

ChromeOS SWG 웹 보호가 작동하지 않으며 연속하여 웹 로그가 활동 검색에 표시되지 않음

목차

문제

조직에 SWG(Secure Web Gateway) 보호가 활성화된 것처럼 보이지만 ChromeOS 사용자에게 대한 웹 로그가 생성되지 않았습니다. 영향을 받는 ChromeOS 엔드포인트는 활동 검색 인터페이스에 표시되는 SWG/웹 로깅 활동이 없는 DNS 수준 보호만 표시하고 있었습니다. SWG 보호 상태가 사용하도록 설정되어 있음을 나타내는 동안 사용자에게 웹 트래픽 로그가 전혀 없습니다.

조사 중에 진단 로그에서는 엔드포인트 <http://407.checkumbrella.com>에 대한 동기화 실패가 반복되고 HTTP 407(프록시 인증 필요) 오류 응답이 있음을 [확인했습니다](#). ChromeOS 클라이언트/확장이 프록시 서비스를 제대로 인증하지 못하여 적절한 SWG 보호 활성화 및 후속 웹 로그 생성을 방지했습니다.

환경

- Cisco 보안 액세스
- Cisco Secure Access 클라이언트/확장이 포함된 ChromeOS 엔드포인트
- ChromeOS 관리용 Google Admin 콘솔

해결

영향을 받는 ChromeOS 사용자가 포함된 Google Admin OU(Organizational Unit)에 대한 기본 인증 체계를 사용하도록 설정하고 SWG 보호를 활성화하기 위해 정책 다시 로드를 수행하여 문제가 해결되었습니다.

1단계: 로그 수집 및 분석

동기화 실패의 근본 원인을 식별하기 위해 수집된 HAR 캡처(네트워크 및 콘솔 로그 검토) Cisco Secure Access 서비스와의 동기화를 시도할 때 로그에 반복적인 인증 실패가 표시되었습니다.

2단계: Google Admin OU에 대한 기본 인증 활성화

Google Admin 콘솔에서 영향받는 ChromeOS 사용자가 포함된 조직 구성 단위로 이동하여 기본 인증 체계를 활성화합니다. 이를 통해 ChromeOS 클라이언트/내선 번호가 Cisco Secure Access 프록시 서비스로 올바르게 인증될 수 있습니다.

3단계: 정책 다시 로드 및 확인

기본 인증을 활성화한 후 영향받는 ChromeOS 디바이스에서 정책 다시 로드를 수행합니다. 보호 상태를 확인하여 SWG 보호가 활성화되는지 확인합니다. SWG 보호는 이제 DNS 레벨 보호만 아니라 활성으로 표시되어야 합니다.

4단계: 검증

영향을 받는 ChromeOS 사용자의 웹 브라우징 활동을 테스트하고 웹 로그가 현재 생성되어 활동 검색 인터페이스에 표시되는지 확인합니다. 로그는 SWG 서비스를 통해 적절한 웹 트래픽 검사 및 로깅을 표시해야 합니다.

원인

ChromeOS 클라이언트/내선 번호에서 영향을 받은 사용자가 포함된 Google Admin 조직 구성 단위 에 대해 기본 인증 체계를 비활성화했습니다. 기본 인증을 활성화하지 않으면 ChromeOS 디바이스에서 Cisco Secure Access 프록시 서비스를 제대로 인증할 수 없으므로 동기화 시도 중에 HTTP 407(프록시 인증 필요) 오류가 발생합니다. 이로 인해 SWG 보호가 제대로 활성화되지 않아 디바이스가 DNS 전용 보호로 다시 전환되고 웹 로그 생성이 방지되었습니다.

관련 콘텐츠

- [Cisco Secure Access에 대한 기본 정보 트러블슈팅 및 수집](#)
- [Cisco Secure Access Chromebook 클라이언트](#)
- [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.