Índice

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 anónima 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. Proviosioned 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 abasteci autenticado e se o tú PAC é pedido igualm
Forneça o PAC a pedido	sim	sim	somente se não foi u

na autenticação			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)	rejeite e don? t fornece o novo	rejeite e don? t fornece o novo	rejeite e don? t fornec 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 recomeçar a sessão. A sessão é usada somente para o abastecimento PAC ao usar um túnel anónimo TLS:

Apátrida (PAC baseado)

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

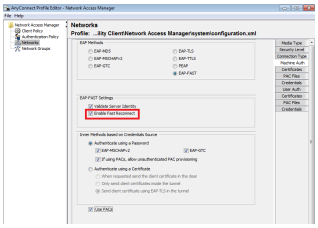
O resumo do lado do cliente é baseado no RFC 4507. O server não precisa de pôr em esconderijo nenhuns dados; em lugar do cliente anexa o PAC na extensão de SessionTicket dos hellos do cliente TLS. Por sua vez, o PAC é validado pelo server. Exemplo baseado no túnel PAC entregado ao server:

	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

```
▽ 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
```

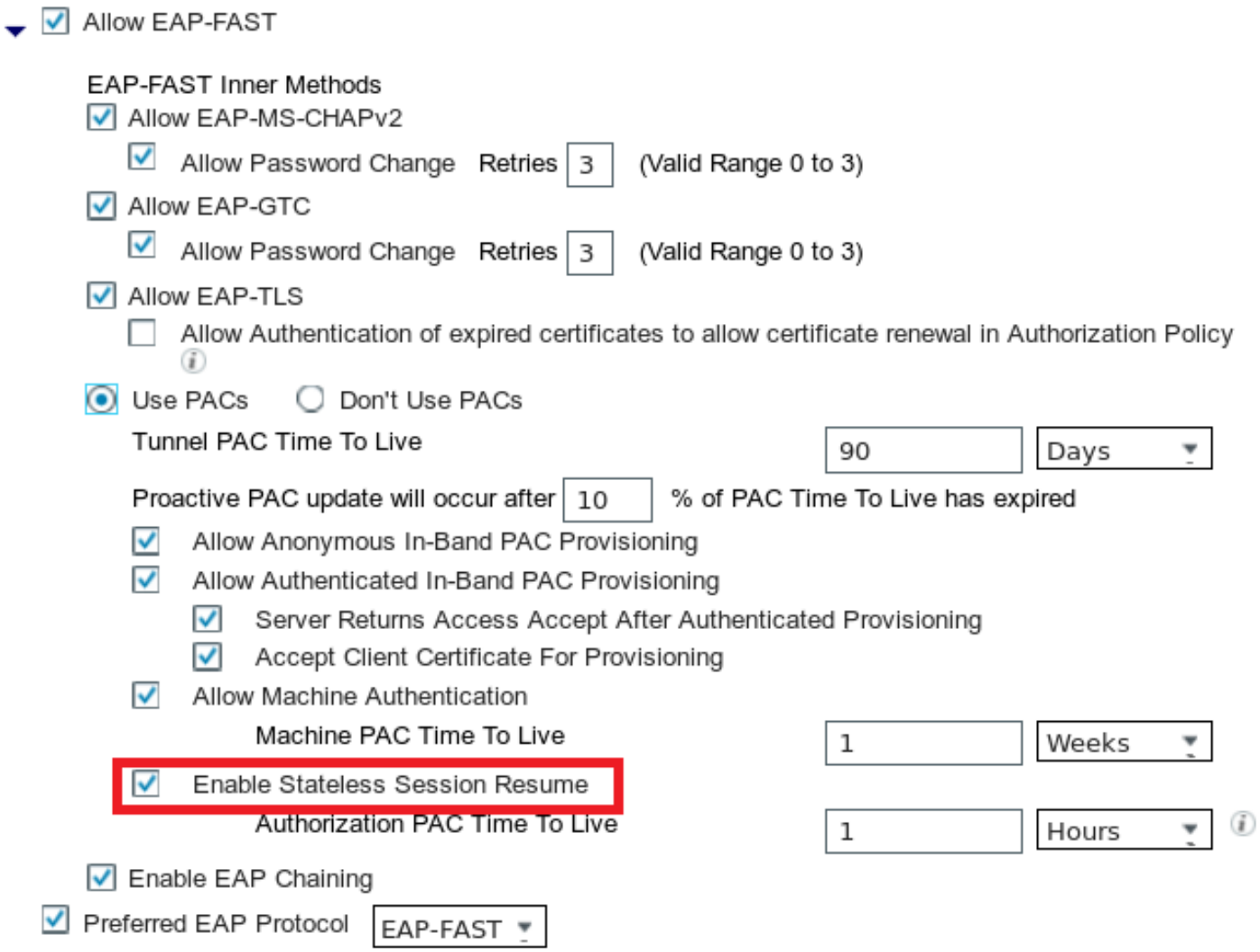
Aplicação de AnyConnect NAM

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.

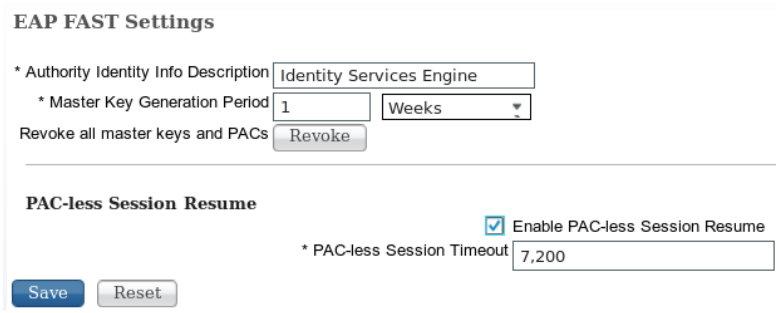
O ISE tem uma opção para permitir o resumo apátrida da sessão. E como no NAM é apenas para a autorização PAC. O uso do túnel PAC é controlado com opções “uso PAC”.



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). Desabilitou à revelia:



Mantenha por favor na mente que somente um tipo de resumo da sessão pode ser usado. SessionID baseou 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 anónimo TLS

Para disposições sem uma infraestrutura PKI, é possível usar um túnel anónimo TLS. O túnel anónimo 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:

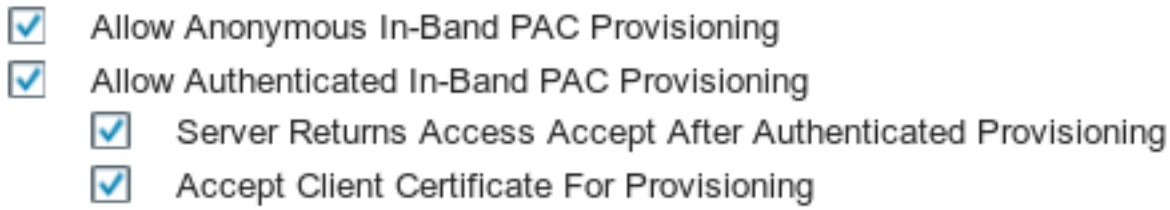
“Permita o abastecimento anónimo da Em-faixa PAC”

O abastecimento anónimo 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:



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 confiado 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):

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:

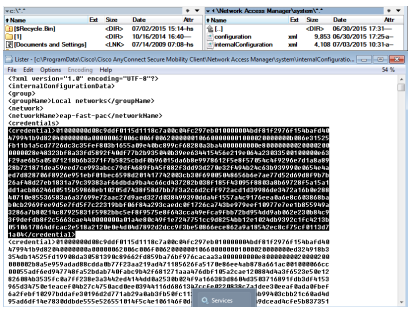
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

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

Àrevelia, 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. Aqueles são armazenados no formulário criptografado.

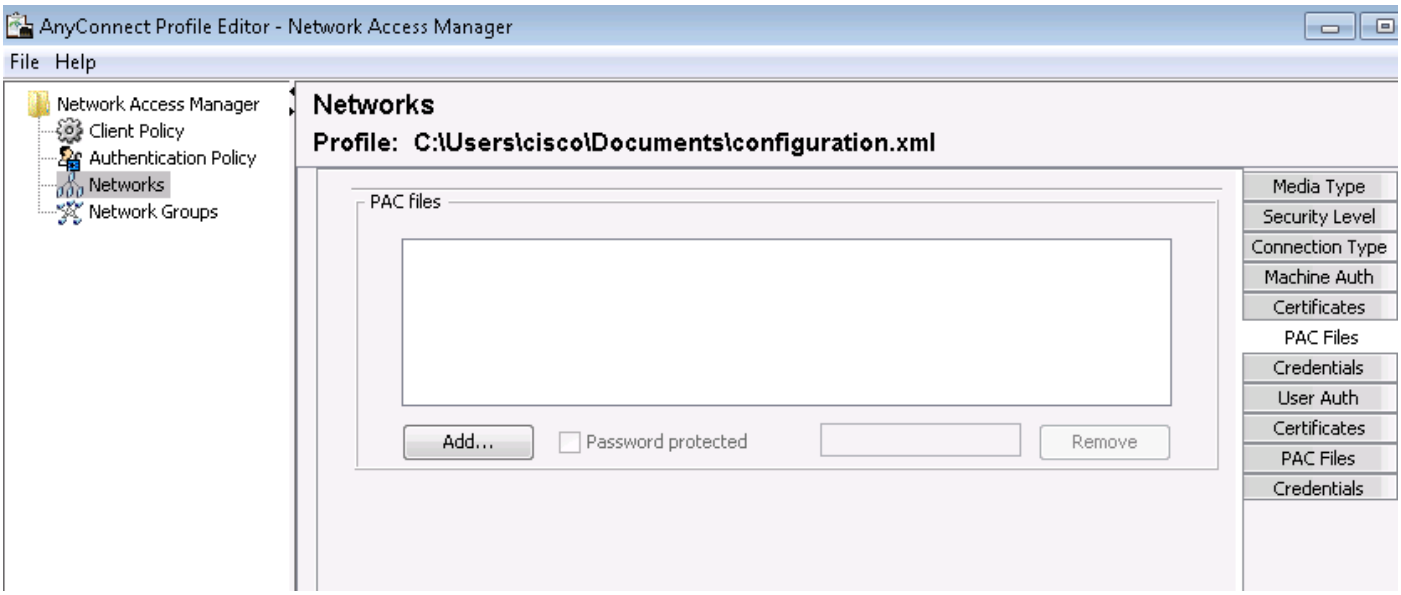


A autorização PAC é armazenada somente na memória e removida depois que repartição ou de serviço NAM reinício.

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.

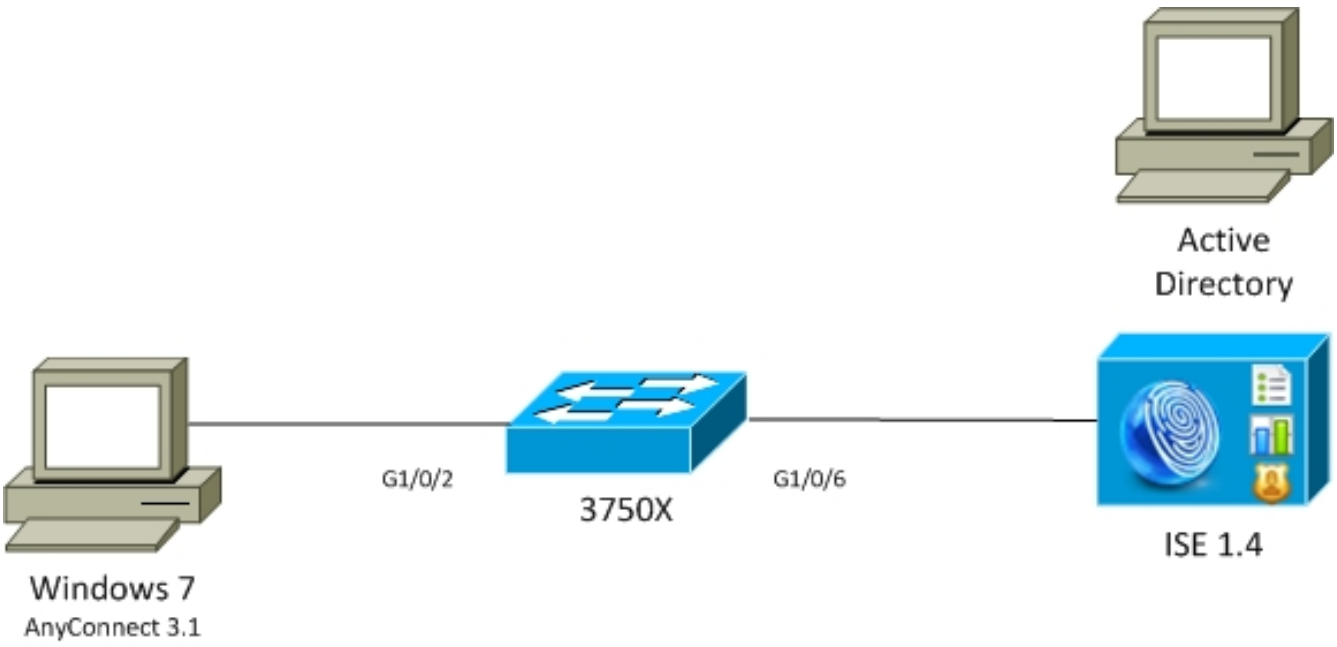


A decisão a remover que a funcionalidade está baseada em CSCuf31422 e em CSCua13140.

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

Àrevelia, 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:

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:

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

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.

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).

EAP-rápido com encadeamento EAP e abastecimento anónimo do túnel PAC TLS

Neste fluxo, o túnel anónimo 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 anónimas 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 anónimo 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 anónimo 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).

Capturas de pacote de informação de Wireshark para a negociação do túnel anónima 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 carreg mas as credenciais do usuário não sãas. 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) consequentemente. a autenticação de usuário falhará quando a máquina será bem sucedida - acesso de rede da condição do authz ISE “

- O suplicante envia hellos do cliente TLS com máquina PAC.
- O server responde com as especs. 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 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 anónimas incompatíveis TLS

Neste fluxo, o ISE é configurado para o abastecimento PAC somente através do túnel anónimo 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 anónimo 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:

Aprovação do pedido PAC:

Validação PAC:

Exemplo do sumário bem sucedido para a geração PAC:

Exemplo do sumário bem sucedido para a validação PAC:

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:

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

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

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