

비 브라우저 웹 트래픽에 대한 보안 액세스 SSO 인증 동작

목차

문제

IPsec 연결을 사용하여 CSA(Cisco Secure Access)를 구현할 때 보안 프로파일의 SSO 인증 동작에 대한 설명이 필요했습니다. 특히, 사이트가 IPsec 터널을 통해 연결될 때 어떤 유형의 아웃바운드 인터넷 트래픽이 SSO 인증을 트리거하는지에 대한 의문이 제기되었습니다.

주요 관심사는 SSO 인증이 TCP 포트 80 및 443을 통한 브라우저 기반 웹 액세스에만 적용되는지 아니면 웹 트래픽을 생성하는 프린터 또는 Windows 엔드포인트 이외의 디바이스와 브라우저 기반이 아닌 애플리케이션에도 적용되는지 여부를 파악하는 것이었습니다. 인증 프롬프트 및 IdP(Identity Providers)로 리디렉션하는 경우에 대한 명확한 설명이 필요한 동작은 연결된 사이트에서 시작되는 다양한 유형의 웹 트래픽에 대해 발생합니다.

환경

- CSA(Cisco Secure Access) 구축
- 사이트와 CSA 간의 IPsec 터널 연결
- SSO 인증으로 구성된 보안 프로파일
- 프린터와 비 Windows 엔드포인트를 비롯한 다양한 디바이스와 혼합된 환경
- HTTPS 검사 사용
- SAML 통합이 구성됨

해결

Cisco Secure Access의 SSO 인증 동작은 브라우저 기반 웹 트래픽만 대상으로 하도록 특별히 설계되었습니다. 시스템은 웹 요청이 SSO 인증 대상이어야 하는지 여부를 확인하기 위해 정교한 검사 프로세스를 수행합니다.

SSO 인증 프로세스

웹 요청을 IdP(Identity Provider)로 리디렉션하기 전에 Cisco Secure Access는 HTTPS 검사를 사용하여 요청이 쿠키를 지원하는 브라우저에서 시작되는지 확인합니다. 이 검사 프로세스는 브라우저 기반 웹 트래픽과 비브라우저 웹 트래픽을 구별하는 핵심 메커니즘입니다.

트래픽 분류

브라우저 기반 트래픽(SSO 인증 대상)

- 쿠키를 지원하는 브라우저에서 시작되는 웹 요청
- 브라우저 애플리케이션의 TCP 포트 80 및 443의 HTTP/HTTPS 트래픽
- HTTPS 검사 쿠키/브라우저 탐지를 전달하는 트래픽

비 브라우저 트래픽(SSO 인증 제외)

- 프린터 및 기타 네트워크 장치의 웹 트래픽
- 쿠키를 지원하지 않거나 브라우저로 식별되지 않는 응용 프로그램
- 브라우저 탐지에 실패한 웹 트래픽을 생성하는 비 Windows 엔드포인트
- HTTPS 검사 브라우저 확인을 통과하지 않는 모든 웹 트래픽

SSO 인증 사전 요구 사항

SSO 인증이 환경에서 제대로 작동하려면 다음과 같은 몇 가지 전제 조건을 충족해야 합니다.

- 작동 중인 SAML 컨피그레이션이 있어야 합니다.
- XFF가 있는 프록시 네트워크 및/또는 NAT가 없는 터널(IP 서로게이트에는 내부 사설 IP에 대한 가시성이 필요함)
- HTTPS 검사를 활성화해야 합니다.
- 브라우저 세션은 쿠키를 유지해야 합니다(세션 종료 시 쿠키 삭제 또는 익명 브라우징은 권장되지 않음).
- 여러 위치에서 겹치지 않는 IP 주소 또는 겹치는 경우 적절한 사이트 분리

원인

이러한 동작은 Cisco Secure Access에서 설계대로 이루어집니다. SSO 인증 메커니즘은 웹 브라우저를 통해 대화형 사용자 세션을 대상으로 하는 동시에 자동화된 시스템과 비대화형 장치가 인증 중단 없이 웹 리소스에 액세스할 수 있도록 특별히 설계되었습니다. 이 설계는 자동화된 프로세스, 디바이스 관리 인터페이스, 인증 리디렉션 또는 쿠키 기반 세션을 처리할 수 없는 애플리케이션의 중단을 방지합니다.

관련 콘텐츠

- [SAML 통합 구성 - SAML에 IP 서로게이트 활성화](#)
- [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.