

보안 클라이언트 TND 수동 VPN 연결 동작 및 URL 차단 고려 사항

목차

문제

Trusted Network(신뢰할 수 있는 네트워크) 설정이 Disconnect(연결 끊기)로 설정된 TND(Trusted Network Detection) 기능을 사용하여 VPN 프로필을 사용하는 경우, 사용자가 Cisco Secure Client를 사용하여 수동으로 연결을 시작할 때 신뢰할 수 있는 네트워크 내에 있는 엔드포인트가 VPN 연결을 성공적으로 설정할 수 있습니다.

이 동작은 엔드포인트가 신뢰할 수 있는 네트워크에서 탐지될 때 VPN 세션의 연결을 끊도록 TND 구성이 설정되었음에도 불구하고 발생합니다.

파악된 구체적인 우려 사항은 다음과 같습니다.

- 신뢰할 수 있는 네트워크 엔드포인트의 수동 VPN 연결은 표준 TND 구성을 통해 제어하거나 차단할 수 없습니다.
- Cisco CSA(Secure Access) 설정이 신뢰할 수 있는 네트워크 엔드포인트로부터의 수동 VPN 연결을 차단할 수 있는지에 대한 불확실성
- VPN 프로필 연결 URL(xxxx.vpn.sse.cisco.com)의 안정성 및 방화벽 기반 차단 전략에 영향을 줄 수 있는 주기적인 변경 여부에 대한 질문

환경

- CSA(Cisco Secure Access) 구축
- VPN 프로필 컨피그레이션을 사용하는 Cisco Secure Client
- TND(Trusted Network Detection) 기능 활성화됨
- 연결 끊기로 구성된 TND 트러스트된 네트워크 설정

- 구성된 신뢰할 수 있는 네트워크 내에 있는 엔드포인트
- 네트워크 액세스 제어를 위한 방화벽 인프라

해결

수동 VPN 연결을 통한 TND 동작 이해

관찰된 동작은 문서화된 Cisco Secure Client 기능과 일치합니다. Cisco 설명서에 따르면 TND는 사용자가 신뢰할 수 있는 네트워크에서 수동으로 시작하는 VPN 세션의 연결을 끊거나 차단하지 않습니다. 이는 TND 컨피그레이션 설정과 상관없이 필요한 동작입니다.

주요 기술적 사실은 다음과 같습니다.

- TND 자동 연결 해제 기능은 자동으로 설정된 VPN 연결에만 적용됩니다.
- 사용자가 시작한 수동 VPN 연결은 TND 연결 끊기 동작을 우회합니다.
- 신뢰할 수 있는 네트워크 엔드포인트에서 수동 VPN 연결을 차단하는 CSA 컨피그레이션 설정이 없습니다.

운영 완화 전략

신뢰할 수 있는 네트워크 엔드포인트에서 수동 VPN 연결을 제어하는 기본 방법은 네트워크 레벨 제어를 통하는 것입니다.

1단계: 방화벽 URL 차단 구현: VPN 프로필 연결 URL(xxxx.vpn.sse.cisco.com)에 대한 액세스를 차단하도록 신뢰할 수 있는 네트워크 방화벽을 구성합니다. 이렇게 하면 신뢰할 수 있는 네트워크의 엔드포인트가 VPN 서비스 엔드포인트에 도달하지 않습니다.

2단계: URL 안정성 확인: VPN 프로필 URL 식별자(xxxx 부분)는 테넌트별로 지정되며 주기적으로 변경되지 않습니다. 이는 방화벽 차단 규칙을 위한 안정적인 대상을 제공합니다.

검증 및 테스트

테스트 결과, 사용자가 Cisco Secure Client를 통해 수동 연결을 시도하는 경우에도 신뢰할 수 있는 네트워크 방화벽에서 VPN 프로파일 연결 URL을 차단하면 엔드포인트에서 VPN 연결을 설정할 수 없습니다.

원인

이 동작은 Cisco Secure Client TND 구현의 설계에 따라 달라집니다. TND 기능은 네트워크 신뢰 상태를 기반으로 자동 VPN 연결을 관리하도록 특별히 설계되었지만, 사용자가 시작한 수동 VPN 연결을 의도적으로 방해하지 않습니다. 이 설계에서는 사용자가 필요할 때 자동 동작을 재정의하면서 일반적인 사용 사례에 대해서는 자동화된 네트워크 탐지 및 연결 관리를 제공할 수 있습니다.

관련 콘텐츠

- [Cisco Secure Client 관리자 설명서 - TND 컨피그레이션](#)
- [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.