Begrijpen van EAP-FAST en het koppelen van implementaties op AnyConnect NAM en ISE

Inhoud

Inleiding

Dit artikel legt details uit over EAP-FAST-implementaties op Cisco AnyConnect Network Access Manager (NAM) en Identity Services Engine (ISE). Het legt verder uit hoe specifieke kenmerken samenwerken en biedt typische gebruiksgevallen en voorbeelden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van het MAP-kader en de MAP-FAST-methoden
- Basiskennis van Identity Services Engine (ISE)
- Basiskennis van AnyConnect NAM en Profile Editor
- Basiskennis van Cisco Catalyst-configuratie voor 802.1x-services

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Windows 7 met Cisco AnyConnect Secure Mobility Client, release 3.1 en 4.0
- Cisco Catalyst 3750X switch met software 15.2.1 en hoger
- Cisco ISE, release 1.4

Theorie

Fases

EAP-FAST is een flexibele MAP-methode die wederzijdse authenticatie van een bedelstaf en een server mogelijk maakt. Het is vergelijkbaar met EAP-PEAP, maar vereist doorgaans niet het gebruik van client- of zelfs servercertificaten. Een voordeel van EAP-FAST is de mogelijkheid om meerdere authenticaties (met behulp van meerdere binnenmethoden) te ketenen en deze cryptografisch te binden (EAP Chaining). Cisco-implementaties gebruiken dit voor gebruikers- en machineauthenticaties.

EAP-FAST gebruikt Protected Access Credentials (PAC) om snel de TLS-tunnel (sessie hervat) op te zetten of de gebruiker/machine te machtigen (skip-binnenmethode voor authenticatie).

Er zijn 3 fasen voor EAP-FAST:

- fase 0 (PAC-voorzieningen)
- fase 1 (TLS-tunnelbouw)
- Fase 2 (Verificatie)

EAP-FAST ondersteunt PAC-loze en PAC-gebaseerde gesprekken. Op PAC gebaseerde componenten bestaan uit PAC-provisioning en op PAC gebaseerde authenticatie. PAC-provisioning kan worden gebaseerd op anonieme of gewaarmerkte TLS-sessie.

PAC

PAC is Protected Access Credentials die gegenereerd zijn door de server en aan de client geleverd worden. Het bestaat uit:

- PAC-toets (willekeurige geheime waarde, gebruikt om TLS-master en sessiesleutels af te

leiden)
- PAC ondoorzichtig (PAC-toets + gebruikersidentiteit - alle versleuteld met EAP-FAST-servermaster.)
- PAC-informatie (serveridentiteit, TTL-timers)

De server die de PAC uitgeeft, versleutelt de PAC-toets en de identiteit met behulp van de EAP-FAST server-master (dat PAC ondoorzichtig is) en stuurt de gehele PAC naar de client. Het bewaart/slaat geen andere informatie op (behalve master key die voor alle PAC's hetzelfde is).

Zodra de PAC ondoorzichtig is ontvangen, wordt het gedecrypteerd met behulp van de EAP-FAST server hoofdsleutel en gevalideerd. De PAC - toets wordt gebruikt om de TLS - master en sessiesleutels af te leiden voor een afgekort TLS - tunnel.

Nieuwe EAP-FAST server master keys worden gegenereerd wanneer de vorige master key afloopt. In sommige gevallen kan een master key worden ingetrokken.

Op dit moment worden een aantal PAC's gebruikt:

- Tunnel PAC: gebruikt voor TLS-tunnelbouw (zonder dat client- of servercertificaat nodig is). Verstuurd in TLS-client Hallo
- Machine PAC: gebruikt voor het aanleggen van een TLS-tunnel en het onmiddellijk machineautoriseren. Verstuurd in TLS-client Hallo
- Gebruikershandleiding: gebruikt voor onmiddellijke gebruikersauthenticatie (skip binnenmethode) indien toegestaan door server. Verstuurd in TLS-tunnel met TLV.
- Machinevergunning PAC: gebruikt voor onmiddellijke machineverantwoording (skip binnenmethode) indien toegestaan door server. Verstuurd in TLS-tunnel met TLV.
- Trustsec PAC: worden gebruikt voor het verkrijgen van een vergunning bij het verfrissen van milieubeleid of beleid.

Al deze PAC's worden gewoonlijk automatisch geleverd in fase 0. Sommige PAC's (Tunnel, machine, Trustsec) kunnen ook handmatig worden geleverd.

Wanneer PAC's worden gegenereerd

- Tunnel PAC: bevoorraad na een succesvolle echtheidscontrole (binnenmethode) indien niet eerder gebruikt.
- PAC: bevoorraad na succesvolle authenticatie (binnenmethode) indien niet eerder gebruikt.
- Machine PAC: na geslaagde machineverantwoording (binnenmethode) indien niet eerder gebruikt en niet wanneer een PAC van de autorisatie wordt gebruikt. Het zal worden verstrekt wanneer de PAC van de Tunnel verstrijkt, maar niet wanneer de PAC van de vergunning verstrijkt. Er zal voor worden gezorgd wanneer EAP-Chaining is ingeschakeld of uitgeschakeld.

Opmerking:

Elke PAC-voorziening vereist succesvolle authenticatie behalve de volgende gebruikszaak: De geautoriseerde gebruiker vraagt de machine-PAC aan voor een machine die geen AD-account heeft.

De volgende tabel geeft een samenvatting van de voorzieningen en de pro-actieve update-functionaliteit:

PAC-type	Tunnel v1/v1a/CTS	machine	Authorization

PAC op verzoek verstrekken over provisioning	ja	alleen op gewaarmerkte levering	alleen bij geauthentis voorziening en indien om de PAC van de Tu wordt gevraagd
PAC's op verzoek verstrekken inzake verificatie	ja	ja	alleen indien het niet deze authenticatie we gebruikt
Proactieve update	ja	nee	nee
Bij terugval naar PAC-voorzieningen na mislukte PAC-gebaseerde verificatie (bv. wanneer PAC is verlopen)	de nieuwe afwijzen en niet verstrekken	de nieuwe afwijzen en niet verstrekken	de nieuwe afwijzen en verstrekken
Ondersteuning van ACS 4.x PAC's	voor Tunnel PAC v1/v1a	ja	nee

EAP-FAST Server hoofdtoets ACS 4.x vs ACS 5x en ISE

Er is een klein verschil in de hoofdtoepassing wanneer ACS 4.x en ISE worden vergeleken

Functie	ACS 4.1.2	ACS 5.x / ISE
Sleutel	De hoofdtoets heeft TTL, kan actief zijn, beëindigd of verlopen	De hoofdtoets wordt automatisch gegenereerd uit zaad op elke geconfigureerde periode. Specifieke Master Key is altijd toegankelijk en is dan nooit verlopen
PAC-vernieuwing	PAC-update wordt verzonden per server wanneer PAC is verlopen, tenzij Master Key, gebruikt voor PAC-encryptie, is verlopen	PAC-update wordt verzonden per server na eerste succesvolle verificatie die wordt uitgevoerd in een specifieke configureerbare periode vóór het PAC-verloopmoment.

Met andere woorden, ISE zal alle oude master keys houden en per week standaard een nieuwe genereren. Aangezien de Master Key niet kan verlopen, zal alleen de PAC TTL worden gevalideerd.

De generatieperiode van de ISE Master Key wordt ingesteld bij *Administratie -> Instellingen -> Protocol -> EAP-FAST -> EAP-FAST-instellingen.*

Sessieoverzicht

Dit is een belangrijk onderdeel dat het gebruik van de PAC-tunnel mogelijk maakt. Het maakt nieuwe onderhandelingen over TLS-tunnels mogelijk zonder gebruik van certificaten.

Er zijn twee soorten sessies op te zetten voor EAP-FAST: Op de serverstaat gebaseerd en stateless (PAC's).

Serverstaat

De standaard op TLS gebaseerde methode is gebaseerd op de TLS SessionID die op de server is gecached. De client die de TLS-client verstuurt, heft de SessionID aan om de sessie te hervatten. De sessie wordt alleen gebruikt voor PAC-provisioning bij gebruik van een anonieme TLS-tunnel:

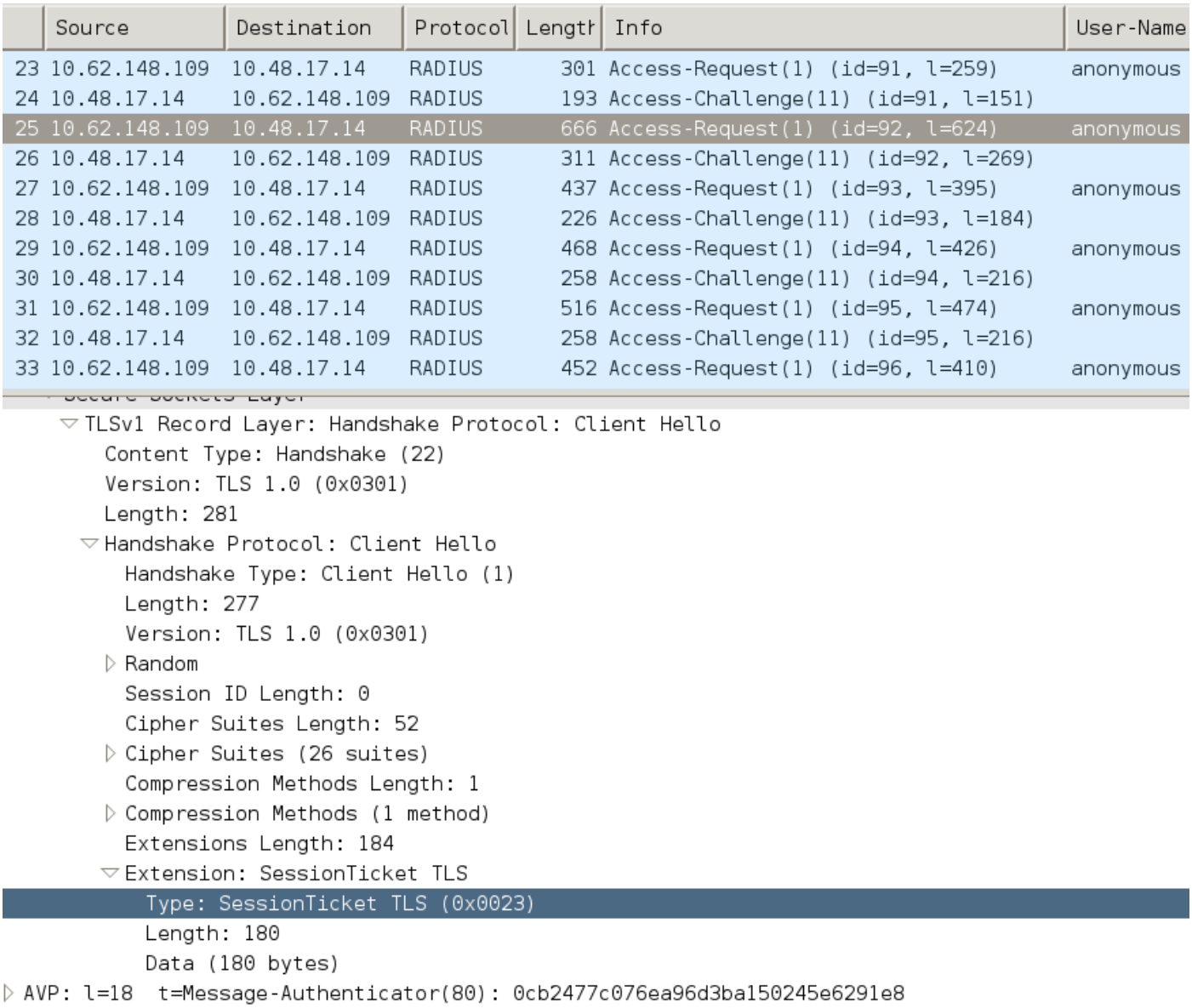
Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l=	anonymous
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l	anonymous
10.48.17.14	10.62.148.109	RADIUS	193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

Stateless (PAC-gebaseerd)

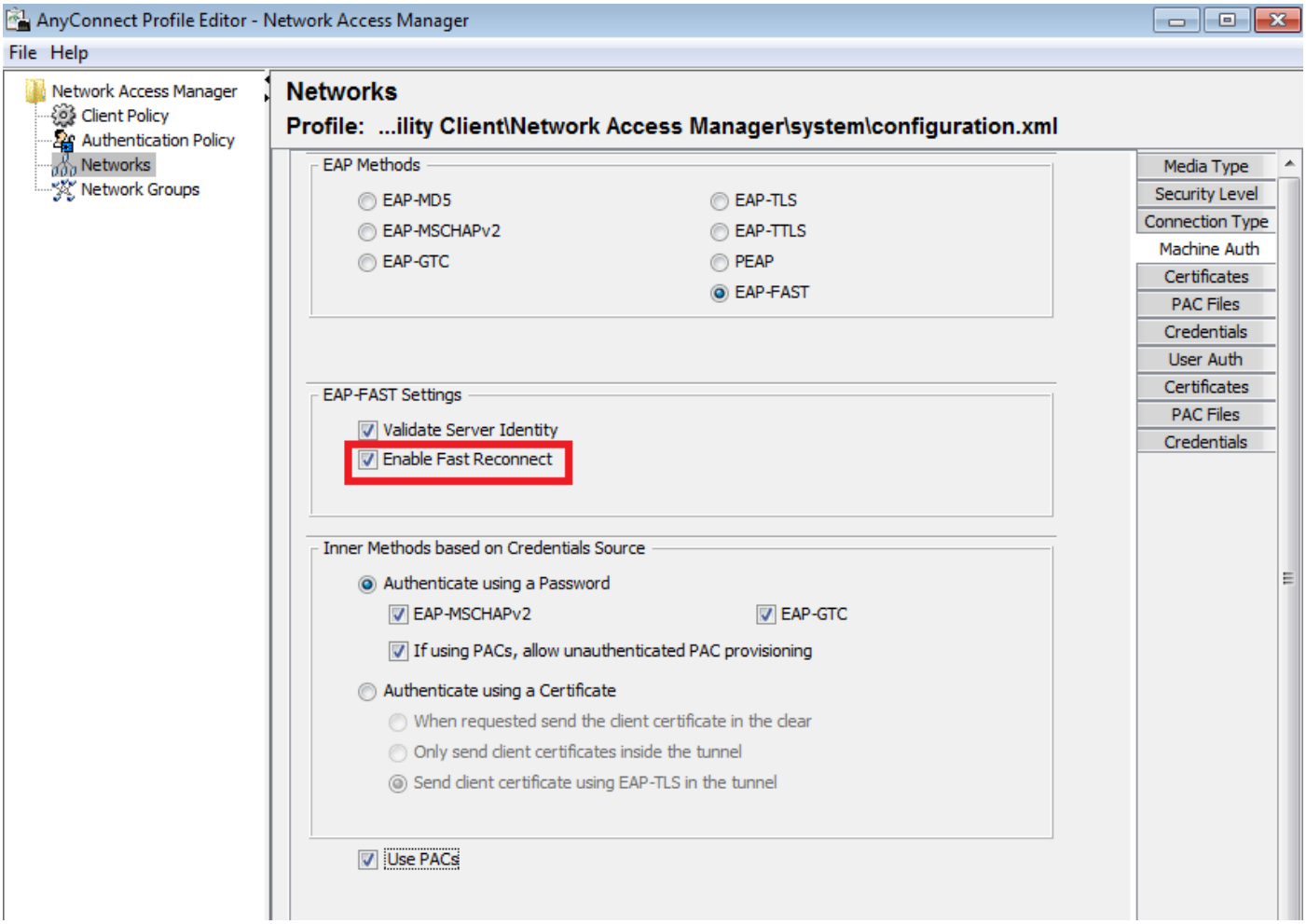
Gebruikershandleiding/Machineautorisatie PAC wordt gebruikt om de eerdere echtheids- en autorisatiestaten voor de peer op te slaan.

Aan clientzijde wordt het programma op RFC 4507 voortgezet. De server hoeft geen gegevens in te houden; in plaats daarvan heft de client de PAC aan in de TLS Client Hallo SessionTicket extensie. De PAC wordt op zijn beurt door de server gevalideerd. Voorbeeld op basis van Tunnel PAC geleverd aan de server:



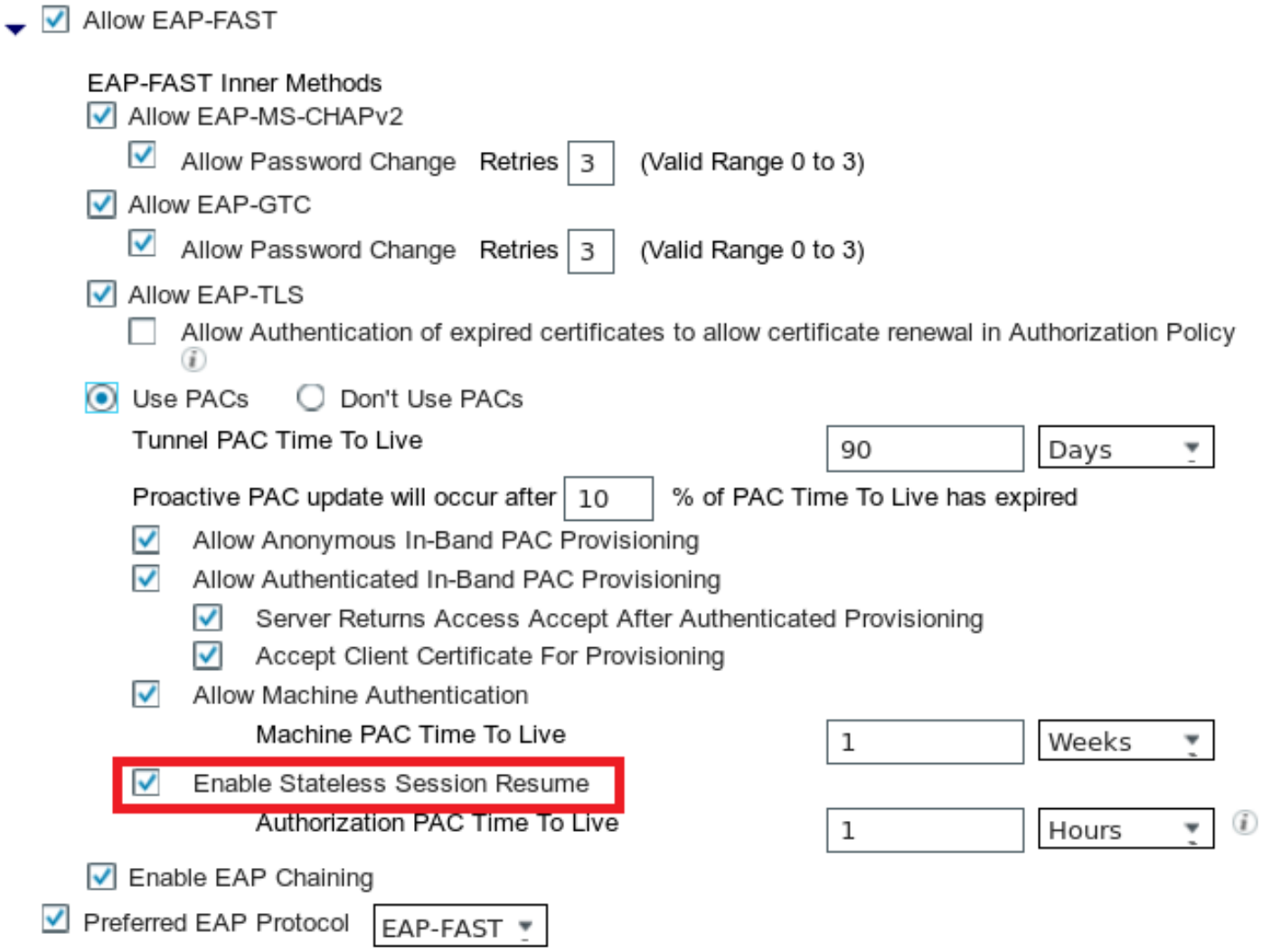
AnyConnect NAM-implementatie

Het is ingeschakeld aan clientzijde (AnyConnect NAM) via Fast Reconconnect - maar het wordt alleen gebruikt om het PAC-gebruik van een vergunning te controleren.



Met de instelling uitgeschakeld zal NAM nog steeds de tunnel PAC gebruiken om de TLS-tunnel aan te leggen (geen certificaten nodig). Dit betekent echter niet dat er geen PAC's van de vergunning worden gebruikt om onmiddellijk een vergunning voor de gebruiker en de machine te verlenen. Als resultaat hiervan zal fase 2 met de binnenmethode altijd nodig zijn.

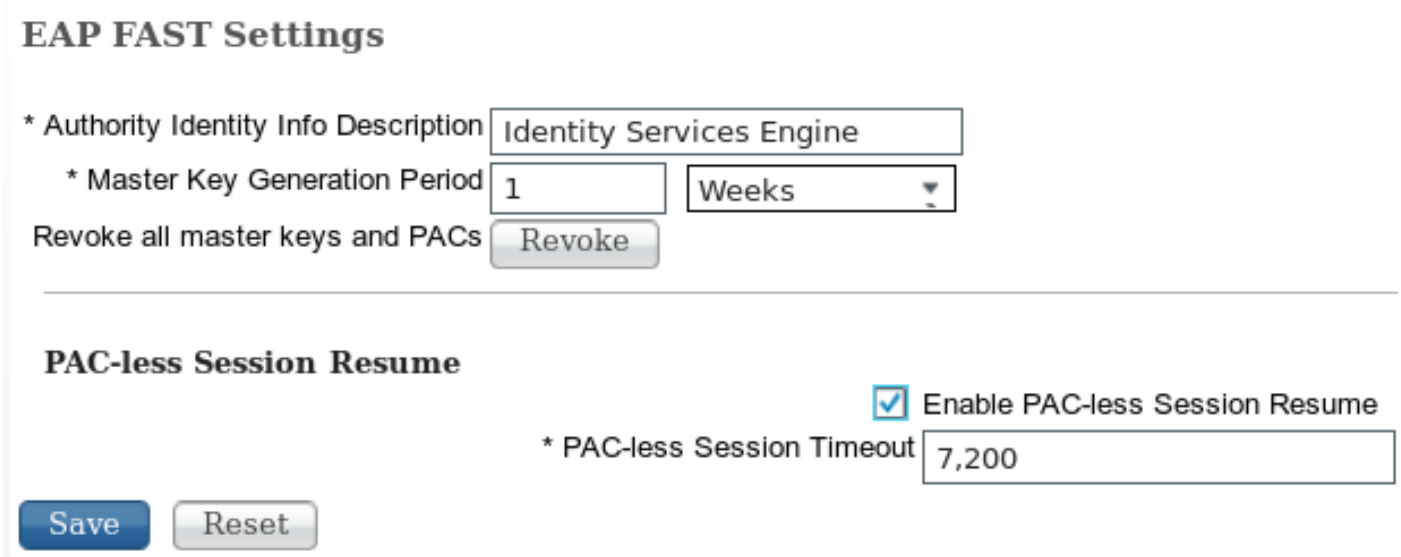
ISE heeft een optie om stateless sessie opnieuw in te schakelen. Net als bij de NAM is het alleen voor autorisatie-PAC. Het PAC-gebruik van de tunnel wordt geregeld met opties "Gebruik PAC's".



NAM zal proberen PAC's te gebruiken als de optie is ingeschakeld. Als "Geen PAC's gebruiken" is ingesteld in ISE en ISE ontvangt een Tunnel PAC in de TLS-extensie, wordt de volgende fout gerapporteerd en wordt een EAP-storing teruggegeven:

invoegen

In ISE is het ook nodig om sessie te kunnen hervatten op basis van TLS SessionID (vanuit de Global EAP-FAST-instellingen). Standaard is het uitgeschakeld:



Houd in gedachten dat slechts één type sessie kan worden gebruikt. Op SessionID gebaseerd wordt alleen gebruikt voor PAC-loze implementaties, wordt RFC 4507-gebaseerd alleen gebruikt voor PAC-implementaties.

PAC-bevoorrading (fase 0)

PAC's kunnen automatisch worden bevoorraad in fase0. Fase 0 bestaat uit:

- TL-tunnelvestiging
- Verificatie (binnenmethode)

PAC's worden geleverd na een succesvolle authenticatie in de TLS - tunnel via PAC - TLV (en PAC - TLV - erkenning)

Anonieme TLS-tunnel

Voor implementaties zonder een PKI-infrastructuur is het mogelijk om een anonieme TLS-tunnel te gebruiken. De anonieme TLS-tunnel wordt gebouwd met behulp van de Diffie Hellman algoritme suite - zonder dat er een server- of client-certificaat nodig is. De mens kan zich in de Midden-aanvallen op deze manier aansluiten (imitatie).

Om deze optie te gebruiken, heeft NAM de volgende geconfigureerde optie nodig:

"Als het gebruik van PAC's niet-geauthenticeerde PAC-provisioning toestaat" (dat alleen zinvol is voor op wachtwoord gebaseerde binnenmethode omdat zonder PKI-infrastructuur het niet mogelijk is om op certificaat gebaseerde binnenmethode te gebruiken).

ISE heeft ook de volgende instellingen nodig onder de toegestane verificatieprotocollen:

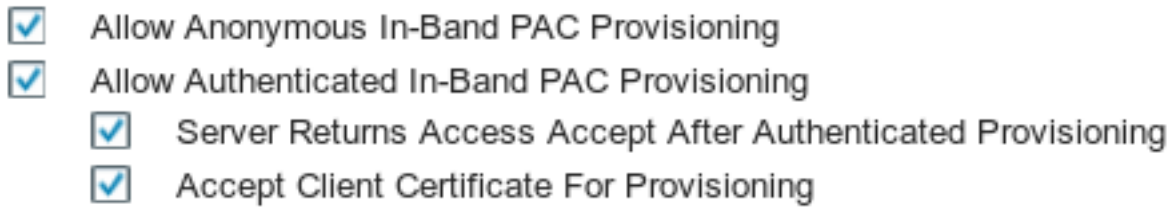
"Anonymous in-band PAC-provisioning toestaan"

Anonymous in-band PAC-provisioning wordt gebruikt in TrustSec NDAC-implementaties (EAP-FAST-sessie overeengekomen tussen netwerkapparaten).

Geautomatiseerde TLS-tunnel

Dit is de best beveiligde en aanbevolen optie. De TLS-tunnel is gebouwd op basis van het servercertificaat dat door de aanvrager is gevalideerd. Hiervoor is alleen een PKI-infrastructuur aan de serverkant nodig, die vereist is voor ISE (op NAM is het mogelijk om optie "Server Identity valideren" uit te schakelen).

Voor ISE zijn er twee aanvullende opties:



Normaal gesproken moet er na de PAC-provisioning een toegangsverworpen worden, waarbij de aanvrager wordt gedwongen het gebruik van PAC's te reauthentiseren. Maar omdat PAC's in de TLS-tunnel werden afgeleverd met authenticatie, is het mogelijk het hele proces te verkorten en

direct na PAC-voorzieningen toegang-Accept terug te geven.

De tweede optie bouwt de TLS-tunnel op basis van een client-certificaat (hiervoor is PKI-implementatie op de eindpunten nodig). Hierdoor kan de TLS-tunnel worden gebouwd met wederzijdse echtheidscontrole, waardoor de binnenmethode wordt overgeslagen en rechtstreeks naar de PAC-voorzieningsfase gaat. Het is belangrijk om hier voorzichtig te zijn - soms zal de aanvrager een certificaat indienen dat niet door ISE (bedoeld voor andere doeleinden) wordt vertrouwd en de sessie zal mislukken.

EAP-Chaining

Hiermee kan gebruikers- en machineverantwoording binnen één Radius/EAP-sessie plaatsvinden. Meerdere MAP-methoden kunnen aan elkaar worden gekoppeld. Nadat de eerste verificatie (doorgaans machine) met succes is voltooid, zal de server een TFV met middelgroot resultaat (binnenste TLS-tunnel) sturen om succes aan te geven. Dat TLV moet vergezeld gaan van een crypto-bindend TLV-verzoek. Cryptobinding wordt gebruikt om aan te tonen dat zowel de server als de peer hebben deelgenomen aan de specifieke opeenvolging van authenticaties. Bij het cryptobindingsproces wordt het sluitmateriaal van fase 1 en fase 2 gebruikt. Daarnaast is nog een TLV toegevoegd: EAP-Payload - dit is het begin van de nieuwe sessie (meestal voor de gebruiker). Zodra de RADIUS-server (ISE) de Crypto-Binding TLV-respons ontvangt en deze geldig maakt, wordt het volgende in het logboek weergegeven en wordt de volgende MAP-methode geprobeerd (doorgaans voor gebruikersverificatie):

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

Als cryptobindende validatie mislukt, faalt de hele MAP-sessie. Als één van de authenticaties binnen mislukt, is het nog steeds ok - als resultaat hiervan staat ISE een beheerder toe om meerdere kettingresultaten te configureren op basis van Authorization Condition Network Access:EapChainingResultaat:

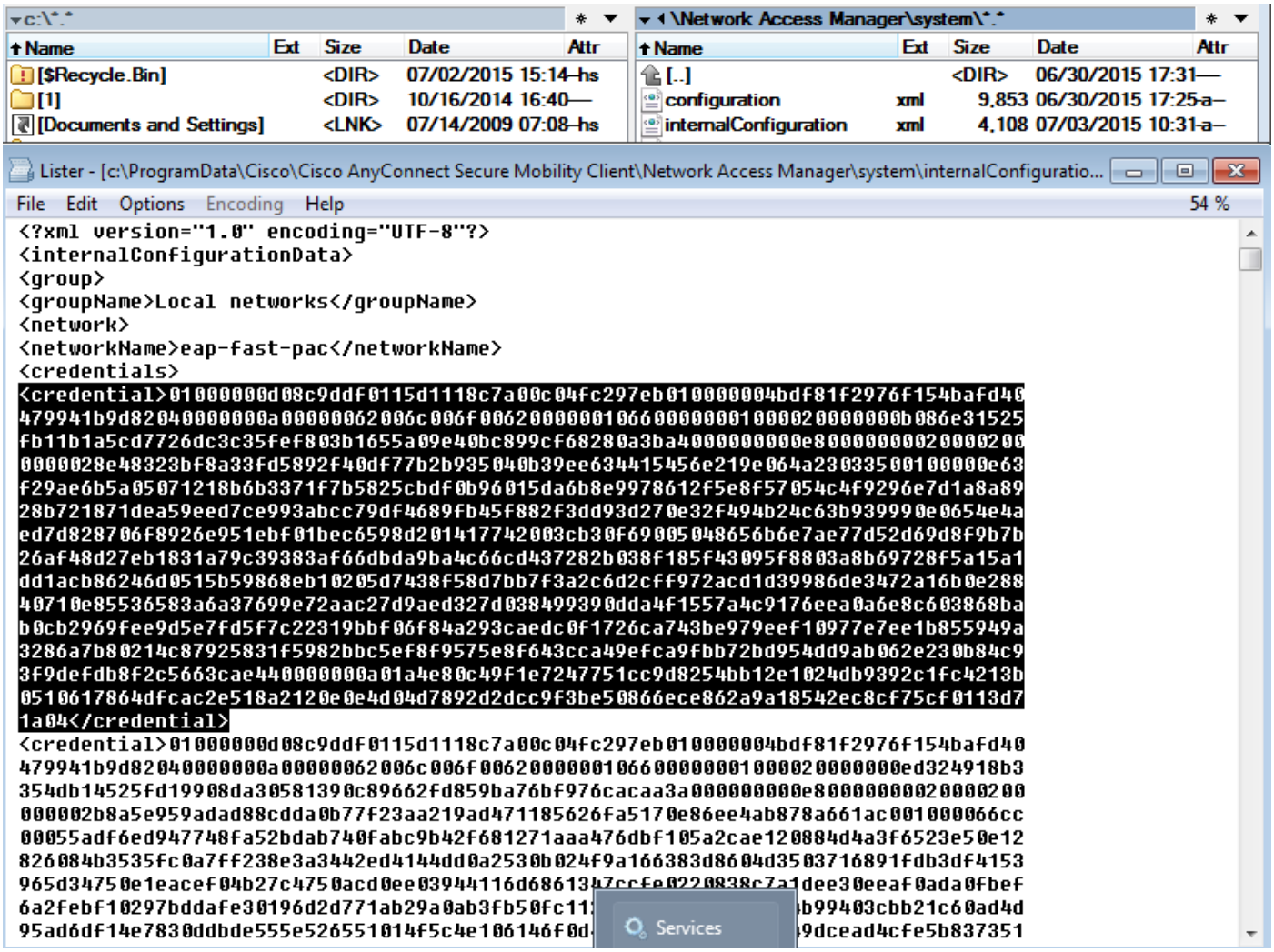
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-Chaining wordt automatisch op NAM ingeschakeld wanneer EAP-FAST-gebruikers en machinale authenticatie is ingeschakeld.

EAP-Chaining moet in ISE worden geconfigureerd.

Waar PAC-bestanden zijn opgeslagen

Standaard worden Tunnel- en machine-PAC's opgeslagen in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml in secties <gecrediteerd>. Die worden opgeslagen in gecodeerde vorm.

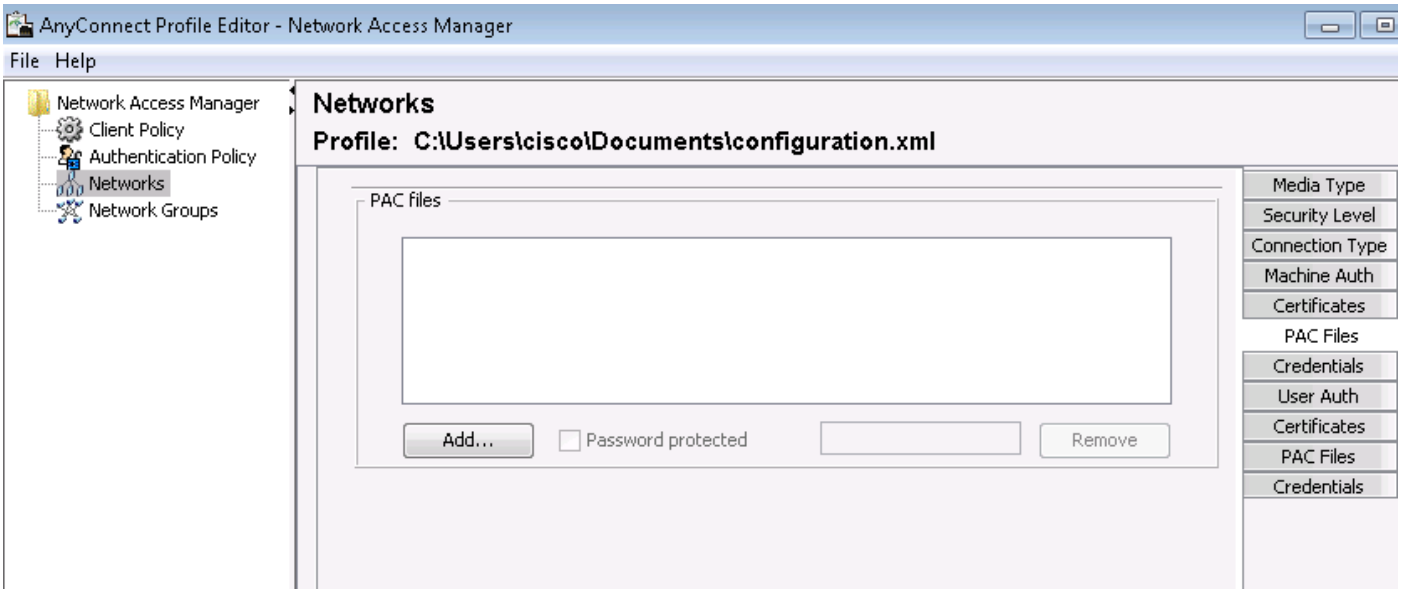


PAC's met een autorisatie worden alleen in het geheugen opgeslagen en worden verwijderd na het opnieuw opstarten of opstarten van de NAM-service.

De service moet opnieuw worden gestart om de PAC van de Tunnel of Machine te verwijderen.

AnyConnect NAM 3.1 vs. 4.0

Met AnyConnect 3.x NAM-profieleditor kon de beheerder PAC's handmatig configureren. Deze optie is verwijderd van AnyConnect 4.x NAM-profieleditor.

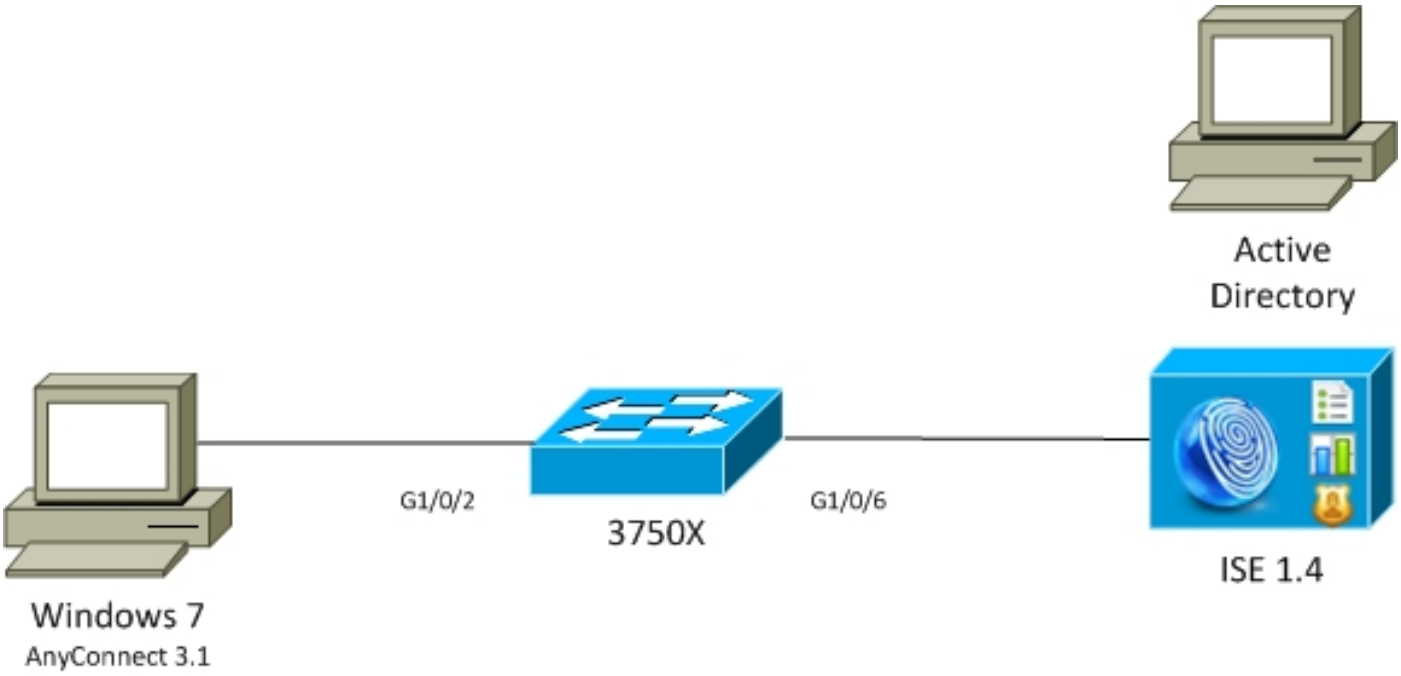


Het besluit om die functionaliteit te verwijderen is gebaseerd op CSCuf31422 en CSCua13140.

Voorbeelden

Netwerkdiagram

Alle voorbeelden werden getest met behulp van de volgende netwerktopologie. Dit geldt ook voor draadloze verbindingen.



EAP-Fast zonder MAP-koppeling met PAC van gebruiker en machine

Standaard is EAP_chaining uitgeschakeld op ISE. Alle andere opties zijn echter ingeschakeld, waaronder PAC's van machines en autorisatie. De aanvrager heeft al een geldige machine- en tunnelPAC. In deze stroom worden er twee afzonderlijke authenticaties uitgevoerd - een voor de machine en een voor de gebruiker - met afzonderlijke logbestanden op ISE. De belangrijkste stappen zoals vastgelegd door ISE. Eerste verificatie (machine):

- Leverancier stuurt TLS Client Hallo met machine-PAC.
- Server valideert de machine PAC en bouwt de TLS tunnel (geen certificaten gebruikt).
- De server bevestigt de machine PAC en voert de rekeningraadpleging in Actieve Map uit en slaat de innerlijke methode over.

```
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
```

De tweede authenticatie (gebruiker):

- Leverancier verstuurt de TLS Client Hallo met Tunnel PAC.
- Server valideert de PAC en bouwt de TLS-tunnel (geen certificaten gebruikt).
- Aangezien de aanvrager geen PAC heeft met een vergunning, wordt de interne methode (EAP-MSCHAP) gebruikt voor de authenticatie.

```
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
```

In het gedeelte "Overige Eigenschappen" van het gedetailleerde rapport in ISE wordt voor zowel gebruiker- als machine-authenticaties opgemerkt:

```
EapChainingResult: No chaining
```

EAP-Fast met MAP-koppeling met PAC snel opnieuw aansluiten

In deze stroom heeft de aanvrager al een geldige Tunnel PAC samen met de User and Machine

Authorization-PAC's:

- Leverancier verstuurt de TLS Client Hallo met Tunnel PAC.
- Server valideert de PAC en bouwt de TLS-tunnel (geen certificaten gebruikt).
- ISE start EAP Chaining, Leverancier bevestigt PAC's van de Vergunning voor gebruiker en machine met TLV binnen de TLS-tunnel.
- ISE valideert de PAC's van de Vergunning (geen binnenmethode nodig), verifieert dat rekeningen in Actieve Map bestaan (geen extra authenticatie), keert succes terug.

```
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
```

In het gedeelte "Overige kenmerken" van het gedetailleerde rapport in ISE wordt het volgende opgemerkt:

```
EapChainingResult: EAP Chaining
```

Bovendien zijn zowel de gebruikers- als de machinereferenties opgenomen in hetzelfde logbestand als hieronder:

```
Username: cisco,host/mgarcarz-PC
```

EAP-Fast met MAP-routing zonder PAC

In deze stroom is NAM ingesteld om geen PAC te gebruiken, maar ISE is ook ingesteld om geen PAC te gebruiken (maar met EAP Chaining)

- Leverancier verstuurt TLS Client Hallo zonder Tunnel PAC.
- De server reageert met de betaling van het TLS-certificaat en certificaataanvraag.
- Leverancier moet het certificaat van een server vertrouwen, zal geen client certificaat sturen (certificatie lading is nul), TLS-tunnel is gebouwd.
- ISE stuurt een TLV-verzoek om het client-certificaat binnen de TLS-tunnel, maar de aanvrager niet (het is niet nodig om dit te hebben om door te gaan).
- Begint EAP Chaining voor gebruiker, met gebruik van innerlijke methode met MSCHAPv2 authenticatie.

- Doorgaat met machinale authenticatie, met behulp van binnenmethode met MSCHAPv2-verificatie.
- Er worden geen PAC's bevoorraad.

```
12102     Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800     Extracted first TLS record; TLS handshake started
12805     Extracted TLS ClientHello message
12806     Prepared TLS ServerHello message
12807     Prepared TLS Certificate message
12809     Prepared TLS CertificateRequest message
12811     Extracted TLS Certificate message containing client certificate
12812     Extracted TLS ClientKeyExchange message

12816     TLS handshake succeeded
12207     Client certificate was requested but not received during tunnel establishment. Will
renegotiate and request client certificate inside the tunnel.
12226     Started renegotiated TLS handshake

12104     Extracted EAP-Response containing EAP-FAST challenge-response
12811     Extracted TLS Certificate message containing client certificate
12812     Extracted TLS ClientKeyExchange message
12804     Extracted TLS Finished message
12801     Prepared TLS ChangeCipherSpec message
12802     Prepared TLS Finished message
12226     Started renegotiated TLS handshake
12205     Client certificate was requested but not received inside the tunnel. Will continue
with inner method.
12176     EAP-FAST PAC-less full handshake finished successfully

12209     Starting EAP chaining
12218     Selected identity type 'User'

11806     Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402     User authentication against Active Directory succeeded - example.com
22037     Authentication Passed

12219     Selected identity type 'Machine'

11806     Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470     Machine authentication against Active Directory is successful - example.com
22037     Authentication Passed

11503     Prepared EAP-Success
11002     Returned RADIUS Access-Accept
```

EAP-Fast met MAP-goedkeuring voor het aflopen van PAC's

In deze stroom heeft Leverancier een geldige OC van de Tunnel, maar is de vergunning van de PAC's verstreken:

- Leverancier verstuurt de TLS Client Hallo met Tunnel PAC.
- Server valideert de PAC en bouwt de TLS-tunnel (geen certificaten gebruikt).
- ISE start EAP Chaining, Leverancier bevestigt PAC's van de Vergunning voor gebruiker en machine met TLV binnen de TLS-tunnel.
- Aangezien de PAC's zijn verlopen, wordt de innerlijke methode voor zowel gebruiker als machine gestart (EAP-MSCHAP).

- Zodra beide authenticaties succesvol zijn, worden zowel gebruiker als machine Authorization PACs voorzien.

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800   Extracted first TLS record; TLS handshake started
12175   Received Tunnel PAC
12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12801   Prepared TLS ChangeCipherSpec message

12816   TLS handshake succeeded
12132   EAP-FAST built PAC-based tunnel for purpose of authentication
12209   Starting EAP chaining
12227   User Authorization PAC has expired - will run inner method
12228   Machine Authorization PAC has expired - will run inner method
12218   Selected identity type 'User'

11806   Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402   User authentication against Active Directory succeeded - example.com
22037   Authentication Passed

12219   Selected identity type 'Machine'

24470   Machine authentication against Active Directory is successful - example.com
22037   Authentication Passed

12171   Successfully finished EAP-FAST user authorization PAC provisioning/update
12179   Successfully finished EAP-FAST machine authorization PAC provisioning/update

11503   Prepared EAP-Success
11002   Returned RADIUS Access-Accept
```

EAP-Fast met MAP-tunnelPAC verlopen

In deze stroom wanneer geen geldige tunnel PAC bestaat, vindt volledige TLS onderhandeling met binnenfase plaats.

- Leverancier verstuurt de TLS Client Hallo zonder Tunnel PAC.
- De server reageert met de betaling van het TLS-certificaat en certificaataanvraag.
- Leverancier moet het certificaat van de vertrouwensserver waarnemen, geen client certificaat sturen (certificatie lading is nul), TLS-tunnel gebouwd.
- ISE stuurt TLV-aanvraag voor het cliëntencertificaat binnen de TLS-tunnel, maar de aanvrager niet (het is niet nodig om dit te hebben om door te gaan).
- Begint EAP Chaining voor gebruiker, met gebruik van innerlijke methode met MSCHAPv2 authenticatie.
- Doorgaat met machinale authenticatie, met behulp van binnenmethode met MSCHAPv2-verificatie.
- Met succes leverde alle PACs (in ISE configuratie ingeschakeld) van voorzieningen.

```
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-Fast met MAP-koppeling en anonieme PAC-tunnelbevoorrading

In deze stroom wordt de tunnel van ISE en van NAM anoniem TLS gevormd voor PAC levering (ISE geauthentiseerde TLS tunnel voor PAC levering is gehandicapt) PAC leveringsverzoek lijkt als:

- Leverancier verstuurt TLS Client Hallo zonder meerdere cheries.
- De server reageert met de TLS Server Hallo en TLS anonieme Diffie Hellman ciphers

(bijvoorbeeld TLS_DH_anon_MET_AES_128_CBC_SHA).

- Leverancier aanvaardt het en de anonieme TLS-tunnel is gebouwd (geen uitgewisselde certificaten).
- Begint EAP Chaining voor gebruiker, met gebruik van innerlijke methode met MSCHAPv2 authenticatie.
- Doorgaat met machinale authenticatie, met behulp van binnenmethode met MSCHAPv2-verificatie.
- Aangezien de anonieme TLS-tunnel wordt aangelegd, zijn PAC's van vergunningen niet toegestaan.
- Radius Afwijzen wordt teruggegeven aan kracht van aanvrager om opnieuw te bevestigen (met bevoorraad 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
```

Wireshark pakketvastlegging voor anonieme TLS tunnelonderhandeling:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=190,	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	498	Access-Request(1) (id=191,	anonymous
10.48.17.14	10.62.148.109	RADIUS	793	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	706	Access-Request(1) (id=192,	anonymous
10.48.17.14	10.62.148.109	RADIUS	232	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=193,	anonymous
10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=194,	anonymous
10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=19	

```
Code: Request (1)
Id: 161
Length: 622
Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)
▷ EAP-TLS Flags: 0x01
▽ Secure Sockets Layer
  ▽ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 74
    ▽ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 70
        Version: TLS 1.0 (0x0301)
      ▷ Random
        Session ID Length: 32
        Session ID: 41aee5db065f48165c56144aa9dccdc93f67167fbae96393...
        Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA (0x0034)
        Compression Method: null (0)
  ▽ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
```

EAP Fast met MAP-gebonden gebruikersauthenticatie

In deze stroom wordt AnyConnect NAM met EAP-FAST en User (EAP-TLS) en Machine-verificatie (EAP-TLS) ingesteld. De Windows PC is opgestart maar de gebruikersreferenties worden niet meegeleverd. Switch start 802.1x sessie, NAM moet reageren maar gebruikersreferenties worden niet geboden (nog geen toegang tot gebruikerswinkel en certificaat). Verificatie van gebruikers mislukt terwijl de machine geslaagd is - ISE autorisatie "Netwerktoegang:EapChainingResultaat EQUALS Gebruiker mislukt en machine geslaagd" is bevonden. Later, de gebruiker logt in en een andere authenticatie zal starten, zowel gebruiker als machine.

- Leverancier stuurt TLS Client Hallo met machine-PAC.
- De server reageert met de TLS Change Cipher Spec - TLS-tunnel en wordt direct op basis van die PAC aangelegd.
- ISE start EAP Chaining en vraagt om gebruikersidentiteit.
- In plaats daarvan (gebruiker nog niet klaar) levert de poster de innerlijke methode van EAP-

TLS op.

- ISE vraagt opnieuw om gebruikersidentiteit en de aanvrager kan deze niet leveren.
- ISE stuurt TLV met een gemiddeld resultaat = storing (voor gebruikersverificatie).
- ISE retourneert het laatste EAP-succesbericht, ISE-conditie Network Access:EapChainingResultaat EQUALS Gebruiker mislukt en machine geslaagd is bevonden.

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800   Extracted first TLS record; TLS handshake started
12174   Received Machine PAC

12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12801   Prepared TLS ChangeCipherSpec message
12802   Prepared TLS Finished message

12816   TLS handshake succeeded
12132   EAP-FAST built PAC-based tunnel for purpose of authentication

12209   Starting EAP chaining
12218   Selected identity type 'User'

12213   Identity type provided by client is not equal to requested type
12215   Client suggested 'Machine' identity type instead

12104   Extracted EAP-Response containing EAP-FAST challenge-response
12523   Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12807   Prepared TLS Certificate message
12809   Prepared TLS CertificateRequest message

12816   TLS handshake succeeded
12509   EAP-TLS full handshake finished successfully

22070   Identity name is taken from certificate attribute
15013   Selected Identity Source - Test-AD
24323   Identity resolution detected single matching account
22037   Authentication Passed

12202   Approved EAP-FAST client Authorization PAC request
12218   Selected identity type 'User'
12213   Identity type provided by client is not equal to requested type
12216   Identity type provided by client was already used for authentication
12967   Sent EAP Intermediate Result TLV indicating failure

12179   Successfully finished EAP-FAST machine authorization PAC provisioning/update
12106   EAP-FAST authentication phase finished successfully
11503   Prepared EAP-Success
11002   Returned RADIUS Access-Accept
```

EAP-Fast met MAP-koppeling en onsamenhangende anonieme TLS-tunnelinstellingen

In deze stroom wordt ISE voor PAC-provisioning alleen via anonieme TLS-tunnels geconfigureerd, maar NAM gebruikt een geauthenticeerde TLS-tunnel, dan wordt het volgende vastgelegd door 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
```

Dit gebeurt wanneer NAM probeert een geauthentiseerde TLS-tunnel te bouwen met speciale TLS-ciphers - en deze worden niet geaccepteerd door ISE die is geconfigureerd voor anonieme TLS-tunnels (alleen DH-ciphers accepteren)

Problemen oplossen

ISE

Voor gedetailleerde logbestanden moeten de knoppen Runtime-AAA zijn ingeschakeld op het corresponderende PSN-knooppunt. Hieronder staan een paar voorbeelden van logbestanden van prt-server.log:

Wisselstroomproductie machine:

```
DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Using IID from PAC request for machine,EapFastTlv.cpp:1234

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Adding PAC of type=Machine Authorization,EapFastProtocol.cpp:3610

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Eap-Fast: Generating Pac, Issued PAC type=Machine Authorization
with expiration time: Fri Jul  3 10:38:30 2015
```

PAC vraagt om goedkeuring:

```
INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,user=host/mgarcarz-
pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine,EapFastProtocol.cpp:955

INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,user=host/mgarcarz-
pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine Authorization,EapFastProtocol.cpp:955
```

PAC-validatie:

```
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
```

Voorbeeld van succesvolle samenvatting voor PAC-generatie:

```
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
```

Voorbeeld van succesvolle samenvatting voor PAC-validatie:

```
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

DART-logbestanden van NAM geven de volgende details:

Voorbeeld voor niet EAP-Chaining sessie, machinale authenticatie zonder snelle herkoppeling:

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

Voorbeeld van de raadpleging van de PAC van de autorisatie (machinaal authentificeren voor niet-EAP-Chaining sessie):

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

Alle staten van de binnenmethode (voor MSCHAP) kunnen worden geverifieerd in de onderstaande stammen:

```
 EAP (0) EAP-MSCHAP-V2: State: 0 (eap_auth_mschapv2_c.c 731
 EAP (0) EAP-MSCHAP-V2: State: 2 (eap_auth_mschapv2_c.c 731
 EAP (0) EAP-MSCHAP-V2: State: 1 (eap_auth_mschapv2_c.c 731
 EAP (0) EAP-MSCHAP-V2: State: 4 (eap_auth_mschapv2_c.c 73
```

NAM staat de configuratie toe van de uitgebreide logoptie, die alle EAP-pakketten zal opnemen en deze in het PPP-bestand zal opslaan. Dit is vooral handig voor Start Vóór aanmelding (EAP-pakketten worden opgenomen voor alle authenticaties die zich voordoen vóór de aanmelding door de gebruiker). Vraag voor hoofdactivering uw TAC-ingenieur.

Referenties

- Cisco AnyConnect Secure Mobility Client-beheerdershandleiding, release 4.0 EAP-FAST-configuratie
- Administrator Guide van Cisco Identity Services Engine, release 1.4 EAP-FAST-

aanbevelingen
- Ontwerphandleidingen voor Cisco Identity Services Engine
- EAP-routing implementeren met AnyConnect NAM en Cisco ISE
- Technische ondersteuning en documentatie – Cisco Systems