보안 액세스 스플릿 터널링 컨피그레이션 문제

목차

문제

스플릿 터널 트래픽에 대해 Cisco TIA(Secure Access) 기능을 구성하는 동안 구성 프로세스 중에 여러 가지 복잡한 문제가 발생하여 제대로 구축할 수 없었습니다.

- 트래픽 식별 문제: 스플릿 터널링을 위해 TIA를 구성할 때 모든 VPN 트래픽을 인터넷 보안 검사에서 제외해야 합니다. 필요한 트래픽 흐름을 파악하는 것이 어려웠으며, 일부 리디렉션 URL의 경우 추적 및 분류가 특히 까다로웠습니다.
- 인증 트래픽 제약: 특정 스플릿 터널 시나리오에서는 프록시에서 제외되는 인증 트래픽이 필요했습니다. 그러나 기존 정책을 기반으로 인증 관련 트래픽을 프록시에서 우회할 수 없어 정책 충돌이 발생했습니다.
- VPN 연결 끊김 시 보안 위험: 스플릿 터널 트래픽은 VPN 연결이 끊어질 때 열린 인터넷에 노출되므로, 구성 중에 고려해야 할 추가 보안 위험이 있습니다.

추가 분석 및 해결이 필요한 프로세스 중에 추가 컨피그레이션 문제가 관찰되기도 했습니다.

환경

- 제품군: SECCS(보안 액세스)
- 기술: 스플릿 터널링 기능이 포함된 Cisco TIA(Secure Access)
- 설정: 기존 정책을 사용하는 스플릿 터널 트래픽 시나리오
- 인증: 프록시 기반 인증 트래픽 처리
- 네트워크 보안: VPN 트래픽에 대한 인터넷 보안 검사 요구 사항

해결

Cisco Secure Access 스플릿 터널링에서 확인된 컨피그레이션 문제를 기반으로 확인된 제한 사항 및 정책 충돌을 해결하기 위한 포괄적인 기능 요청이 제출되었습니다.

기능 요청 제출

기능 요청(CSE-I-5636)이 열려 있으며, 다음과 같은 구성 과제를 해결하기 위해 관련 엔지니어링 팀에서 검토를 위해 제출했습니다.

- 인터넷 보안 검사에서 VPN 트래픽 제외를 위한 향상된 트래픽 식별 기능
- 추적 및 분류가 어려운 리디렉션 URL 처리 개선
- 기존 정책을 통한 인증 트래픽 바이패스 제한 해결
- VPN 연결 해제 중 스플릿 터널 트래픽 노출을 위한 보안 위험 완화

원인

컨피그레이션 문제는 복잡한 엔터프라이즈 구축 시나리오를 적절히 처리하지 못하는 Cisco TIA(Secure Access) 스플릿 터널링 구현의 현재 제한에서 비롯됩니다. 특히, 시스템은 트래픽 식별 및 범주화를 위한 충분한 세분화된 제어가 부족하고, 정책이 시행될 때 인증 트래픽을 우회하는 데 제약이 있으며, VPN 연결이 중단될 때 스플릿 터널 트래픽을 위한 적절한 보안 조치를 제공하지 않습니다.

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.