Comprensión del EAP-FAST y encadenamiento de las implementaciones en AnyConnect NAM y ISE

Contenido

Introducción

Este artículo explica los detalles con respecto a las implementaciones del EAP-FAST en el administrador del acceso a la red de Cisco AnyConnect (NAM) y el Identity Services Engine (ISE). Explica más lejos cómo las características específicas trabajan juntas y proporciona los casos típicos y los ejemplos del uso.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del marco EAP y de los métodos del EAP-FAST
- Conocimiento básico del Identity Services Engine (ISE)
- Conocimiento básico de AnyConnect NAM y del editor del perfil
- Conocimiento básico de la configuración del Cisco Catalyst para los servicios del 802.1x

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Windows 7 con el Cliente de movilidad Cisco AnyConnect Secure, versión 3.1 y 4.0
- Cisco Catalyst 3750X Switch con el software 15.2.1 y posterior
- Cisco ISE, versión 1.4

Teoría

Fases

El EAP-FAST es un método EAP flexible que permite la autenticación recíproca de un supplicant y de un servidor. Es similar a EAP-PEAP, pero no requiere típicamente el uso del cliente o aún de los certificados de servidor. Una ventaja del EAP-FAST es la capacidad de encadenar las autenticaciones múltiples (usando los métodos internos múltiples) y de atarlas criptográficamente juntas (EAP que encadena). Las implementaciones de Cisco utilizan esto para las autenticaciones del usuario y de la máquina.

El EAP-FAST utiliza las credenciales protegidas del acceso (PAC) para establecer rápidamente el túnel de TLS (curriculum vitae de la sesión) o autorizar el usuario/la máquina (método de autenticación interno del salto).

Hay 3 fases para el EAP-FAST:

- fase 0 (aprovisionamiento PAC)
- fase 1 (establecimiento del túnel de TLS)
- fase 2 (autenticación)

El EAP-FAST soporta el PAC-menos y la conversación PAC-basada. PAC-basado consiste en el aprovisionamiento PAC y la autenticación PAC-basada. El aprovisionamiento PAC se puede basar en la sesión anónima o autenticada de TLS.

PAC

El PAC es credenciales protegidas del acceso generadas por el servidor y con tal que al cliente. Consiste en:

- Clave PAC (valor secreto al azar, usado para derivar el master y las claves de la sesión de TLS)
- PAC opaco (clave + Identificación del usuario PAC - cifrada todo por la clave principal del servidor del EAP-FAST)
- Información PAC (identidad del servidor, temporizadores de TTL)

El servidor que publica el PAC cifrará la clave y la identidad PAC usando la clave principal del servidor del EAP-FAST (que es PAC opaco) y envía el PAC entero al cliente. No hace guardar/almacén ninguna otra información (excepto la clave principal que es lo mismo para todos los PAC).

Una vez que el PAC opaco se recibe, se desencripta usando la clave principal del servidor del EAP-FAST y se valida. La clave PAC se utiliza para derivar al master de TLS y las claves de la sesión para TLS abreviado hacen un túnel.

Se generan las nuevas claves principales del servidor del EAP-FAST cuando expira la clave principal anterior. En algunos casos, una clave principal puede ser revocada.

Hay algunos tipos de PAC que son utilizados actualmente:

- Túnel PAC: utilizado para el establecimiento del túnel de TLS (sin la necesidad del cliente o del certificado de servidor). Enviado en los saludos del cliente de TLS
- Máquina PAC: utilizado para el establecimiento del túnel de TLS y la autorización inmediata de la máquina. Enviado en los saludos del cliente de TLS
- Autorización de usuario PAC: utilizado para la autenticación de usuario inmediata (método interno del salto) si es permitido por el servidor. Túnel interior enviado de TLS usando el TLV.
- Autorización PAC de la máquina: utilizado para la autenticación inmediata de la máquina (método interno del salto) si es permitido por el servidor. Túnel interior enviado de TLS usando el TLV.
- Trustsec PAC: utilizado para la autorización cuando la ejecución ambiental o la directiva restaura.

Todos esos PAC se entregan generalmente automáticamente en la fase 0. Algunos de los PAC (túnel, máquina, Trustsec) se pueden también entregar manualmente.

Cuando se generan los PAC

- Túnel PAC: el aprovisionado después de una autenticación satisfactoria (método interno) si no utilizó previamente.
- Autorización PAC: el aprovisionado después de la autenticación satisfactoria (método interno) si no utilizó previamente.
- Máquina PAC: el aprovisionado después de la autenticación acertada de la máquina (método interno) si no utilizó previamente y cuando una autorización PAC no se utiliza. Proviosioned cuando expira el túnel PAC; sin embargo, no cuando expira la autorización PAC. Será aprovisionado cuando se habilita o se inhabilita el EAP-encadenamiento.

Nota:

Cada aprovisionamiento PAC requiere la autenticación satisfactoria a menos que del caso siguiente del uso: el usuario autorizado pide la máquina PAC para una máquina que no tenga una

cuenta AD.

La tabla siguiente resume el aprovisionamiento y las funciones dinámicas de la actualización:

Tipo PAC	Túnel v1/v1a/CTS	Máquina	Autorización
Proporcione el PAC a petición en el aprovisionamiento	sí	solamente en el aprovisionamiento autenticado	solamente en el aprovisionamiento autenticado y si el túr
Proporcione el PAC a petición en la autenticación	sí	sí	PAC se pide también solamente si no fue utilizada en esta autenticación
Actualización dinámica	sí	no	no
Al recurrir al aprovisionamiento PAC después de la autenticación PAC-basada fallada (e.g cuando se expira el PAC)	el rechazo y no proporciona el nuevo	el rechazo y no proporciona el nuevo	el rechazo y no proporciona el nuevo
Soporte ACS 4.x PAC	para el túnel PAC v1/v1a	sí	no

Clave principal ACS 4.x del servidor del EAP-FAST contra ACS 5x y ISE

Hay una leve diferencia en la clave principal que dirige al comparar ACS 4.x y ISE

Función	ACS 4.1.2	ACS 5.x/ISE
Clave principal	La clave principal tiene TTL, puede ser activa, retirada o expirada	La clave principal se genera automáticamente del germen en cada periodo configurado del tiempo. La clave principal específica es siempre accesible y después nunca expirada
El PAC restaura	La actualización PAC es enviada por el servidor cuando se expira el PAC, a menos que se expire la clave principal usada para el cifrado PAC	La actualización PAC es enviada por el servidor después de la primera autenticación satisfactoria que se realiza en el período configurable específico de tiempo antes del momento de la expiración PAC.

Es decir el ISE guardará todas las claves de maestro anterior y generará un nuevo por abandono una vez por la semana. Pues la clave principal no puede expirar, sólo el PAC TTL será validado.

El período de la generación de clave principal ISE se configura de la *administración - > las configuraciones - > protocolo - > EAP-FAST - > las configuraciones del EAP-FAST.*

Curriculum vitae de la sesión

Esto es un componente importante teniendo en cuenta el uso del túnel PAC. Permite la renegociación del túnel de TLS sin el uso de los Certificados.

Hay dos tipos del curriculum vitae de la sesión para el EAP-FAST: Estado del servidor basado y apátrida (PAC basado).

Estado del servidor

El método basado TLS estándar se basa en TLS SessionID ocultado en el servidor. El cliente que envía los saludos del cliente de TLS asocia el SessionID para reanudar la sesión. La sesión se utiliza solamente para el aprovisionamiento PAC al usar un túnel anónimo de TLS:

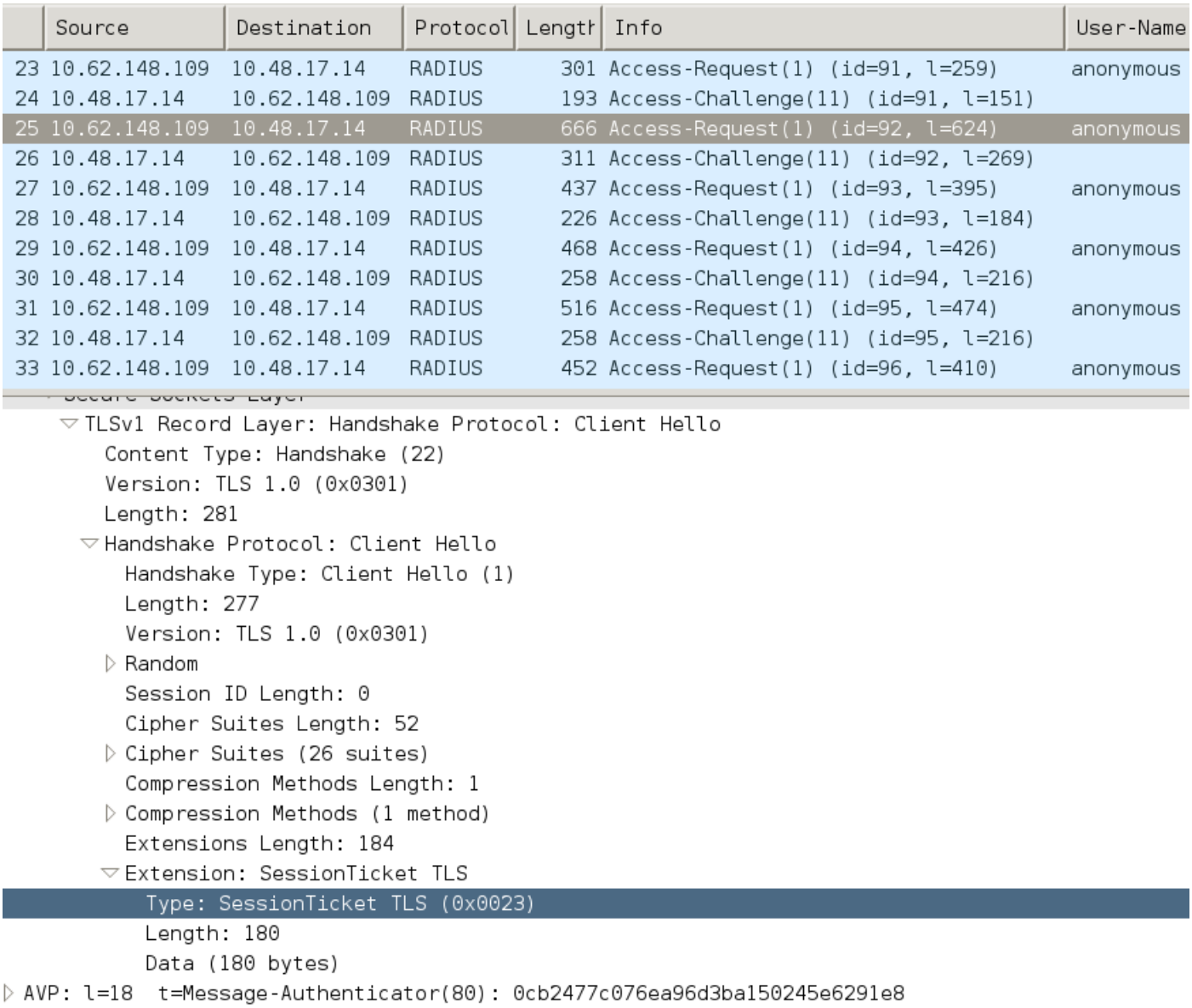
Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l=	anonymous
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l	anonymous
10.48.17.14	10.62.148.109	RADIUS	193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

Apátrida (PAC basado)

Se utiliza la autorización PAC del usuario/de la máquina de salvar los estados anteriores de la autenticación y autorización para el par.

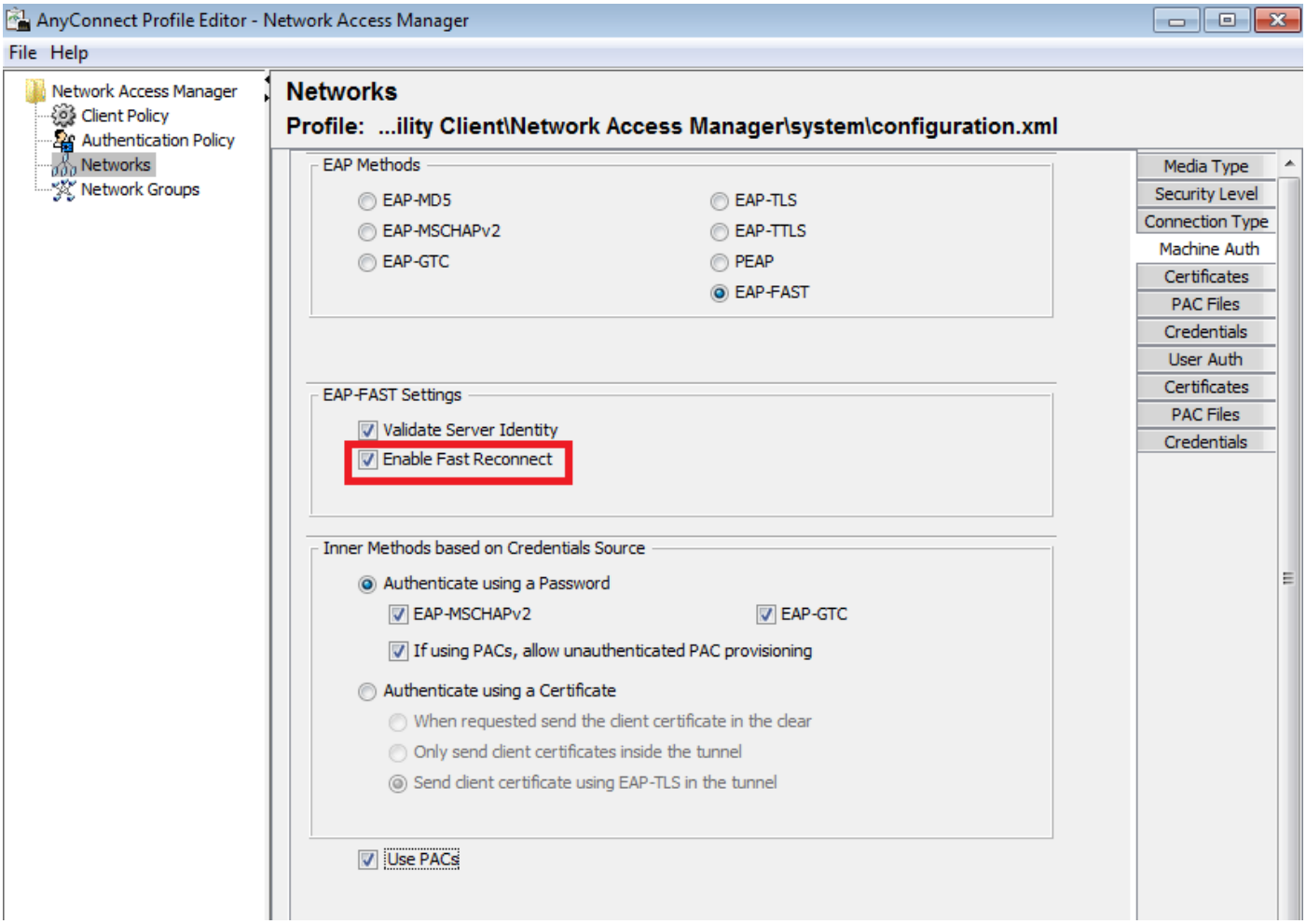
El curriculum vitae del lado del cliente se basa en el RFC 4507. El servidor no necesita ocultar ningunos datos; en lugar el cliente asocia el PAC en la extensión de SessionTicket de los saludos del cliente de TLS. A su vez, el PAC es validado por el servidor. Ejemplo basado en el túnel PAC entregado al servidor:



	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

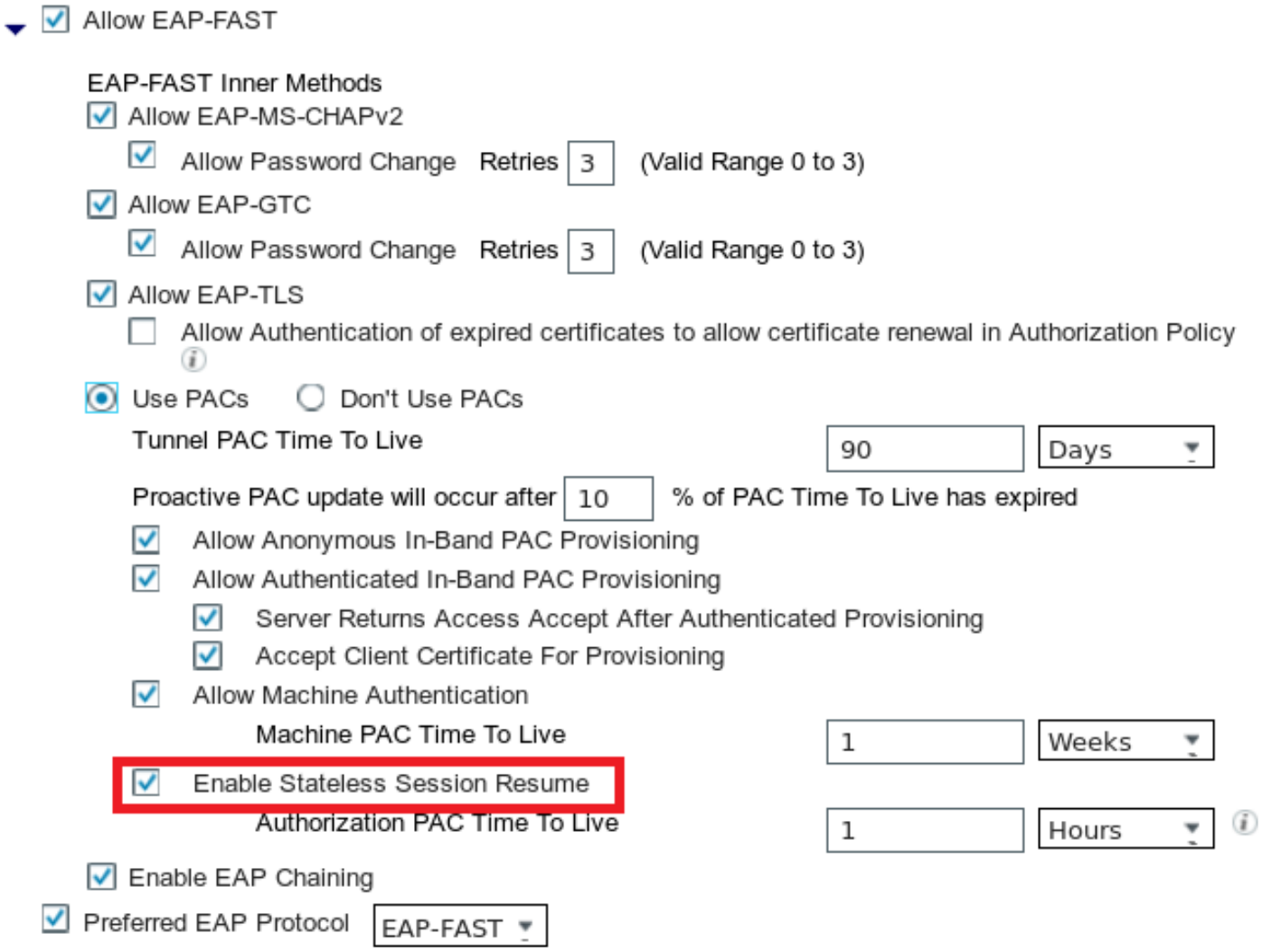
Implementación de AnyConnect NAM

Ha habilitado en el cliente que el lado (AnyConnect NAM) vía rápido vuelve a conectar - pero controlaba solamente el uso de la autorización PAC.



Con la configuración inhabilitada, el NAM todavía utilizará el túnel PAC para construir el túnel de TLS (ningunos Certificados necesarios). Sin embargo, esto no utilizará la autorización PAC para realizar la autorización inmediata del usuario y de la máquina. Como consecuencia, la fase 2 con el método interno será requerida siempre.

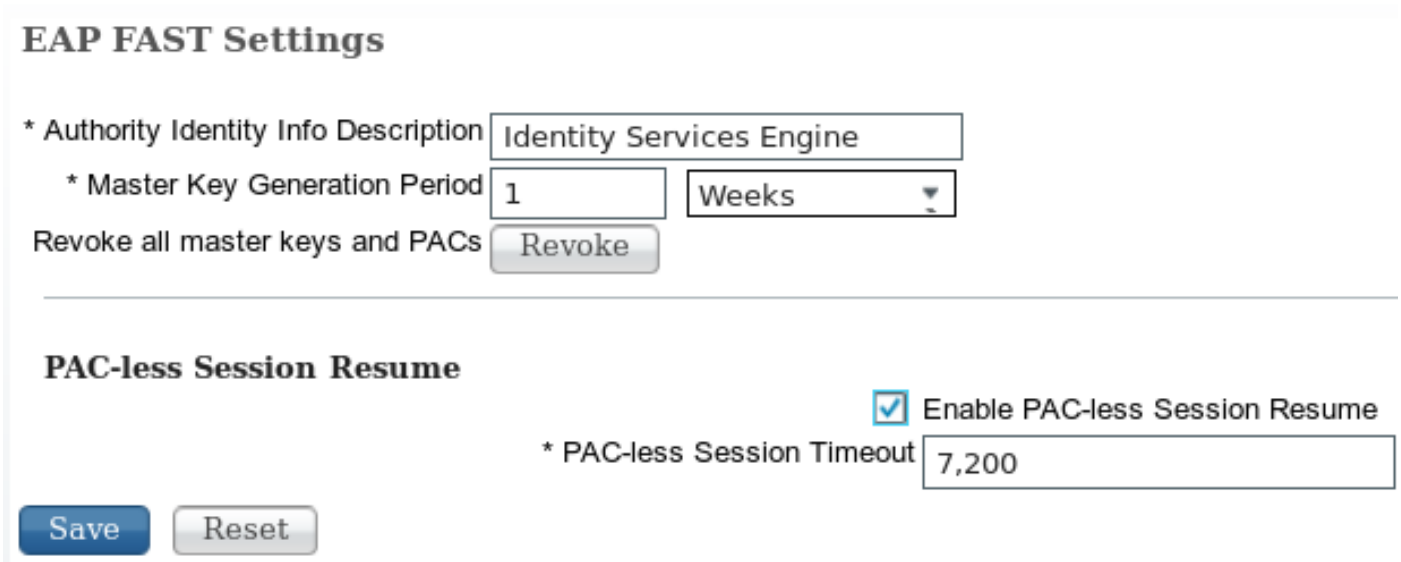
El ISE tiene una opción para habilitar el curriculum vitae apátrida de la sesión. Y como en el NAM está apenas para la autorización PAC. El uso del túnel PAC se controla con las opciones “uso PAC”.



El NAM intentará utilizar los PAC si se habilita la opción. Si “no utilice los PAC” se configura en el ISE y el ISE recibe un túnel PAC en la extensión de TLS que el error siguiente será señalado y vuelven a un error EAP:

inserte aquí

En el ISE, es también necesario habilitar el curriculum vitae de la sesión basado en TLS SessionID (de las configuraciones globales del EAP-FAST). Ha inhabilitado por abandono:



Tenga por favor presente que solamente un tipo de curriculum vitae de la sesión puede ser utilizado. SessionID basó se utiliza solamente para las implementaciones PAC-menos, RFC 4507 basado se utiliza solamente para las implementaciones PAC.

Aprovisionamiento PAC (fase 0)

Los PAC pueden ser automáticamente aprovisionado en phase0. La fase 0 consiste en:

- Establecimiento del túnel de TLS
- Autenticación (método interno)

Los PAC se entregan después de una autenticación satisfactoria dentro del túnel de TLS vía el acuse de recibo PAC TLV (y PAC TLV)

Túnel anónimo de TLS

Para las implementaciones sin una infraestructura PKI, es posible utilizar un túnel anónimo de TLS. El túnel anónimo de TLS será construido usando la habitación de la cifra del Diffie Hellman - sin la necesidad de un servidor o de un certificado del cliente. Este acercamiento es hombre propenso en los ataques medios (personificación).

Para utilizar esta opción, el NAM requiere la opción configurada siguiente:

“Si usa los PAC tenga en cuenta el aprovisionamiento del unauthenticated PAC” (que tiene sentido solamente para el método interno basado en la contraseña porque sin la infraestructura PKI no es posible utilizar el método interno basado en el certificado).

También, el ISE necesitará el siguiente configurado bajo autenticación no prohibida los protocolos:

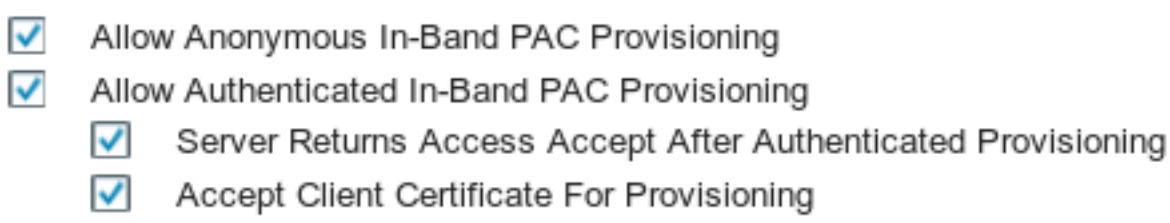
“Permita el aprovisionamiento anónimo de la En-banda PAC”

El aprovisionamiento anónimo de la en-banda PAC se está utilizando en las implementaciones NDAC de TrustSec (sesión del EAP-FAST negociada entre los dispositivos de red).

Túnel autenticado de TLS

Ésta es la opción más segura y recomendada. El túnel de TLS se construye sobre la base del certificado de servidor que es validado por el supplicant. Esto requiere una infraestructura PKI en el lado del servidor solamente, que se requiere para el ISE (en el NAM es posible inhabilitar la opción “valida la identidad del servidor”.

Para el ISE hay dos opciones adcionales:



Normalmente, después del aprovisionamiento PAC, un Access-Reject se debe enviar forzando el supplicant a reauthenticate usando los PAC. Pero puesto que los PAC fueron entregados en el

túnel de TLS con la autenticación, es posible acortar el access-accept del proceso completo y de la vuelta inmediatamente después del aprovisionamiento PAC.

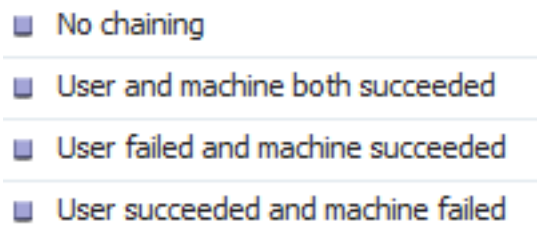
La segunda opción construye el túnel de TLS basado en el certificado del cliente (ésta requiere el despliegue PKI en los puntos finales). Esto permite que el túnel de TLS sea construido con la autenticación recíproca, que salta el método interno y va directamente a la fase del aprovisionamiento PAC. Es importante tener cuidado aquí - el supplicant presentará a veces un certificado que no sea confiado en por el ISE (previsto para otros fines) y la sesión fallará.

EAP-encadenamiento

Permite la autenticación del usuario y de la máquina dentro de una sesión Radius/EAP. Los métodos EAP múltiples se pueden encadenar juntos. Después de que la primera autenticación (típicamente máquina) haya acabado con éxito, el servidor enviará un Intermedio-resultado TLV (túnel de TLS del interior) que indica el éxito. Ese TLV se debe acompañar por una petición Crypto-obligatoria TLV. Cryptobinding se utiliza para probar que el servidor y el par han participado en la secuencia específica de autenticaciones. El proceso de Cryptobinding utiliza el material de codificación a partir de la fase 1 y de la fase 2. Además, se asocia un más TLV: EAP-payload - esto está iniciando la nueva sesión (típicamente para el usuario). Una vez que el servidor de RADIUS (ISE) recibe la respuesta Crypto-obligatoria TLV y la valida, lo que sigue será mostrado en el registro y el método EAP siguiente será intentado (típicamente para la autenticación de usuario):

12126 **EAP-FAST cryptobinding verification passed**

Si la validación cryptobinding falla, la sesión entera EAP falla. Si una de las autenticaciones dentro de fallado entonces le es todavía fina - como consecuencia, el ISE permite que un administrador configure el múltiplo que encadena los resultados basados en la condición NetworkAccess de la autorización: EapChainingResult:

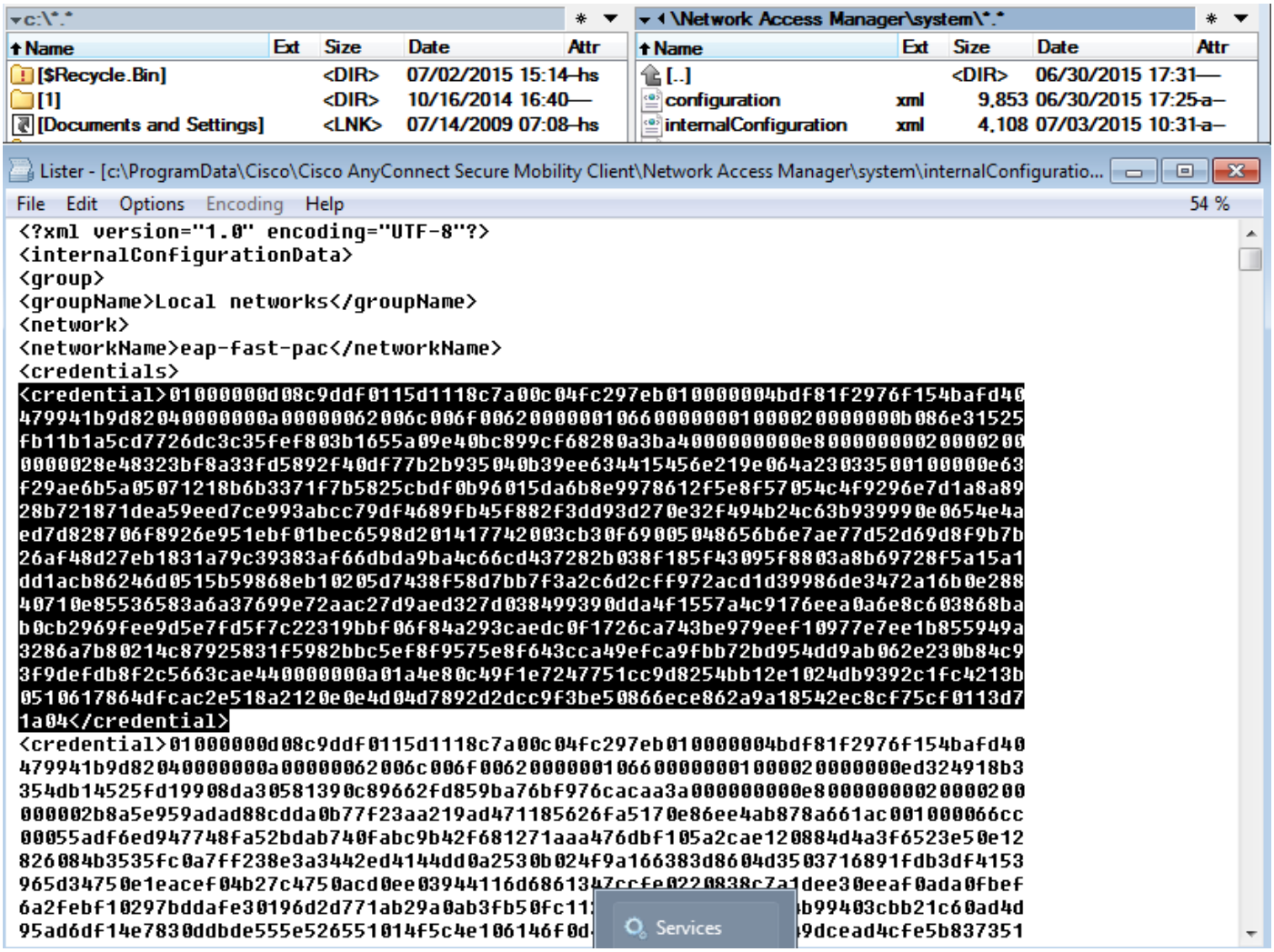


El EAP-encadenamiento se habilita en el NAM automáticamente cuando se habilita la autenticación del usuario y de la máquina del EAP-FAST.

El EAP-encadenamiento se debe configurar en el ISE.

Donde se salvan los archivos PAC

Por abandono, el túnel y la máquina PAC se salvan en el cliente de la movilidad de C:\ProgramData\Cisco\Cisco AnyConnect \ el administrador del acceso a la red \ el sistema seguros \ internalConfiguration.xml en el <credential> de las secciones. Ésos se salvan en la forma encriptada.

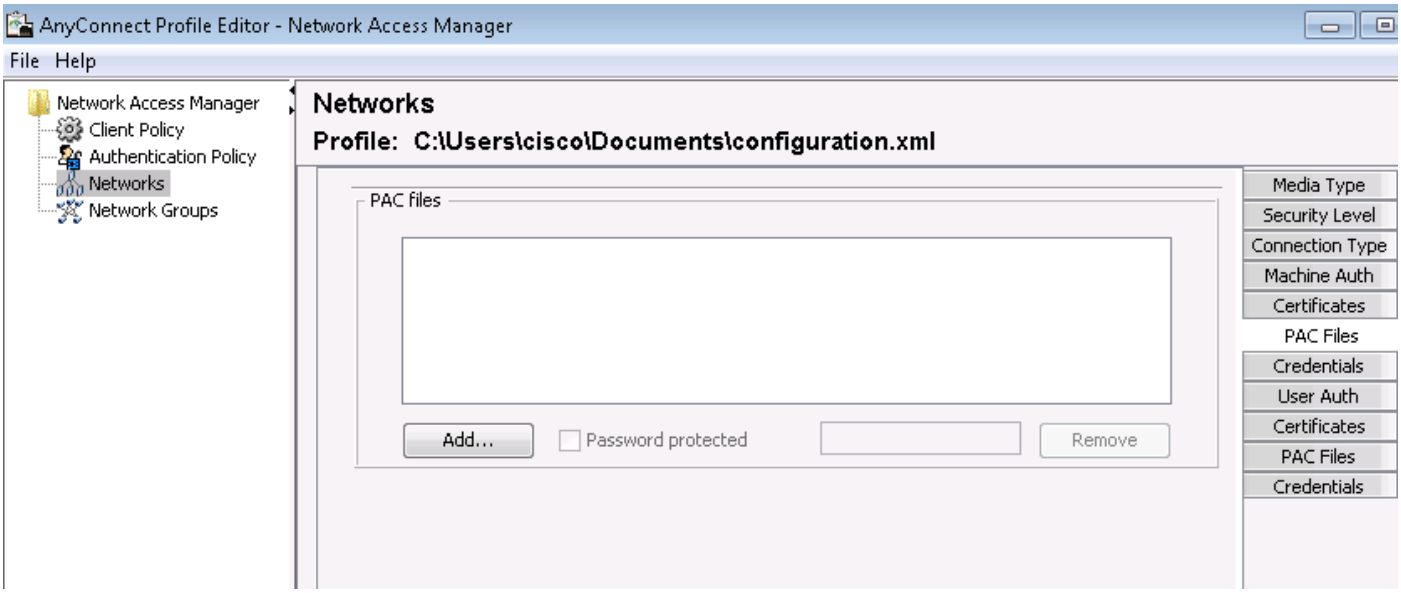


La autorización PAC se salva solamente en la memoria y se quita después de que reinicialización o reinicio del servicio NAM.

Un reinicio del servicio se requiere para quitar el túnel o la máquina PAC.

AnyConnect NAM 3.1 contra 4.0

El editor del perfil de AnyConnect 3.x NAM permitió que el administrador configurara los PAC manualmente. Esta característica se ha quitado del editor del perfil de AnyConnect 4.x NAM.

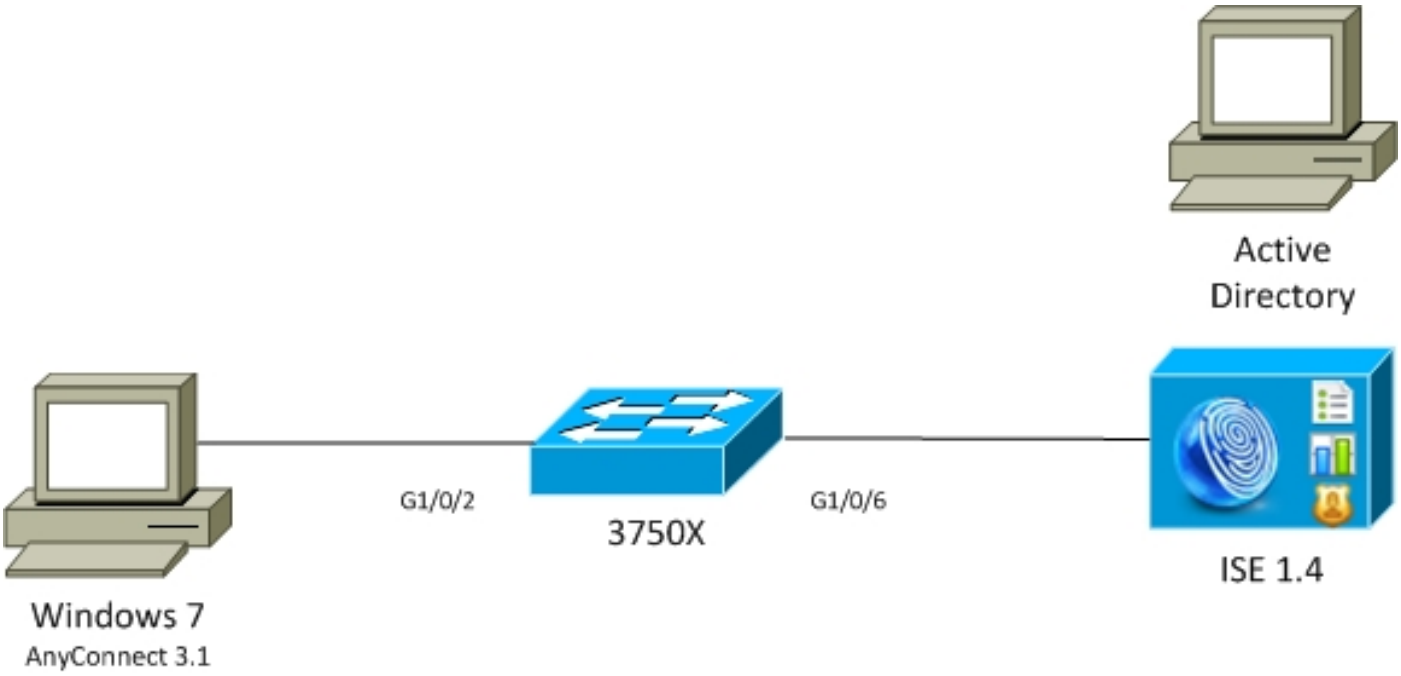


La decisión a quitar que las funciones están basadas en CSCuf31422 y CSCua13140.

Ejemplos

Diagrama de la red

Todos los ejemplos fueron probados usando la topología de red siguiente. Lo mismo se aplica también al usar la Tecnología inalámbrica.



EAP-rápido sin el EAP que encadena con el usuario y la máquina PAC

Por abandono, EAP_chaining se inhabilita en el ISE. Sin embargo, todas las otras opciones se habilitan incluyendo la máquina y la autorización PAC. El supplicant tiene ya una máquina y un túnel válidos PAC. En este flujo, habrá dos autenticaciones separadas - una para la máquina y una para el usuario - con separado abre una sesión el ISE. Los pasos principales según lo registrado por el ISE. Primera autenticación (máquina):

- El supplicant envía los saludos del cliente de TLS con la máquina PAC.
- El servidor valida la máquina PAC y construye el túnel de TLS (ningunos Certificados usados).
- El servidor valida la máquina PAC y realiza las operaciones de búsqueda de la cuenta en el Active Directory y salta el método interno.

```
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 segunda autenticación (usuario):

- El supplicant envía los saludos del cliente de TLS con el túnel PAC.
- El servidor valida el PAC y construye el túnel de TLS (ningunos Certificados usados).
- Pues el supplicant no tiene ninguna autorización PAC, el método interno (EAP-MSCHAP) se utiliza para la autenticación.

```
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
```

En la sección de “otros atributos” del informe detallado en el ISE, lo que sigue se observa para las autenticaciones del usuario y de la máquina:

```
EapChainingResult: No chaining
```

EAP-rápido con el EAP que encadena con el PAC rápidamente vuelva a conectar

En este flujo, el supplicant tiene ya un túnel válido PAC junto con la autorización PAC del usuario y de la máquina:

- El supplicant envía los saludos del cliente de TLS con el túnel PAC.
- El servidor valida el PAC y construye el túnel de TLS (ningunos Certificados usados).
- El ISE enciende el encadenamiento EAP, la autorización PAC de los attaches del supplicant para el usuario y la máquina usando el TLV dentro del túnel de TLS.
- El ISE valida la autorización PAC (ningún método interno necesario), verifica que las cuentas existen en el Active Directory (ninguna autenticación adicional), éxito de las devoluciones.

```
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
```

En la sección de “otros atributos” del informe detallado en el ISE, se observa lo que sigue:

```
EapChainingResult: EAP Chaining
```

Además, las credenciales del usuario y de la máquina se incluyen en el mismo registro según lo visto abajo:

```
EapChainingResult: EAP Chaining
```

EAP-rápido con el EAP que encadena sin el PAC

En este flujo, el NAM se configura para no utilizar un PAC, el ISE también se configura para no utilizar el PAC (pero con el encadenamiento EAP)

- El supplicant envía los saludos del cliente de TLS sin el túnel PAC.
- El servidor responde con las cargas útiles del certificado y del pedido de certificado de TLS.
- Se construye el supplicant debe certificado de servidor de confianza, no enviará ningún certificado del cliente (el payload del certificado es cero), túnel de TLS.
- El ISE envía una petición TLV el certificado del cliente dentro del túnel de TLS, pero el supplicant no hace (no es necesario tenerlo para continuar).
- Comienzo EAP que encadena para el usuario, usando el método interno con la autenticación del MSCHAPv2.

- Continúa con la autenticación de la máquina, usando el método interno con la autenticación del MSCHAPv2.
- No hay PAC aprovisionado.

```
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-rápido con el EAP que encadena la expiración de la autorización PAC

En este flujo, el supplicant tiene un túnel válido PAC pero tiene autorización expirada PAC:

- El supplicant envía los saludos del cliente de TLS con el túnel PAC.
- El servidor valida el PAC y construye el túnel de TLS (ningunos Certificados usados).
- El ISE enciende el encadenamiento EAP, la autorización PAC de los attaches del supplicant para el usuario y la máquina usando el TLV dentro del túnel de TLS.
- Mientras que se expiran los PAC, el método interno para el usuario y la máquina se comienza (EAP-MSCHAP).

- Una vez que ambas autenticaciones son acertadas, el usuario y la autorización PAC de la máquina son aprovisionado.

```
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-rápido con el EAP el encadenamiento del túnel PAC expiró

En este flujo cuando existe ningún túnel válido PAC, la negociación completa de TLS con la fase interna ocurre.

- El supplicant envía los saludos del cliente de TLS sin el túnel PAC.
- El servidor responde con las cargas útiles del certificado y del pedido de certificado de TLS.
- El supplicant debe certificado de servidor de confianza, no enviará el certificado del cliente (el payload del certificado es cero), túnel de TLS construido.
- El ISE envía la petición TLV el certificado del cliente dentro del túnel de TLS, pero el supplicant no hace (no es necesario tenerlo para continuar).
- Comienzo EAP que encadena para el usuario, usando el método interno con la autenticación del MSCHAPv2.
- Continúa con la autenticación de la máquina, usando el método interno con la autenticación del MSCHAPv2.
- Con éxito aprovisionado todos los PAC (habilitados en los 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

EAP-rápido con el encadenamiento EAP y el aprovisionamiento anónimo del túnel PAC de TLS

En este flujo, el túnel anónimo ISE y NAM TLS se configura para los parecer de la petición del aprovisionamiento del aprovisionamiento PAC (el túnel autenticado ISE para el aprovisionamiento PAC se inhabilita) PAC de TLS:

- El supplicant envía los saludos del cliente de TLS sin los ciphersuites múltiples.

- El servidor responde con las cifras anónimas de los saludos del servidor de TLS y del Diffie Hellman de TLS (por ejemplo TLS_DH_anon_WITH_AES_128_CBC_SHA).
- El supplicant lo valida y se construye el túnel anónimo de TLS (ningunos Certificados intercambiados).
- Comienzo EAP que encadena para el usuario, usando el método interno con la autenticación del MSCHAPv2.
- Continúa con la autenticación de la máquina, usando el método interno con la autenticación del MSCHAPv2.
- Puesto que se está construyendo el túnel anónimo de TLS la autorización PAC no se permite.
- El rechazo del radio se vuelve al supplicant de la fuerza para reauthenticate (usando el aprovisionado 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
```

Capturas de paquetes de Wireshark para la negociación de túnel anónima de TLS:

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-rápido con el EAP que encadena la autenticación de usuario solamente

En este flujo, AnyConnect NAM con la autenticación del EAP-FAST y del usuario (EAP-TLS) y de la máquina (EAP-TLS) se configura. Se inicia el PC de Windows pero los credenciales de usuario no se proporcionan. El Switch inicia la sesión del 802.1x, NAM debe responder sin embargo, los credenciales de usuario no se proporciona, (ningún acceso al almacén y al certificado del usuario con todo) por lo tanto. la autenticación de usuario fallará mientras que la máquina será acertada - acceso a la red de la condición del authz ISE “: El usuario de los IGUALES de EapChainingResult falló y la máquina tenida éxito” se satisface. Más adelante, el usuario abre una sesión y otra autenticación comenzará, usuario y la máquina tendrá éxito.

- El supplicant envía los saludos del cliente de TLS con la máquina PAC.
- El servidor responde con espec. de la cifra del cambio de TLS - túnel de TLS es inmediatamente estructura basada en ese PAC.
- El ISE inicia el EAP que encadena y que pide la Identificación del usuario.

- El supplicant proporciona la identidad de la máquina en lugar de otro (usuario no todavía listo), método interno del EAP-TLS de los finales.
- El ISE pide la Identificación del usuario otra vez, supplicant no puede proporcionarlo.
- El ISE envía el TLV con el resultado = el error intermedios (para la autenticación de usuario).
- El ISE devuelve el Mensaje de éxito final EAP, acceso a la red de la condición ISE: El usuario de los IGUALES de EapChainingResult falló y la máquina tenida éxito se satisface.

```
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-rápido con el encadenamiento EAP y las Configuraciones del túnel anónimas contrarias de TLS

En este flujo, el ISE se configura para el PAC provisioning solamente vía el túnel anónimo de TLS, pero el NAM está utilizando un túnel autenticado de TLS, el siguiente será registrado por el 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
```

Esto ocurre cuando el NAM está intentando construir un túnel autenticado de TLS con él es cifras speciphic de TLS - y ésos no son validados por el ISE que se configura para el túnel anónimo de TLS (que valida las cifras DH solamente)

Troubleshooting

ISE

Para los registros detallados, los debugs Runtime-AAA se deben habilitar en el nodo correspondiente PSN. Abajo están algunos registros del ejemplo de prrt-server.log:

Generación de la máquina 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
```

Aprobación de la petición PAC:

```
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
```

Validación PAC:

```
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
```

Ejemplo del resumen acertado para la generación PAC:

```
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
```

Ejemplo del resumen acertado para la validación PAC:

```
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

Los registros del DARDO del NAM proporcionan los detalles siguientes:

El ejemplo para no EAP-encadenar la sesión, autenticación de la máquina sin rápido vuelve a conectar:

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

Ejemplo de las operaciones de búsqueda de la autorización PAC (autenticación de la máquina para la sesión no de EAP-encadenamiento):

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

Todos los estados del método interno (para el MSCHAP) se pueden verificar de los registros abajo:

```
 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
```

El NAM permite la configuración de la característica de registro extendida que capturará todos los paquetes EAP y los salvará en el archivo del pcap. Esto es especialmente útil para el comienzo antes de las funciones del inicio (los paquetes EAP se capturan incluso para las autenticaciones que ocurren antes de que inicio del usuario). Para la activación de la característica pregunte a su ingeniero de TAC.

Referencias

- El guía del administrador del Cliente de movilidad Cisco AnyConnect Secure, libera la

configuración del EAP-FAST 4.0

- El guía del administrador del Cisco Identity Services Engine, libera 1.4 recomendaciones del EAP-FAST
- Guías de diseño del Cisco Identity Services Engine
- EAP que despliega que encadena con AnyConnect NAM y Cisco ISE
- Soporte Técnico y Documentación - Cisco Systems