보안 액세스 인증서 검사 상태 확인 인증 실패

목차

문제

인증서 검사 기능을 사용하여 엔드포인트 보안 상태 프로파일을 사용하여 보안 액세스를 구축하려고 하면 DART 번들 로그에서 구체적인 실패 원인을 식별할 수 없음에도 불구하고 모든 로그인 시도가 실패합니다. 사용자는 보안 상태 검사 메커니즘을 통해 인증서 검증을 적용하려고 하면서 SAML IDP 인증을 활용하려고 하지만 이 컨피그레이션을 수행하면 백엔드 인증서 일치가 성공하더라도 일관성 있는 인증 실패가 발생합니다.

환경

- Cisco Secure Access - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- SAML IDP 인증 통합
- 인증서 검사 기능이 활성화된 엔드포인트 상태 프로파일
- 이메일 주소와 일치하는 SAN의 UPN 필드가 있는 사용자 인증서
- 사용자, 그룹 및 엔드포인트 디바이스를 사용한 보안 액세스 테넌트 컨피그레이션

해결

상태 인증서 엔드 포인트 확인은 사용자 인증서 및 시스템 인증서 검증을 모두 필요 한 다중 인증서 인증을 사용 할 때만 적용 됩니다. 구축 시나리오에는 단일 VPN 프로파일을 사용해야 하는 사용자 인증서만 있는 사용자가 포함되므로, 이 솔루션에서는 포스처 인증서 검사에 의존하는 대신 SAML + 단일 인증서 인증을 구현합니다.

인증 컨피그레이션 단계

1단계: SAML + 단일 인증서 인증 구성

보안 상태 확인을 통해 인증서 검증을 적용하는 대신 단일 인증서 인증과 결합된 SAML 인증을 사용하도록 인증 방법을 구성합니다.

2단계: 인증서 UPN 일치 구성

인증서의 SAN(주체 대체 이름)의 UPN 필드에 Users, Groups, and Endpoint devices(사용자, 그룹, 엔드포인트 디바이스) 아래의 Secure Access(보안 액세스)에서 사용자에 대해 구성된 인증 속성과 일치하는 사용자의 이메일 주소가 포함되어 있는지 확인합니다.

3단계: Set Primary Authentication(기본 인증 설정) 필드

인증서의 UPN을 사용하여 인증하도록 기본 필드를 구성하여 Secure Access 사용자 데이터베이스에 있는 사용자의 이메일 주소와 일치하는지 확인합니다.

인증서 구조 요구 사항

인증서의 UPN 또는 보조 값이 Secure Access의 사용자에 대한 인증 속성과 일치하도록 인증서 구조를 구성해야 합니다. 사용자가 Secure Access에서 해당 사용자에 대해 구성된 인증 속성과 일치하지 않는 UPN 또는 보조 값이 있는 인증서를 제시하면 인증이 거부됩니다.

중요 구성 참고 사항

보안 상태 인증서 확인 적용이 필요한 경우 다중 인증서 인증(IDP SAML + Multi-Cert Auth)이 필요하지만, 여기에는 사용자 인증서와 머신 인증서가 모두 필요합니다. 사용자가 사용자 인증서만 갖고 단일 VPN 프로파일을 사용해야 하는 구축의 경우 SAML + 단일 인증서 인증을 통해 적절한 솔루션을 제공하면서 인증서 기반 보안 제어를 유지할 수 있습니다.

원인

상태 인증서 엔드 포인트 확인은 다중 인증서 인증이 구성 된 경우에 만 적용 됩니다. 보안 상태 인증서 확인과 함께 SAML 인증을 사용할 경우, 시스템에서는 사용자 인증서와 머신 인증서가 모두

유효성 검사를 위해 있어야 합니다. 구축에서는 SAML 인증을 사용하는 사용자 인증서만 사용했기 때문에, 상태 인증서 검사 기능은 단일 인증서 인증 시나리오와 작동하도록 설계되지 않았기 때문에 성공적인 백엔드 인증서 매칭에도 불구하고 인증 시도에 지속적으로 실패했습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.