EAP-FAST- und Verkettungsimplementierungen auf AnyConnect NAM und ISE

Inhalt

Einführung

In diesem Artikel werden Details zu EAP-FAST-Implementierungen auf dem Cisco AnyConnect Network Access Manager (NAM) und der Identity Services Engine (ISE) erläutert. Darüber hinaus wird erläutert, wie bestimmte Funktionen zusammenarbeiten, und es werden typische Anwendungsfälle und Beispiele vorgestellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse des EAP-Frameworks und der EAP-FAST-Methoden
- Grundkenntnisse der Identity Services Engine (ISE)
- Grundkenntnisse von AnyConnect NAM und Profile Editor
- Grundkenntnisse der Cisco Catalyst-Konfiguration für 802.1x-Services

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Windows 7 mit Cisco AnyConnect Secure Mobility Client, Version 3.1 und 4.0
- Cisco Catalyst 3750X Switch mit Software 15.2.1 und höher
- Cisco ISE, Version 1.4

Theorie

Phasen

EAP-FAST ist eine flexible EAP-Methode, die die gegenseitige Authentifizierung von Supplicant und Server ermöglicht. Sie ähnelt EAP-PEAP, erfordert jedoch in der Regel keine Client- oder Serverzertifikate. Ein Vorteil von EAP-FAST ist die Fähigkeit, mehrere Authentifizierungen (mit mehreren inneren Methoden) zu verketten und kryptografisch zusammenzubinden (EAP Chaining). In Implementierungen von Cisco wird dies für Benutzer- und Computerauthentifizierungen verwendet.

EAP-FAST verwendet Protected Access Credentials (PAC), um schnell den TLS-Tunnel (Sitzungswiederaufnahme) einzurichten oder den Benutzer/das System zu autorisieren (überspringen Sie die innere Authentifizierungsmethode).

EAP-FAST umfasst drei Phasen:

- Phase 0 (PAC-Bereitstellung)
- Phase 1 (TLS-Tunneleinrichtung)
- Phase 2 (Authentifizierung)

EAP-FAST unterstützt Konversationen ohne PAC und PAC. PAC-basiert besteht aus PAC-Bereitstellung und PAC-basierter Authentifizierung. Die PAC-Bereitstellung kann auf einer anonymen oder authentifizierten TLS-Sitzung basieren.

PAC

PAC ist die geschützten Zugriffsberechtigungen, die vom Server generiert und dem Client bereitgestellt werden. Es besteht aus:

- PAC-Schlüssel (willkürlicher geheimer Wert, der zum Ableiten von TLS-Master- und Sitzungsschlüsseln verwendet wird)
- PAC Opak (PAC-Schlüssel + Benutzeridentität - alle verschlüsselt mit EAP-FAST-Server-Master-Schlüssel)
- PAC-Informationen (Serveridentität, TTL-Timer)

Der Server, der die PAC ausgibt, verschlüsselt den PAC-Schlüssel und die PAC-Identität mithilfe des EAP-FAST-Server-Master-Schlüssels (d. h. PAC-deckend) und sendet die gesamte PAC an den Client. Es werden keine anderen Informationen gespeichert bzw. gespeichert (mit Ausnahme des Master-Schlüssels, der für alle PACs identisch ist).

Sobald die PAC-Opak empfangen wurde, wird sie mithilfe des EAP-FAST-Server-Master-Schlüssels entschlüsselt und validiert. Der PAC-Schlüssel wird zum Ableiten der TLS-Master- und Sitzungsschlüssel für einen abgekürzten TLS-Tunnel verwendet.

Nach Ablauf des vorherigen Master-Schlüssels werden neue EAP-FAST-Servermaster-Schlüssel generiert. In einigen Fällen kann ein Master-Schlüssel widerrufen werden.

Derzeit werden einige PAC-Typen verwendet:

- Tunnel PAC (Tunnel-PAC): wird für die TLS-Tunneleinrichtung (ohne Client- oder Serverzertifikat) verwendet. Gesendet in TLS-Client Hello
- Rechner-PAC: wird für die TLS-Tunneleinrichtung und die sofortige Maschinenautorisierung verwendet. Gesendet in TLS-Client Hello
- PAC für Benutzerautorisierung: wird für die sofortige Benutzerauthentifizierung verwendet (überspringen Sie die innere Methode), wenn der Server dies zulässt. Gesendet im TLS-Tunnel unter Verwendung von TLV.
- PAC für die Maschinenautorisierung: wird für die sofortige maschinelle Authentifizierung (Überspringen der inneren Methode) verwendet, wenn der Server dies zulässt. Gesendet im TLS-Tunnel unter Verwendung von TLV.
- TrustSec-PAC: für die Zulassung bei der Durchführung von Umgebungs- oder Richtlinienaktualisierungen.

Alle diese PACs werden in der Regel automatisch in Phase 0 ausgeliefert. Einige der PACs (Tunnel, Machine, TrustSec) können auch manuell bereitgestellt werden.

Wenn PACs generiert werden

- Tunnel-PAC: nach erfolgreicher Authentifizierung (innere Methode) bereitgestellt, wenn zuvor nicht verwendet.
- Autorisierungs-PAC: nach erfolgreicher Authentifizierung (innere Methode) bereitgestellt, wenn zuvor nicht verwendet.
- Rechner-PAC: wird nach erfolgreicher maschineller Authentifizierung (innere Methode) bereitgestellt, wenn zuvor keine Autorisierungs-PAC verwendet wurde. Sie wird bereitgestellt, wenn die Tunnel-PAC abläuft, jedoch nicht, wenn die Autorisierungs-PAC abläuft. Sie wird bereitgestellt, wenn EAP-Chaining aktiviert oder deaktiviert ist.

Hinweis:

Für jede PAC-Bereitstellung ist eine erfolgreiche Authentifizierung erforderlich, mit Ausnahme des folgenden Anwendungsfalls: Autorisierter Benutzer bittet um die PAC des Computers für einen Computer, der über kein AD-Konto verfügt.

Die folgende Tabelle fasst die Bereitstellungs- und die proaktive Aktualisierungsfunktion zusammen:

PAC-Typ	Tunnel v1/v1a/CTS	Maschine	Autorisierung
			nur bei authentifizierte
PAC auf Anfrage bei Bereitstellung bereitstellen	Ja	Nur bei authentifizierter Bereitstellung	Bereitstellung und we Tunnel-PAC ebenfalls angefordert wird
PAC auf Anfrage bei Authentifizierung bereitstellen	Ja	Ja	Nur wenn es in diese Authentifizierung nich verwendet wurde
Proaktive Aktualisierung	Ja	Nein	Nein
Wenn nach fehlgeschlagener PAC-basierter Authentifizierung (z. B. wenn PAC abgelaufen ist) auf PAC-Bereitstellung zurückgegriffen wird	die neue nicht weitergeben	die neue nicht weitergeben	die neue nicht weiterg
Unterstützung von ACS 4.x-PACs	für Tunnel PAC v1/v1a	Ja	Nein

EAP-FAST Server Master Key ACS 4.x vs. ACS 5x und ISE

Beim Vergleich von ACS 4.x und ISE besteht ein leichter Unterschied in der Master-Schlüsselbearbeitung.

Funktion	ACS 4.1.2	ACS 5.x/ISE
Master-Schlüssel	Der Master-Schlüssel hat TTL, kann aktiv, außer Kraft gesetzt oder abgelaufen sein.	Der Master-Schlüssel wird automatisch aus dem Seed in jedem konfigurierten Zeitraum generiert. Spezifischer Master Key ist immer zugänglich und niemals abgelaufen
PAC-Aktualisierung	PAC-Update wird vom Server gesendet, wenn PAC abgelaufen ist, es sei denn, der für die PAC-Verschlüsselung verwendete Master-Schlüssel ist abgelaufen	Die PAC-Aktualisierung wird vom Server nach der ersten erfolgreichen Authentifizierung gesendet, die innerhalb eines bestimmten konfigurierbaren Zeitraums vor dem Ablaufdatum der PAC durchgeführt wird.

Mit anderen Worten: Die ISE behält alle alten Master-Schlüssel bei und generiert standardmäßig einmal pro Woche einen neuen. Da der Master-Schlüssel nicht ablaufen kann, wird nur die PAC-TTL validiert.

Der Zeitraum für die ISE-Master-Key-Generierung wird über *Administration -> Settings -> Protocol -> EAP-FAST -> EAP-FAST Settings* konfiguriert.

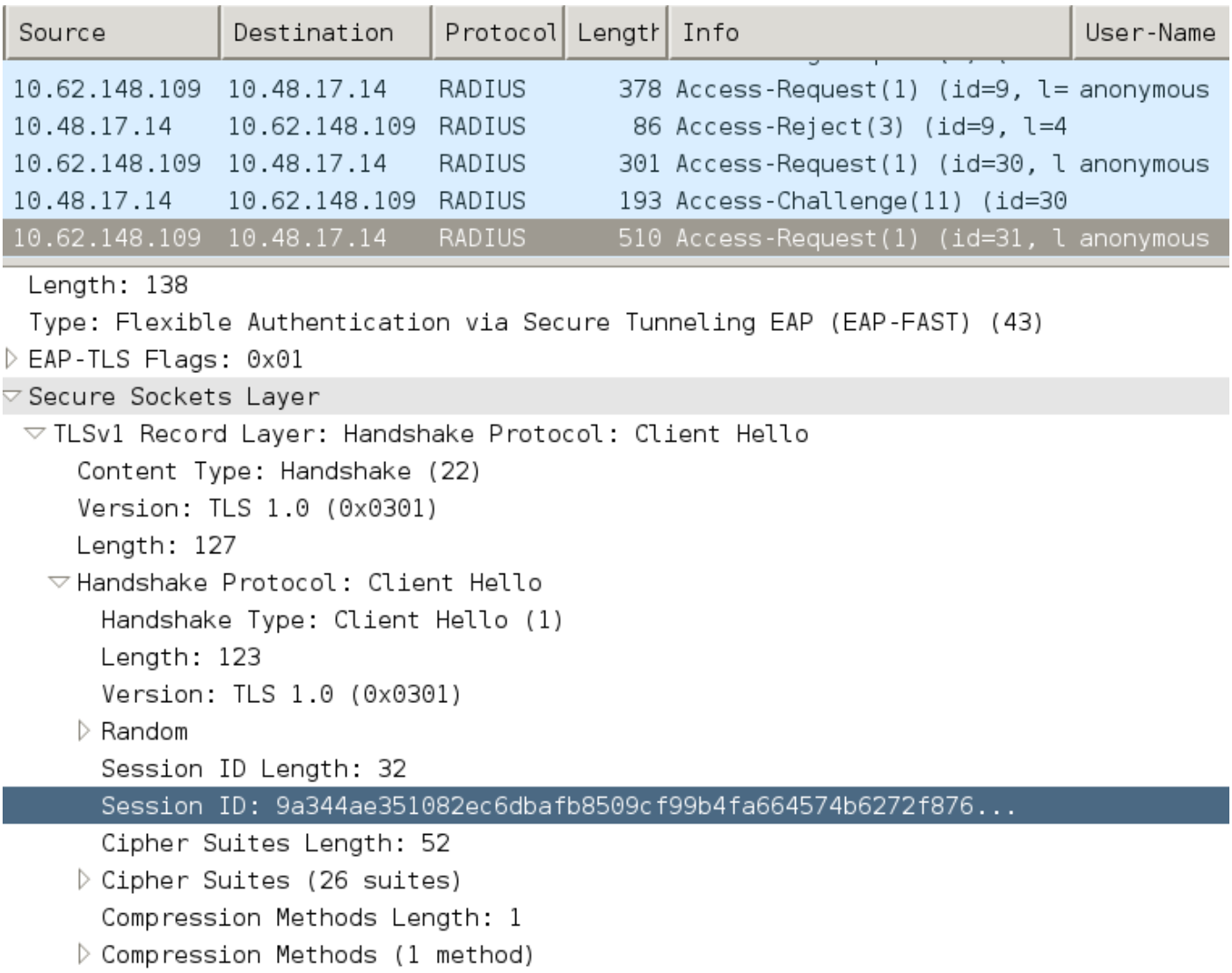
Sitzungswiederaufnahme

Dies ist eine wichtige Komponente, die die PAC-Nutzung durch Tunnel ermöglicht. Sie ermöglicht die Neuverhandlung von TLS-Tunneln ohne Verwendung von Zertifikaten.

Es gibt zwei Sitzungswiederaufnahmetypen für EAP-FAST: Serverstatus basiert und stateless (PAC-basiert).

Serverstatus

Die standardmäßige TLS-basierte Methode basiert auf der auf dem Server zwischengespeicherten TLS SessionID. Der Client, der den TLS-Client-Hello sendet, fügt die SessionID hinzu, um die Sitzung wieder aufzunehmen. Die Sitzung wird nur für die PAC-Bereitstellung bei Verwendung eines anonymen TLS-Tunnels verwendet:



Stateless (PAC-basiert)

Benutzer-/Maschinenautorisierungs-PAC wird zum Speichern der vorherigen Authentifizierungs- und Autorisierungsstatus für den Peer verwendet.

Die clientseitige Wiederaufnahme basiert auf RFC 4507. Der Server muss keine Daten zwischenspeichern. Stattdessen fügt der Client die PAC in die Erweiterung TLS Client Hello

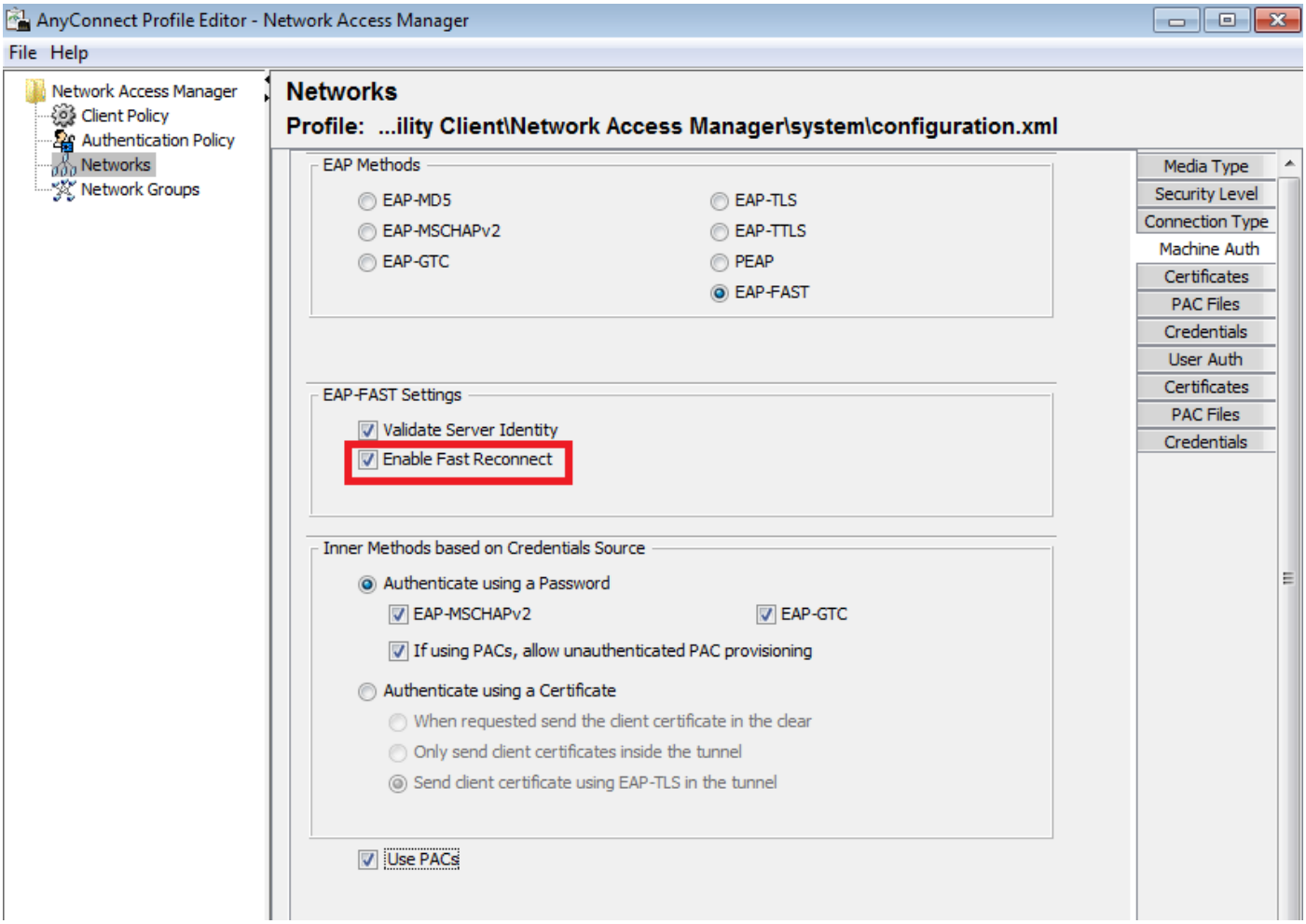
SessionTicket hinzu. Die PAC wird wiederum vom Server validiert. Beispiel basierend auf dem Tunnel-PAC, der dem Server bereitgestellt wird:

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

```
▽ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 281
  ▽ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 277
      Version: TLS 1.0 (0x0301)
    ▷ Random
      Session ID Length: 0
      Cipher Suites Length: 52
    ▷ Cipher Suites (26 suites)
      Compression Methods Length: 1
    ▷ Compression Methods (1 method)
      Extensions Length: 184
    ▽ Extension: SessionTicket TLS
        Type: SessionTicket TLS (0x0023)
        Length: 180
        Data (180 bytes)
▷ AVP: l=18  t=Message-Authenticator(80): 0cb2477c076ea96d3ba150245e6291e8
```

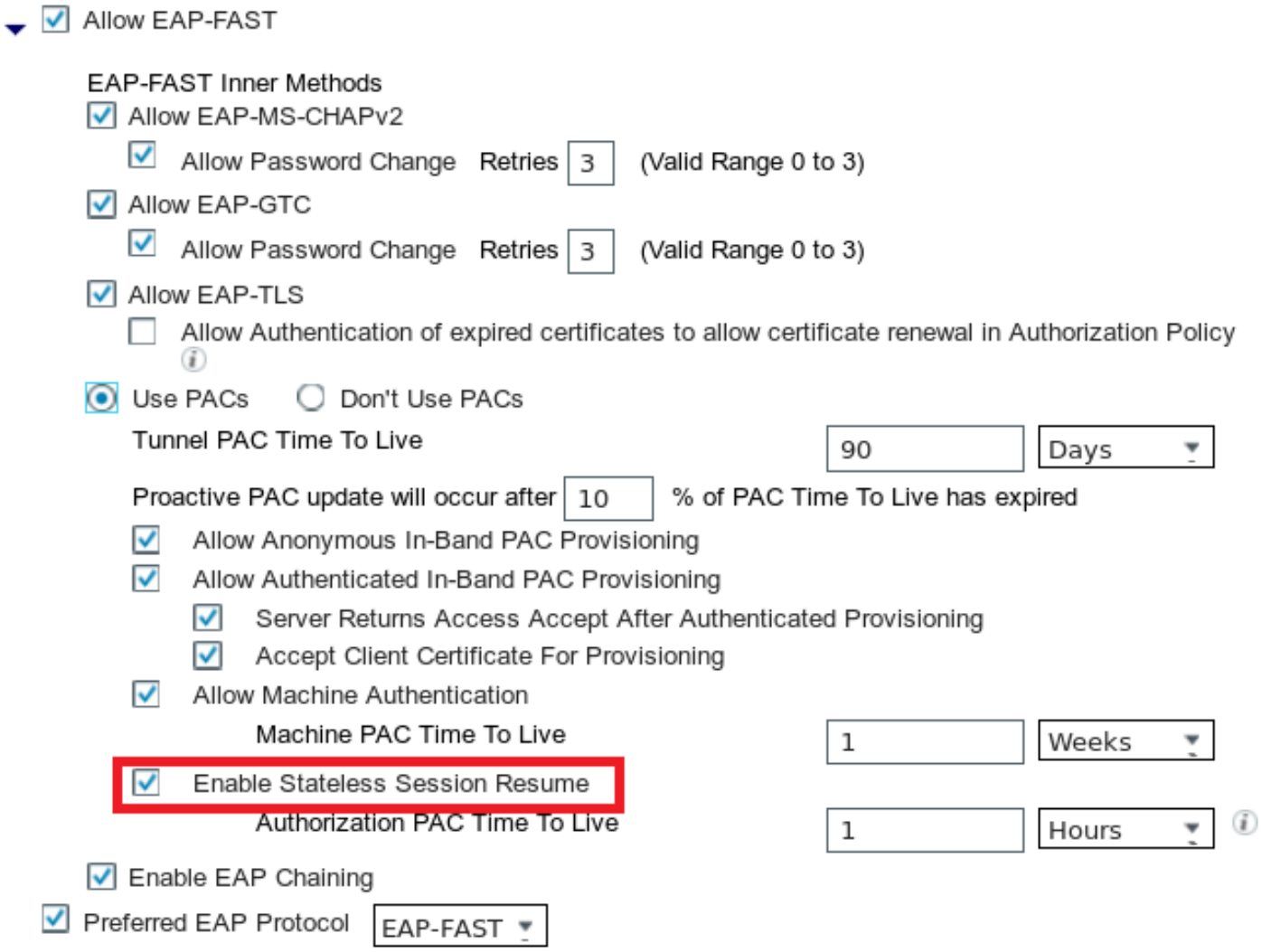
AnyConnect NAM-Implementierung

Sie wird auf Client-Seite (AnyConnect NAM) über Fast Reconnect aktiviert, dient jedoch nur zur Steuerung der PAC-Nutzung.



Wenn die Einstellung deaktiviert ist, verwendet NAM weiterhin die Tunnel-PAC, um den TLS-Tunnel zu erstellen (keine Zertifikate erforderlich). Dies verwendet jedoch keine Autorisierungs-PACs, um eine sofortige Benutzer- und Computerautorisierung durchzuführen. Daher wird immer Phase 2 mit der inneren Methode benötigt.

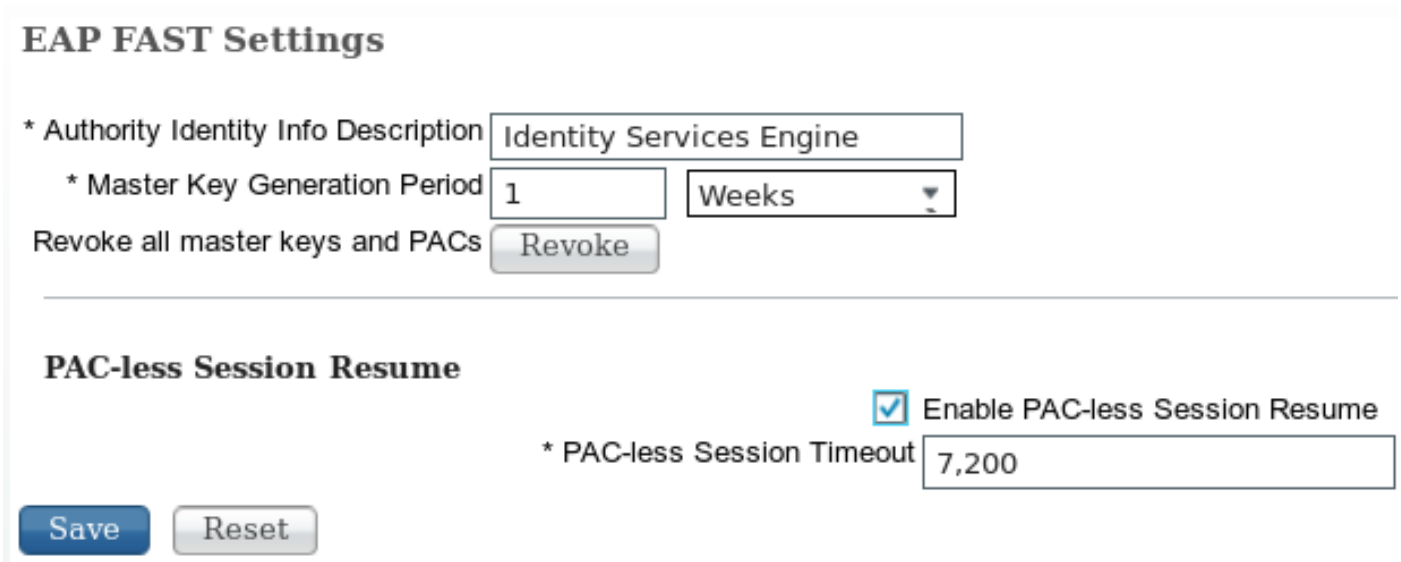
Die ISE hat die Option, das Stateless Session Resume zu aktivieren. Und wie bei NAM ist es nur für Autorisierungs-PAC. Die PAC-Nutzung für Tunnel wird über die Option "Use PACs" (PACs verwenden) gesteuert.



NAM versucht, PACs zu verwenden, wenn die Option aktiviert ist. Wenn in der ISE "PACs nicht verwenden" konfiguriert ist und die ISE eine Tunnel-PAC in der TLS-Erweiterung empfängt, wird folgender Fehler gemeldet und ein EAP-Fehler wird zurückgegeben:

hier einfügen

In der ISE muss auch die Sitzungswiederaufnahme auf der Grundlage der TLS-SessionID (von den globalen EAP-FAST-Einstellungen) aktiviert werden. Es ist standardmäßig deaktiviert:



Bitte beachten Sie, dass nur ein Sitzungswiederaufnahmetyp verwendet werden kann. Sitzungs-ID-basiert wird nur für PAC-lose Bereitstellungen verwendet, RFC 4507-basiert nur für PAC-Bereitstellungen.

PAC-Bereitstellung (Phase 0)

PACs können automatisch in Phase0 bereitgestellt werden. Phase 0 umfasst:

- TLS-Tunneleinrichtung
- Authentifizierung (innere Methode)

PACs werden nach erfolgreicher Authentifizierung im TLS-Tunnel über PAC TLV (und PAC TLV-Bestätigung) bereitgestellt.

Anonymer TLS-Tunnel

Für Bereitstellungen ohne PKI-Infrastruktur kann ein anonymer TLS-Tunnel verwendet werden. Der anonyme TLS-Tunnel wird mithilfe der Diffie Hellman-Verschlüsselungs-Suite erstellt, ohne dass ein Server- oder Clientzertifikat erforderlich ist. Dieser Ansatz ist anfällig für Man in the Middle Attacks (Identitätswechsel).

Um diese Option verwenden zu können, benötigt NAM die folgende konfigurierte Option:

"Wenn PACs eine nicht authentifizierte PAC-Bereitstellung ermöglichen" (das ist nur für eine kennwortbasierte innere Methode sinnvoll, da es ohne PKI-Infrastruktur nicht möglich ist, eine zertifikatsbasierte innere Methode zu verwenden).

Darüber hinaus muss die ISE die folgenden, unter den Authentifizierungsprotokollen konfigurierten Protokolle konfigurieren:

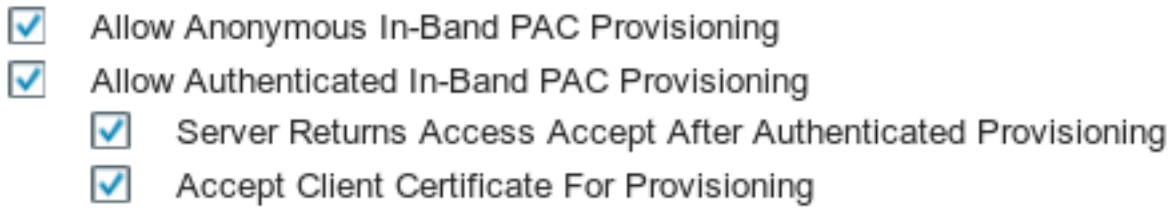
"Anonyme In-Band-PAC-Bereitstellung zulassen"

Anonyme In-Band-PAC-Bereitstellung wird in TrustSec NDAC-Bereitstellungen (EAP-FAST-Sitzungen, die zwischen Netzwerkgeräten ausgehandelt werden) verwendet.

Authentifizierter TLS-Tunnel

Dies ist die sicherste und empfohlene Option. Der TLS-Tunnel basiert auf dem Serverzertifikat, das vom Supplicant validiert wird. Dies erfordert eine PKI-Infrastruktur nur auf Serverseite, die für ISE erforderlich ist (bei NAM ist es möglich, die Option "Serveridentität validieren" zu deaktivieren.

Für die ISE gibt es zwei zusätzliche Optionen:



Normalerweise sollte nach der PAC-Bereitstellung eine Access-Reject gesendet werden, die die Komponente zwingt, sich mithilfe von PACs erneut zu authentifizieren. Da die PACs jedoch im TLS-Tunnel mit Authentifizierung bereitgestellt wurden, ist es möglich, den gesamten Prozess zu

verkürzen und die Access-Accept-Option unmittelbar nach der PAC-Bereitstellung zurückzugeben.

Bei der zweiten Option wird der TLS-Tunnel basierend auf dem Clientzertifikat erstellt (hierfür ist die PKI-Bereitstellung auf den Endpunkten erforderlich). Dadurch kann der TLS-Tunnel mit gegenseitiger Authentifizierung erstellt werden. Dadurch wird die innere Methode übersprungen und die PAC-Bereitstellungsphase direkt abgeschlossen. Es ist wichtig, hier vorsichtig zu sein. Manchmal präsentiert der Supplicant ein Zertifikat, das von der ISE nicht als vertrauenswürdig eingestuft wird (das für andere Zwecke bestimmt ist), und die Sitzung schlägt fehl.

EAP-Verkettung

Ermöglicht die Benutzer- und Computerauthentifizierung innerhalb einer Radius/EAP-Sitzung. Mehrere EAP-Methoden können verkettet werden. Nachdem die erste Authentifizierung (in der Regel der Computer) erfolgreich abgeschlossen wurde, sendet der Server eine TLV mit Zwischenergebnissen (im TLS-Tunnel), die auf Erfolg hinweist. Diese TLV muss von einer Krypto-Binding-TLV-Anforderung begleitet sein. Cryptobinding wird verwendet, um zu beweisen, dass sowohl der Server als auch der Peer an der bestimmten Authentifizierungssequenz teilgenommen haben. Der Cryptobindungsprozess verwendet das Keying-Material aus Phase 1 und Phase 2. Zusätzlich ist eine weitere TLV angehängt: EAP-Payload: Diese Funktion initiiert die neue Sitzung (in der Regel für den Benutzer). Sobald der Radius-Server (ISE) die Crypto-Binding TLV Response empfängt und validiert hat, wird im Protokoll Folgendes angezeigt und die nächste EAP-Methode ausprobiert (in der Regel für die Benutzerauthentifizierung):

12126 **EAP-FAST cryptobinding verification passed**

Wenn die Verschlüsselungsvalidierung fehlschlägt, schlägt die gesamte EAP-Sitzung fehl. Wenn eine der Authentifizierungen innerhalb des Netzwerks fehlgeschlagen ist, ist es immer noch in Ordnung. Infolgedessen kann ein Administrator mit der ISE mehrere Ketingergebnisse auf Grundlage der Autorisierungsbedingung Netzwerkzugriff:EapChainingResult:

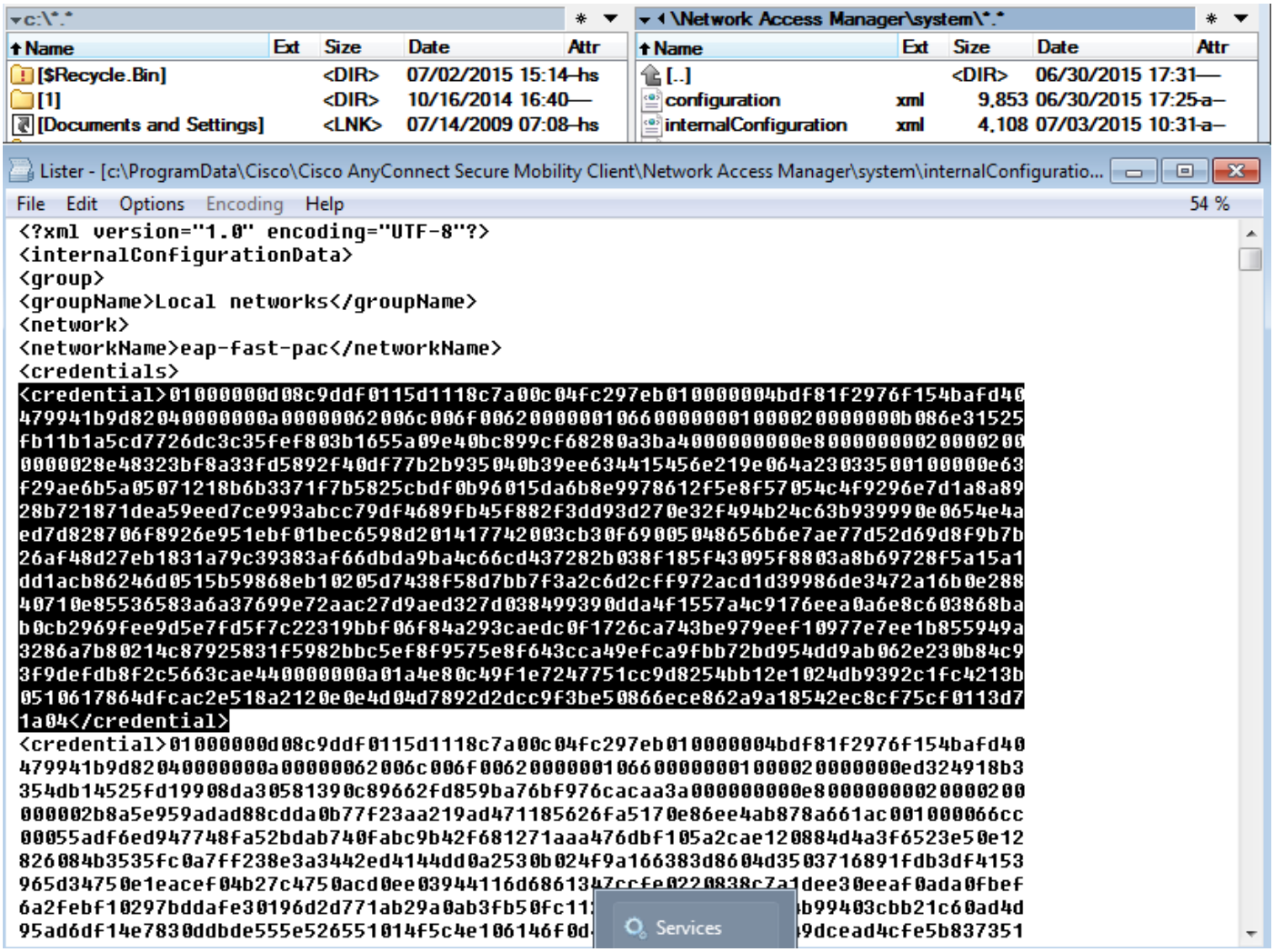
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-Chaining wird im NAM automatisch aktiviert, wenn die EAP-FAST-Benutzer- und Maschinenauthentifizierung aktiviert ist.

EAP-Verkettung muss in der ISE konfiguriert werden.

Wo PAC-Dateien gespeichert werden

Standardmäßig werden Tunnel- und Machine-PACs in den Abschnitten <credential> unter C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml gespeichert. Diese werden verschlüsselt gespeichert.

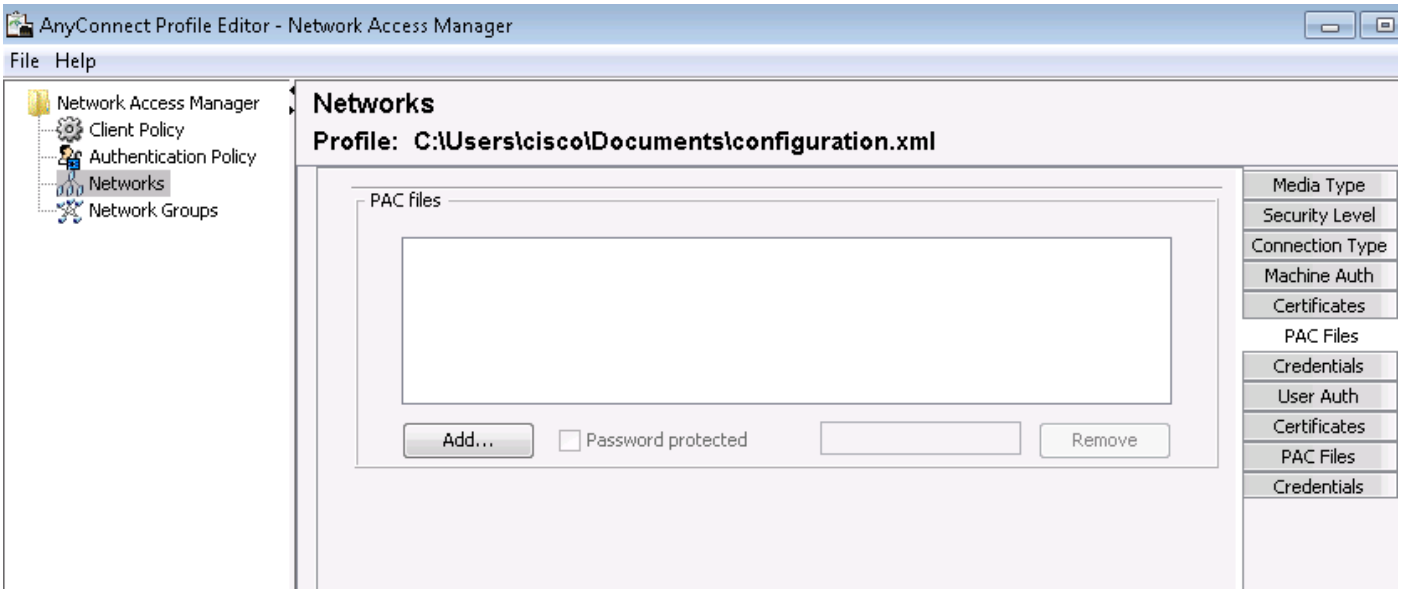


Autorisierungs-PACs werden nur im Speicher gespeichert und nach einem Neustart oder einem Neustart des NAM-Services entfernt.

Ein Service-Neustart ist erforderlich, um den Tunnel- oder Computer-PAC zu entfernen.

AnyConnect NAM 3.1 im Vergleich zu 4.0

Mit dem AnyConnect 3.x NAM-Profil-Editor konnte der Administrator PACs manuell konfigurieren. Diese Funktion wurde aus dem AnyConnect 4.x NAM-Profil-Editor entfernt.

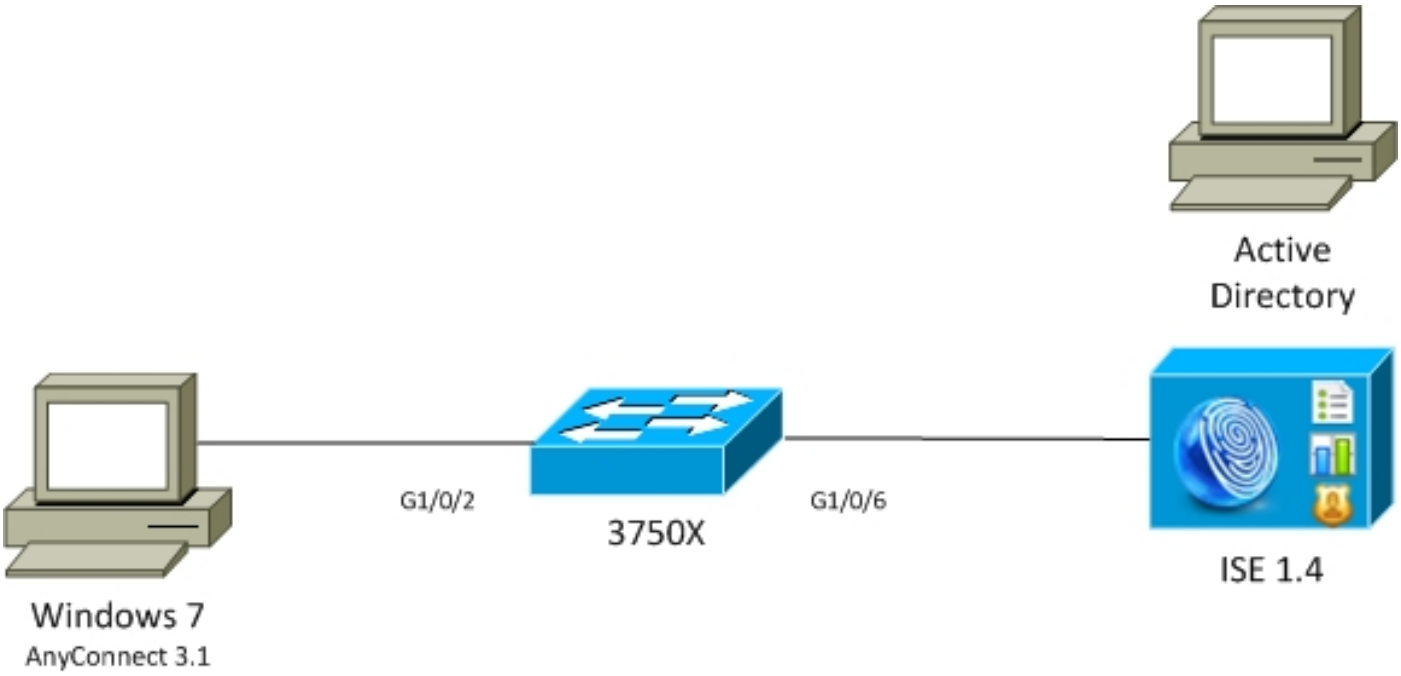


Die Entscheidung, diese Funktionalität zu entfernen, basiert auf CSCuf31422 und CSCua13140 .

Beispiele

Netzwerkdiagramm

Alle Beispiele wurden mithilfe der folgenden Netzwerktopologie getestet. Gleiches gilt auch bei der Verwendung von Wireless-Netzwerken.



EAP-Fast ohne EAP-Verkettung mit Benutzer- und Computer-PAC

EAP_Chaining ist auf der ISE standardmäßig deaktiviert. Alle anderen Optionen sind jedoch aktiviert, einschließlich Rechner- und Autorisierungs-PACs. Der Supplicant verfügt bereits über eine gültige Computer- und Tunnel-PAC. In diesem Datenfluss gibt es zwei separate Authentifizierungen - eine für den Computer und eine für den Benutzer - mit separaten Protokollen für die ISE. Die Hauptschritte werden von der ISE protokolliert. Erste Authentifizierung (Rechner):

- Der Supplicant sendet TLS-Client Hello mit Machine PAC.
- Der Server validiert die Computer-PAC und erstellt den TLS-Tunnel (es werden keine Zertifikate verwendet).
- Der Server validiert die Computer-PAC, führt die Kontosuche in Active Directory durch und überspringt die innere Methode.

```
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
```

Die zweite Authentifizierung (Benutzer):

- Der Supplicant sendet den TLS-Client Hello mit Tunnel-PAC.
- Der Server validiert die PAC und erstellt den TLS-Tunnel (es werden keine Zertifikate verwendet).
- Da der Supplicant über keine Autorisierungs-PAC verfügt, wird die innere Methode (EAP-MSCHAP) für die Authentifizierung verwendet.

```
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
```

Im Abschnitt "Andere Attribute" des detaillierten Berichts in der ISE wird Folgendes sowohl für die Benutzer- als auch für die Computerauthentifizierung angegeben:

```
EapChainingResult: No chaining
```

EAP-Fast mit EAP-Verkettung mit PAC Fast Reconnect

In diesem Datenfluss verfügt der Supplicant bereits über eine gültige Tunnel-PAC sowie die Benutzer- und Maschinenautorisierungs-PACs:

- Der Supplicant sendet den TLS-Client Hello mit Tunnel-PAC.
- Der Server validiert die PAC und erstellt den TLS-Tunnel (es werden keine Zertifikate verwendet).
- ISE startet EAP-Verkettung, die Komponente fügt Autorisierungs-PACs für Benutzer und Computer mithilfe von TLV im TLS-Tunnel an.
- Die ISE validiert die Autorisierungs-PACs (keine interne Methode erforderlich), überprüft, ob Konten in Active Directory vorhanden sind (keine zusätzliche Authentifizierung), gibt den Erfolg zurück.

```
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
```

Im Abschnitt "Andere Attribute" des detaillierten Berichts in der ISE wird Folgendes vermerkt:

```
EapChainingResult: EAP Chaining
```

Darüber hinaus sind sowohl Benutzer- als auch Computeranmeldeinformationen im gleichen Protokoll enthalten, wie im Folgenden dargestellt:

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

EAP-Fast mit EAP-Verkettung ohne PAC

In diesem Datenfluss ist das NAM so konfiguriert, dass es keine PAC verwendet. Die ISE ist auch so konfiguriert, dass sie keine PAC verwendet (jedoch mit EAP-Verkettung).

- Supplicant sendet TLS-Client-Hello ohne Tunnel-PAC.
- Der Server reagiert mit den Payloads für TLS-Zertifikat und Zertifikatsanforderung.
- Der Supplicant muss dem Serverzertifikat vertrauen, kein Clientzertifikat senden (Zertifikatsnutzlast ist Null), TLS-Tunnel wird erstellt.
- Die ISE sendet eine TLV-Anfrage für das Client-Zertifikat im TLS-Tunnel, der Supplicant jedoch nicht (es ist nicht erforderlich, das Zertifikat zu besitzen, um fortzufahren).

- Startet die EAP-Verkettung für den Benutzer mithilfe der inneren Methode mit der MSCHAPv2-Authentifizierung.
- Fortsetzung der Maschinenauthentifizierung unter Verwendung der internen Methode mit MSCHAPv2-Authentifizierung.
- Es werden keine PACs bereitgestellt.

```
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 mit EAP-Verkettung, Autorisierung, PAC-Ablauf

In diesem Datenfluss verfügt der Supplicant über eine gültige Tunnel-PAC, hat jedoch abgelaufene Autorisierungs-PACs:

- Der Supplicant sendet den TLS-Client Hello mit Tunnel-PAC.
- Der Server validiert die PAC und erstellt den TLS-Tunnel (es werden keine Zertifikate verwendet).
- ISE startet EAP-Verkettung, die Komponente fügt Autorisierungs-PACs für Benutzer und

Computer mithilfe von TLV im TLS-Tunnel an.
- Da die PACs abgelaufen sind, wird die innere Methode für Benutzer und Rechner gestartet (EAP-MSCHAP).
- Sobald beide Authentifizierungen erfolgreich sind, werden Benutzer- und Rechnerautorisierungs-PACs bereitgestellt.

```
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 mit EAP-Verkettungstunnel-PAC ist abgelaufen

Wenn in diesem Fluss kein gültiger Tunnel-PAC vorhanden ist, wird eine vollständige TLS-Aushandlung mit der inneren Phase durchgeführt.

- Der Supplicant sendet den TLS-Client Hello ohne Tunnel-PAC.
- Der Server reagiert mit den Payloads für TLS-Zertifikat und Zertifikatsanforderung.
- Der Supplicant muss dem Serverzertifikat vertrauen, sendet kein Client-Zertifikat (Zertifikatsnutzlast ist Null), TLS-Tunnel erstellt.
- Die ISE sendet eine TLV-Anfrage für das Client-Zertifikat im TLS-Tunnel, der Supplicant jedoch nicht (es ist nicht erforderlich, das Zertifikat zu besitzen, um fortzufahren).
- Startet die EAP-Verkettung für den Benutzer mithilfe der inneren Methode mit der MSCHAPv2-Authentifizierung.
- Fortsetzung der Maschinenauthentifizierung unter Verwendung der internen Methode mit MSCHAPv2-Authentifizierung.
- Erfolgreiche Bereitstellung aller PACs (in ISE-Konfiguration aktiviert).

```
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 mit EAP-Verkettung und anonymer TLS-Tunnel-PAC-Bereitstellung

In diesem Datenfluss wird der ISE- und der anonyme NAM-TLS-Tunnel für die PAC-Bereitstellung konfiguriert (ISE-authentifizierter TLS-Tunnel für PAC-Bereitstellung ist deaktiviert). Die PAC-Bereitstellungsanfrage sieht wie folgt aus:

- Supplicant sendet TLS-Client-Hello ohne mehrere Skripte.
- Der Server antwortet mit dem TLS-Server Hello und den anonymen TLS-Diffie-Hellman-Chiffren (z. B. TLS_DH_Anon_WITH_AES_128_CBC_SHA).
- Der Supplicant akzeptiert diese und der anonyme TLS-Tunnel wird erstellt (es werden keine Zertifikate ausgetauscht).
- Startet die EAP-Verkettung für den Benutzer mithilfe der inneren Methode mit der MSCHAPv2-Authentifizierung.
- Fortsetzung der Maschinenauthentifizierung unter Verwendung der internen Methode mit MSCHAPv2-Authentifizierung.
- Da der anonyme TLS-Tunnel erstellt wird, sind Autorisierungs-PACs nicht zulässig.
- Radius Reject wird zurückgegeben, um zu erzwingen, dass die Komponente erneut authentifiziert wird (mithilfe von bereitgestellter 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-Paketerfassung für anonyme TLS-Tunnelverhandlung:

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 mit EAP-Verkettung - nur Benutzerauthentifizierung

In diesem Datenfluss wird AnyConnect NAM mit EAP-FAST und User (EAP-TLS) und Machine Authentication (EAP-TLS) konfiguriert. Der Windows-PC wird gestartet, es werden jedoch keine Benutzeranmeldeinformationen bereitgestellt. Switch initiiert 802.1x-Sitzung, NAM muss jedoch antworten, Benutzeranmeldeinformationen werden nicht bereitgestellt (noch kein Zugriff auf Benutzerspeicher und -zertifikat). Die Benutzerauthentifizierung schlägt fehl, während der Computer erfolgreich ist - ISE-Authentifizierungsbedingung "Netzwerkzugriff:EapChainingResult EQUALS User failed and machine successfully" (Netzwerkzugriff:EapChainingResult EQUALS User fehlgeschlagen und maschinell erfolgreich ausgeführt) ist erfüllt. Später meldet sich der Benutzer an, und eine weitere Authentifizierung wird gestartet, sowohl der Benutzer als auch der Computer sind erfolgreich.

- Der Supplicant sendet TLS-Client Hello mit Machine PAC.
- Der Server reagiert mit der TLS-Change-Cipher-Spez. - Der TLS-Tunnel wird sofort auf Basis

dieser PAC erstellt.

- Die ISE initiiert die EAP-Verkettung und fragt nach der Benutzeridentität.
- Supplicant stellt stattdessen die Geräteidentität bereit (Benutzer noch nicht bereit), beendet die innere EAP-TLS-Methode.
- Die ISE fragt erneut nach der Benutzeridentität, die Komponente kann sie nicht bereitstellen.
- ISE sendet TLV mit Zwischenergebnis = Fehler (für Benutzerauthentifizierung).
- ISE gibt die letzte EAP-Erfolgsmeldung zurück, ISE Conditional Network Access:EapChainingResult EQUALS User failed (ISE-Bedingung für Netzwerkzugriff), und der erfolgreiche Computer ist zufrieden.

```
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 mit EAP-Verkettung und inkonsistenten anonymen TLS-Tunneleinstellungen

In diesem Datenfluss wird die ISE für die PAC-Bereitstellung nur über einen anonymen TLS-Tunnel konfiguriert. Das NAM verwendet jedoch einen authentifizierten TLS-Tunnel. Folgendes wird von der ISE protokolliert:

```
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
```

Dies tritt auf, wenn NAM versucht, einen authentifizierten TLS-Tunnel mit den spezifischen TLS-Chiffren zu erstellen - und diese werden von der ISE nicht akzeptiert, die für einen anonymen TLS-Tunnel konfiguriert ist (nur DH-Chiffre akzeptiert).

Fehlerbehebung

ISE

Für detaillierte Protokolle sollten LaufzeitAAA-Debugger auf dem entsprechenden PSN-Knoten aktiviert werden. Nachfolgend finden Sie einige Beispielprotokolle von prt-server.log:

PAC-Generierung für Systeme:

```
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-Anforderungsgenehmigung:

```
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-Validierung:

```
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
```

Beispiel für eine erfolgreiche Zusammenfassung für die PAC-Erstellung:

```
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
```

Beispiel für eine erfolgreiche Zusammenfassung für die PAC-Validierung:

```
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

Die DART-Protokolle von NAM enthalten folgende Details:

Beispiel für Nicht-EAP-Verkettung, Machine Authentication ohne schnelle Wiederherstellung der Verbindung:

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

Beispiel für die PAC-Suche für die Autorisierung (maschinelle Authentifizierung für Sitzungen ohne EAP-Verkettung):

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

Alle Zustände der inneren Methode (für MSCHAP) können aus den folgenden Protokollen überprüft werden:

```
 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 ermöglicht die Konfiguration der erweiterten Protokollierungsfunktion, mit der alle EAP-Pakete erfasst und in der pcap-Datei gespeichert werden. Dies ist besonders bei der Funktion "Start Before Logon" (Vor Anmeldung anmelden) hilfreich (EAP-Pakete werden auch für Authentifizierungen erfasst, die vor der Anmeldung beim Benutzer auftreten). Fragen Sie Ihren TAC-Techniker zur Funktionsaktivierung.

Referenzen

- Administratorhandbuch für den Cisco AnyConnect Secure Mobility Client, Version 4.0 EAP-FAST-Konfiguration
- Administratoranleitung für Cisco Identity Services Engine, Release 1.4, EAP-FAST-Empfehlungen
- Designleitfäden für die Cisco Identity Services Engine
- Bereitstellung von EAP-Verkettung mit AnyConnect NAM und Cisco ISE
- Technischer Support und Dokumentation - Cisco Systems