Cisco Secure Access - IDP를 통한 SAML 인증서 갱신(Microsoft Entra ID)

목차

문제

Microsoft Entra ID SAML을 Cisco Secure Access의 IdP(Identity Provider)로 사용하는 SSO 인증을 사용할 경우 SAML 확인 인증서가 만료될 예정입니다.

인증 중단을 방지하기 위해 올바른 인증서 갱신 프로세스를 이해하고 Entra ID SAML 인증서를 갱신할 때 Secure Access에서 새 SSO(Single Sign On) 컨피그레이션을 생성해야 하는지 여부를 결정해야 합니다.

환경

- SSO 인증이 구성된 Cisco Secure Access
- ID 공급자로 Microsoft Entra ID SAML
- 만료 날짜가 다가오는 SAML 확인 인증서
- SWG(Secure Web Gateway) 및 ZTNA(Zero Trust Network Access)에 대한 기존 SSO 컨피그레이션

해결

1단계 - 인증서 갱신 탐지

- IdP(Identity Provider)가 SAML 서명 인증서를 갱신하거나 교체합니다.
- 이는 일반적으로 인증서가 만료에 가까워지면 발생합니다.

2단계 - 업데이트된 IdP 메타데이터 가져오기

- IdP에서 새 IdP 메타데이터 XML 또는 새 서명 인증서를 내보냅니다.

3단계 - 인증서 변경 확인

인증서가 실제로 변경되었는지 확인합니다.

확인:

- 지문
- 만료 날짜
- 발급자

이렇게 하면 SP가 올바른 인증서로 업데이트됩니다

서비스 공급자 컨피그레이션 업데이트

Cisco Secure Access Dashboard(Cisco Secure Access 대시보드)에 로그인하여 구성을 업데이트합니다.

연결 - 사용자 및 그룹으로 이동합니다.

Configuration Management를 클릭합니다.

SSO Authentication(SSO 인증) - Edit the SSO Authentication Profile(SSO 인증 프로파일 수정)에서 새 인증서를 사용하여 메타데이터 파일을 업로드하거나 수동 컨피그레이션인 경우 인증서를 업로드합니다.

5단계 - 구성 저장 및 적용

- 업데이트된 컨피그레이션 저장

6단계 - SSO 인증 확인

SSO 로그인 테스트를 수행합니다.

원인

IdP(ID 공급자) 서명 인증서는 서비스 공급자가 SAML 어설션 서명을 확인하는 데 사용되며, IdP가 인증서를 갱신하는 경우 SP는 신뢰할 수 있는 인증서를 업데이트하여 인증 요청의 유효성을 계속 검사해야 합니다

관련 콘텐츠

- Cisco Secure Access - SAML Single Sign-On 개요 및 컨피그레이션
- Cisco Secure Access에 대한 SAML SSO 구성(Microsoft Entra ID 예)
- 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.