보안 클라이언트에서 보안 액세스 도메인 우회 확인

문제

Cisco Secure Access를 사용하는 조직은 특정 웹 사이트, 응용 프로그램 또는 서비스가 Secure Access로 전송되거나 Secure Web Gateway에 의해 처리되지 않고 인터넷에 직접 연결하도록 Bypass 도메인을 구성하는 경우가 많습니다. 이러한 Bypass 규칙이 Secure Access 대시보드에 올바르게 구성되어 표시될 수 있지만, 관리자는 Cisco Secure Client 엔드포인트에 Bypass 정책이 실제로 적용되고 적용되는지 확인하는 문제에 자주 직면합니다.

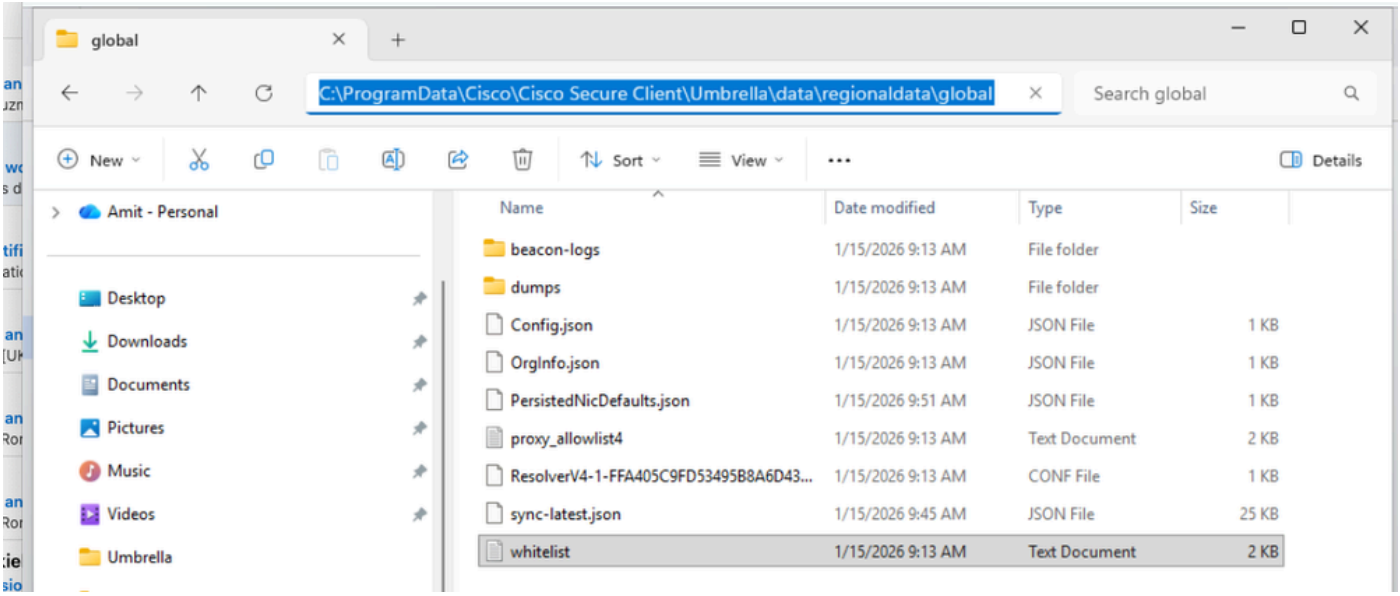
환경

- Cisco Secure Access with Roaming Security Modules with Domain Bypass.

해결

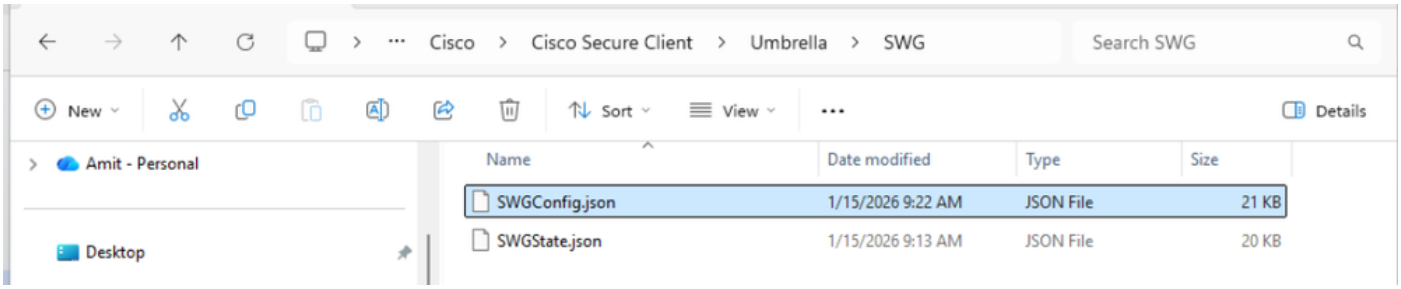
다음으로 도메인을 구성할 때:

- 보안 액세스를 우회합니다. 컨피그레이션은 allowlist.txt 파일의 C: > Program Data > Cisco > Cisco Secure Client > Umbrella > Data > Regional Data > Global Folder 아래에 있는 클라이언트로 푸시됩니다.



inline_image_0.png

- SWG를 우회하면 컨피그레이션이 SWGConfig.json 파일의 C: > Program Data(프로그램 데이터) > Cisco > Cisco Secure Client(Cisco 보안 클라이언트) > Umbrella > SWG:



인라인 이미지_1.png

참고: 클라이언트와 클라우드 간의 동기화 타이머는 약 25분이지만 이를 재정의하려는 경우 Umbrella 서비스를 다시 시작할 수 있습니다.

원인

문제의 근본 원인은 사용자가 SWG Bypass에 대해 잘못된 파일을 확인했기 때문입니다.

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.