

SAML 인증 및 PAC 기반 트래픽 포워딩을 사용하는 공유 컴퓨터 환경을 위한 SWG(Secure Web Gateway)의 사용자별 식별 및 정책 시행 과제

목차

문제

SAML 인증 및 PAC 기반 보안 액세스를 사용하는 Cisco SWG(Secure Web Gateway) 배포에서 공유 컴퓨터에 로그인한 첫 번째 사용자만 웹 트래픽 및 정책 적용을 위해 올바르게 식별됩니다. 사용자를 전환할 때 IP 서로게이트 옵션이 비활성화되고 PAC 파일이 사용되더라도 후속 웹 트래픽은 계속해서 초기 사용자에게 귀속됩니다. DNS 쿼리는 Umbrella Virtual Appliance를 통해 올바른 활성 사용자를 반영하지만 웹 및 방화벽 로그는 작업을 이전 사용자에게 지속적으로 매핑합니다. 이 요청은 SWG가 공유 컴퓨터 환경에서 사용자별 식별 및 정책 적용을 지원하는지 여부와 올바른 사용자 매핑을 확인하는 것입니다.

환경

- DNS 확인을 위한 가상 어플라이언스입니다.
- 사용자 ID에 대한 SAML 인증
- PAC 파일 없이 PAC로 트래픽 포워딩을 혼합합니다.
- 쿠키 서로게이트를 위해 우회된 특정 서브넷 및 호스트와 함께 IP 서로게이트 옵션이 활성화되었습니다.
- 온프레미스 디바이스, 원격 엔드포인트 또는 사용자 없음

해결

이 문제는 사용자 교육 및 구성 지침을 통해 다음과 같은 사항을 염두에 두고 해결되었습니다.

- PAC 파일과 함께 쿠키 서로게이트 ID를 사용합니다. 트래픽은 네트워크 터널로 또는 네트워크 터널에서 라우팅될 수 있습니다.
- PAC 파일 없이 쿠키 서로게이트 ID를 사용하지만 트래픽은 네트워크 터널을 통과해야 합니다.
- 쿠키 서로게이트를 적용하려는 액세스 정책에는 보안 프로필에서 SAML 인증이 활성화되어 있어야 합니다.
- 쿠키 서로게이트 트래픽은 브라우저 기반 트래픽에만 사용됩니다. 소스 ID를 네트워크로 사용하여 컴퓨터에서 비 쿠키 트래픽(예: Teams 또는 Webex 트래픽)을 식별하려면 별도의 규칙이 필요합니다.
- 쿠키 서로게이트가 작동하려면 SWG 모듈을 사용 중이지 않아야 합니다.
- IP 서로게이트도 활성화된 경우, 쿠키 서로게이트를 사용하려는 프라이빗 IP 주소/서브넷을

우회 목록에 추가해야 합니다(Users and Groups - Configuration Management - Advanced Settings).

- 쿠키 서로게이트의 우회 목록도 더 짧은 접두사와 일치합니다. 예를 들어, 10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must 추가할 경우.
- 쿠키 서로게이트는 여러 ID를 유지하기 위해 로그아웃할 필요 없이 시스템에서 사용자 전환을 지원합니다.

많은 트러블슈팅이 정책 테스트 및 활동 검색이었습니다.

원인

공유 컴퓨터 환경에서 잘못된 사용자 식별의 근본 원인은 주로 사용자 교육에 기인합니다.

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.