로밍 클라이언트 SWG 트래픽용 Duo IdP를 사용하는 Cisco Secure Access SSO 인증

목차

문제

로밍 클라이언트에서 시작되는 Secure Access SWG(Secure Web Gateway) 트래픽을 위해 Duo IdP를 사용하여 SSO 인증을 사용하려고 하면 사용자에게 Duo SSO 인증 프롬프트가 표시되지 않으며 사용자 ID가 Secure Access 대시보드에 채워지지 않습니다. 웹 트래픽이 의도된 SWG 규칙과 일치하고 인증이 활성화되며 트래픽의 암호가 해독되더라도 인증 흐름은 로밍 클라이언트 트래픽에 대해 시작되지 않으므로 웹 활동의 사용자 레벨 식별을 방해합니다.

특히 다음과 같은 동작이 관찰되었습니다.

- SWG 로깅 및 활동에서 트래픽이 의도한 SWG 규칙과 일치하고 목적지 트래픽이 해독되었음을 나타냄
- 로그 및 Secure Access 활동 보기에는 PC ID 및 네트워크 ID만 표시됩니다. Duo/SAML 인증 챌린지, SSO 리디렉션 또는 대화형 프롬프트가 관찰되지 않았습니다.
- 정책 항목에는 로밍 및 발신지 정보만 표시되었습니다. AD 조인 전에 사용자 ID가 없습니다.
- 트러블슈팅 중에 테스트 VM이 Active Directory에 조인되면 Secure Access Activity Search(보안 액세스 활동 검색)에서 사용자 ID가 표시되지만 Duo/SAML 대화형 프롬프트는 여전히 발생하지 않았습니다

환경

- Cisco Secure Access with SWG 기능
- Secure Client 버전 5.1.13.177
- SSO 인증을 위해 구성된 Duo IdP
- 조직 구독: 보안 액세스 필수 요소
- Reauthenticate web proxy interval set to Daily(웹 프록시 재인증 간격이 일별로 설정됨)
- 테스트 중에 사용 중인 PAC 파일 또는 VPN 없음
- 로밍 컴퓨터 구성을 사용하여 환경 테스트

해결

종합적인 분석 및 테스트 결과, 제품 설계 제한으로 인해 보안 액세스 로밍 클라이언트 트래픽에 대해서는 SAML을 사용한 SSO 인증이 지원되지 않는 것으로 확인되었습니다. 이러한 제한을 확인하기 위해 다음 트러블슈팅 단계를 수행했습니다.

1단계: 실시간 문제 해결 및 동작 재현

테스트 결과 SWG 정책 일치 및 SSL 암호 해독이 올바르게 수행되었지만 로밍 클라이언트 트래픽에 대해 인증 흐름(대화형 SAML/Duo SSO 리디렉션 및 챌린지)이 시작되지 않았습니다.

2단계: 규칙 및 소스 수정

SWG 규칙 원본이 재프로 시도 중에 로밍 컴퓨터 이름에서 특정 사용자 ID로 변경되었습니다. Secure Client 서비스가 다시 시작되었고 정책 전파가 관찰되었습니다. 이러한 수정으로 인증 흐름 문제가 해결되지 않았습니다.

3단계: Active Directory 가입 테스트

테스트 VM이 사용자 ID 가시성에 미치는 영향을 확인하기 위해 Active Directory에 조인되었습니다. 이 경우 사용자 ID가 Secure Access Activity Search(보안 액세스 활동 검색)에서 표시되지만 Duo/SAML 인터랙티브 프롬프트는 여전히 발생하지 않았으므로 문제가 사용자 ID 가시성에만 관련된 것이 아님을 확인할 수 있습니다.

4단계: DART 번들 분석

DART 번들을 수집하고 분석했습니다. 분석 결과 SWG 정책 애플리케이션이 확인되었지만 로밍 클라이언트 트래픽에 대한 인증 흐름 시작은 표시되지 않았으며, 이러한 동작이 설계에 의한 것이라는 결론을 뒷받침합니다.

5단계: Duo IdP 컨피그레이션 검증

Duo IdP 메타데이터 및 컨피그레이션에 대한 독립적인 테스트가 성공적으로 수행되고 완료되었으며, Duo 컨피그레이션 자체가 문제의 원인이 아님을 확인했습니다.

6단계: 내부 검증

SAML을 사용한 SSO 인증은 Secure Access 로밍 클라이언트 트래픽에 대해 제품 설계 제한으로 지원되지 않습니다.

결론: 설정에서 잘못된 컨피그레이션을 찾지 못했습니다. 인터랙티브 SSO 프롬프트가 없는 것은 수정 가능한 컨피그레이션 문제가 아니라 명시적 제품 지원 제한 때문이었습니다.

원인

이 문제는 SAML(Duo IdP 통합 포함)을 사용하는 SSO 인증이 Secure Access 로밍 클라이언트 트래픽에 지원되지 않는 제품 설계 제한으로 인해 발생합니다. 이는 현재 Secure Access 플랫폼 아키텍처의 고유한 제한이며 컨피그레이션 문제 또는 소프트웨어 버그와 관련이 없습니다.

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.