

# Compreensão EAP-FAST e encadeamento de aplicações em AnyConnect NAM e ISE

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Teoria](#)

[Fases](#)

[PAC](#)

[Quando os PAC forem gerados](#)

[Chave mestre EAP-FAST ACS 4.x do server contra ACS 5x e ISE](#)

[Resumo da sessão](#)

[Estado do servidor](#)

[Apátrida \(PAC baseado\)](#)

[Aplicação de AnyConnect NAM](#)

[Abastecimento PAC \(fase 0\)](#)

[Túnel anônimo TLS](#)

[Túnel autenticado TLS](#)

[EAP-encadeamento](#)

[Onde os arquivos PAC são armazenados](#)

[AnyConnect NAM 3.1 contra 4.0](#)

[Exemplos](#)

[Diagrama de Rede](#)

[EAP-rápido sem EAP que acorrenta com usuário e máquina PAC](#)

[EAP-rápido com o EAP que acorrenta com PAC reconecte rapidamente](#)

[EAP-rápido com o EAP que acorrenta sem PAC](#)

[EAP-rápido com o EAP que acorrenta a expiração da autorização PAC](#)

[EAP-rápido com EAP acorrentar o túnel PAC expirou](#)

[EAP-rápido com encadeamento EAP e abastecimento anônimo do túnel PAC TLS](#)

[EAP-rápido com o EAP que acorrenta a autenticação de usuário somente](#)

[EAP-rápido com encadeamento EAP e configurações de túnel anônimas incompatíveis TLS](#)

[Troubleshooting](#)

[ISE](#)

[AnyConnect NAM](#)

[Referências](#)

## Introdução

Este artigo explica detalhes em relação às aplicações EAP-FAST no gerente do acesso de rede de Cisco AnyConnect (NAM) e no Identity Services Engine (ISE). Explica mais como as características específicas trabalham junto e fornece casos típicos e exemplos do uso.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da estrutura EAP e de métodos EAP-FAST
- Conhecimento básico do Identity Services Engine (ISE)
- Conhecimento básico de AnyConnect NAM e de editor do perfil
- Conhecimento básico da configuração do Cisco catalyst para serviços do 802.1x

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Windows 7 com Cliente de mobilidade Cisco AnyConnect Secure, libera 3.1 e 4.0
- Cisco Catalyst 3750X Switch com software 15.2.1 e mais atrasado
- Cisco ISE, liberação 1.4

## Teoria

### Fases

EAP-FAST é um método de EAP flexível que permita a autenticação mútua de um suplicante e de um server. É similar a EAP-PEAP, mas tipicamente não exige o uso do cliente ou mesmo dos certificados de servidor. Uma vantagem de EAP-FAST é a capacidade para acorrentar as autenticações múltiplas (que usam métodos internos múltiplos) e para ligá-las criptograficamente junto (EAP que acorrenta). As implementações Cisco usam esta para autenticações do usuário e da máquina.

EAP-FAST utiliza as credenciais protegidas do acesso (PAC) a fim estabelecer rapidamente o túnel TLS (resumo da sessão) ou autorizar o usuário/máquina (método de autenticação interno da faixa clara).

Há 3 fases para EAP-FAST:

- fase 0 (abastecimento PAC)
- fase 1 (estabelecimento de túnel TLS)
- fase 2 (autenticação)

Apoios EAP-FAST PAC-menos e conversação PAC-baseada. PAC-baseado consiste no abastecimento PAC e na autenticação PAC-baseada. O abastecimento PAC pode ser baseado na sessão anônima ou autenticada TLS.

### PAC

O PAC é credenciais protegidas do acesso geradas pelo server e desde que ao cliente. Consiste:

- Chave PAC (valor secreto aleatório, usado para derivar o mestre e as chaves de sessão TLS)

- PAC opaco (chave PAC + identidade do usuário - cifrada toda pelo chave mestre EAP-FAST do server)
- Informação PAC (identidade do server, temporizadores TTL)

O server que emite o PAC cifrará a chave e a identidade PAC usando o chave mestre EAP-FAST do server (de que é PAC opaco) e envia o PAC inteiro ao cliente. Não faz manter-se/loja nenhuma outra informação (exceto o chave mestre que é o mesmo para todos os PAC).

Uma vez que o PAC opaco é recebido, está decifrado usando o chave mestre EAP-FAST do server e validado. A chave PAC é usada para derivar o mestre TLS e as chaves de sessão para um TLS abreviado escavam um túnel.

Os chaves mestres EAP-FAST novos do server são gerados quando o chave mestre precedente expira. Em alguns casos, um chave mestre pode ser revogado.

Há alguns tipos de PAC que estão sendo usados atualmente:

- Túnel PAC: usado para o estabelecimento de túnel TLS (sem a necessidade de cliente ou de certificado de servidor). Enviado em hellos do cliente TLS
- Máquina PAC: usado para o estabelecimento de túnel TLS e a autorização imediata da máquina. Enviado em hellos do cliente TLS
- Autorização de usuário PAC: usado para a autenticação de usuário imediata (método interno da faixa clara) se permitido pelo server. Túnel interno enviado TLS usando o TLV.
- Autorização PAC da máquina: usado para a autenticação imediata da máquina (método interno da faixa clara) se permitido pelo server. Túnel interno enviado TLS usando o TLV.
- Trustsec PAC: usado para a autorização quando a execução ambiental ou a política refrescarem.

Todos aqueles PAC são entregados geralmente automaticamente na fase 0. Alguns dos PAC (túnel, máquina, Trustsec) podem igualmente ser entregados manualmente.

### Quando os PAC forem gerados

- Túnel PAC: fornecida após uma autenticação bem sucedida (método interno) se não usou-se previamente.
- Autorização PAC: fornecida após a autenticação bem sucedida (método interno) se não usou-se previamente.
- Máquina PAC: fornecida após a autenticação bem sucedida da máquina (método interno) se não usou-se previamente e quando uma autorização PAC não for usada. Provisioned quando o túnel PAC expira; contudo, não quando a autorização PAC expirar. Será fornecida quando EAP-acorrentar é permitido ou desabilitado.

Nota:

Cada abastecimento PAC exige a autenticação bem sucedida a não ser que do seguinte exemplo do uso: o usuário autorizado pede a máquina PAC para uma máquina que não tenha uma conta AD.

A tabela a seguir resume o abastecimento e a funcionalidade dinâmica da atualização:

Tipo PAC	Túnel v1/v1a/CTS	Máquina	Autorização
Forneça o PAC a pedido no abastecimento	sim	somente no abastecimento autenticado	somente no abastecimento autenticado e se o túnel

Forneça o PAC a pedido na autenticação	sim	sim	PAC é pedido igualmente somente se não foi usado nesta autenticação
Atualização dinâmica	sim	não	não
Ao cair de volta ao abastecimento PAC após a autenticação PAC-baseada falhada (por exemplo quando o PAC for expirado)	a rejeição e não fornece o novo	a rejeição e não fornece o novo	a rejeição e não fornece o novo
Apoio ACS 4.x PAC	para o túnel PAC v1/v1a	sim	não

## Chave mestre EAP-FAST ACS 4.x do server contra ACS 5x e ISE

Há uma pequena diferença no chave mestre que segura ao comparar ACS 4.x e ISE

Recurso	ACS 4.1.2	ACS 5.x/ISE
Chave mestre	O chave mestre tem o TTL, pode ser ativo, aposentado ou expirado	O chave mestre é gerado automaticamente da semente em cada período configurado de tempo. O chave mestre específico é sempre acessível e então nunca expirado
O PAC refresca	A atualização PAC está enviada pelo server quando o PAC está expirado, a menos que o chave mestre usado para a criptografia PAC estiver expirado	A atualização PAC é enviada pelo server após a primeira autenticação bem sucedida que é executada no período configurável específico de tempo antes do momento da expiração PAC.

Ou seja o ISE manterá todas as chaves de mestre antigo e gerará um novo à revelia uma vez pela semana. Porque o chave mestre não pode expirar, simplesmente o PAC TTL será validado.

O período da geração de chave mestre ISE é configurado da *administração - > ajustes - > protocolo - > EAP-FAST - > ajustes EAP-FAST*.

## Resumo da sessão

Este é um componente importante permitindo o uso do túnel PAC. Permite a negociação nova do túnel TLS sem uso dos Certificados.

Há dois tipos do resumo da sessão para EAP-FAST: Estado do servidor baseado e apátrida (PAC baseado).

## Estado do servidor

O método baseado TLS do padrão é baseado no TLS SessionID posto em esconderijo no server. O cliente que envia os hellos do cliente TLS anexa o SessionID a fim recomençar a sessão. A sessão é usada somente para o abastecimento PAC ao usar um túnel anônimo 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 baseado)

A autorização PAC do usuário/máquina é usada armazenar os estados precedentes da authentication e autorização para o par.

O resumo do lado do cliente é baseado no RFC 4507. O server não precisa de pôr em esconderijo nenhuns dados; em lugar do cliente anexa o PAC na extensão de SessionTicket dos hellos do cliente TLS. Por sua vez, o PAC é validado pelo server. Exemplo baseado no túnel PAC entregue ao server:

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

Secure Sockets Layer

▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 281

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 277

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 0

Cipher Suites Length: 52

▷ Cipher Suites (26 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

Extensions Length: 184

▼ Extension: SessionTicket TLS

Type: SessionTicket TLS (0x0023)

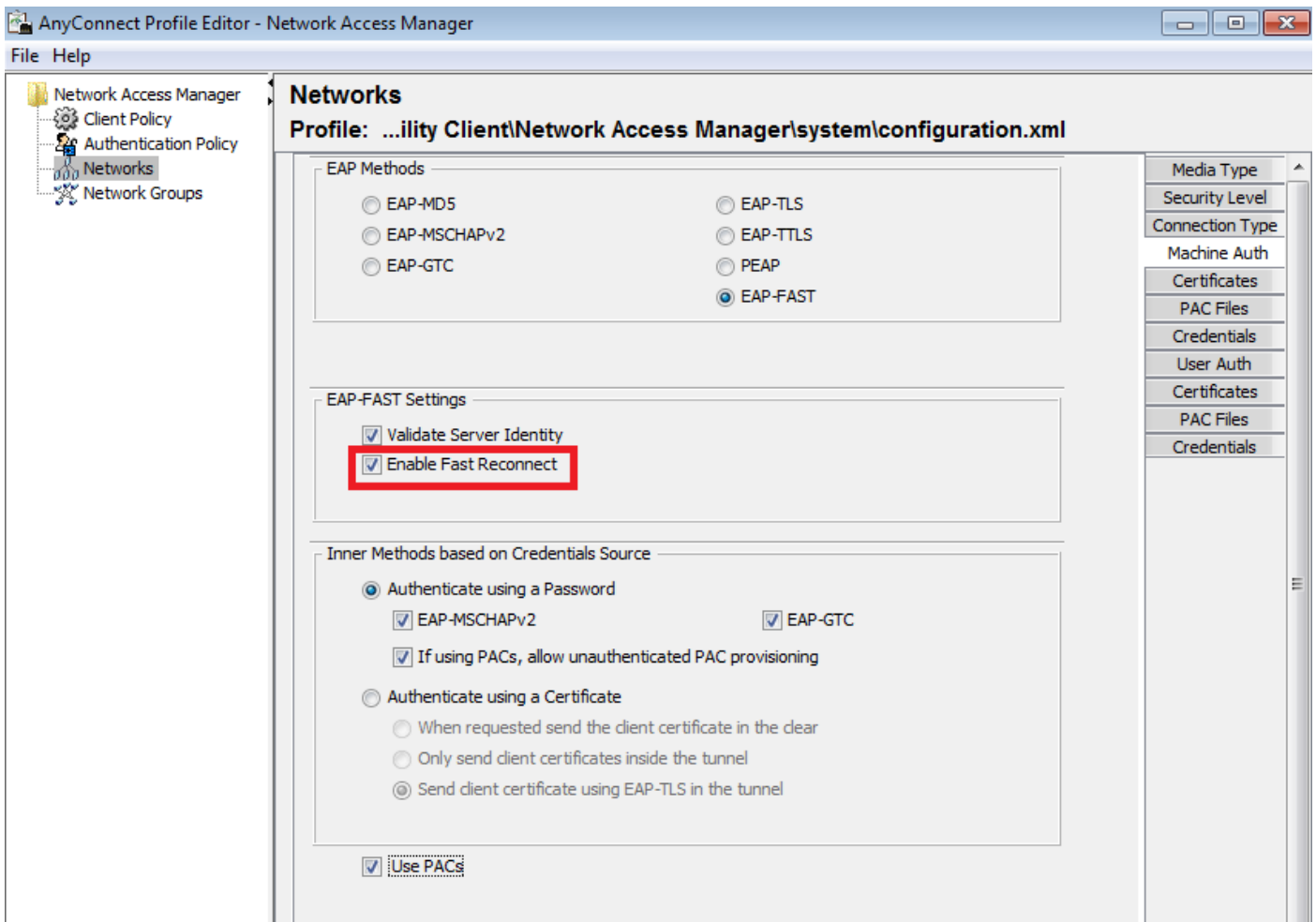
Length: 180

Data (180 bytes)

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

## Aplicação de AnyConnect NAM

Permitiu no cliente que o lado (AnyConnect NAM) através de rápido reconecta - mas usou-se para controlar somente o uso da autorização PAC.



Com o ajuste desabilitado, o NAM ainda usará o túnel PAC para construir o túnel TLS ( nenhuns Certificados necessários). Contudo, isto não usará a autorização PAC a fim executar a autorização imediata do usuário e da máquina. Em consequência, a fase 2 com o método interno será exigida sempre.

O ISE tem uma opção para permitir o resumo apátrida da sessão. E como no NAM é apenas para a autorização PAC. O uso do túnel PAC é controlado com opções “uso PAC”.

Allow EAP-FAST

EAP-FAST Inner Methods


Allow EAP-MS-CHAPv2

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-TLS

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

Use PACs  Don't Use PACs

Tunnel PAC Time To Live

Proactive PAC update will occur after  % of PAC Time To Live has expired

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning


Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

Allow Machine Authentication

Machine PAC Time To Live

Enable Stateless Session Resume

Authorization PAC Time To Live   

Enable EAP Chaining

Preferred EAP Protocol

O NAM tentará usar PAC se a opção é permitida. Se “não use PAC” é configurado no ISE e no ISE recebe um túnel PAC na extensão que TLS o seguinte erro estará relatado e uma falha EAP é retornada:

introduza aqui

No ISE, é igualmente necessário permitir o resumo da sessão baseado em TLS SessionID (dos ajustes EAP-FAST globais). Desabilite a revelia:

## EAP FAST Settings

\* Authority Identity Info Description

\* Master Key Generation Period

Revoke all master keys and PACs

## PAC-less Session Resume

Enable PAC-less Session Resume

\* PAC-less Session Timeout



Mantenha por favor na mente que somente um tipo de resumo da sessão pode ser usado. SessionID baseado é usado somente para as disposições PAC-menos, RFC 4507 baseado é usado somente para disposições PAC.

## Abastecimento PAC (fase 0)

Os PAC podem ser automaticamente fornecida em phase0. A fase 0 consiste:

- Estabelecimento de túnel TLS
- Autenticação (método interno)

Os PAC são entregados após uma autenticação bem sucedida dentro do túnel TLS através do reconhecimento PAC TLV (e PAC TLV)

## Túnel anônimo TLS

Para disposições sem uma infraestrutura PKI, é possível usar um túnel anônimo TLS. O túnel anônimo TLS será construído usando a série da cifra do Diffie Hellman - sem a necessidade de um server ou de um certificado de cliente. Esta aproximação é homem inclinado nos ataques médios (personificação).

Para usar esta opção, o NAM exige a seguinte opção configurada:

“Se usando PAC permita o abastecimento não-autenticado PAC” (que faz o sentido somente para o método interno senha-baseado porque sem infraestrutura PKI não é possível usar o método interno certificado-baseado).

Também, o ISE precisará o seguinte configurado sob a autenticação permitida protocolos:

“Permita o abastecimento anônimo da Em-faixa PAC”

O abastecimento anônimo da em-faixa PAC está sendo usado em disposições NDAC de TrustSec (sessão EAP-FAST negociada entre dispositivos de rede).

## Túnel autenticado TLS

Esta é a opção a mais segura e a mais recomendada. O túnel TLS é construído com base no certificado de servidor que é validado pelo suplicante. Isto exige uma infraestrutura PKI no lado de servidor somente, que é exigido para o ISE (no NAM é possível desabilitar a opção “valida a identidade do server”).

Para o ISE há duas opções adicionais:

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

Normalmente, após o abastecimento PAC, uma Rejeição de acesso deve ser enviada forçando o suplicante a reauthenticate usando PAC. Mas desde que os PAC foram entregados no túnel TLS com autenticação, é possível encurtar a aceitação de acesso do processo inteiro e do retorno

imediatamente depois do abastecimento PAC.

A segunda opção constrói o túnel TLS baseado no certificado de cliente (esta exige o desenvolvimento PKI nos valores-limite). Isto permite que o túnel TLS seja construído com autenticação mútua, que salta o método interno e vai diretamente à fase do abastecimento PAC. É importante ser cuidadoso aqui - às vezes o suplicante apresentará um certificado que não seja confiável pelo ISE (pretendido para outros fins) e a sessão falhará.

## EAP-encadeamento

Permite a autenticação do usuário e da máquina dentro de uma sessão Radius/EAP. Os métodos de EAP múltiplos podem ser acorrentados junto. Depois que a primeira autenticação (tipicamente máquina) terminou com sucesso, o server enviará um Intermediário-resultado TLV (túnel do interior TLS) que indica o sucesso. Esse TLV deve ser acompanhado de um pedido Cripto-obrigatório TLV. Cryptobinding é usado para mostrar que o server e o par participaram na sequência específica das autenticações. O processo de Cryptobinding usa o material de ajuste da fase 1 e da fase 2. Adicionalmente, um mais TLV é anexado: EAP-payload - isto está iniciando a sessão nova (tipicamente para o usuário). Uma vez que o servidor Radius (ISE) recebe a resposta Cripto-obrigatória TLV e a valida, o seguinte estará mostrado no log e o método de EAP seguinte será tentado (tipicamente para a autenticação de usuário):

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

Se a validação cryptobinding falha, a sessão inteira EAP falha. Se uma das autenticações dentro do falhado então lhe é ainda fina - em consequência, o ISE permite que um administrador configure o encadeamento do múltiplo baseado em resultados na condição NetworkAccess da autorização: EapChainingResult:

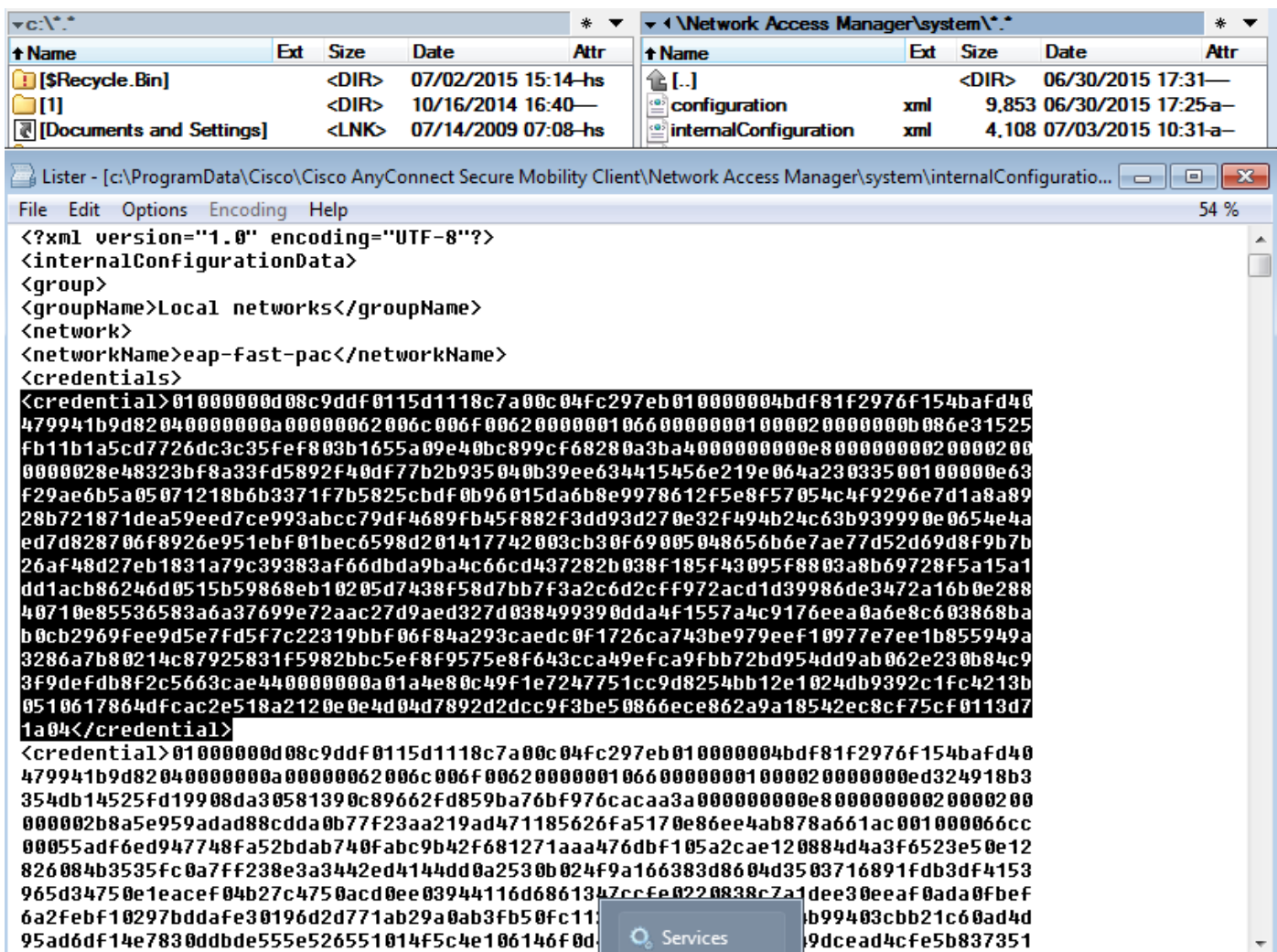
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-acorrentar está permitido no NAM automaticamente quando a autenticação EAP-FAST do usuário e da máquina é permitida.

EAP-acorrentar deve ser configurado no ISE.

## Onde os arquivos PAC são armazenados

À revelia, o túnel e a máquina PAC são armazenados no cliente da mobilidade de C:\ProgramData\Cisco\Cisco AnyConnect \ gerente do acesso de rede \ sistema seguros \ internalConfiguration.xml no <credential> das seções. Aquelas são armazenados no formulário criptografado.

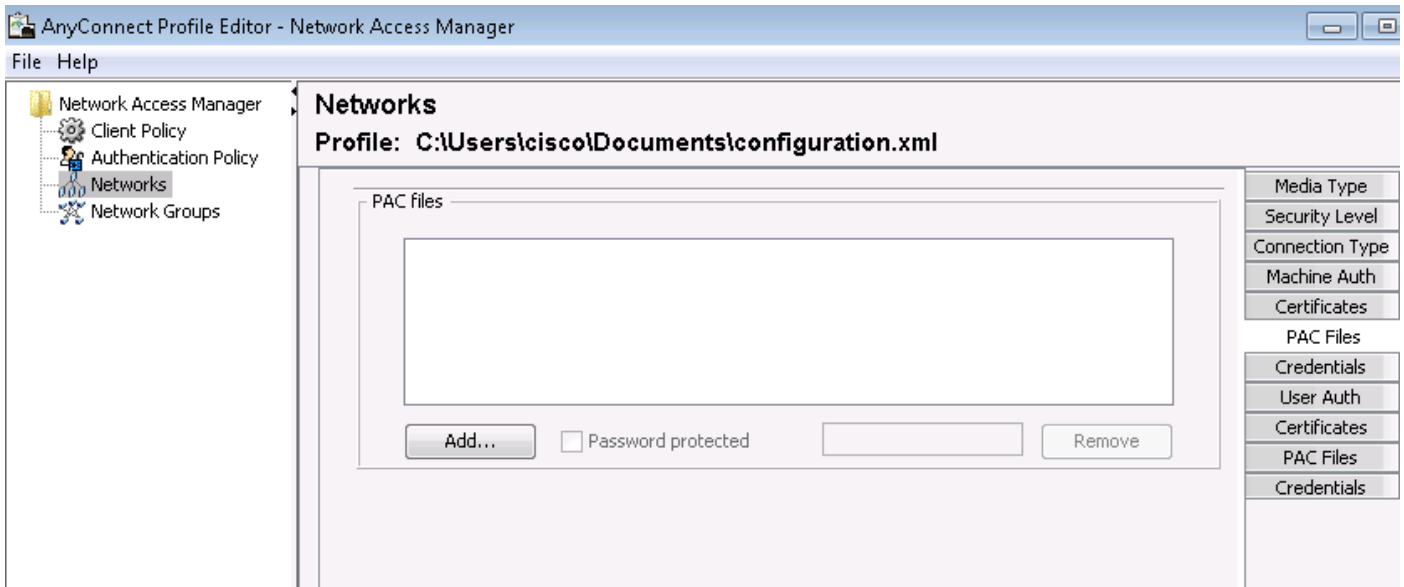


A autorização PAC é armazenada somente na memória e removida depois que repartição ou de serviço NAM reinício.

Um reinício do serviço é exigido para remover o túnel ou a máquina PAC.

## AnyConnect NAM 3.1 contra 4.0

O editor do perfil de AnyConnect 3.x NAM permitiu que o administrador configurasse PAC manualmente. Esta característica foi removida do editor do perfil de AnyConnect 4.x NAM.

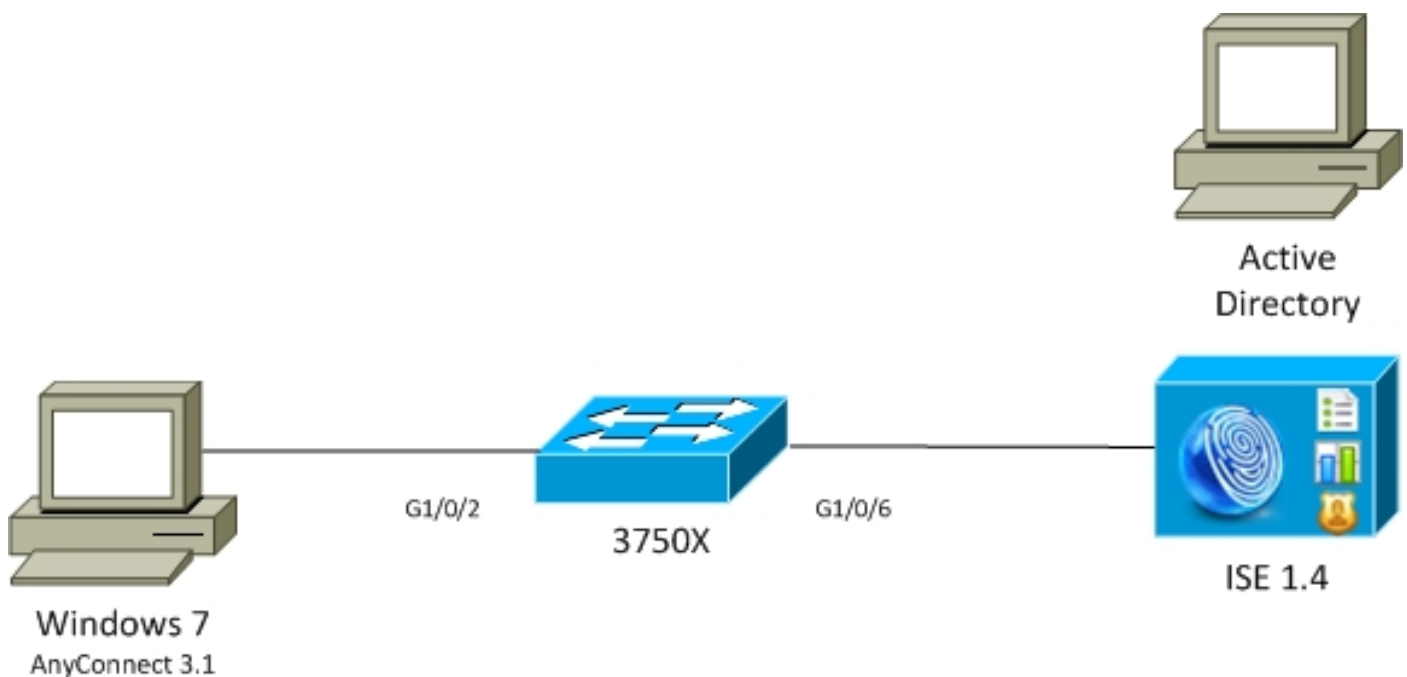


A decisão a remover que a funcionalidade está baseada em [CSCuf31422](#) e em [CSCua13140](#).

## Exemplos

### Diagrama de Rede

Todos os exemplos foram testados usando a seguinte topologia de rede. O mesmo aplica-se igualmente ao usar o Sem fio.



### EAP-rápido sem EAP que acorrenta com usuário e máquina PAC

À revelia, EAP\_chaining é desabilitado no ISE. Contudo, todas as outras opções são permitidas que incluem a máquina e a autorização PAC. O suplicante já tem uma máquina e um túnel válidos PAC. Neste fluxo, haverá duas autenticações separadas - uma para a máquina e uma para o usuário - com separado entra o ISE. As etapas principais como registradas pelo ISE. Primeira autenticação (máquina):

- O suplicante envia hellos do cliente TLS com máquina PAC.
- O server valida a máquina PAC e constrói o túnel TLS ( nenhuns Certificados usados).
- O server valida a máquina PAC e executa a consulta da conta no diretório ativo e salta o 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

**A segunda autenticação (usuário):**

- O suplicante envia os hellos do cliente TLS com túnel PAC.
- O server valida o PAC e constrói o túnel TLS ( nenhuns Certificados usados).
- Porque o suplicante não tem nenhuma autorização PAC, o método interno (EAP-MSCHAP) é usado para a autenticação.

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

De “na seção outros atributos” do relatório detalhado no ISE, o seguinte é notado para autenticações do usuário e da máquina:

EapChainingResult: **No chaining**

## **EAP-rápido com o EAP que acorrenta com PAC reconecte rapidamente**

Neste fluxo, o suplicante já tem um túnel válido PAC junto com a autorização PAC do usuário e

da máquina:

- O suplicante envia os hellos do cliente TLS com túnel PAC.
- O server valida o PAC e constrói o túnel TLS ( nenhuns Certificados usados).
- O ISE começa o EAP acorrentar, o suplicante anexa a autorização PAC para o usuário e a máquina usando o TLV dentro do túnel TLS.
- O ISE valida a autorização PAC (nenhum método interno necessário), verifica que as contas existem no diretório ativo (nenhuma autenticação adicional), sucesso dos retornos.

```
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
```

De “na seção outros atributos” do relatório detalhado no ISE, o seguinte é notado:

```
EapChainingResult: EAP Chaining
```

Adicionalmente, as credenciais do usuário e da máquina são incluídas no mesmo log que consideradas abaixo:

```
EapChainingResult: EAP Chaining
```

## **EAP-rápido com o EAP que acorrenta sem PAC**

Neste fluxo, o NAM é configurado para não usar um PAC, o ISE é configurado igualmente para não usar o PAC (mas com encadeamento EAP)

- O suplicante envia hellos do cliente TLS sem túnel PAC.
- O server responde com as cargas úteis do certificado e do pedido do certificado TLS.
- O suplicante deve certificado de servidor de confiança, não enviará nenhum certificado de cliente (o payload do certificado é zero), túnel TLS é construído.
- O ISE envia um pedido TLV para o certificado de cliente dentro do túnel TLS, mas o suplicante não faz (não é necessário o ter a fim continuar).
- Começos EAP que acorrentam para o usuário, usando o método interno com autenticação MSCHAPv2.
- Continua com autenticação da máquina, usando o método interno com autenticação

## MSCHAPv2.

- Nenhum PAC está sendo fornecida.

```
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 com o EAP que acorrenta a expiração da autorização PAC

Neste fluxo, o suplicante tem um túnel válido PAC mas tem a autorização expirada PAC:

- O suplicante envia os hellos do cliente TLS com túnel PAC.
- O server valida o PAC e constrói o túnel TLS ( nenhuns Certificados usados).
- O ISE começa o EAP acorrentar, o suplicante anexa a autorização PAC para o usuário e a máquina usando o TLV dentro do túnel TLS.
- Enquanto os PAC são expirados, o método interno para o usuário e a máquina está começado (EAP-MSCHAP).
- Uma vez que ambas as autenticações são bem sucedidas, o usuário e a autorização PAC da

máquina são fornecida.

```
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 com EAP acorrentar o túnel PAC expirou**

Neste fluxo quando nenhum túnel válido PAC existe, a negociação completa TLS com fase interna ocorre.

- O suplicante envia os hellos do cliente TLS sem túnel PAC.
- O server responde com as cargas úteis do certificado e do pedido do certificado TLS.
- O suplicante deve certificado de servidor de confiança, não enviará o certificado de cliente (o payload do certificado é zero), túnel TLS construído.
- O ISE envia o pedido TLV para o certificado de cliente dentro do túnel TLS, mas o suplicante não faz (não é necessário o ter a fim continuar).
- Começos EAP que acorrentam para o usuário, usando o método interno com autenticação MSCHAPv2.
- Continua com autenticação da máquina, usando o método interno com autenticação MSCHAPv2.
- Com sucesso fornecida todos os PAC (permitidos na configuração 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 com encadeamento EAP e abastecimento anônimo do túnel PAC TLS

Neste fluxo, o túnel anônimo ISE e NAM TLS é configurado para olhares do pedido do abastecimento do abastecimento PAC (o túnel autenticado ISE para o abastecimento PAC é desabilitado) PAC TLS como:

- O suplicante envia hellos do cliente TLS sem ciphersuites múltiplos.
- O server responde com as cifras anônimas dos servidores hello TLS e do Diffie Hellman TLS (por exemplo TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA).

- O suplicante aceita-o e o túnel anônimo TLS é construído ( nenhuns Certificados trocados).
- Começos EAP que acorrentam para o usuário, usando o método interno com autenticação MSCHAPv2.
- Continua com autenticação da máquina, usando o método interno com autenticação MSCHAPv2.
- Desde que o túnel anônimo TLS está sendo construído a autorização PAC não é permitida.
- A rejeição do raio é retornada ao suplicante da força para reauthenticate (usando o PAC fornecida).

```

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 pacote de informação de Wireshark para a negociação do túnel anônima 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 com o EAP que acorrenta a autenticação de usuário somente

Neste fluxo, AnyConnect NAM com autenticação EAP-FAST e do usuário (EAP-TLS) e da máquina (EAP-TLS) é configurado. O PC Windows é carregado mas as credenciais do usuário não são. O interruptor iniciado a sessão do 802.1x, NAM deve responder contudo, usuário que as credenciais não são fornecidas, (nenhum acesso à loja e ao certificado do usuário contudo) conseqüentemente. a autenticação de usuário falhará quando a máquina será bem sucedida - acesso de rede da condição do authz ISE "O usuário dos IGUAIS de EapChainingResult falhou e a máquina sucedida" é satisfeita. Mais tarde, o usuário entra e uma outra autenticação começará, usuário e a máquina sucederá.

- O suplicante envia hellos do cliente TLS com máquina PAC.
- O server responde com as specs. da cifra da mudança TLS - túnel TLS é imediatamente construção baseada nesse PAC.
- O ISE inicia o EAP que acorrenta e que pede a identidade do usuário.

- O suplicante fornece a identidade da máquina pelo contrário (usuário não ainda pronto), método interno do EAP-TLS dos revestimentos.
- O ISE pede a identidade do usuário outra vez, suplicante não pode fornecê-lo.
- O ISE envia o TLV com resultado = falha intermediários (para a autenticação de usuário).
- O ISE retorna o mensagem de sucesso final EAP, acesso de rede da condição ISE: O usuário dos IGUAIS de EapChainingResult falhou e a máquina sucedida é satisfeita.

```

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 com encadeamento EAP e configurações de túnel anônimas incompatíveis TLS

Neste fluxo, o ISE é configurado para o abastecimento PAC somente através do túnel anônimo TLS, mas o NAM está usando um túnel autenticado TLS, o seguinte será registrado pelo 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
```

Isto ocorre quando o NAM está tentando construir um túnel autenticado TLS com ele é cifras speciphic TLS - e aqueles não são aceitados pelo ISE que é configurado para o túnel anônimo TLS (que aceita cifras DH somente)

## Troubleshooting

### ISE

Para logs detalhados, o Runtime-AAA debuga deve ser permitido no nó correspondente PSN. Estão abaixo alguns logs do exemplo de prrt-server.log:

#### Geração da máquina PAC:

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

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

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

#### Aprovação do pedido PAC:

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

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

#### Validação PAC:

```
DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-
ise14/223983918/29243,CPMSessionID=0A3E946D0000FE5131F9D26,user=anonymous,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC is valid,EapFastProtocol.cpp:3403
```

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

Exemplo do sumário bem sucedido para a geração PAC:

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

Exemplo do sumário bem sucedido para a validação PAC:

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

## AnyConnect NAM

Os logs do DARDO do NAM fornecem os seguintes detalhes:

O exemplo para não EAP-acorrentar a sessão, autenticação da máquina sem rápido reconecta:

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

Exemplo da consulta da autorização PAC (autenticação da máquina para a sessão não deencadeamento):

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

Todos os estados de método interno (para o MSCHAP) podem ser verificados dos logs abaixo:

```
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
```

O NAM permite a configuração dos recursos de registro prolongados que capturarão todos os pacotes EAP e salvar os no arquivo do pcap. Isto é especialmente útil para o começo antes da funcionalidade do fazer logon (os pacotes EAP são capturados mesmo para as autenticações que ocorram antes que fazer logon do usuário). Para a ativação da característica pergunte a seu coordenador TAC.

## Referências

- [O guia do administrador do Cliente de mobilidade Cisco AnyConnect Secure, libera a configuração 4.0 EAP-FAST](#)
- [O guia do administrador do Cisco Identity Services Engine, libera 1.4 recomendações EAP-](#)

## FAST

- [Guias de Design do Cisco Identity Services Engine](#)
- [EAP de distribuição que acorrenta com AnyConnect NAM e Cisco ISE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)