EAP-PEAP에 대한 ISE 상태 저장 TLS 세션 재개 이해

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)의 TLS(Transport Layer Security) 세션 재개에 대해 설명합니다.

사전 요구 사항

요구 사항

- TLS(Transport Layer Security) 핸드셰이크 프로세스에 대한 지식
- PEAP(Protected Extensible Authentication Protocol) 흐름 지식
- Cisco Identity Services Engine에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 3.2
- ISE VM(가상 머신)
- 윈도우 10 PC

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

TLS 세션 재개는 초기 TLS 핸드셰이크의 오버헤드를 제거하는 데 사용되는 기술입니다. 이 기술을 사용하면 이전에 TLS 세션을 설정한 클라이언트와 서버가 리소스 집약적인 핸드셰이크 프로세스를 반복하지 않고 해당 세션을 재개할 수 있습니다.

장점

- 초기 핸드셰이크의 리소스 집약적인 단계 및 이를 수행하는 데 필요한 시간을 방지하여 레이턴시를 줄입니다.
- 또한 집약적인 키 교환 및 인증서 검증 프로세스를 건너뛰어 서버의 연산 부하를 줄입니다.

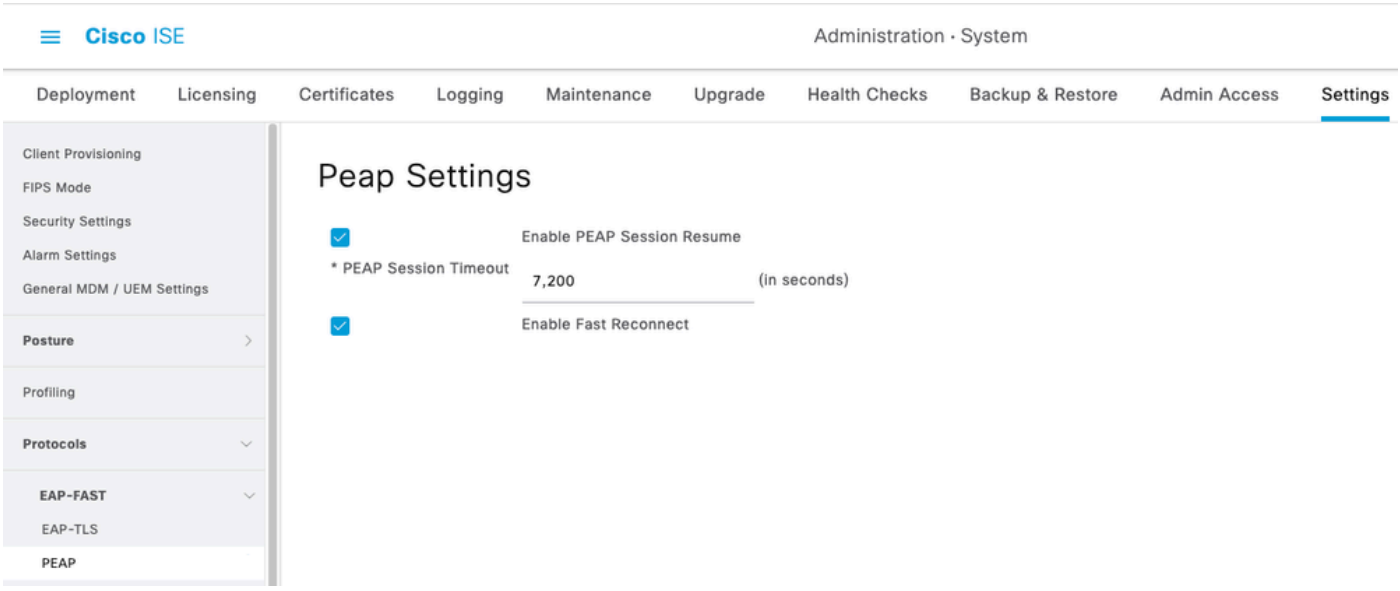
구성

ISE에서 TLS 세션을 활성화하려면 PEAP에 대해 다시 시작합니다.

Administration > System > Settings > Protocols > PEAP > Enable PEAP Session Resume을 선택합니다

기본적으로 ISE는 7200초 동안 세션을 유지합니다.

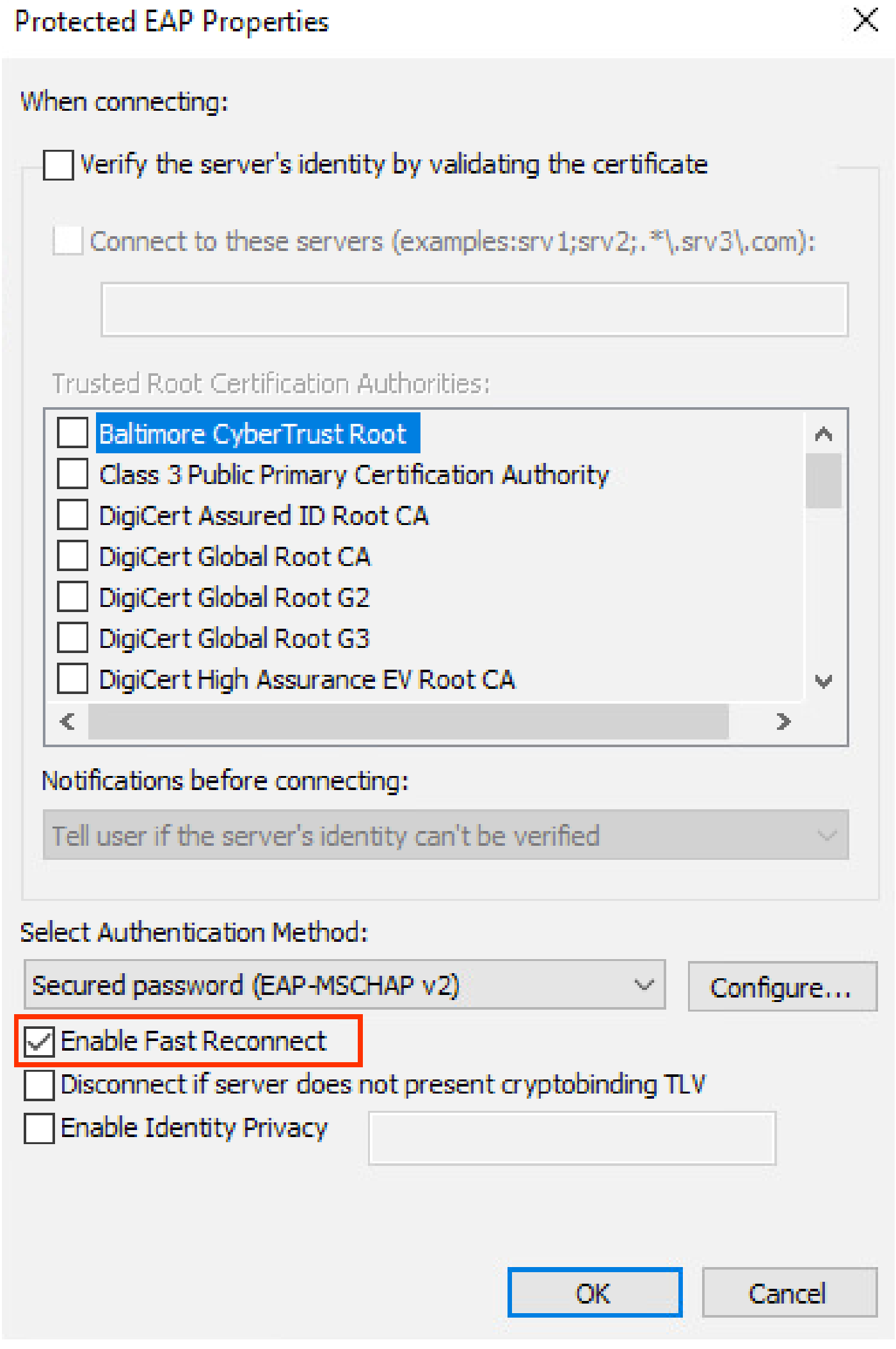
선택적으로, Enable Fast Reconnect(빠른 재연결 활성화)를 활성화할 수 있습니다. 그러면 PEAP의 내부 방법이 우회되고 더 빠른 재인증이 허용됩니다. 무선 로밍과 같은 애플리케이션에서 바람직하다.



ISE PEAP 세션 재개 컨피그레이션

빠른 재연결은 신청자에서도 활성화되어야 합니다.

이 컨피그레이션은 Windows 기본 신청자가 빠른 재연결을 사용하도록 설정하기 위한 것입니다.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
DigiCert Global Root G3
DigiCert High Assurance EV Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

로 응답하면서 해당 세션을 다시 설정합니다. 이렇게 하면 이전에 협상한 세션 데이터를 다시 사용하므로 보안 연결을 신속하게 설정하고 보안을 잃지 않을 수 있습니다.

3) TLS 세션 ID가 다른 노드로 복제됩니까?

아니요. TLS 세션 ID는 PSN 자체에 저장됩니다. 다른 PSN으로 복제되지 않습니다. PSN의 재부팅 또는 서비스 재시작의 경우 모든 세션 ID가 캐시에서 손실될 수 있으며 다음에 전체 TLS 핸드셰이크가 발생해야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.