

# Zurücksetzen der Cisco Secure Client VPN-Verbindung durch Peer mit Zscaler SSL/TLS-Entschlüsselungsstörungen

## Inhalt

---

---

## Problem

Bei einem Benutzer treten VPN-Verbindungsfehler auf, wenn versucht wird, eine Verbindung über den Cisco Secure Client herzustellen.

## Umwelt

- Technologie: Cisco Secure Access - Sicherer Client-Remote-Zugriff (VPN, Status, private Ressource)
- Produktfamilie: SECACS
- Betriebssystem: macOS (basiert auf Protokolldateipfaden, die /Users/admin/workspace/secure-client-macos\_Raccoon\_MR15/ anzeigen)
- Software anderer Anbieter: Zscaler ist auf dem Client-System installiert
- VPN-Protokoll: CSTP (Cisco SSL Tunnel Protocol)
- TLS-Version: TLS 1.3 mit Chiffre TLS\_AES\_256\_GCM\_SHA384

## Auflösung

Die Lösung umfasst die Identifizierung und Behebung des Konflikts zwischen dem Cisco Secure Client und der SSL/TLS-Verschlüsselungsfunktion von Zscaler.

### Schritt 1: Protokollanalyse und -diagnose

Erfassen und analysieren Sie die Cisco Secure Client DART-Protokolle, um das Muster für Verbindungsfehler zu identifizieren. Die Protokolle zeigen den erfolgreichen Aufbau der TLS-Sitzung an, gefolgt von einem sofortigen Zurücksetzen der Verbindung.

Wichtige Diagnoseanzeigen in den Protokollen:

- TLS 1.3-Verbindungsaufbau mit Chiffre TLS\_AES\_256\_GCM\_SHA384
- MTU-Berechnung und HTTP-Aushandlung werden normal ausgeführt
- Verbindungsrücksetzung durch Peer-Fehler (Rückgabecode: 54) während des Socket-Lesevorgangs

Die TLS 1.3-Sitzung wird mithilfe des Schlüssels TLS\_AES\_256\_GCM\_SHA384 erfolgreich hergestellt. Unmittelbar nach dem Aufbau der Sitzung wird jedoch ein Reset-Paket gesendet, das die Verbindung beendet, sodass der VPN-Tunnel abgebrochen wird. Der in den Protokollen festgestellte spezifische Fehler zeigt während des Socket-Lesevorgangs "Connection reset by peer" mit dem Rückgabecode 54 (0x00000036) an.

Die folgende Fehlersequenz tritt bei Verbindungsversuchen auf:

```
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
```

## Phase 2: Identifikation von Drittanbietersoftware

Untersuchen Sie das Vorhandensein von Sicherheitssoftware eines Drittanbieters, die möglicherweise eine SSL/TLS-Prüfung oder -Entschlüsselung auf dem Client-System durchführt. In diesem Fall wurde Zscaler als störende Anwendung identifiziert.

## Schritt 3: Konfliktlösung bei SSL/TLS-Entschlüsselung

Bewältigung des Konflikts zwischen dem VPN-Datenverkehr des Cisco Secure Client und der SSL/TLS-Verschlüsselungsfunktion von Zscaler Der VPN-Datenverkehr wird anscheinend von Zscaler SSL/TLS-entschlüsselt, was die Einrichtung des VPN-Tunnels beeinträchtigt und zum

Zurücksetzen der Verbindung führt.

Mögliche Lösungsansätze umfassen:

- Konfigurieren von Zscaler zum Ausschluss von Cisco Secure Client VPN-Datenverkehr von der SSL/TLS-Prüfung
- Erstellen von Umgehungsregeln in Zscaler für die VPN-Server-Endpunkte
- Deaktivieren Sie Zscaler während des VPN-Verbindungstests vorübergehend, um den Konflikt zu bestätigen.
- Koordination mit dem Netzwerksicherheits-Team, um geeignete Ausnahmen festzulegen

## Ursache

Die Ursache dieses Problems liegt in einem Konflikt zwischen dem VPN-Datenverkehr des Cisco Secure Client und der SSL/TLS-Verschlüsselungsfunktion von Zscaler. Wenn Zscaler versucht, den TLS-Datenverkehr des VPNs zu entschlüsseln oder zu überprüfen, beeinträchtigt dies den sicheren Tunnelherstellungsprozess. Diese Interferenz äußert sich in einem Verbindungsrücksetzvorgang unmittelbar nach der TLS-Sitzung, der verhindert, dass der VPN-Tunnel seine Verhandlungsphase abschließt. Der Zeitpunkt des Reset-Pakets (unmittelbar nach erfolgreicher TLS-Einrichtung, aber vor Tunnelabschluss) ist charakteristisch für SSL/TLS-Prüfungsstörungen durch Sicherheitsgeräte oder Software.

## Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.