AnyConnect NAM 및 ISE의 EAP-FAST 및 체인 구현 이해

목차

소개

이 문서에서는 Cisco AnyConnect NAM(Network Access Manager) 및 ISE(Identity Services Engine)의 EAP-FAST 구현에 대한 세부 정보를 설명합니다. 또한 특정 기능이 어떻게 연동되는지 설명하고 일반적인 활용 사례와 예를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- EAP 프레임워크 및 EAP-FAST 방법에 대한 기본 지식
- ISE(Identity Services Engine)에 대한 기본 지식
- AnyConnect NAM 및 프로파일 편집기에 대한 기본 지식
- 802.1x 서비스를 위한 Cisco Catalyst 구성에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Windows 7 with Cisco AnyConnect Secure Mobility Client, 릴리스 3.1 및 4.0
- Cisco Catalyst 3750X 스위치(소프트웨어 15.2.1 이상)
- Cisco ISE, 릴리스 1.4

이론

단계

EAP-FAST는 신청자와 서버의 상호 인증을 허용하는 유연한 EAP 방법입니다.EAP-PEAP와 비슷하지만 일반적으로 클라이언트 또는 서버 인증서를 사용할 필요가 없습니다.EAP-FAST의 한 가지 이점은 여러 인증을 연결(여러 내부 방법 사용)하고 암호 방식으로 연결(EAP 연결)하는 기능입니다. Cisco 구현에서는 사용자 및 머신 인증에 이 기능을 사용합니다.

EAP-FAST는 PAC(Protected Access Credentials)를 사용하여 TLS 터널(세션 재개)을 신속하게 설정하거나 사용자/머신(인증에 대한 내부 방법 건너뛰기)을 인증합니다.

EAP-FAST에는 3가지 단계가 있습니다.

- 단계 0(PAC 프로비저닝)
- 1단계(TLS 터널 설정)
- 2단계(인증)

EAP-FAST는 PAC-less 및 PAC 기반 대화를 지원합니다.PAC 기반은 PAC 프로비저닝 및 PAC 기반 인증으로 구성됩니다.PAC 프로비저닝은 익명 또는 인증된 TLS 세션을 기반으로 할 수 있습니다.

PAC

PAC는 서버에서 생성되어 클라이언트에 제공되는 보호 액세스 자격 증명입니다.구성 요소:

- PAC 키(TLS 마스터 및 세션 키 파생에 사용되는 임의 비밀 값)
- PAC 불투명(PAC 키 + 사용자 ID - 모두 EAP-FAST 서버 마스터 키로 암호화됨)
- PAC 정보(서버 ID, TTL 타이머)

PAC를 실행하는 서버는 EAP-FAST 서버 마스터 키(PAC 불투명)를 사용하여 PAC 키와 ID를 암호

화하고 전체 PAC를 클라이언트로 보냅니다.다른 정보는 보관/저장하지 않습니다(모든 PAC에 대해 동일한 마스터 키 제외).

PAC 불투명 키를 수신하면 EAP-FAST 서버 마스터 키를 사용하여 해독되고 검증됩니다.PAC 키는 축약 TLS 터널에 대한 TLS 마스터 및 세션 키를 파생시키는 데 사용됩니다.

이전 마스터 키가 만료되면 새 EAP-FAST 서버 마스터 키가 생성됩니다. 경우에 따라 마스터 키를 취소할 수 있습니다.

현재 사용 중인 PAC 유형은 몇 가지가 있습니다.

- 터널 PAC: TLS 터널 설정에 사용됩니다(클라이언트 또는 서버 인증서가 필요하지 않음). TLS 클라이언트 Hello로 전송됨
- 컴퓨터 PAC:TLS 터널 설정 및 즉시 시스템 권한 부여에 사용됩니다.TLS 클라이언트 Hello로 전송됨
- 사용자 권한 부여 PAC:서버에서 허용하는 경우 즉시 사용자 인증(내부 방법 건너뛰기)에 사용됩니다.TLV를 사용하여 TLS 터널 내부에서 전송됨.
- 머신 권한 부여 PAC:서버에서 허용하는 경우 즉시 시스템 인증(내부 방법 건너뛰기)에 사용됩니다.TLV를 사용하여 TLS 터널 내부에서 전송됨.
- Trustsec PAC:환경 또는 정책 새로 고침을 수행할 때 권한 부여에 사용됩니다.

이러한 모든 PAC는 일반적으로 0단계에서 자동으로 전달됩니다. PAC의 일부(터널, 머신, Trustsec)도 수동으로 전달할 수 있습니다.

PAC가 생성되는 경우

- 터널 PAC:이전에 사용하지 않은 경우 성공적인 인증(내부 방법) 후에 프로비저닝됨
- 권한 부여 PAC:인증 성공 후 프로비저닝됨(내부 방법)(이전에 사용되지 않음)
- 컴퓨터 PAC:이전에 사용되지 않거나 권한 부여 PAC가 사용되지 않는 경우, 성공적인 머신 인증(내부 방법) 후에 프로비저닝됨이는 터널 PAC가 만료될 때 제공되지만, 인증 PAC가 만료될 때는 제공되지 않습니다.EAP 체이닝이 활성화되거나 비활성화되면 프로비저닝됩니다.

참고:

각 PAC 프로비저닝에는 다음 활용 사례를 제외하고 성공적인 인증이 필요합니다.권한이 있는 사용자가 AD 계정이 없는 컴퓨터에 대해 머신 PAC를 요청합니다.

다음 표에는 프로비저닝 및 사전 대응적 업데이트 기능이 요약되어 있습니다.

PAC 유형	터널 v1/v1a/CTS	컴퓨터	Ahthorization(권한 부
프로비저닝 요청 시 PAC 제공	예	인증된 프로비저닝만	인증된 프로비저닝에 터널 PAC가 요청된 경
인증 요청 시 PAC 제공	예	예	이 인증에서 사용되지 경우에만
사전 업데이트	예	아니요	아니요
실패한 PAC 기반 인증(예: PAC가 만료된 경우) 후 PAC 프로비저닝으로 다시 전환할 때	거부 및 새 기능 제공 안 함	거부 및 새 기능 제공 안 함	거부 및 새 기능 제공
ACS 4.x PAC 지원	터널 PAC v1/v1a용	예	아니요

EAP-FAST 서버 마스터 키 ACS 4.x와 ACS 5x 및 ISE 비교

ACS 4.x와 ISE를 비교할 때 마스터 키 처리에 약간의 차이가 있습니다.

기능	ACS 4.1.2	ACS 5.x / ISE
마스터 키	마스터 키에 TTL이 있으며 활성, 폐기 또는 만료될 수 있습니다.	마스터 키는 구성된 기간마다 시드에서 자동으로 생성됩니다.특정 마스터 키는 항상 액세스 가능하며 만료되지 않음
PAC 새로 고침	PAC 암호화에 사용된 마스터 키가 만료되지 않는 한 PAC가 만료될 때 서버에서 PAC 업데이트를 보냅니다.	PAC 업데이트는 PAC 만료 시점 이전의 특정 구성 가능한 기간에 수행된 첫 번째 인증 성공 후 서버에서 전송됩니다.

즉, ISE는 모든 이전 마스터 키를 유지하고 기본적으로 매주 한 번 새 마스터 키를 생성합니다.마스터 키가 만료될 수 없으므로 PAC TTL만 검증됩니다.

ISE 마스터 키 생성 기간은 *Administration(관리) -> Settings(설정) -> Protocol(프로토콜) -> EAP-FAST -> EAP-FAST Settings(EAP-FAST 설정)*에서 구성됩니다.

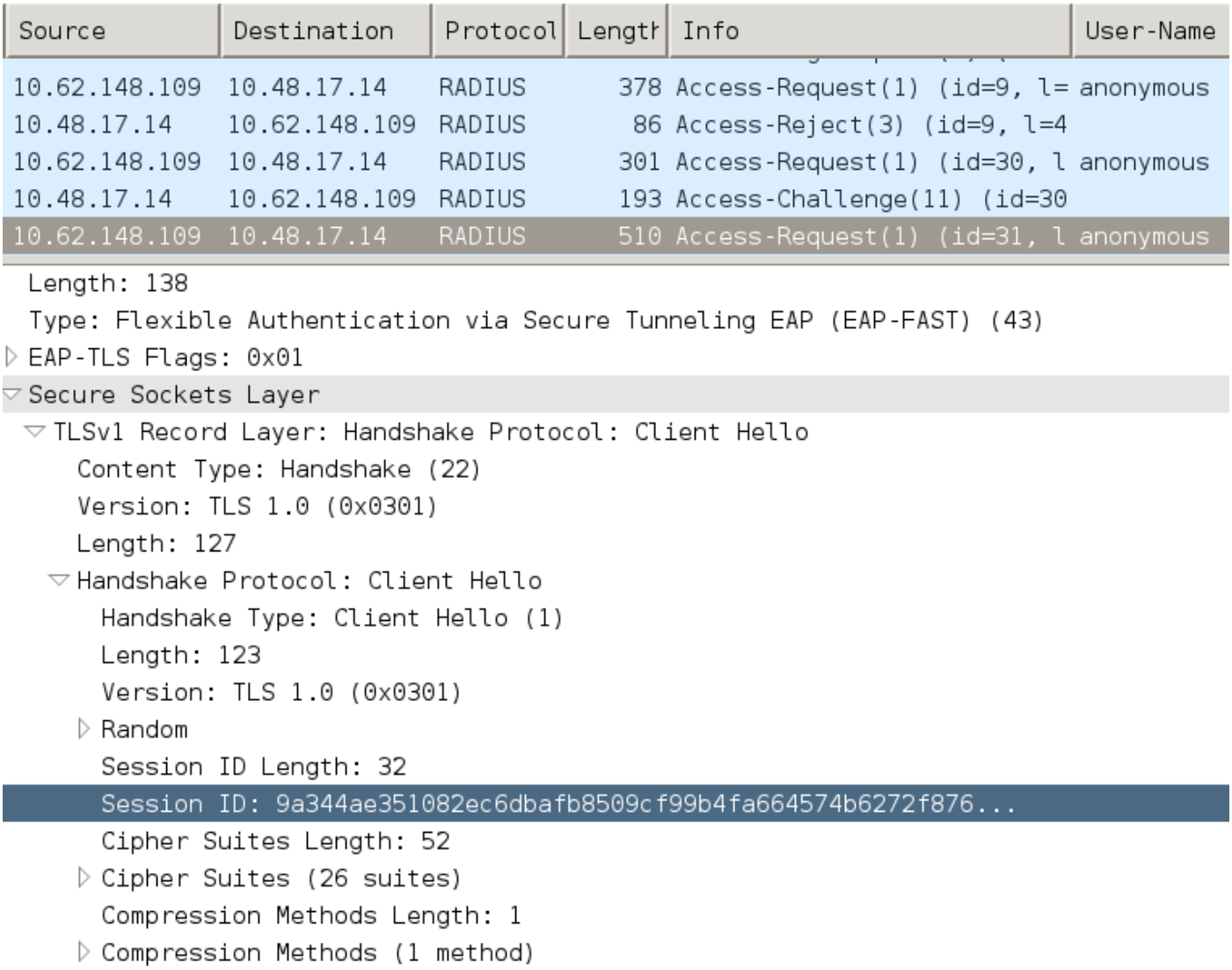
세션 다시 시작

이는 터널 PAC 사용을 허용하는 중요한 구성 요소입니다.인증서 사용 없이 TLS 터널 재협상이 가능합니다.

EAP-FAST에 대한 두 가지 세션 재시작 유형이 있습니다.서버 상태 기반 및 상태 비저장(PAC 기반)

서버 상태

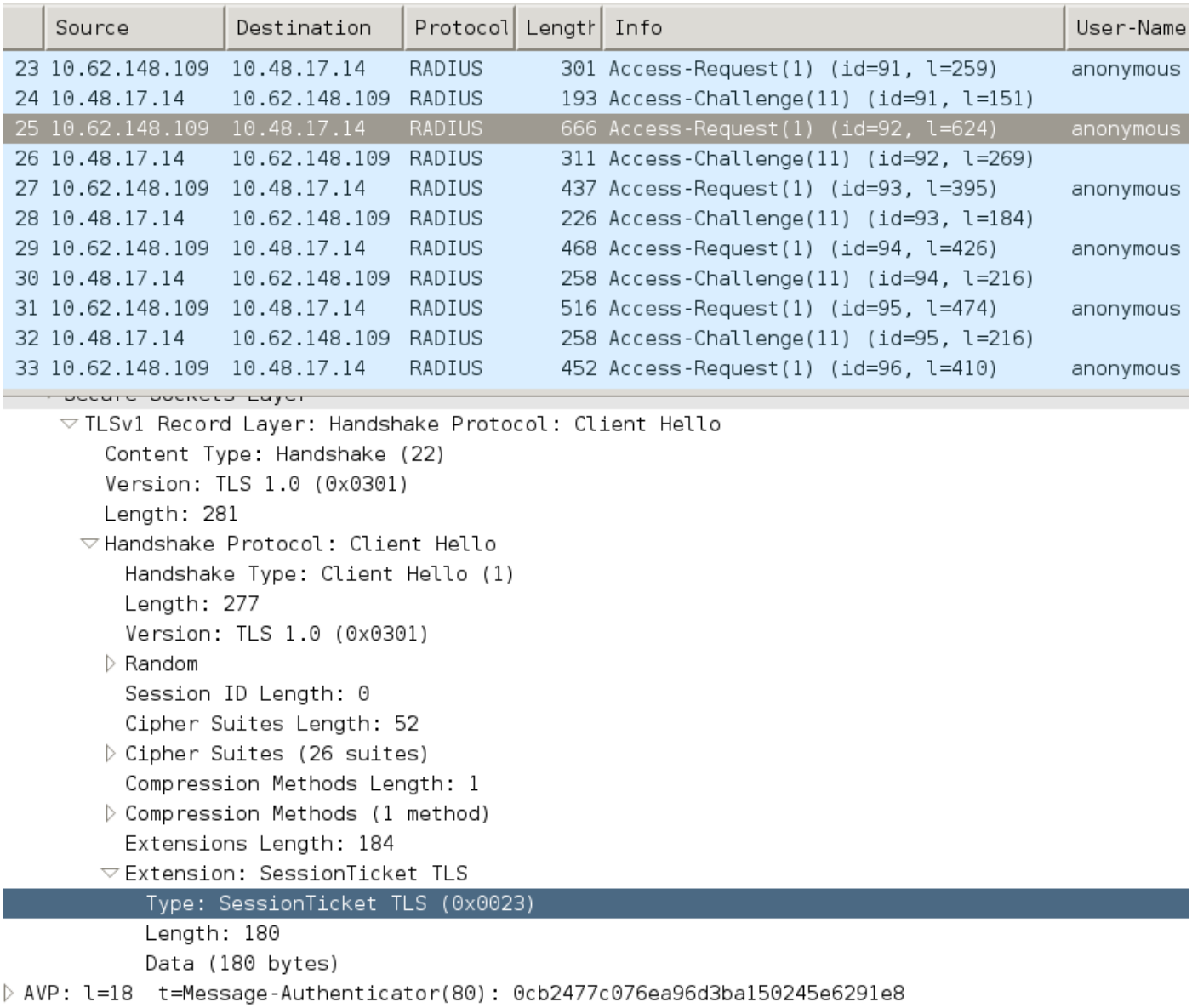
표준 TLS 기반 메서드는 서버에 캐시된 TLS SessionID를 기반으로 합니다.TLS Client Hello를 보내는 클라이언트는 세션을 재개하기 위해 SessionID를 연결합니다.세션은 익명 TLS 터널을 사용할 때 PAC 프로비저닝에만 사용됩니다.



상태 비저장(PAC 기반)

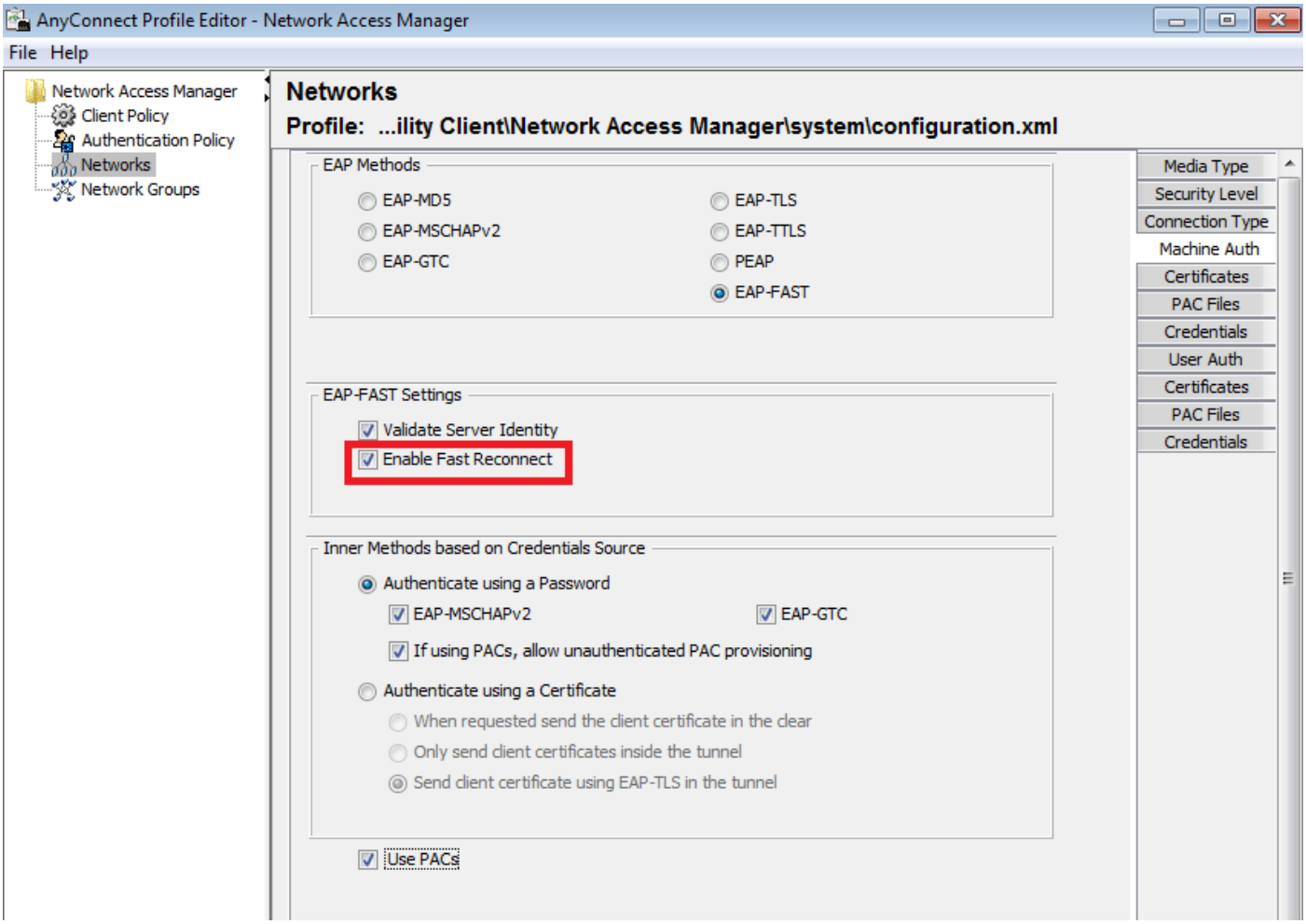
사용자/머신 권한 부여 PAC는 피어에 대한 이전 인증 및 권한 부여 상태를 저장하는 데 사용됩니다.

클라이언트 측 재시작은 RFC 4507을 기반으로 합니다.서버는 데이터를 캐시할 필요가 없습니다 .대신 클라이언트는 TLS Client Hello SessionTicket 확장에 PAC를 연결합니다.그러면 PAC는 서버에 의해 검증됩니다. 서버에 전달된 터널 PAC를 기반으로 한 예:



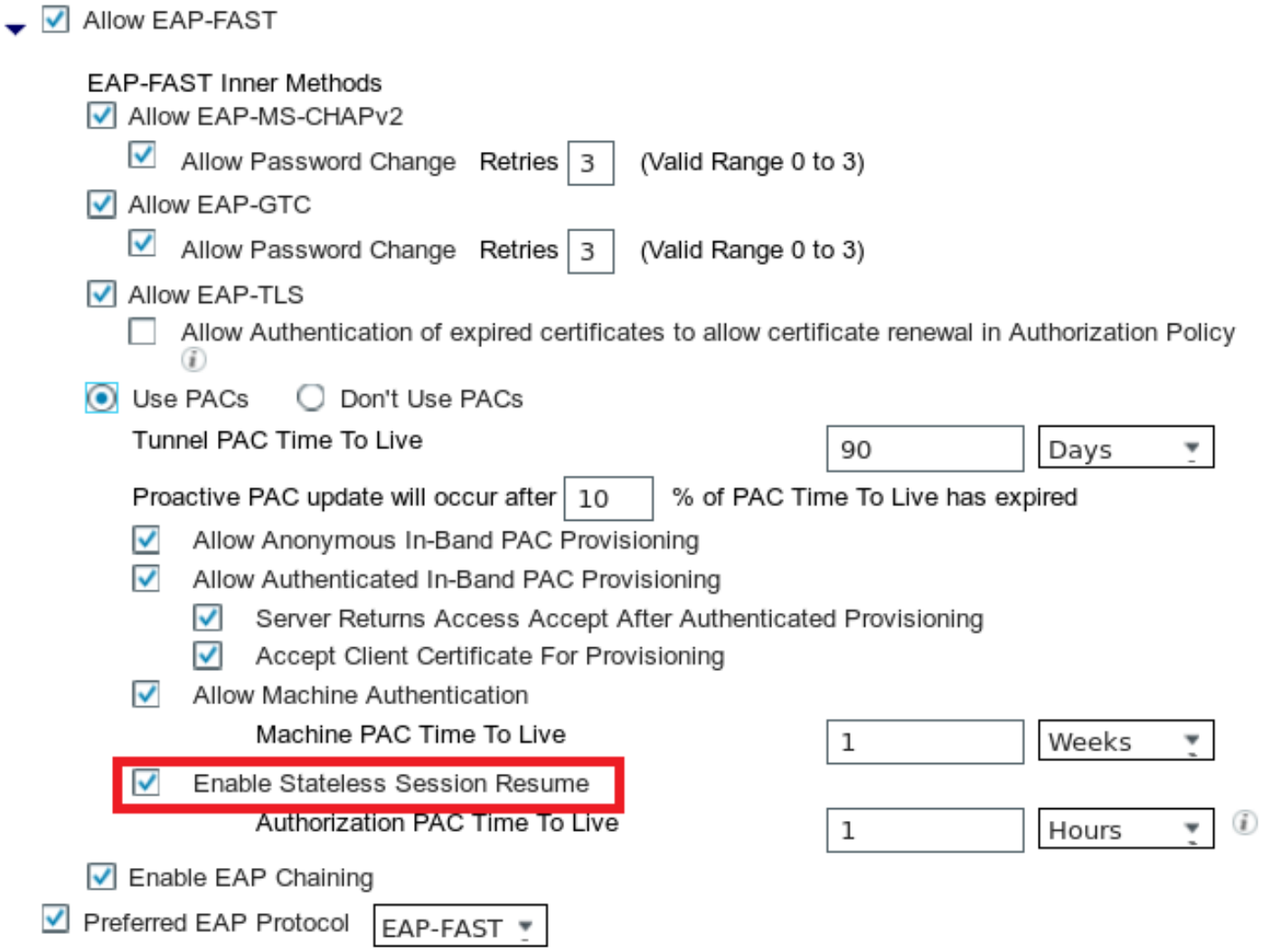
AnyConnect NAM 구현

빠른 재연결을 통해 클라이언트 측(AnyConnect NAM)에서 활성화되지만 권한 부여 PAC 사용만 제어하는 데 사용됩니다.



설정이 비활성화된 상태에서 NAM은 터널 PAC를 사용하여 TLS 터널을 구축합니다(인증서 필요 없음). 그러나 즉시 사용자 및 머신 권한 부여를 수행하기 위해 권한 부여 PAC를 사용하지 않습니다 .따라서 내부 방법을 사용하는 2단계가 항상 필요합니다.

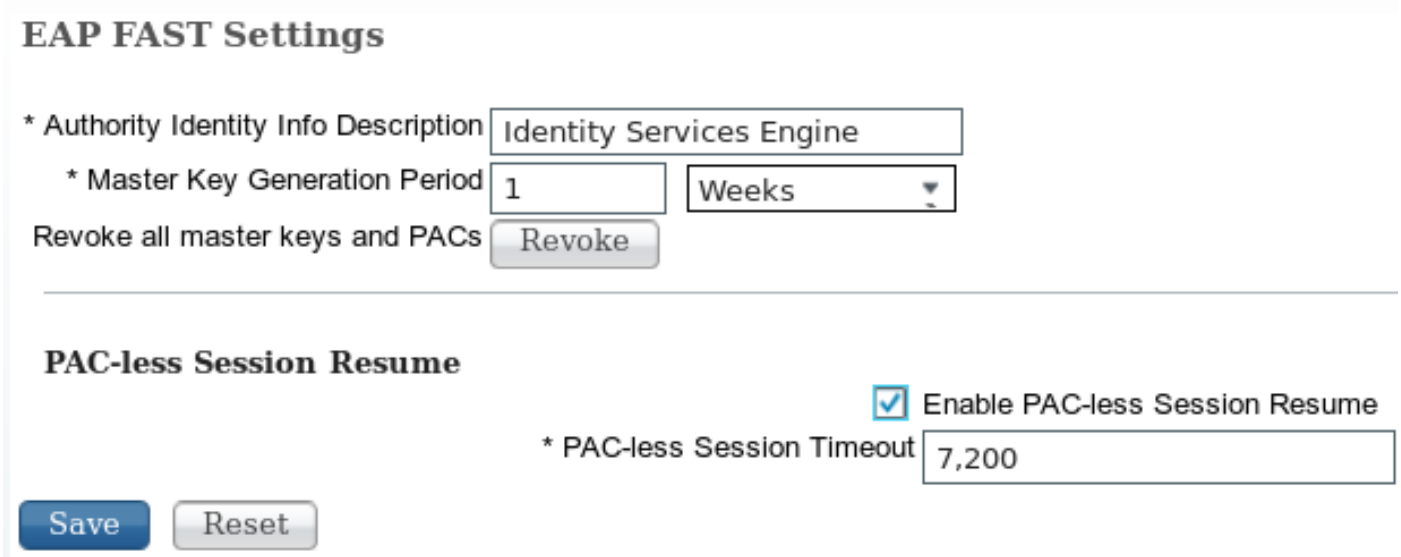
ISE에는 스테이트리스 세션 재개를 활성화하는 옵션이 있습니다.그리고 NAM과 마찬가지로 이는 단지 Authorization PAC를 위한 것입니다.터널 PAC 사용은 "Use PACs(PAC 사용)" 옵션으로 제어됩니다.



옵션이 활성화된 경우 NAM은 PAC를 사용하려고 시도합니다.ISE에서 "Don't Use PACs(PACs 사용 안 함)"가 구성되고 ISE가 TLS 확장에서 터널 PAC를 수신하면 다음 오류가 보고되고 EAP 실패가 반환됩니다.

여기에 삽입

ISE에서는 TLS SessionID(전역 EAP-FAST 설정에서)를 기반으로 세션 재개를 활성화해야 합니다. 기본적으로 비활성화되어 있습니다.



세션 재개 유형은 하나만 사용할 수 있습니다.SessionID 기반은 PAC-less 구축에만 사용되며 RFC 4507 기반은 PAC 구축에만 사용됩니다.

PAC 프로비저닝(0 단계)

PAC는 단계 0에서 자동으로 프로비저닝될 수 있습니다. 단계 0은 다음과 같이 구성됩니다.

- TLS 터널 설정
- 인증(내부 방법)

PAC는 PAC TLV(및 PAC TLV Acknowledgement)를 통해 TLS 터널 내에서 성공적인 인증 후 전달됩니다.

익명 TLS 터널

PKI 인프라가 없는 구축의 경우 익명 TLS 터널을 사용할 수 있습니다.익명 TLS 터널은 서버 또는 클라이언트 인증서 없이 Diffie Hellman 암호 그룹을 사용하여 구축됩니다.이러한 접근 방식은 Man in the Middle 공격(가장)에 영향을 주기 쉽습니다.

이 옵션을 사용하려면 NAM에 다음 구성 옵션이 필요합니다.

"PAC를 사용하면 인증되지 않은 PAC 프로비저닝이 허용됩니다."(PKI 인프라가 없으면 인증서 기반 내부 방법을 사용할 수 없기 때문에 비밀번호 기반 내부 방법에만 적합합니다.)

또한 ISE는 Authentication Allowed Protocols(인증 허용 프로토콜) 아래에 다음과 같이 구성해야 합니다.

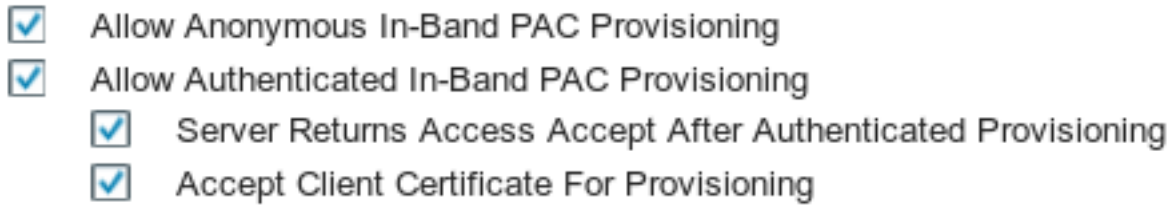
"익명 대역 내 PAC 프로비저닝 허용"

익명 대역 내 PAC 프로비저닝이 TrustSec NDAC 구축(네트워크 디바이스 간에 협상된 EAP-FAST 세션)에서 사용되고 있습니다.

인증된 TLS 터널

가장 안전하고 권장되는 옵션입니다.TLS 터널은 신청자가 검증한 서버 인증서를 기반으로 구축됩니다.이렇게 하려면 서버 측에만 PKI 인프라가 필요합니다. ISE에 필요합니다(NAM에서는 "Validate Server Identity" 옵션을 비활성화할 수 있습니다).

ISE의 경우 두 가지 추가 옵션이 있습니다.



일반적으로 PAC 프로비저닝 후, 신청자가 PAC를 사용하여 재인증하도록 강제하는 액세스 거부 전송 해야 합니다.그러나 PAC가 인증과 함께 TLS 터널에 제공되었으므로 전체 프로세스를 단축하고 PAC 프로비저닝 직후에 Access-Accept를 반환할 수 있습니다.

두 번째 옵션은 클라이언트 인증서를 기반으로 TLS 터널을 구축합니다(엔드포인트에서 PKI 구축이 필요함). 이를 통해 상호 인증을 통해 TLS 터널을 구축할 수 있으며, 내부 방법을 건너뛰고 PAC 프

로비저닝 단계로 바로 이동합니다.여기서 주의해야 합니다. 경우에 따라 신청자가 ISE에서 신뢰하지 않는 인증서(다른 용도로 사용)를 표시하고 세션이 실패합니다.

EAP 연결

하나의 RADIUS/EAP 세션 내에서 사용자 및 머신 인증을 허용합니다.여러 EAP 방법을 함께 연결할 수 있습니다.첫 번째 인증(일반적으로 머신)이 성공적으로 완료되면 서버는 성공을 나타내는 중간 결과 TLV(내부 TLS 터널)를 보냅니다.해당 TLV는 Crypto-Binding TLV 요청과 함께 사용해야 합니다.암호화 바인딩은 서버와 피어가 모두 특정 인증 시퀀스에 참여했음을 입증하는 데 사용됩니다.암호화 바인딩 프로세스에서는 1단계 및 2단계의 키 자료를 사용합니다. 또한 다음 TLV를 하나 더 추가합니다.EAP-Payload(EAP-페이로드) - 새 세션을 시작합니다(일반적으로 사용자에 대해). ISE(Radius Server)가 Crypto-Binding TLV 응답을 수신하고 이를 검증하면 다음 EAP 방법이 로그에 표시되고 다음 EAP 방법이 시도됩니다(일반적으로 사용자 인증을 위해).

12126 **EAP-FAST cryptobinding verification passed**

암호화 바인딩 검증이 실패하면 전체 EAP 세션이 실패합니다.인증 내에서 실패 한 인증 이 계속 정상 인 경우 ISE는 관리자가 권한 부여 조건 NetworkAccess:EapChainingResult를 기반으로 여러 연결 결과를 구성 할 수 있습니다.

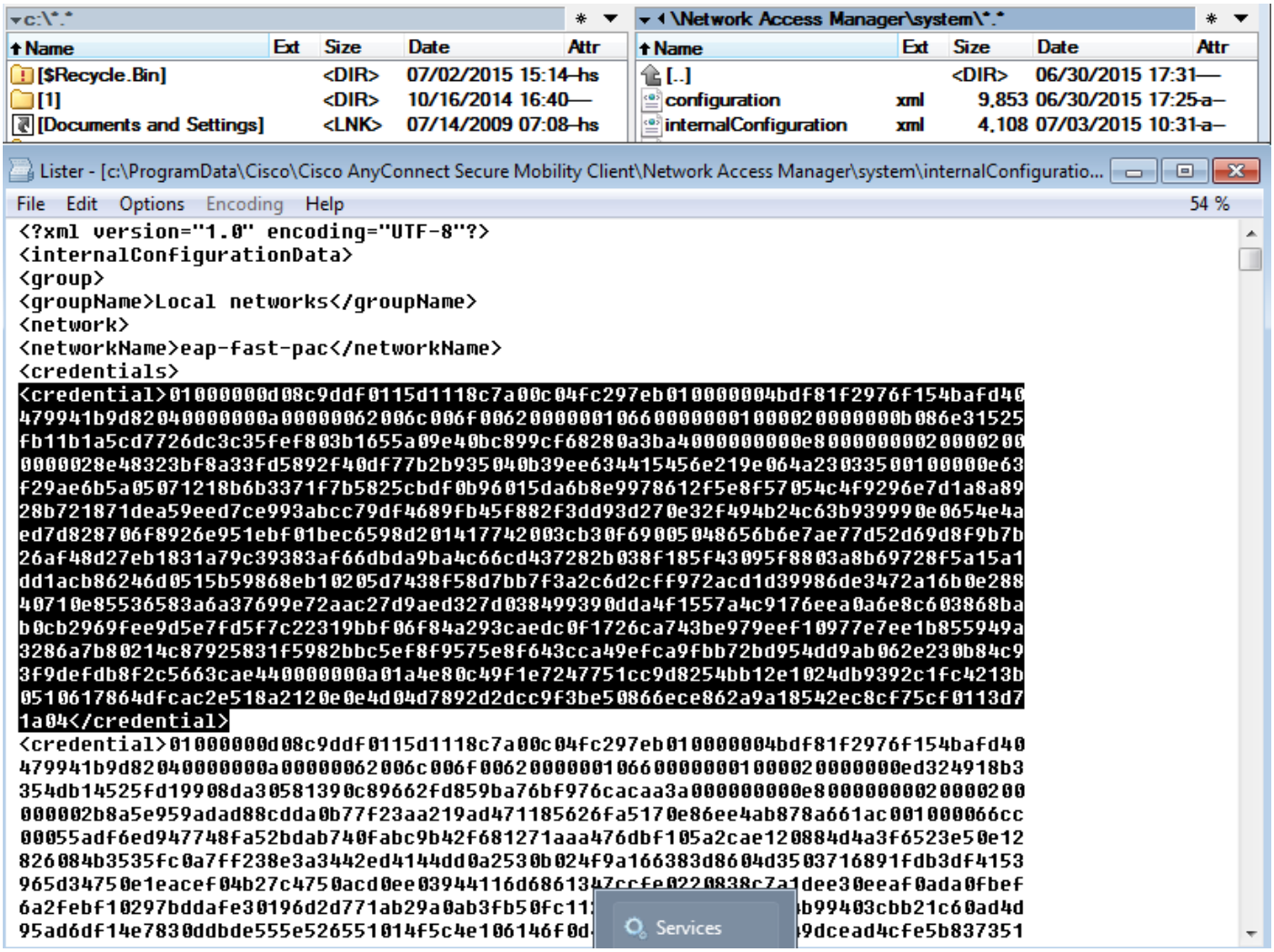
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-FAST 사용자 및 머신 인증이 활성화되면 NAM에서 EAP 체이닝이 자동으로 활성화됩니다.

ISE에서 EAP 체이닝이 구성되어야 합니다.

PAC 파일이 저장되는 위치

기본적으로 Tunnel 및 Machine PAC는 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml섹션에 <credential>에 저장됩니다.암호화된 형태로 저장됩니다.

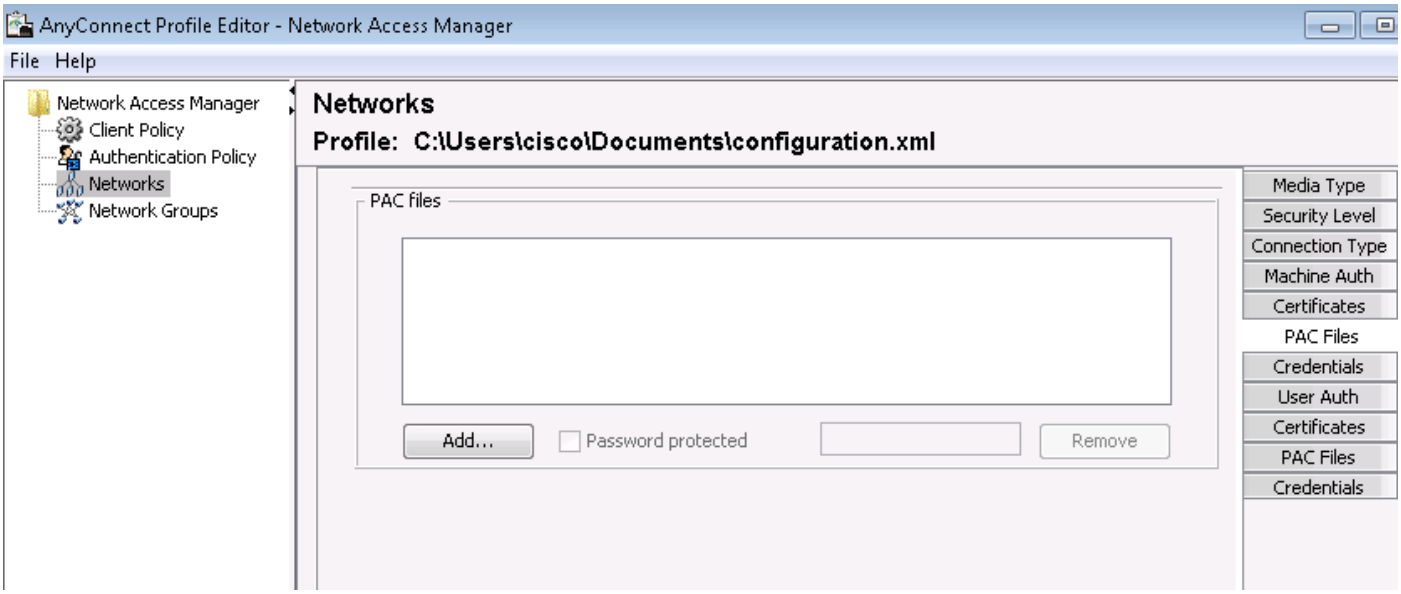


권한 부여 PAC는 메모리에만 저장되며 리부팅 또는 NAM 서비스를 다시 시작한 후에 제거됩니다.

터널 또는 시스템 PAC를 제거하려면 서비스를 다시 시작해야 합니다.

AnyConnect NAM 3.1 vs 4.0

관리자는 AnyConnect 3.x NAM 프로파일 편집기를 사용하여 PAC를 수동으로 구성할 수 있습니다 .이 기능은 AnyConnect 4.x NAM 프로파일 편집기에서 제거되었습니다.

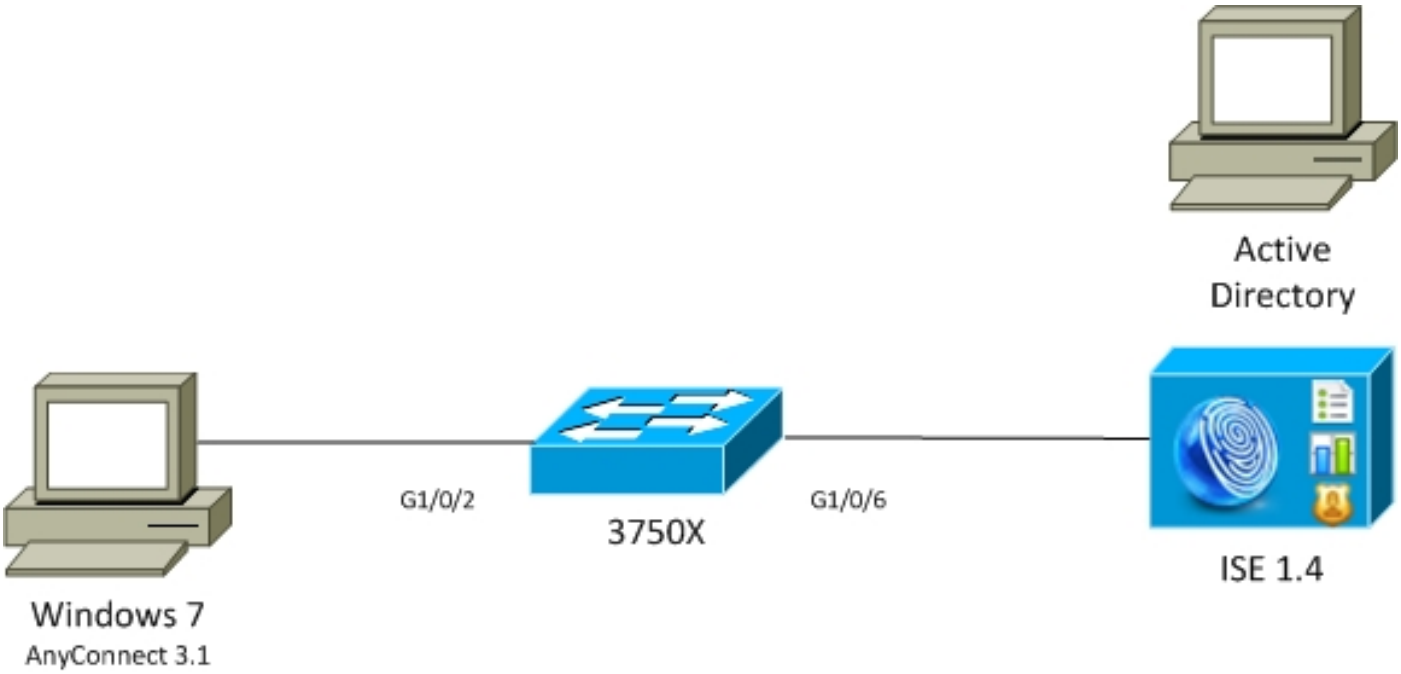


이 기능을 제거하기로 결정한 것은 CSCuf31422 및 CSCua13140을 기반으로 합니다.

예

네트워크 다이어그램

모든 예는 다음 네트워크 토폴로지를 사용하여 테스트되었습니다.무선을 사용할 때도 마찬가지입니다.



사용자 및 머신 PAC와 EAP 연결 없이 EAP-Fast

기본적으로 ISE에서 EAP_chaining이 비활성화됩니다.그러나 시스템 및 권한 부여 PAC를 비롯한 다른 모든 옵션이 활성화됩니다.신청자에 이미 유효한 시스템 및 터널 PAC가 있습니다.이 플로우에서는 ISE에 별도의 로그가 있는 두 개의 개별 인증(시스템에 대해 하나씩, 사용자에 대해 하나씩)이 있습니다.ISE에 의해 로깅된 기본 단계.첫 번째 인증(컴퓨터):

- 서 플리 컨 트가 시스템 PAC와 함께 TLS 클라이언트 hello를 보냅니다.
- 서버가 머신 PAC를 검증하고 TLS 터널을 구축합니다(사용된 인증서 없음).
- 서버는 시스템 PAC를 확인하고 Active Directory에서 계정 조회를 수행하고 내부 방법을 건너뜁니다.

```
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

두 번째 인증(사용자):

- 서 플리 컨 트가 터널 PAC와 함께 TLS 클라이언트 Hello를 전송 합니다.
- 서버는 PAC를 검증하고 TLS 터널을 구축합니다(사용된 인증서 없음).
- 서 플리 컨 트에 권한 부여 PAC가 없으므로 내부 방법 (EAP-MSCHAP) 인증에 사용 됩니다.

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

ISE의 상세 보고서의 "기타 특성" 섹션에서 사용자 및 머신 인증에 대해 다음과 같이 표시됩니다.

EapChainingResult: **No chaining**

PAC 빠른 재연결을 통한 EAP 연결을 사용하는 EAP-Fast

이 흐름에서 신청자는 사용자 및 머신 권한 부여 PAC와 함께 이미 유효한 터널 PAC를 가지고 있습니다.

- 서 플리 컨 트가 터널 PAC와 함께 TLS 클라이언트 Hello를 전송 합니다.
- 서버는 PAC를 검증하고 TLS 터널을 구축합니다(사용된 인증서 없음).
- ISE는 EAP 체인을 시작하고, 신청자는 TLS 터널 내에서 TLV를 사용하여 사용자 및 시스템에 대한 권한 부여 PAC를 연결합니다.
- ISE는 권한 부여 PACs(내부 방법 필요 없음)를 확인하고, Active Directory에 계정이 있는지 확인(추가 인증 없음), 성공 반환

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

ISE의 상세 보고서의 "기타 특성" 섹션에서 다음과 같은 내용이 표시됩니다.

EapChainingResult: **EAP Chaining**

또한 사용자 및 머신 자격 증명이 아래와 같은 로그에 포함됩니다.

Username: cisco,host/mgarcarz-PC

PAC 없이 EAP 연결을 사용하는 EAP-Fast

이 흐름에서 NAM은 PAC를 사용하지 않도록 구성되며 ISE는 PAC를 사용하지 않도록 구성됩니다(그러나 EAP 체이닝으로).

- 서 플리 컨 트가 터널 PAC 없이 TLS 클라이언트 Hello를 보냅니다.
- 서버는 TLS 인증서 및 인증서 요청 페이로드로 응답합니다.
- 서 플리 컨 트가 서버 인증서를 신뢰 해야 하며 클라이언트 인증서를 전송 하지 않습니다(인증서 페이로드는 0). TLS 터널이 구축 됩니다.
- ISE는 TLS 터널 내에서 클라이언트 인증서에 대한 TLV 요청을 전송하지만 서 플리 컨 트는 그렇지 않습니다(계속하려면 TLV를 가질 필요가 없음).
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 사용자에 대한 EAP 체이닝을 시작합니다.
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 머신 인증을 계속합니다.
- 프로비저닝 중인 PAC가 없습니다.

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 연결 권한 부여 PAC 만료를 사용하는 EAP-Fast

이 흐름에서 신청자는 유효한 터널 PAC를 가지고 있지만 권한 부여 PAC가 만료되었습니다.

- 서 플리 컨 트가 터널 PAC와 함께 TLS 클라이언트 Hello를 전송 합니다.
- 서버는 PAC를 검증하고 TLS 터널을 구축합니다(사용된 인증서 없음).
- ISE는 EAP 체인을 시작하고, 신청자는 TLS 터널 내에서 TLV를 사용하여 사용자 및 머신에 대한 권한 부여 PAC를 연결합니다.
- PAC가 만료되면 사용자와 머신 모두에 대한 내부 방법이 시작됩니다(EAP-MSCHAP).
- 두 인증이 모두 성공하면 사용자 및 머신 권한 부여 PAC가 모두 프로비저닝됩니다.

```
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 연결 터널 PAC가 만료된 EAP-Fast

유효한 터널 PAC가 없을 경우 이 흐름에서 내부 단계를 사용한 전체 TLS 협상이 발생합니다.

- 서 플리 컨 트가 터널 PAC 없이 TLS 클라이언트 Hello 를 전송 합니다.
- 서버는 TLS 인증서 및 인증서 요청 페이로드로 응답합니다.
- 서 플리 컨 트는 서버 인증서를 신뢰 해야 하며 클라이언트 인증서를 전송 하지 않습니다(인증서 페이로드는 0). TLS 터널이 구축됩니다.
- ISE는 TLS 터널 내에서 클라이언트 인증서에 대한 TLV 요청을 전송하지만 서 플리 컨 트는 그렇지 않습니다(계속하려면 TLV를 가질 필요가 없음).
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 사용자에 대한 EAP 체이닝을 시작합니다.
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 머신 인증을 계속합니다.
- 모든 PAC를 프로비저닝했습니다(ISE 컨피그레이션에서 활성화됨).

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 연결 및 익명 TLS 터널 PAC 프로비저닝을 사용하는 EAP-Fast

이 흐름에서 ISE 및 NAM 익명 TLS 터널은 PAC 프로비저닝(PAC 프로비저닝을 위한 ISE 인증 TLS 터널이 비활성화됨)에 대해 구성됩니다. PAC 프로비저닝 요청은 다음과 같습니다.

- 서 플리 컨 트가 여러 암호 그룹 없이 TLS 클라이언트 Hello를 보냅니다.
- 서버는 TLS Server Hello 및 TLS 익명 Diffie Hellman 암호(예: TLS_DH_anon_WITH_AES_128_CBC_SHA)로 응답합니다.
- 서 플리 컨 트가 이를 수락 하고 익명 TLS 터널이 구축 (교환 된 인증서 없음) 됩니다.
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 사용자에 대한 EAP 체이닝을 시작합니다.
- MSCHAPv2 인증과 함께 내부 방법을 사용하여 머신 인증을 계속합니다.
- 익명 TLS 터널이 빌드되고 있으므로 권한 부여 PAC는 허용되지 않습니다.
- Radius Reject(RADIUS 거부)가 반환되어 서 플리 컨 트가 다시 인증(프로비저닝된 PAC 사용)합니다.

```
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
```

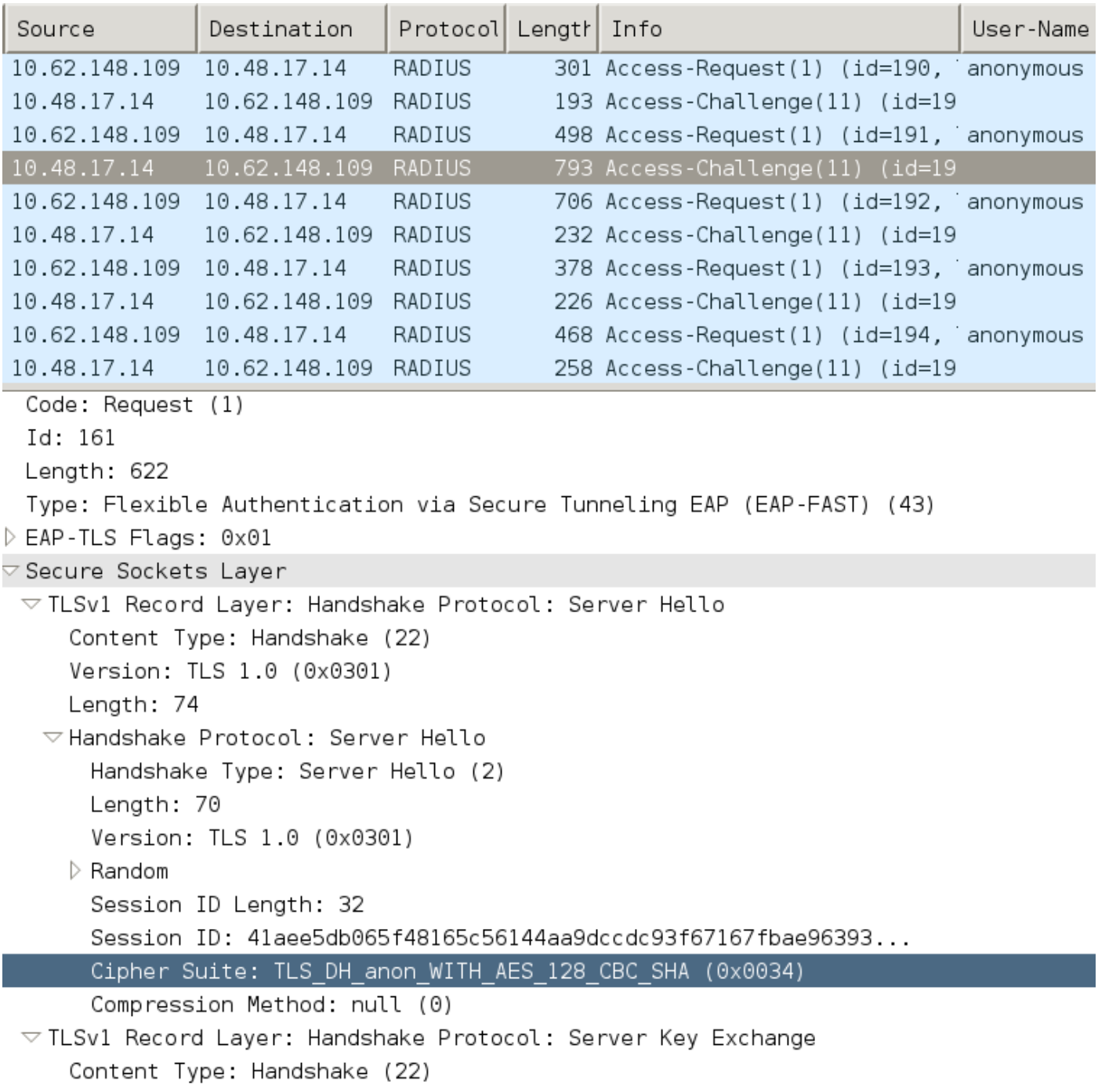
```
12200     Approved EAP-FAST client Tunnel PAC request
12219     Selected identity type 'Machine'

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
```

익명 TLS 터널 협상을 위한 Wireshark 패킷 캡처:



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 연결 사용자 인증만 있는 EAP-Fast

이 흐름에서 AnyConnect NAM with EAP-FAST and User (EAP-TLS) and Machine authentication

(EAP-TLS)이 구성됩니다.Windows PC가 부팅되지만 사용자 자격 증명이 제공되지 않습니다.스위치가 802.1x 세션을 시작합니다. 그러나 NAM은 응답해야 합니다. 그러나 사용자 자격 증명이 제공되지 않습니다(사용자 저장소 및 인증서에 대한 액세스 권한이 아직 없음).사용자 인증이 실패하는 동안 시스템이 성공합니다. - ISE authz 조건 "Network Access:EapChainingResult EQUALS User failed and machine succeeded"가 충족됩니다.나중에 사용자가 로그인하고 다른 인증이 시작되며 사용자와 시스템 모두 성공합니다.

- 서 플리 컨 트가 시스템 PAC와 함께 TLS 클라이언트 hello를 보냅니다.
- 서버가 TLS 암호 변경 사양에 응답합니다. TLS 터널은 해당 PAC를 기반으로 즉시 구축됩니다.
- ISE는 EAP 체이닝을 시작하고 사용자 ID를 요청합니다.
- 서 플리 컨 트가 대신 머신 ID를 제공 합니다(사용자가 아직 준비 되지 않음). EAP-TLS 내부 방법을 완료합니다.
- ISE가 사용자 ID를 다시 요청합니다. 신청자가 이를 제공할 수 없습니다.
- ISE는 중간 결과 = 실패(사용자 인증용)로 TLV를 보냅니다.
- ISE는 최종 EAP 성공 메시지, ISE 조건 네트워크 액세스:EapChainingResult EQUALS 사용자 실패 및 머신 성공을 반환합니다.

```
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 연결 및 일관성 없는 익명 TLS 터널 설정을 사용하는 EAP-Fast

이 흐름에서 ISE는 익명 TLS 터널을 통해서만 PAC 프로비저닝에 대해 구성되지만 NAM은 인증된 TLS 터널을 사용 중이며 ISE는 다음을 기록합니다.

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

이 문제는 NAM이 특정 TLS 암호를 사용하여 인증된 TLS 터널을 구축하려고 할 때 발생합니다. 이 터널은 익명 TLS 터널에 대해 구성된 ISE에서 수락되지 않습니다(DH 암호만 적용).

문제 해결

ISE

자세한 로그를 보려면 해당 PSN 노드에서 Runtime-AAA 디버그를 활성화해야 합니다.다음은 prrt-server.log의 로그 예입니다.

시스템 PAC 생성:

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 요청 승인:

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 검증:

```
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
```

PAC 생성을 위한 성공적인 요약 예:

```
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
```

PAC 검증을 위한 성공적인 요약 예:

```
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

NAM의 DART 로그에는 다음 세부 정보가 제공됩니다.

비 EAP 연결 세션, 빠른 재연결 없이 머신 인증의 예:

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

권한 부여 PAC 조회 예(비 EAP 연결 세션에 대한 머신 인증):

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

MSCHAP의 모든 내부 방법 상태는 아래 로그에서 확인할 수 있습니다.

```
 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
```

NAM은 모든 EAP 패킷을 캡처하여 pcap 파일에 저장할 확장 로깅 기능의 컨피그레이션을 허용합니다.이는 로그온 전 시작 기능에 특히 유용합니다(EAP 패킷은 사용자 로그온 전에 발생하는 인증에도 캡처됨). 기능 활성화에 대해서는 TAC 엔지니어에게 문의하십시오.

참조

- Cisco AnyConnect Secure Mobility Client 관리자 가이드, 릴리스 4.0 EAP-FAST 컨피그레이션
- Cisco Identity Services Engine 관리자 가이드, 릴리스 1.4 EAP-FAST 권장 사항
- Cisco Identity Services Engine 설계 가이드
- AnyConnect NAM 및 Cisco ISE로 EAP 체이닝 구축
- 기술 지원 및 문서 – Cisco Systems