보안 액세스 RA-VPN IPv6 연결 실패 - 프로토콜 구성 문제

문제

IPv6를 통한 Cisco Secure Access로의 RA-VPN 연결이 설정되지 않고 Cisco Secure Client UI에 일반 연결 실패 메시지가 표시됩니다. 이 문제는 기존 RA-VPN 프로필을 사용하는 IPv6 기반 원격 액세스 연결 테스트에 영향을 줍니다. 조사 결과 SSE RA-VPN 프로필이 IPv6 연결에 대한 프로토콜 필드를 제대로 설정하지 않는 것으로 나타났습니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스 - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- 소프트웨어 버전: 모두
- IPv6 RA-VPN 연결을 시도하는 Cisco Secure Client
- Cisco Secure Access SSE 플랫폼
- 기존 RA-VPN 프로파일 컨피그레이션

해결

IPv6 RA-VPN 연결 실패를 해결하려면 RA-VPN 프로파일에서 IP Protocol Supported(IP 프로토콜 지원됨) 설정을 올바르게 구성해야 합니다. IPv6 지원을 활성화하려면 다음 단계를 수행합니다.

1단계: 액세스 클라이언트 설정

Cisco Secure Access 관리 인터페이스에서 Client Settings(클라이언트 설정) 섹션으로 이동합니다.

2단계: 관리자 설정 구성

Client Settings(클라이언트 설정)에서 Administrator Settings(관리자 설정) 섹션을 찾아 액세스합니다.

3단계: 지원되는 IP 프로토콜 설정

IPv6 지원을 포함하도록 IP Protocol Supported(IP 프로토콜 지원됨) 드롭다운을 구성합니다. 이 설정은 RA-VPN 프로파일이 클라이언트 연결에 어떤 IP 프로토콜을 지원할지를 제어합니다.

4단계: 구성 저장

IPv6 프로토콜 설정이 적용되었는지 확인하기 위해 업데이트된 RA-VPN 프로필 컨피그레이션을 저장합니다.

5단계: 연결 테스트

Cisco Secure Client를 사용하여 IPv6 RA-VPN 연결을 다시 테스트하여 이제 연결이 성공적으로 설정되었는지 확인합니다.

원인

IPv6 RA-VPN 연결 실패의 근본 원인은 RA-VPN 프로필의 IP Protocol Supported(IP 프로토콜 지원됨) 설정이 IPv6 연결을 지원하도록 구성되지 않았기 때문입니다. SSE RA-VPN 프로필에서는 IPv6 연결을 활성화하기 위해 프로토콜 필드의 명시적 컨피그레이션이 필요합니다. 이 설정을 제대로 구성하지 않으면 Cisco Secure Client에서 Cisco Secure Access 플랫폼에 대한 IPv6 기반 VPN 연결을 설정할 수 없습니다.

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.