보안 액세스를 위한 SWG SAML 인증 쿠키 서로게이트 문제 해결

목차

문제

Cisco Secure Access를 통해 웹 애플리케이션에 액세스하는 사용자는 애플리케이션이 도메인 간 리디렉션을 수행하거나 여러 관련 도메인의 리소스를 가져올 때 인증 실패를 경험합니다. 이 문제는 다음과 같이 나타납니다.

- SAML 인증 후 웹 응용 프로그램이 제대로 초기화되지 않았습니다.
- 도메인 간 리소스에 대한 요청(CORS 오류)이 기본 거부 규칙에 의해 차단되고 있습니다.
- 인증된 사용자 ID 대신 네트워크 또는 터널 ID에 속하는 요청을 표시하는 활동 로그
- 리디렉션된 요청에 대해 브라우저 콘솔에 나타나는 CORS 정책 오류입니다.
- IP 서로게이트를 사용하는 경우 물리적 컴퓨터에서 올바르게 작동하지만 쿠키 서로게이트를 사용하는 Citrix 가상 데스크톱 환경에서는 작동하지 않는 애플리케이션.

이 문제는 특히 가상화된 환경에서 쿠키 서로게이트 인증이 사용될 때 발생합니다. 즉 도메인 간 리소스 가져오기 중에 리디렉션된 요청이 사용자-쿠키 매핑을 잃게 됩니다.

환경

- SAML 인증이 구성된 Cisco Secure Access
- Citrix 가상 데스크톱 환경에 대해 쿠키 서로게이트 인증 사용
- 물리적 컴퓨터에 사용되는 IP 서로게이트 인증
- 도메인 간 리디렉션을 수행하는 웹 애플리케이션(웹 개발자 도구 콘솔 로그의 CORS 오류)
- 물리적 및 가상 데스크탑 인프라가 혼합된 환경

해결

영향을 받는 네트워크 범위에 대해 IP 서로게이트 우회를 구현하여 도메인 간 리디렉션 중에도 적절한 사용자 ID 특성을 허용하면 문제가 해결됩니다.

1단계: IP Surrogate Configuration(IP 서로게이트 구성)으로 이동합니다.

Cisco Secure Access 대시보드에 액세스하고 Connect(연결) > Users and Groups(사용자 및 그룹) > Configuration Management(컨피그레이션 관리) > Advanced Settings(고급 설정) > IP Surrogate(IP 서로게이트)로 이동합니다.

2단계: 내부 네트워크 우회 사용

영향을 받는 네트워크 범위를 Internal Network Bypass 컨피그레이션에 추가합니다. 이를 통해 시스템은 이러한 네트워크에서 시작되는 요청에 대한 사용자 ID 특성을 유지 관리할 수 있습니다.

3단계: 애플리케이션 액세스 테스트

IP 서로게이트를 구현한 후, 영향을 받는 애플리케이션을 테스트하여 다음을 확인합니다.

- 도메인 간 리소스 요청은 사용자 ID에 적절하게 속함
- CORS 오류 없이 애플리케이션을 초기화했습니다.
- 작업 로그는 모든 요청에 대한 네트워크 또는 터널 기반 ID 대신 사용자 ID를 표시합니다

5단계: 활동 보고서 모니터링

Monitor(모니터) > Activity Search(활동 검색)를 사용하여 이제 요청이 네트워크 또는 터널 기반 ID로 표시되지 않고 인증된 사용자에게 올바르게 귀속되는지 확인합니다.

원인

이 동작은 가상화된 환경에서 SAML 인증이 Cookie Surrogate와 결합된 특성 때문에 예상됩니다. 웹 애플리케이션이 도메인 간 리디렉션을 수행하거나 여러 관련 도메인의 리소스를 가져올 때 리디렉션된 요청은 Cisco Secure Access가 인증된 사용자 세션에 다시 연결할 수 있는 방식으로 서로게이트 쿠키를 전달하지 않을 수 있습니다.

근본 원인은 다음과 같습니다.

- Cookie Surrogate는 리디렉션 전반에서 브라우저 쿠키 전파를 사용합니다.
- CORS(Cross-Domain Security Policy)는 307/리디렉션 시나리오에서 쿠키를 제거할 수 있습니다.
- 브라우저 보안 조치로 인해 여러 도메인에서 쿠키가 공유되지 않습니다.
- 가상 데스크톱 환경은 물리적 시스템과 다르게 쿠키 전파를 처리합니다.

사용자-쿠키 매핑이 손실되면 Secure Access에서 인증된 사용자에 대한 요청을 확인할 수 없으므로, 요청이 등록된 네트워크/다른 ID에만 소스 역할을 하며 그 후 기본 거부 규칙에 의해 차단됩니다.

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.