TLS/DTLS 및 IPsec(IKEv2) 듀얼 컨피그레이션을 사용하는 Cisco Secure Access RAVPN 프로토콜 동작

목차

문제

기본 프로토콜이 IPsec(IKEv2)으로 설정된 Cisco Secure Access RAVPN에서 TLS/DTLS 및 IPsec(IKEv2) 프로토콜이 모두 활성화된 경우, IPsec 트래픽(UDP 포트 500/4500)이 차단된 네트워크에서 VPN 연결을 설정하려고 시도할 때 연결 오류가 발생합니다. Secure Client(보안 클라이언트)는 기본적으로 클라이언트 UI 드롭다운의 IPsec 옵션으로 설정되며 IPsec 연결이 실패할 경우 TLS/DTLS로 자동 장애 조치되지 않으므로 연결 오류가 발생하고 제한된 네트워크 환경에서 RAVPN 연결을 설정할 수 없습니다.

환경

- 듀얼 프로토콜 컨피그레이션을 사용하는 Cisco Secure Access RAVPN
- TLS/DTLS 및 IPsec(IKEv2) 프로토콜 모두 활성화됨
- IPsec(IKEv2)으로 구성된 기본 프로토콜 설정
- 별도의 IPsec 및 TLS 옵션이 포함된 프로토콜 선택 드롭다운을 사용하는 보안 클라이언트
- UDP 포트 500 및 4500에서 IPsec 트래픽을 차단하는 네트워크 환경

해결

관찰된 동작은 설계에 따라 필요합니다. Cisco Secure Access RAVPN은 두 프로토콜이 모두 활성화되어 있고 기본 프로토콜에서 연결 문제가 발생할 경우 IPsec(IKEv2)에서 TLS/DTLS로의 자동 프로토콜 장애 조치를 수행하지 않습니다.

수동 프로토콜 선택 필요

IPsec 트래픽을 차단하는 네트워크에서 연결하는 경우 사용자는 Secure Client에서 적절한 프로토콜을 수동으로 선택해야 합니다.

1단계: Secure Client 애플리케이션 열기

2단계: 클라이언트 인터페이스에서 프로토콜 선택 드롭다운 메뉴를 찾습니다

3단계: IPsec 옵션에서 TLS 옵션으로 선택 사항을 수동으로 변경합니다

4단계: TLS/DTLS 프로토콜을 사용하여 VPN 연결 시작

프로토콜 동작 설명

Cisco Secure Access RAVPN의 기본 프로토콜 설정은 보안 클라이언트에 제공되는 기본 프로토콜을 결정하지만 자동 장애 조치 기능을 활성화하지는 않습니다. TLS/DTLS와 IPsec(IKEv2)이 모두 활성화된 경우:

- Secure Client는 드롭다운 메뉴에 별도의 프로토콜 옵션을 표시합니다
- 클라이언트는 기본적으로 기본 프로토콜 설정(이 경우 IPsec)을 사용합니다
- 네트워크 연결 조건에 따라 프로토콜 간에 자동 스위칭이 발생하지 않음
- 사용자는 네트워크 환경에 따라 적절한 프로토콜을 수동으로 선택해야 합니다

원인

Cisco Secure Access RAVPN은 자동 프로토콜 장애 조치 기능 없이 설계되었습니다. TLS/DTLS 및 IPsec(IKEv2) 프로토콜이 모두 활성화된 경우, 시스템에서는 보안 클라이언트 인터페이스를 통해 수동 프로토콜을 선택해야 합니다. 기본 프로토콜 설정은 클라이언트 드롭다운 메뉴의 기본 선택만 결정하며, 기본 프로토콜에서 연결 문제가 발생할 경우 자동 스위칭 논리를 구현하지 않습니다.

관련 콘텐츠

- Cisco Secure Access 설명서
- 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.