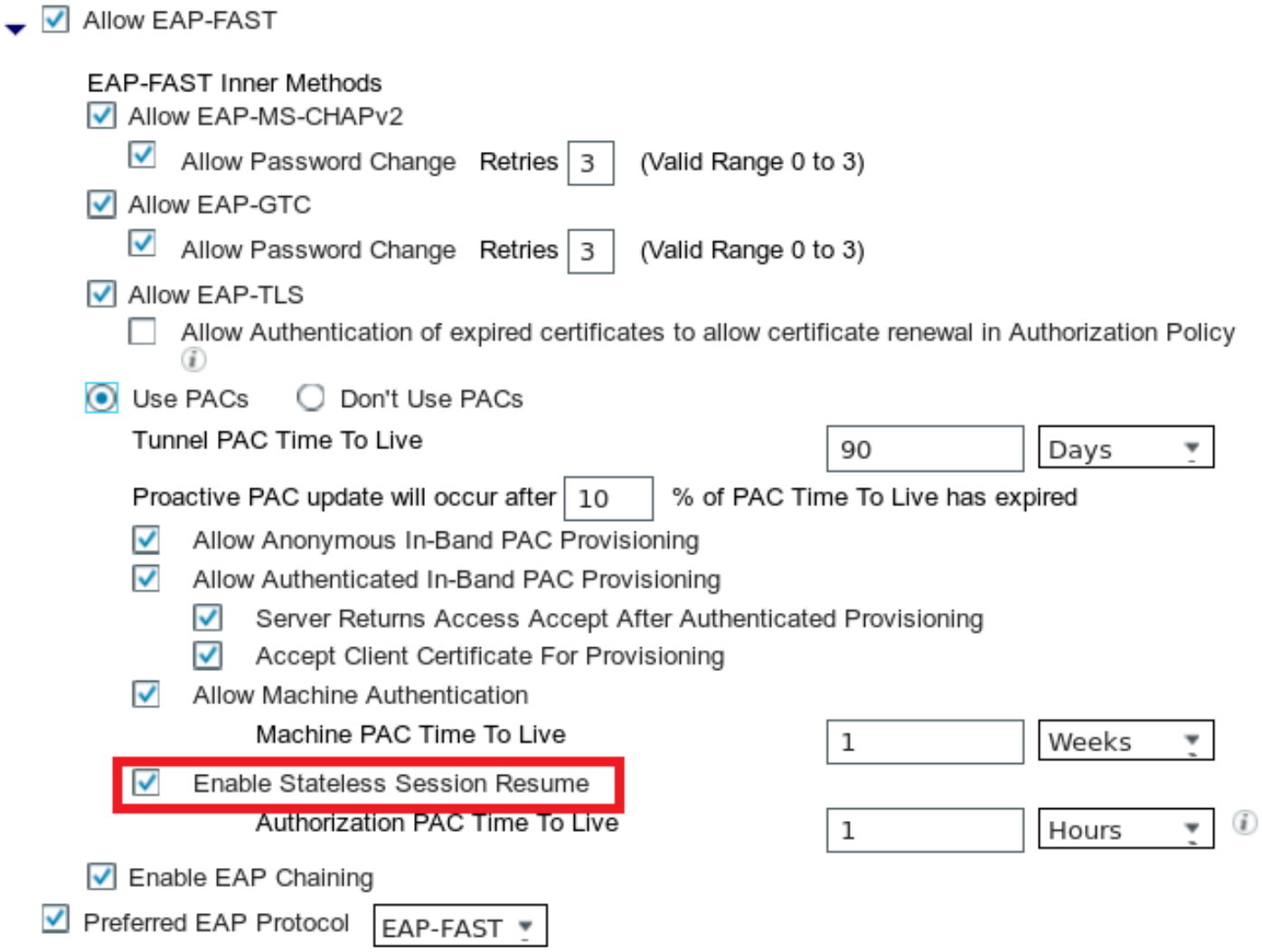
AnyConnect NAM實施

它通過快速重新連線在客戶端(AnyConnect NAM)上啟用，但僅用於控制授權PAC使用。



禁用設定後，NAM仍將使用隧道PAC來構建TLS隧道（無需證書）。 但是，這不會使用授權PAC來執行即時使用者和機器授權。因此，總是需要具有內部方法的階段2。

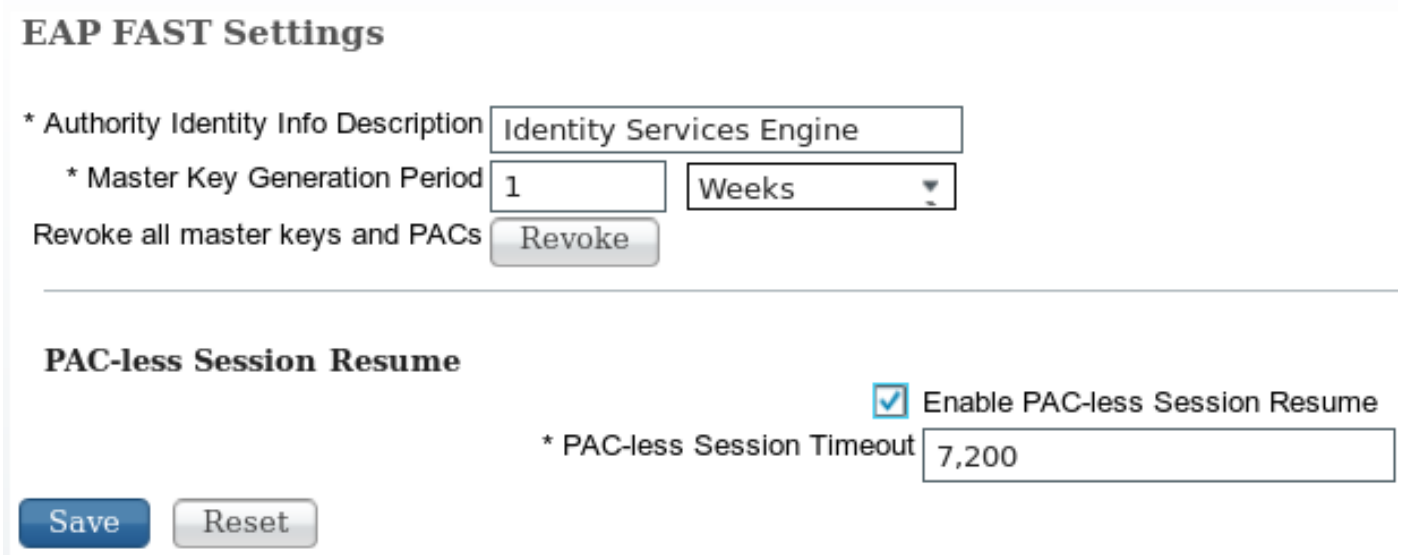
ISE可以選擇啟用無狀態會話恢復。對於NAM，它僅用於授權PAC。通道PAC使用通過「使用PAC」選項進行控制。



如果啟用了此選項，NAM將嘗試使用PAC。如果在ISE中配置了「不使用PAC」並且ISE在TLS擴展中收到隧道PAC，將報告以下錯誤並返回EAP故障：

插入此處

在ISE中，還需要啟用基於TLS SessionID的會話恢復（從全域性EAP-FAST設定）。 預設情況下禁用：



請記住，只能使用一種型別的會話恢復。基於SessionID的部署僅用於無PAC部署，基於RFC

4507的部署僅用於PAC部署。

PAC調配（第0階段）

PAC可以在階段0中自動調配。階段0包括：

- TLS隧道建立
- 身份驗證（內部方法）

在通過PAC TLV（和PAC TLV確認）在TLS隧道內成功進行身份驗證後，會傳送PAC

匿名TLS隧道

對於沒有PKI基礎設施的部署，可以使用匿名TLS隧道。匿名TLS隧道將使用Diffie Hellman密碼套件構建 — 不需要伺服器或客戶端證書。此方法容易受到Man in the Middle攻擊（模擬）。

要使用此選項，NAM需要以下配置選項：

「如果使用PAC允許未經驗證的PAC調配」（這僅適用於基於密碼的內部方法，因為如果不使用PKI基礎設施，則無法使用基於證書的內部方法）。

此外，ISE需要在Authentication Allowed Protocols下配置以下內容：

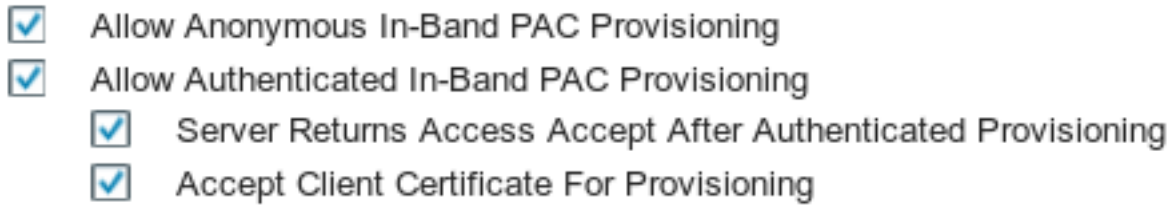
"允許匿名帶內PAC調配"

匿名帶內PAC設定正在用於TrustSec NDAC部署（網路裝置之間協商的EAP-FAST會話）。

已驗證的TLS隧道

這是最安全和推薦的選項。TLS隧道基於由請求方驗證的伺服器證書構建。這僅在伺服器端需要PKI基礎設施，ISE需要該基礎設施(在NAM上，可以禁用「驗證伺服器身份」選項。

對於ISE，有兩個附加選項：



通常，在PAC調配後，應傳送訪問拒絕，強制請求方使用PAC重新進行身份驗證。但是，由於PAC是通過身份驗證在TLS隧道中傳遞的，因此可以縮短整個過程，並在PAC調配後立即返回Access-Accept。

第二個選項基於客戶端證書構建TLS隧道（這需要在端點上部署PKI）。 這允許使用相互身份驗證來構建TLS隧道，該身份驗證將跳過內部方法並直接進入PAC調配階段。此處需要小心謹慎 — 有時請求方會提供不受ISE信任的證書（用於其他用途），並且會話將失敗。

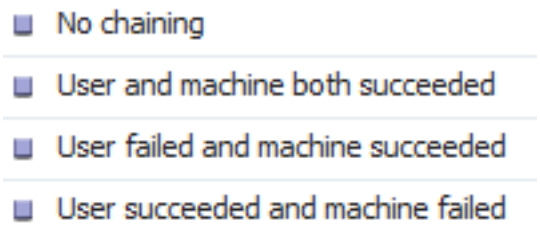
EAP連結

允許在一個Radius/EAP會話中進行使用者和電腦身份驗證。多個EAP方法可以連結在一起。在第一

個身份驗證（通常是電腦）成功完成後，伺服器將傳送一個指示成功的中間結果TLV（在TLS隧道中）。該TLV必須伴有加密繫結TLV請求。Cryptobinding用於證明伺服器和對等體都參與了特定的身份驗證序列。Cryptobinding過程使用第1階段和第2階段的金鑰材料。此外，還附加了一個額外的TLV:EAP-Payload — 正在啟動新會話（通常針對使用者）。 一旦radius伺服器(ISE)收到加密繫結TLV響應並驗證該響應，日誌中將顯示以下內容，並嘗試下一個EAP方法（通常用於使用者身份驗證）：

12126 **EAP-FAST cryptobinding verification passed**

如果加密繫結驗證失敗，則整個EAP會話將失敗。如果其中一個身份驗證失敗，則仍可以正常使用 — 因此，ISE允許管理員根據授權條件NetworkAccess:EapChainingResult：配置多個連結結果

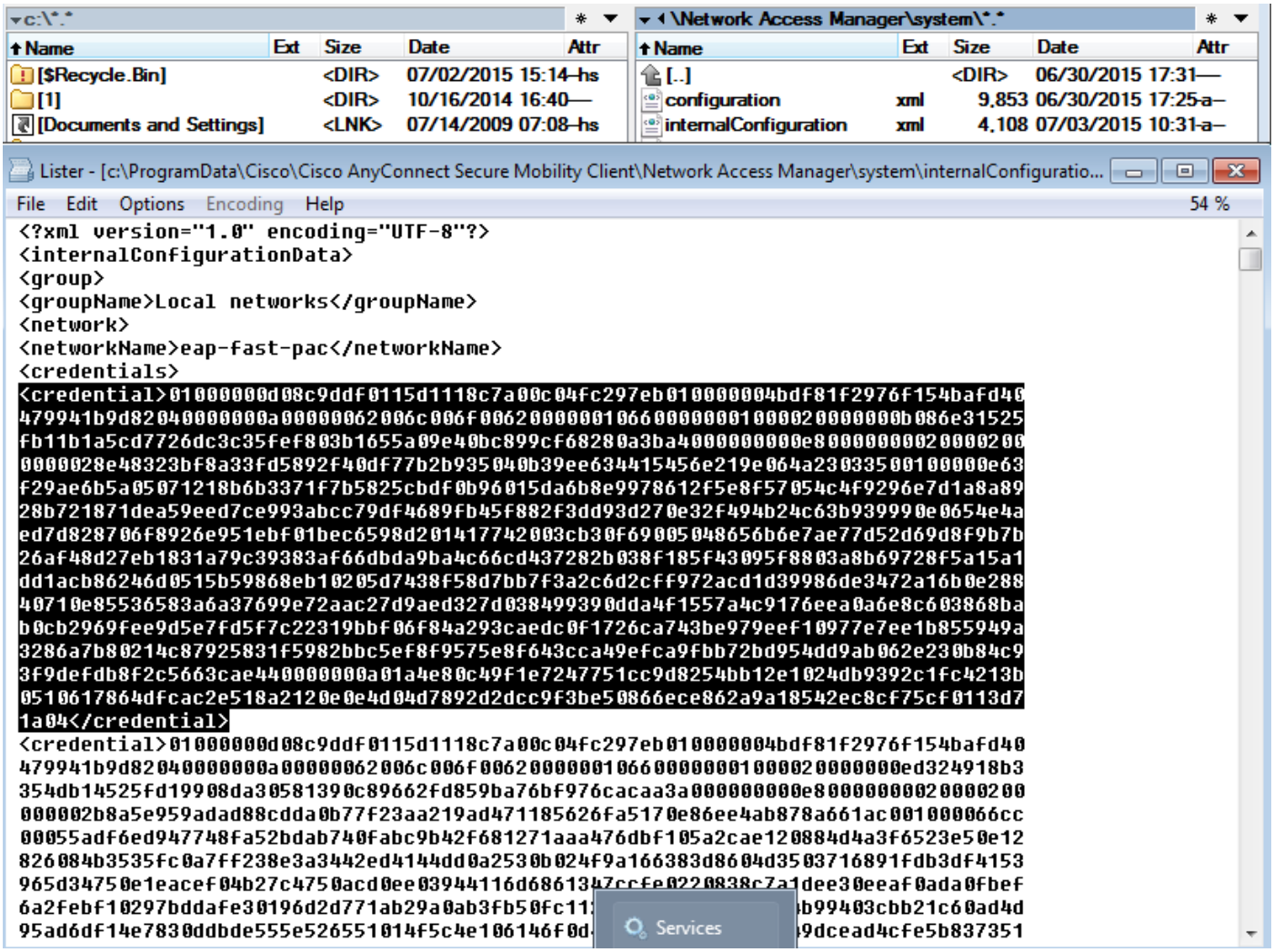


啟用EAP-FAST使用者和電腦身份驗證後，NAM上會自動啟用EAP-Chaining。

必須在ISE中配置EAP連結。

PAC檔案的儲存位置

預設情況下，隧道和電腦PAC儲存在<credential>一節中的C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml中。這些以加密形式儲存。

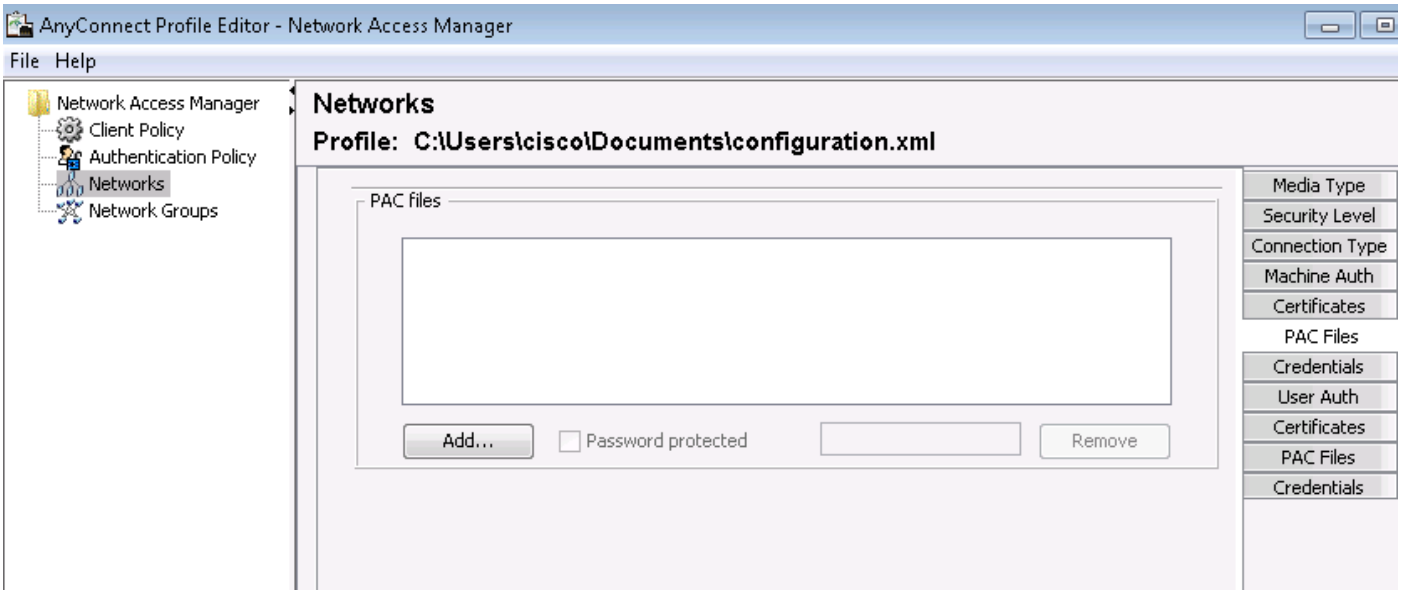


授權PAC僅儲存在記憶體中，並在重新啟動或NAM服務重新啟動後刪除。

需要重新啟動服務才能刪除隧道或電腦PAC。

AnyConnect NAM 3.1與4.0

AnyConnect 3.x NAM配置檔案編輯器允許管理員手動配置PAC。此功能已從AnyConnect 4.x NAM配置檔案編輯器中刪除。

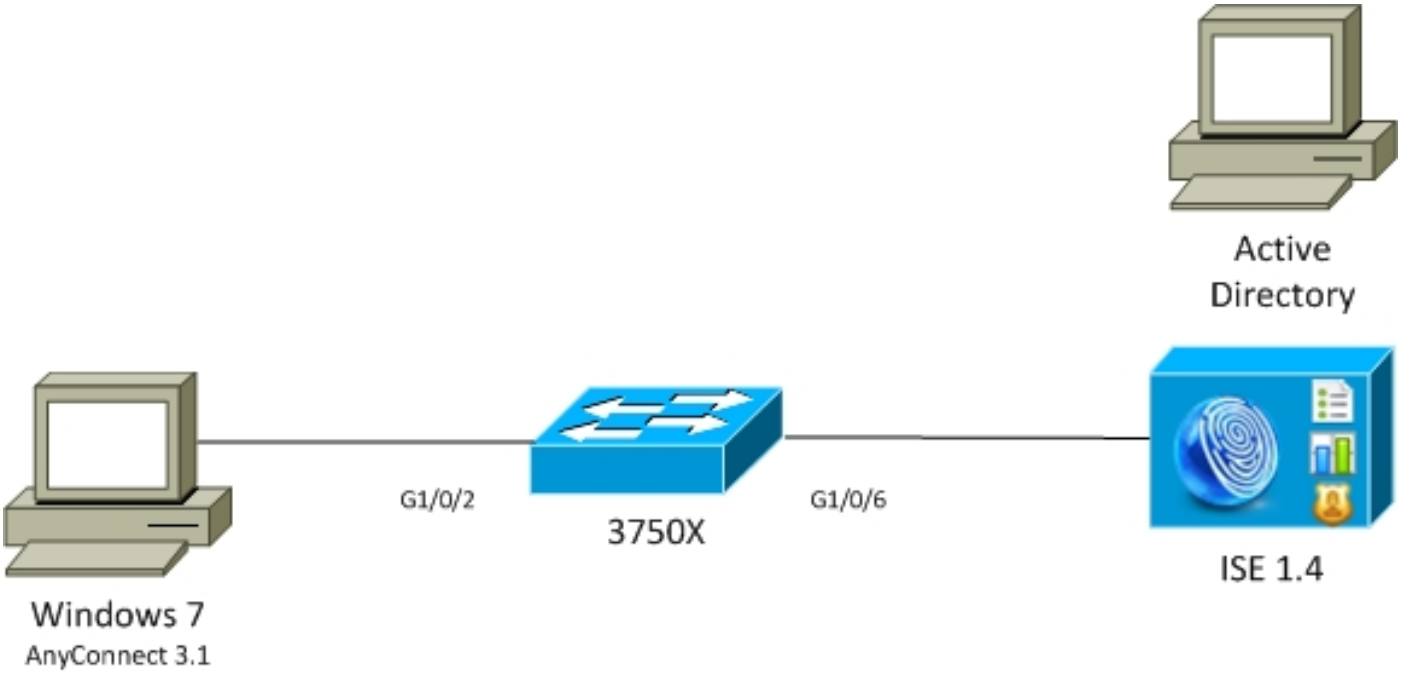


移除該功能的決定基於CSCuf3142和CSCua13140。

範例

網路圖表

已使用以下網路拓撲測試了所有示例。使用無線技術時也同樣如此。



EAP-Fast，不與使用者和電腦PAC建立EAP連結

預設情況下，ISE上禁用EAP_chaining。但是，所有其他選項均已啟用，包括電腦和授權PAC。請求方已經具有有效的電腦和隧道PAC。在此流程中，ISE上將提供兩個獨立的身份驗證（一個用於電腦，一個用於使用者），具有獨立的日誌。ISE記錄的主要步驟。第一次身份驗證（電腦）：

- 請求方使用電腦PAC傳送TLS客戶端Hello。
- 伺服器驗證電腦PAC並構建TLS隧道（未使用證書）。
- 伺服器驗證電腦PAC並在Active Directory中執行帳戶查詢並跳過內部方法。

```
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

第二個身份驗證（使用者）：

- 請求方通過隧道PAC傳送TLS客戶端Hello。
- 伺服器驗證PAC並構建TLS隧道（未使用證書）。
- 由於請求方沒有任何授權PAC，因此使用內部方法(EAP-MSCHAP)進行身份驗證。

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

在ISE中詳細報告的「其他屬性」部分中，針對使用者和電腦身份驗證注意以下事項：

EapChainingResult: **No chaining**

EAP-Fast（具有PAC Fast Reconnect的EAP連結）

在此流程中，請求方已擁有有效的隧道PAC以及使用者和機器授權PAC:

- 請求方通過隧道PAC傳送TLS客戶端Hello。
- 伺服器驗證PAC並構建TLS隧道（未使用證書）。
- ISE啟動EAP連結，請求方使用TLS隧道中的TLV為使用者和電腦附加授權PAC。
- ISE驗證授權PAC（無需內部方法），驗證Active Directory中是否存在帳戶（無其他身份驗證），返回成功。

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

在ISE中詳細報告的「其他屬性」部分中，注意以下事項：

EapChainingResult: **EAP Chaining**

此外，使用者和電腦憑據都包括在同一日誌中，如下所示：

Username: cisco,host/mgarcarz-PC

EAP-Fast，帶EAP連結，無PAC

在此流程中，NAM配置為不使用PAC，ISE也配置為不使用PAC（但使用EAP連結）

- 請求方在不使用隧道PAC的情況下傳送TLS客戶端Hello。
- 伺服器使用TLS證書和證書請求負載進行響應。
- 請求方必須信任伺服器證書，將不會傳送任何客戶端證書（證書負載為零），TLS隧道已生成。
- ISE在TLS隧道內傳送客戶端證書的TLV請求，但請求方不傳送請求（不需要擁有該請求才能繼續）。
- 使用內部方法和MSCHAPv2身份驗證為使用者啟動EAP連結。
- 繼續機器身份驗證，使用內部方法和MSCHAPv2身份驗證。
- 未調配任何PAC。

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，帶EAP連結授權PAC過期

在此流程中，請求方具有有效的隧道PAC，但已過期授權PAC:

- 請求方通過隧道PAC傳送TLS客戶端Hello。
- 伺服器驗證PAC並構建TLS隧道（未使用證書）。
- ISE啟動EAP連結，請求方使用TLS隧道中的TLV為使用者和電腦附加授權PAC。
- 當PAC過期時，使用者和電腦的內部方法都已啟動(EAP-MSCHAP)。
- 兩個身份驗證成功後，使用者和電腦授權PAC均會調配。

```
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
```

EAP-Fast（EAP連結隧道PAC已過期）

在此流程中，如果不存在有效的隧道PAC，則會發生具有內部階段的完整TLS協商。

- 請求方傳送不帶隧道PAC的TLS客戶端Hello。
- 伺服器使用TLS證書和證書請求負載進行響應。
- 請求方必須信任伺服器證書，不會傳送客戶端證書（證書負載為零），已建立TLS隧道。
- ISE在TLS隧道內傳送客戶端證書的TLV請求，但請求方不傳送（無需擁有該請求才能繼續）。
- 使用內部方法和MSCHAPv2身份驗證為使用者啟動EAP連結。
- 繼續機器身份驗證，使用內部方法和MSCHAPv2身份驗證。
- 已成功調配所有PAC（在ISE配置中啟用）。

```
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
```

採用EAP連結和匿名TLS隧道PAC調配的EAP-Fast

在此流程中，為PAC調配配置了ISE和NAM匿名TLS隧道（禁用了用於PAC調配的ISE身份驗證TLS隧道），PAC調配請求如下所示：

- 請求方傳送TLS客戶端Hello，但不傳送多個密碼套件。
- 伺服器使用TLS伺服器Hello和TLS匿名Diffie Hellman密碼（例如TLS_DH_anon_WITH_AES_128_CBC_SHA）進行響應。
- 請求方接受該請求，並構建匿名TLS隧道（不交換證書）。
- 使用內部方法和MSCHAPv2身份驗證為使用者啟動EAP連結。
- 繼續機器身份驗證，使用內部方法和MSCHAPv2身份驗證。
- 由於正在構建匿名TLS隧道，因此不允許使用授權PAC。
- 返回Radius Reject以強制請求方重新進行身份驗證（使用調配的PAC）。

```
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隧道協商的Wireshark資料包捕獲：

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，僅使用EAP連結使用者身份驗證

在此流程中，配置了採用EAP-FAST和使用者(EAP-TLS)的AnyConnect NAM以及電腦身份驗證(EAP-TLS)。Windows PC已啟動，但未提供使用者憑據。交換機啟動802.1x會話，NAM必須響應，但是未提供使用者憑據（尚未訪問使用者儲存和證書）。使用者身份驗證將失敗，但電腦將成功 — ISE身份驗證條件「Network Access:EapChainingResult EQUALS User failed and machine succeeded」已滿足。稍後，使用者登入且將啟動另一個身份驗證，使用者和電腦都將成功。

- 請求方使用電腦PAC傳送TLS客戶端Hello。
- 伺服器使用TLS更改密碼規范進行響應 — 系統會立即基於該PAC構建TLS隧道。
- ISE啟動EAP連結並請求使用者身份。
- 請求方改為提供機器身份（使用者尚未就緒），完成EAP-TLS內部方法。
- ISE再次請求使用者身份，請求方無法提供。

- ISE傳送TLV，中間結果=失敗（用於使用者身份驗證）。
- ISE返回最終的EAP成功消息，ISE條件Network Access:EapChainingResult EQUALS User failed and machine succeeded已滿足。

```
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，具有EAP連結和不一致的匿名TLS隧道設定

在此流程中，ISE僅通過匿名TLS隧道配置PAC調配，但NAM使用經過驗證的TLS隧道，ISE將記錄以下內容：

```
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

當NAM嘗試使用特定的TLS密碼構建經過驗證的TLS隧道時，會發生這種情況 — 並且配置為匿名TLS隧道的ISE不接受這些密碼（僅接受DH密碼）

疑難排解

ISE

對於詳細日誌，應在相應的PSN節點上啟用運行時AAA調試。以下是來自prrt-server.log的幾個日誌示例：

生成電腦PAC:

```
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請求審批：

```
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驗證：

```
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
```

成功生成PAC的摘要示例：

```
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驗證成功摘要示例：

```
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

來自NAM的DART日誌提供以下詳細資訊：

例如，非EAP鏈會話，機器身份驗證無需快速重新連線：

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

授權PAC查詢示例（非EAP鏈會話的電腦身份驗證）：

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

內部方法（用於MSCHAP）的所有狀態都可從以下日誌中驗證：

```
 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允許配置擴展日誌記錄功能，該功能將捕獲所有EAP資料包並將其儲存在pcap檔案中。這對於登入前啟動功能特別有用（即使是在使用者登入前進行的身份驗證，也會捕獲EAP資料包）。 要啟用功能，請諮詢您的TAC工程師。

參考資料

- Cisco AnyConnect安全移動客戶端管理員指南，版本4.0 EAP-FAST配置
- 思科身份服務引擎管理員指南，版本1.4 EAP-FAST建議
- 思科身分識別服務引擎設計手冊
- 使用AnyConnect NAM和Cisco ISE部署EAP連結
- 技術支援與文件 - Cisco Systems