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

Contents

Issue

A user experiences VPN connection failures when attempting to establish a connection using Cisco Secure Client.

Environment

- Technology: Cisco Secure Access - Secure Client Remote Access (VPN, Posture, Private Resource)
- Product Family: SECACCS
- Operating System: macOS (based on log file paths showing /Users/admin/workspace/secure-client-macos_Raccoon_MR15/)
- Third-party software: Zscaler installed on the client system
- VPN Protocol: CSTP (Cisco SSL Tunnel Protocol)
- TLS Version: TLS 1.3 with cipher TLS_AES_256_GCM_SHA384

Resolution

The resolution involves identifying and addressing the conflict between Cisco Secure Client and Zscaler's SSL/TLS decryption functionality.

Step 1: Log Analysis and Diagnosis

Capture and analyze the Cisco Secure Client DART logs to identify the connection failure pattern. The logs will show successful TLS session establishment followed by an immediate connection reset.

Key diagnostic indicators in the logs:

- TLS 1.3 connection establishment with cipher TLS_AES_256_GCM_SHA384
- MTU calculation and HTTP negotiation proceeding normally
- Connection reset by peer error (Return Code: 54) during socket read operation

The TLS 1.3 session establishes successfully using cipher TLS_AES_256_GCM_SHA384, but immediately after session establishment, a reset packet is sent which terminates the connection, resulting in the VPN tunnel being torn down. The specific error observed in the logs shows "Connection reset by peer" with return code 54 (0x00000036) during the socket read operation.

The following error sequence occurs during connection attempts:

```
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
```

Step 2: Third-Party Software Identification

Investigate the presence of third-party security software that may be performing SSL/TLS inspection or decryption on the client system. In this case, Zscaler was identified as the interfering application.

Step 3: SSL/TLS Decryption Conflict Resolution

Address the conflict between Cisco Secure Client VPN traffic and Zscaler's SSL/TLS decryption functionality. The VPN traffic appears to be undergoing SSL/TLS decryption by Zscaler, which interferes with the VPN tunnel establishment and causes the connection reset.

Potential resolution approaches include:

- Configure Zscaler to exclude Cisco Secure Client VPN traffic from SSL/TLS inspection
- Create bypass rules in Zscaler for the VPN server endpoints
- Temporarily disable Zscaler during VPN connection testing to confirm the conflict
- Coordinate with network security team to establish proper exclusions

Cause

The root cause of this issue is a conflict between Cisco Secure Client VPN traffic and Zscaler's SSL/TLS decryption functionality. When Zscaler attempts to decrypt or inspect the VPN's TLS traffic, it interferes with the secure tunnel establishment process. This interference manifests as a connection reset immediately after the TLS session is established, preventing the VPN tunnel from completing its negotiation phase. The timing of the reset packet (occurring right after successful TLS establishment but before tunnel completion) is characteristic of SSL/TLS inspection interference from security appliances or software.

Related Content

- Cisco Technical Support & Downloads