Cisco Secure Client VPN Connection Reset by Peer with Zscaler SSL/TLS Decryption Interference

목차

문제

사용자는 Cisco Secure Client를 사용하여 연결을 설정하려고 시도할 때 VPN 연결 실패를 경험합니다.

환경

- 기술: Cisco Secure Access - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- 제품군: 초
- 운영 체제: macOS(/Users/admin/workspace/secure-client-macos_Raccoon_MR15/를 표시하는 로그 파일 경로 기반)
- 타사 소프트웨어: 클라이언트 시스템에 설치된 Zscaler
- VPN 프로토콜: CSTP(Cisco SSL Tunnel Protocol)
- TLS 버전: 암호화 TLS_AES_256_GCM_SHA384를 사용하는 TLS 1.3

해결

해결에는 Cisco Secure Client와 Zscaler의 SSL/TLS 암호 해독 기능 간의 충돌을 식별하고 해결하는 작업이 포함됩니다.

1단계: 로그 분석 및 진단

Cisco Secure Client DART 로그를 캡처하고 분석하여 연결 실패 패턴을 식별합니다. 로그에는 성공적인 TLS 세션 설정 후 즉시 연결 재설정이 표시됩니다.

로그의 주요 진단 표시기:

- 암호화 TLS_AES_256_GCM_SHA384를 사용하는 TLS 1.3 연결 설정
- MTU 계산 및 HTTP 협상이 정상적으로 진행됨
- 피어 오류(반환 코드: 54) 소켓 읽기 작업 중

TLS 1.3 세션은 암호화 TLS_AES_256_GCM_SHA384를 사용하여 성공적으로 설정되지만, 세션 설정 직후 재설정 패킷이 전송되어 연결이 종료되고 VPN 터널이 해제됩니다. 로그에서 관찰된 특정 오류는 소켓 읽기 작업 중에 반환 코드 54(0x00000036)와 함께 "Connection reset by peer(피어에 의한 연결 재설정)"를 표시합니다.

연결 시도 중에 다음 오류 시퀀스가 발생합니다.

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

2단계: 서드파티 소프트웨어 식별

클라이언트 시스템에서 SSL/TLS 검사 또는 암호 해독을 수행할 수 있는 타사 보안 소프트웨어가 있는지 조사합니다. 이 경우 Zscaler는 간섭 애플리케이션으로 식별되었습니다.

3단계: SSL/TLS 암호 해독 충돌 해결

Cisco Secure Client VPN 트래픽과 Zscaler의 SSL/TLS 암호 해독 기능 간의 충돌을 해결합니다. VPN 트래픽이 Zscaler에 의한 SSL/TLS 암호 해독을 받고 있는 것으로 보이며, 이는 VPN 터널 설정을 방해하고 연결 재설정을 유발합니다.

잠재적 해결 방법은 다음과 같습니다.

- SSL/TLS 검사에서 Cisco Secure Client VPN 트래픽을 제외하도록 Zscaler 구성
- VPN 서버 엔드포인트에 대한 Zscaler에서 우회 규칙 만들기
- 충돌을 확인하기 위해 VPN 연결 테스트 중에 Zscaler를 일시적으로 비활성화합니다.
- 네트워크 보안 팀과 협력하여 적절한 제외 항목 설정

원인

이 문제의 근본 원인은 Cisco Secure Client VPN 트래픽과 Zscaler의 SSL/TLS 암호 해독 기능 간의 충돌입니다. Zscaler가 VPN의 TLS 트래픽을 해독하거나 검사하려고 할 때 보안 터널 설정 프로세스를 방해합니다. 이 간섭은 TLS 세션이 설정된 직후 연결 재설정으로 나타나므로 VPN 터널이 협상 단계를 완료하지 못합니다. 재설정 패킷의 타이밍(TLS를 설정한 직후, 터널이 완료되기 전에 발생)은 보안 어플라이언스 또는 소프트웨어에서 발생하는 SSL/TLS 검사 간섭의 특성입니다.

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.