Cisco Secure Access에서 개인 Google 계정을 사용하는 게스트 사용자에 대한 ZTNA 등록 실패

목차

문제

ZTNA(Zero Trust Network Access)를 사용하여 프라이빗 액세스를 구축하는 동안 Entra ID에 등록하고 보안 액세스에서 프로비저닝한 후 개인 Google 계정으로 게스트 사용자를 등록하지 못합니다. 발생하는 구체적인 증상은 다음과 같습니다.

- 클라이언트 기반 등록: 등록 프로세스가 SSO 인증에 도달하고 자격 증명이 제공되지만 ZTNA에 "I/O 오류"가 표시되고 등록 프로세스가 중단됩니다
- 클라이언트 없는 액세스: "Cisco Secure Access Login failure(Cisco 보안 액세스 로그인 실패)" 오류 메시지를 반환합니다. 트랜잭션 ID와 함께 "IDP 컨피그레이션 확인"

이러한 장애로 인해 프라이빗 리소스에 대한 액세스가 차단되고, 비기업 ID를 사용하는 하청업체 스타일 액세스에 대한 ZTNA 기능 테스트에 영향을 미치게 됩니다.

환경

- ZTNA 구축을 통한 Cisco Secure Access
- Microsoft Enterprise ID(이전의 Azure AD)를 ID 공급자로 사용
- 개인 Google 계정(@gmail.com)이 Entra ID에 게스트 사용자로 등록되었습니다.
- 게스트 계정이 프로비저닝되고 Secure Access에 표시됨
- Entra ID와 Cisco Secure Access 간에 구성된 SAML 인증

해결

Microsoft Entra ID에서 SAML 특성 매핑 구성을 수정하여 등록 실패를 해결했습니다. 이 문제를 해결하기 위해 다음 단계를 수행했습니다.

1단계: DART 번들 및 클라이언트 동작 분석

DART 번들을 검토하여 Cisco Secure Client 및 ZTA 구성 요소가 정상적으로 작동하는지 확인합니다. 분석에서는 등록 플로우가 Cisco Secure Access에 성공적으로 도달하고 ID 공급자와의 SAML 인증 중에 오류가 발생하는지 확인해야 합니다.

2단계: Entra ID 인증 로그 검토

Entra ID 인증 로그를 확인하여 ID 제공자 관점에서 인증 프로세스가 성공적으로 완료되는지 확인합니다. 로그에는 성공적인 인증이 표시되어야 하지만, Secure Access는 특성 불일치로 인해 로그인을 거부합니다.

3단계: SAML 특성 매핑 문제 확인

Entra ID가 SAML 클레임으로 UPN(User Principal Name)을 발급하고 있으며, 이는 Secure Access에서 예상한 개인 Gmail 계정 ID와 일치하지 않음을 확인합니다. 어설션된 IdP 특성이 필요한 사용자 식별자와 일치하지 않습니다.

4단계: SAML 속성 매핑 수정

Microsoft Entra ID의 SAML 특성 매핑을 UPN에서 이메일 주소로 변경합니다. 이렇게 하면 이메일 주소 클레임이 개인 Google 계정 ID와 일치합니다.

5단계: 등록 성공 확인

특성 매핑 변경을 구현한 후 ZTNA 등록 프로세스를 재시도합니다. 이제 Cisco Secure Access ZTA에서 Gmail 주소를 인식하고 등록이 성공적으로 완료되도록 해야 합니다.

원인

등록 실패는 Microsoft Entra ID에서 어설션하는 SAML 특성과 Cisco Secure Access의 예상 사용자 식별자가 일치하지 않아서 발생했습니다. Entra ID는 UPN(User Principal Name)을 SAML 클레임으로 전송하도록 구성되었지만 개인 Google 계정(@gmail.com)의 경우 이 UPN이 실제 이메일 주소 ID와 일치하지 않습니다. Cisco Secure Access는 프로비저닝된 게스트 사용자 계정에 대해 매칭할 식별 특성으로 이메일 주소를 수신해야 하므로 IdP 인증이 성공하더라도 인증이 거부됩니다.

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.