了解EAP-FAST和连锁实施在AnyConnect NAM和ISE

目录

简介

此条款说明关于EAP-FAST实施的详细信息在思科AnyConnect网络访问管理器(NAM)和身份服务引擎(ISE)。它进一步解释特定功能如何一起运作和提供典型的使用案件和示例。

先决条件

要求

Cisco 建议您了解以下主题：

- EAP框架和EAP-FAST方法基础知识
- 基础知识身份服务引擎(ISE)
- AnyConnect NAM和配置文件编辑器基础知识
- 思科Catalyst配置基础知识802.1x服务的

使用的组件

本文档中的信息基于以下软件版本：

- 与Cisco AnyConnect安全移动客户端的Windows 7，版本3.1和4.0
- 思科有软件的15.2.1 Catalyst 3750X交换机及以后
- 思科ISE，版本1.4

理论

相位

EAP-FAST是允许请求方和服务器的相互验证的一个灵活EAP方法。它类似于EAP-PEAP，但是不典型地要求使用客户端甚至服务器证书。EAP-FAST一个优点是能力串连多次认证(使用多个内在方法)和密码在一起地粘合它(连锁发送的EAP)。Cisco实施使用此用户和计算机认证。

EAP-FAST使用受保护的访问凭证(PAC)为了迅速设立TLS建立隧道(会话恢复)或授权用户/计算机(验证的跳过内在方法)。

有EAP-FAST的3个相位：

- 相位0 (PAC设置)
- 相位1 (TLS隧道建立)
- 第2阶段(验证)

PAC少EAP-FAST的支持和基于PAC的会话。基于PAC包括PAC设置和基于PAC的验证。PAC设置可以根据匿名或已验证TLS会话。

PAC

PAC是服务器生成的受保护的访问凭证和，假设对客户端。它包括：

- PAC密钥(随机的加密值，用于派生TLS主控和会话密钥)
- 不透明的PAC (PAC锁上+用户标识-所有已加密由EAP-FAST服务器主密钥)
- PAC信息(服务器标识， TTL计时器)

发出PAC的服务器将加密PAC密钥和标识使用是不透明的PAC)的EAP-FAST服务器主密钥(并且发送全部的PAC给客户端。它不保持/存储其他信息(除了是相同的为所有PACs)的主密钥。

一旦不透明的PAC接收，解密使用EAP-FAST服务器主密钥并且验证。PAC密钥用于派生TLS主控，并且的会话密钥缩写的TLS建立隧道。

当上一个主密钥超时时，新的EAP-FAST服务器主密钥生成。 有时，主密钥可以取消。

有当前使用的PAC的一些种类型：

- 通道PAC ： 使用TLS隧道建立(没有客户端或服务器证书需要)。发送在TLS客户端Hello
- 计算机PAC ：使用TLS隧道建立和立即计算机授权。发送在TLS客户端Hello
- 用户授权PAC ：使用立即用户认证(跳过内在方法)，如果允许由服务器。发送的内部的TLS通道使用TLV。
- 计算机授权PAC ：使用立即计算机验证(跳过内在方法)，如果允许由服务器。发送的内部的TLS通道使用TLV。
- Trustsec PAC ：使用授权，当执行的环境或策略刷新。

所有那些PAC在相位0自动地通常传送。某些PAC (通道，计算机， Trustsec)可以手工也传送。

当PACs生成

- 通道PAC ：设置在成功认证(内在方法)以后，如果以前没使用。
- 授权PAC ：设置在成功认证(内在方法)以后，如果以前没使用。
- 计算机PAC ：设置在成功的计算机验证(内在方法)以后，如果以前没使用，并且，当没有使用授权PAC。当通道PAC超时，它proviosioned; 然而，没有，当授权PAC超时。当EAP连锁是启用或禁用的，它将设置。

注意：

每PAC设置要求除了以下用例的成功认证：没有一个AD帐户的授权用户请求计算机的计算机PAC。

下表汇总供应和积极的更新功能：

PAC类型	通道v1/v1a/CTS	计算机	授权
应要求提供PAC在供应	是	仅在已验证供应	仅在已验证供应，并且果通道PAC也请求
应要求提供PAC在验证	是	是	只有当未用于此验证
积极的更新	是	否	否
当落回到设置在失败的基于PAC的验证以后时的PAC (即，当PAC超时)	拒绝，并且不提供新的	拒绝，并且不提供新的	拒绝，并且不提供新的
支持ACS 4.x PACs	通道PAC v1/v1a	是	否

EAP-FAST服务器主密钥ACS 4.x与ACS 5x和ISE

当比较ACS 4.x和ISE时，有在主密钥处理的一个轻微的区别

功能	ACS 4.1.2	ACS 5.x/ISE
主密钥	主密钥有TTL，可以是活跃，退休或超时	主密钥从在每个配置的周期的种子自动地生成时间。特定主密钥总是可访问从未然后超时
PAC刷新	PAC更新由服务器发送，当PAC超时时，除非用于PAC加密的主密钥超时	PAC更新由服务器发送在特定可配置周期进行在PAC有效期瞬间前的时间的第一成

功认证以后。

默认情况下换句话说， ISE将保持所有原有主万能钥匙并且生成新的一次每周。因为主密钥不能超时，只有PAC TTL将验证。

ISE主密钥生成期限从*管理*配置- >*设置*- >*协议*- > *EAP-FAST* - > *EAP-FAST设置*。

会话恢复

这是允许通道PAC使用情况的必备组件。它允许TLS通道重新协商，不用证书使用情况。

有EAP-FAST的两个会话恢复类型：无状态的服务器状态基于和(基于的PAC)。

服务器状态

英文虎报TLS基于方法根据TLS在服务器缓存的SessionID。发送TLS客户端Hello的客户端附加SessionID为了恢复会话。会话只使用设置的PAC，当曾经匿名TLS时建立隧道：

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)
```

无状态(基于的PAC)

用户/计算机授权PAC用于存储对等体的上一个认证和授权状态。

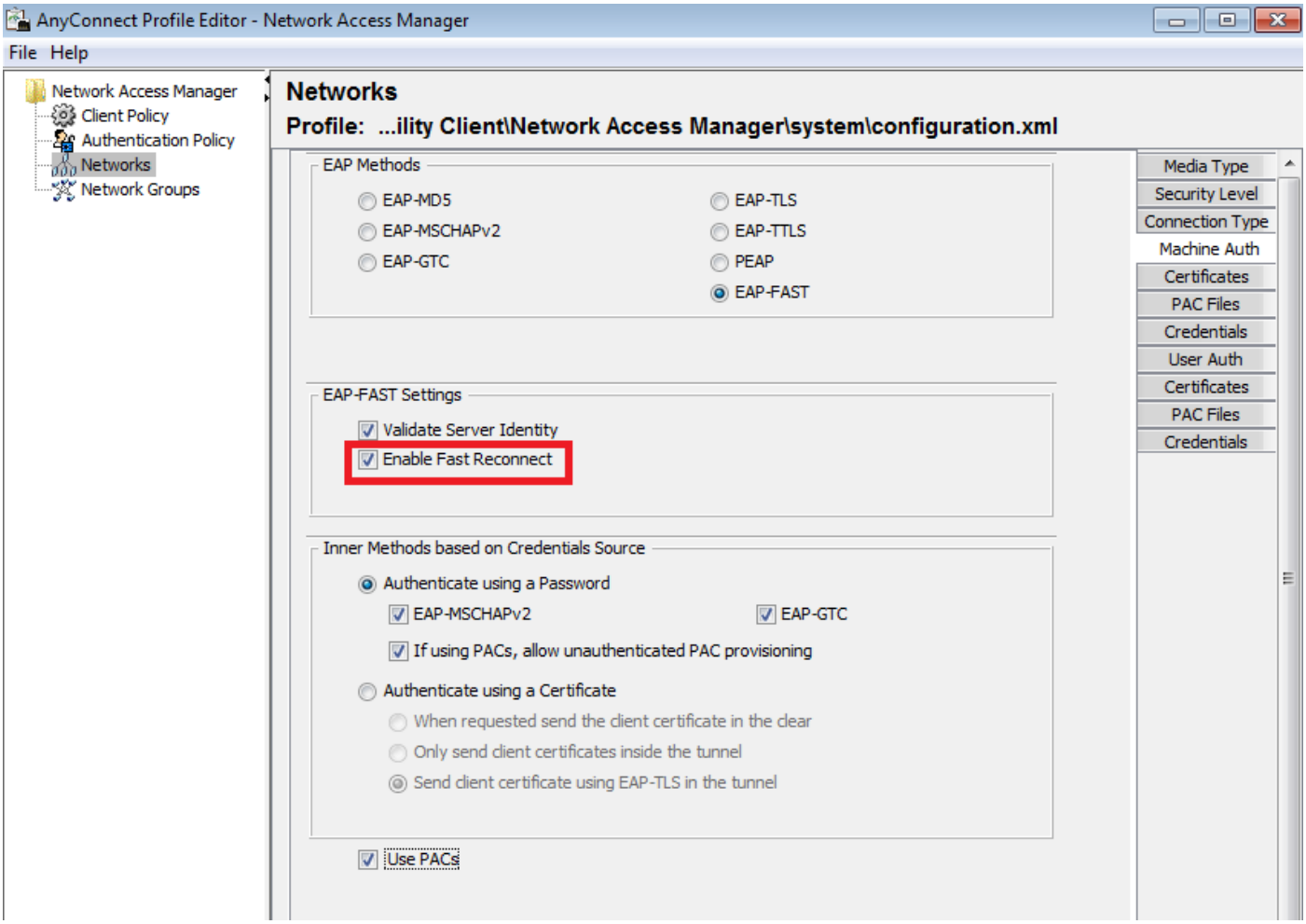
客户端恢复根据RFC 4507。服务器不需要缓存任何数据;反而客户端附加在TLS客户端Hello SessionTicket分机的PAC。反过来， PAC由服务器验证。 根据通道PAC的示例传送对服务器：

	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
```

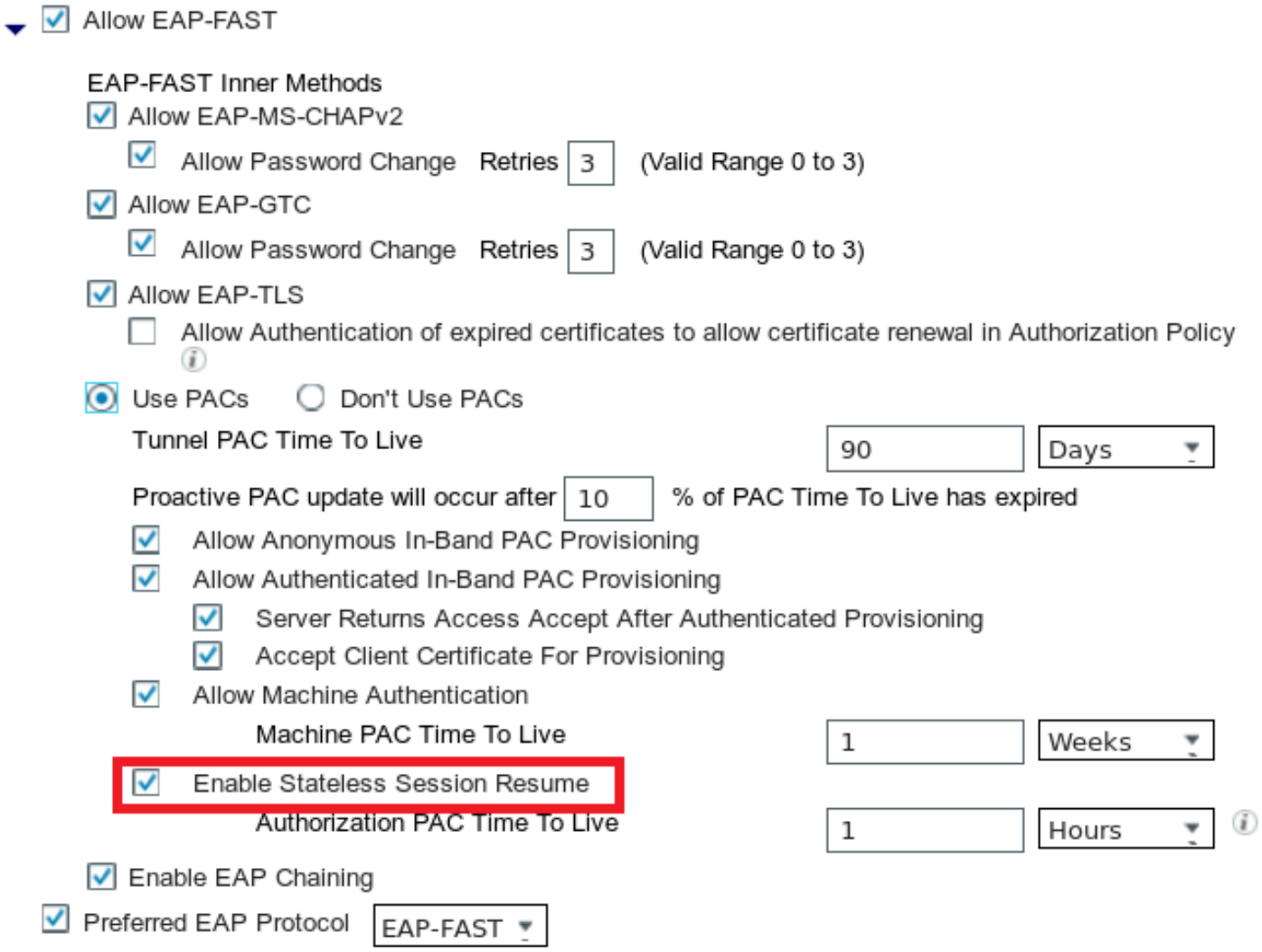
AnyConnect NAM实施

它在客户端(AnyConnect NAM)启用通过法塞特重新连接-，但是曾经控制授权仅PAC使用情况。



当设置禁用， NAM将使用通道PAC构建TLS通道(没有需要的证书)。然而，这不会使用授权PACs为了执行立即用户和计算机授权。结果，与内在方法的第2阶段永远将要求。

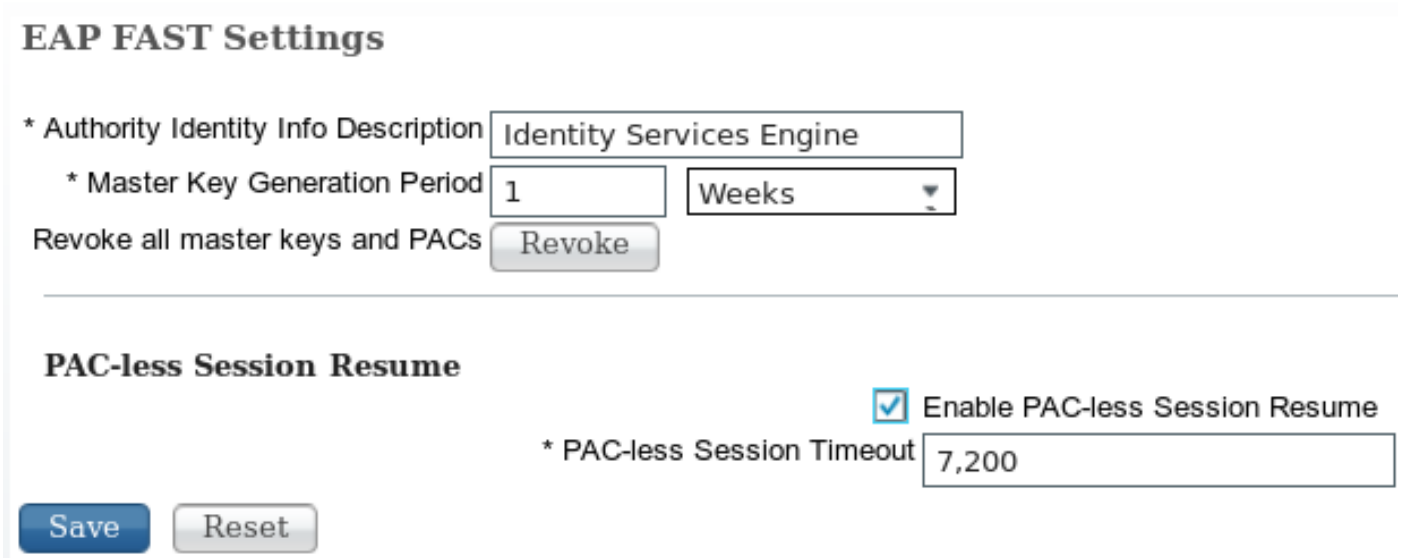
ISE有一个选项启用无状态的会话恢复。并且和在NAM它是为授权PAC。通道PAC使用情况控制与选项“使用PACs”。



如果选项启用， NAM将设法使用PAC。如果“请勿使用PACs”配置在ISE，并且ISE接收在以下错误将报告，并且的TLS分机的通道PAC EAP失败返回：

此处插入

在ISE，也是必要的启用根据TLS的会话恢复SessionID (从全局EAP-FAST设置)。默认情况下它禁用：



请记住仅可以使用会话恢复的一种类型。SessionID根据仅使用PAC少的部署，基于的RFC 4507仅

使用PAC部署。

PAC设置(相位0)

PACs在phase0可以自动地设置。相位0包括：

- TLS隧道建立
- 验证(内在方法)

PACs在一成功认证以后传送在TLS通道里面通过PAC TLV (和PAC TLV确认)

匿名TLS通道

对于没有PKI基础设施的部署，使用匿名TLS通道是可能的。匿名TLS通道将被构建使用Dffie Hellman密码器套件-，不用服务器或客户端证书的需要。此方法是倾向的供以人员在中间攻击(模拟)。

要使用此选项， NAM要求以下已配置的选项：

“如果使用PACs请允许设置未经鉴定的PAC” (有仅意义基于密码的内在方法的，因为没有PKI基础设施使用基于认证的内在方法)是不可能的。

并且， ISE将需要以下已配置的在允许的验证下协议：

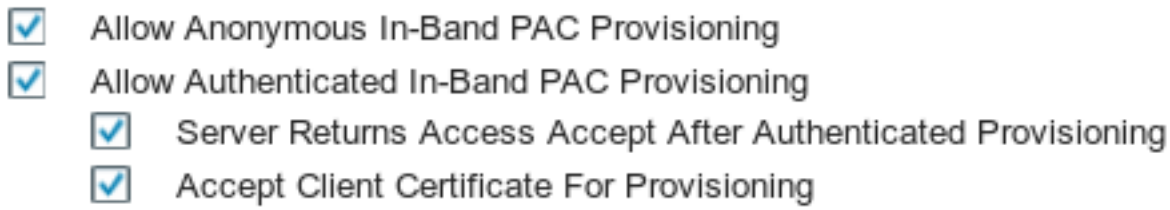
“请允许匿名带内PAC设置”

匿名带内PAC设置用于TrustSec NDAC部署(EAP-FAST会话协商在网络设备之间)。

已验证TLS通道

这是多数安全和推荐的选项。TLS通道根据由请求方验证的服务器证书被构建。这要求在仅服务器端的PKI基础设施，为ISE要求(在NAM是可能的对Disable选项“验证服务器标识”。

对于ISE有两个其它选项：



通常，使用PACs，在设置的PAC以后，应该发送访问拒绝强制请求方重新鉴别。但是，因为PACs在TLS传送请建立隧道与验证，它是可能缩短整个进程和返回Access-Accept在PAC设置之后。

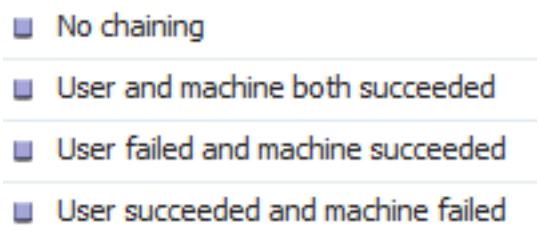
第二个选项构件TLS建立隧道基于客户端证书(这要求在终端的PKI部署)。这允许用相互验证将建立的TLS通道，跳过内在方法并且去直接地设置相位的PAC。小心在这里-重要的请求方有时将提交没有由ISE委托的一证书(在其他目的打算)，并且会话将出故障。

EAP连锁

在一Radius/EAP会话之内允许用户和计算机验证。多个EAP方法可以同时串联。在第一验证(典型地计算机)后顺利地完成，服务器将发送指示成功的中间结果TLV (里面TLS通道)。必须由加密绑定TLV请求随附于该TLV。cryptobinding用于证明，服务器和对等体参加了认证特定顺序。cryptobinding进程使用从相位1和第2阶段的密钥材料。另外，一TLV还附加：EAP有效负载-这启动个新会话(典型地为用户)。一旦RADIUS服务器(ISE)收到加密绑定TLV答复并且验证它，下列在日志将显示，并且下个EAP方法将尝试(典型地用户认证) ：

12126 **EAP-FAST cryptobinding verification passed**

如果cryptobinding验证发生故障，全部的EAP会话发生故障。如果其中一个在然后失败内的认证它是细致的-结果， ISE允许管理员配置根据授权情况Networkaccess的多种连锁结果：EapChainingResult ：

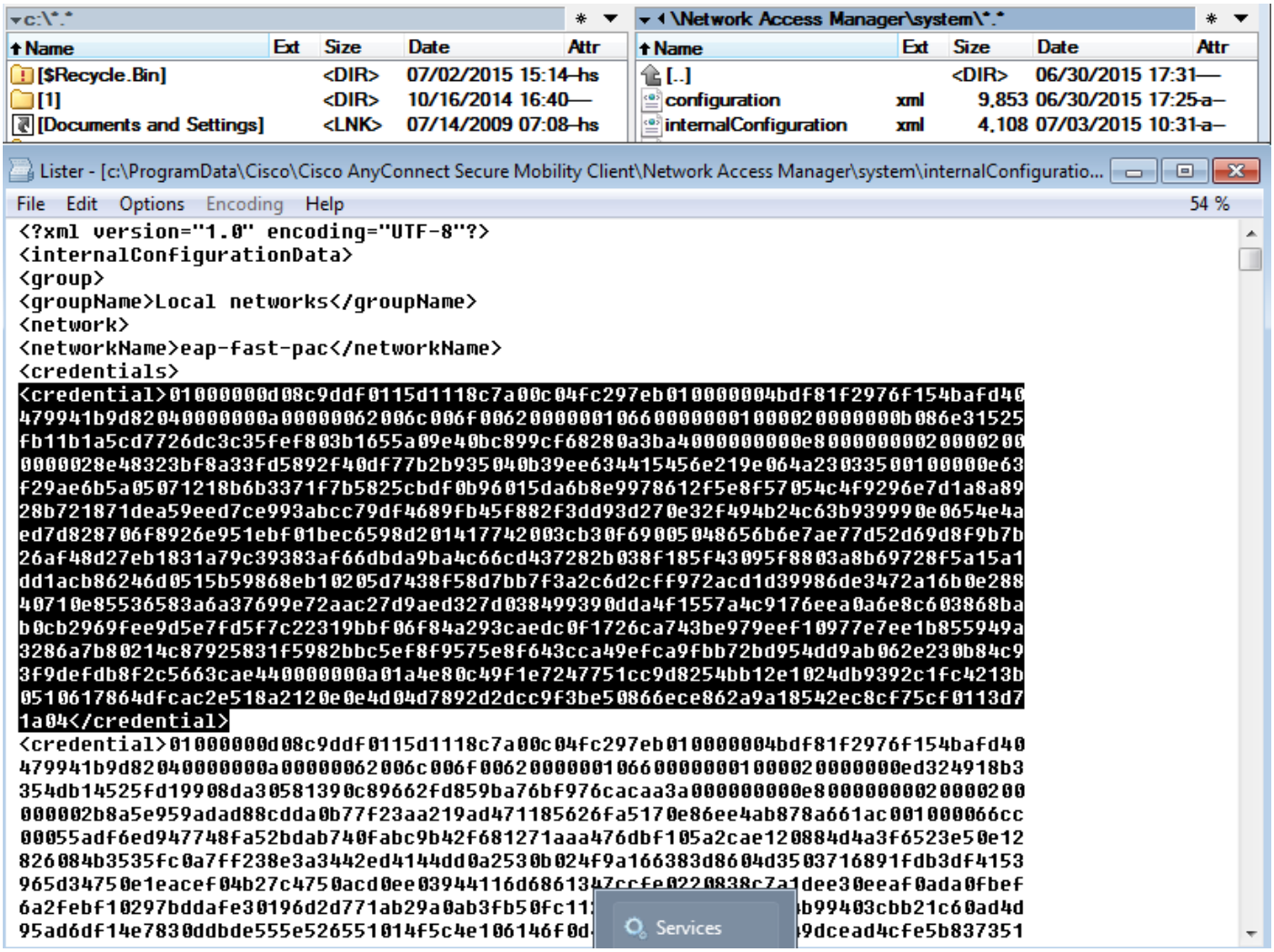


当EAP-FAST用户和计算机验证启用时， EAP连锁在NAM自动地启用。

在ISE必须配置EAP连锁。

那里PAC文件存储

默认情况下，通道和计算机PACs在C:\ProgramData\Cisco\Cisco AnyConnect安全移动性客户端\网络访问管理器\系统\在部分<credential>的internalConfiguration.xml存储。那些存储以加密形式。

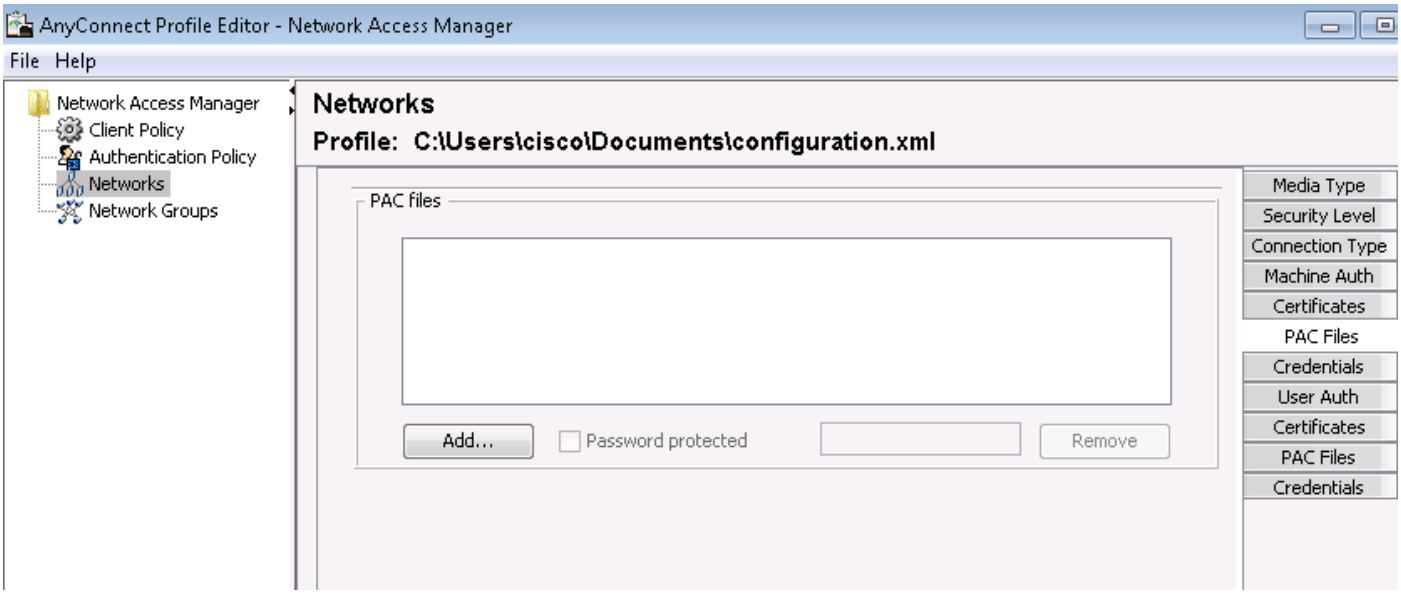


授权PACs在内存仅存储和删除，在重新启动或NAM服务重新启动后。

服务重新启动要求删除通道或计算机PAC。

AnyConnect NAM 3.1与4.0

AnyConnect 3.x NAM配置文件编辑器允许管理员手工配置PACs。此功能从AnyConnect 4.x NAM配置文件编辑器删除。

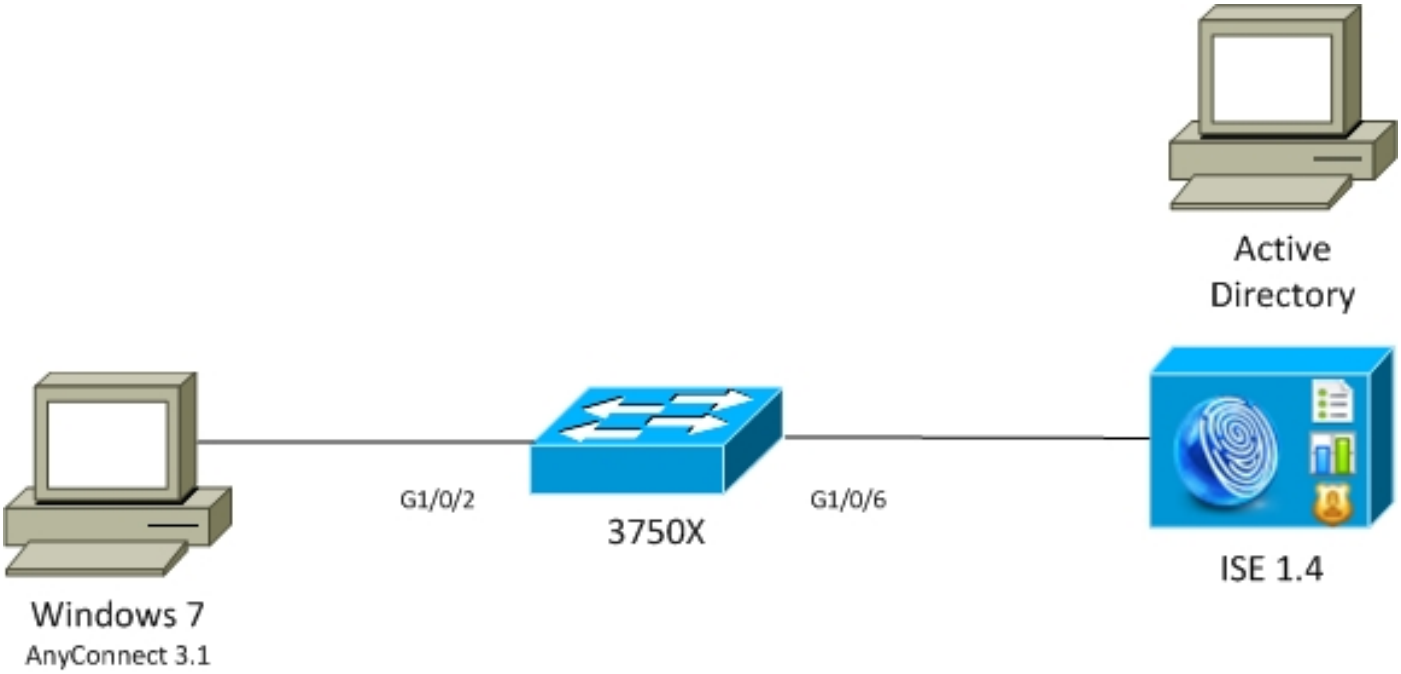


决策删除功能根据CSCuf31422和CSCua13140。

示例

网络图

使用以下网络拓扑，所有示例测试了。当使用无线时，同样也应用。



没有EAP的EAP法塞特连锁发送与用户和计算机PAC

默认情况下， EAP_chaining在ISE禁用。然而，所有其它选项启用包括计算机和授权PACs。请求方已经有一有效计算机和通道PAC。在此流，将有两个独立的认证-一个计算机的和一个用户的-与分开注册ISE。主要步骤如记录由ISE。第一验证(计算机) ：

- 请求方发送有计算机PAC的TLS客户端Hello。
- 服务器验证计算机PAC并且构建TLS通道(没有使用的证书)。
- 服务器在活动目录验证计算机PAC并且执行帐户查找并且跳过内在方法。

```
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

第二验证(用户) ：

- 请求方发送有通道PAC的TLS客户端Hello。
- 服务器验证PAC并且构建TLS通道(没有使用的证书)。
- 因为请求方没有任何授权PAC，内在方法(EAP-MSCHAP)使用验证。

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

在详细的报告的“其他属性”部分在ISE的，下列以用户和计算机认证是要注意的：

EapChainingResult: **No chaining**

有EAP连锁的EAP法塞特与PAC法塞特重新连接

在此流，请求方已经有有效通道PAC与用户和计算机授权PACs一起：

- 请求方发送有通道PAC的TLS客户端Hello。
- 服务器验证PAC并且构建TLS通道(没有使用的证书)。
- ISE开始EAP连锁，请求方附加用户的授权PACs，并且计算机使用TLV在TLS里面建立隧道。
- ISE验证授权PACs (没有需要的内在方法)，验证帐户在活动目录(没有另外的验证)存在，回归成功。

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

在详细的报告的"其他属性"部分在ISE的，下列是要注意的：

EapChainingResult: **EAP Chaining**

另外，用户和计算机凭证在日志包括和如下被看到一样：

EapChainingResult: **EAP Chaining**

有EAP的EAP法塞特连锁发送没有PAC

在此流， NAM配置不使用PAC， ISE也配置不使用PAC (但是与连锁发送的EAP)

- 请求方发送TLS客户端Hello，不用通道PAC。
- 服务器回应TLS证书和证书请求有效载荷。
- 请求方必须服务器证书，不是发送所有客户端证书(证书有效负载零)，通道被构建的TLS。
- 一个TLV要求客户端证书在TLS里面建立隧道的ISE发送，但是请求方不(是不必要的有它为了继续)。
- 使用与MSCHAPv2验证的内在方法启动EAP为用户连锁发送。
- 使用与MSCHAPv2验证的内在方法继续计算机验证。
- PACs没有设置。

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
```

有EAP连锁授权PAC有效期的EAP法塞特

在此流，请求方有有效通道PAC，但是超时授权PACs ：

- 请求方发送有通道PAC的TLS客户端Hello。
- 服务器验证PAC并且构建TLS通道(没有使用的证书)。
- ISE开始EAP连锁，请求方附加用户的授权PACs，并且计算机使用TLV在TLS里面建立隧道。
- 当PACs超时，用户和计算机的内在方法开始(EAP-MSCHAP)。
- 一旦两个认证是成功的，用户和计算机授权PACs设置。

```
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
```

有EAP连锁超时的通道PAC的EAP法塞特

在此流，当有效通道PAC不存在时，与内在相位的全双工TLS协商发生。

- 请求方发送TLS客户端Hello，不用通道PAC。

- 服务器回应TLS证书和证书请求有效载荷。
- 请求方必须服务器证书，不是发送客户端证书(证书有效负载零)， TLS建立隧道构件。
- ISE发送TLV要求客户端证书在TLS里面建立隧道，但是请求方不(是不必要的有它为了继续)。
- 使用与MSCHAPv2验证的内在方法启动EAP为用户连锁发送。
- 使用与MSCHAPv2验证的内在方法继续计算机验证。
- 顺利地设置了所有PACs (启用在ISE设置)。

```
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
```

有EAP连锁的EAP法塞特和匿名TLS建立隧道PAC设置

在此流， ISE和NAM匿名TLS通道为设置(ISE已验证TLS为PAC设置建立隧道禁用) PAC的PAC配置设置请求看起来：

- 请求方发送TLS客户端Hello，不用多ciphersuites。
- 服务器回应TLS服务器问候和TLS匿名Dffie Hellman密码器(例如TLS_DH_anon_WITH_AES_128_CBC_SHA)。
- 请求方接受它，并且匿名TLS通道被构建(没有交换的证书)。
- 使用与MSCHAPv2验证的内在方法启动EAP为用户连锁发送。
- 使用与MSCHAPv2验证的内在方法继续计算机验证。
- 因为匿名TLS通道被构建授权PACs没有允许。
- Radius拒绝返回强制请求方重新鉴别(使用已配置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隧道协商的Wireshark数据包捕获：

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)
```

有EAP仅连锁用户认证的EAP法塞特

在此流，与EAP-FAST和用户(EAP-TLS)和计算机验证(EAP-TLS)的AnyConnect NAM配置。Windows PC是启动，但是没有提供用户凭证。然而交换机启动802.1x会话， NAM必须回应，用户凭证没有提供， (对用户存储和证书的没有访问)因此。用户认证将发生故障，当计算机将是成功的时- ISE authz情况“网络访问：EapChainingResult等于用户失败，并且成功的计算机”是满足的。以后，用户登录和另一验证将开始，用户，并且计算机将成功。

- 请求方发送有计算机PAC的TLS客户端Hello。
- 服务器回应TLS更改密码器Spec - TLS通道立即是根据该PAC的构建。
- ISE启动连锁发送和询问为用户标识的EAP。
- 请求方提供计算机标识(不就绪的用户)，完成EAP-TLS内在方法。
- ISE再请求用户标识，请求方不能提供它。
- 与半成品结果=失败的ISE发送TLV (用户认证)。
- ISE返回最终EAP成功消息， ISE情况网络访问：EapChainingResult等于用户失败，并且成功

的计算机是满足的。

```
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
```

有EAP连锁和不一致匿名TLS隧道设置的EAP法塞特

在此流， ISE为仅设置通过匿名TLS的PAC配置建立隧道，但是NAM使用一个已验证TLS通道，以下将由ISE记录：

```
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
```

这发生，当NAM尝试构件已验证TLS建立隧道与为匿名TLS通道配置的它是speciphic TLS密码器-，并且那些没有由ISE接受(接受仅DH密码器)

故障排除

ISE

对于详细的日志，在对应的PSN节点应该启用运行时间AAA调试。下面从prrt-server.log的一些本示例日志：

计算机PAC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请求批准：

```
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验证：

```
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
```

成功的摘要示例PAC生成的：

```
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
```

成功的摘要示例PAC验证的：

```
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

从NAM的箭日志提供以下细节：

非EAP连锁会话的示例，没有快速的计算机验证重新连接：

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

授权PAC查找(非EAP连锁会话的计算机验证)示例：

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

内在方法的所有状态(MSCHAP)可以从下面日志验证：

```
 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允许在pcap文件将获取所有EAP数据包并且储存他们延长的操作日志功能的配置。这为开始是特别设立的在登录功能前(EAP数据包在用户登录前发生)的认证的是捕获的。对于功能激活请要求您的TAC工程师。

参考

- Cisco AnyConnect安全移动客户端管理员指南，版本4.0 EAP-FAST配置
- 思科身份服务引擎管理员指南，版本1.4 EAP-FAST建议
- 思科身份服务引擎设计指南
- 部署EAP连锁发送与AnyConnect NAM和思科ISE
- 技术支持和文档 - Cisco Systems