Zscaler SSL/TLS復号干渉によるピアによるCisco Secure Client VPN接続のリセット

内容

お問い合わせ内容

Cisco Secure Clientを使用して接続を確立しようとすると、VPN接続障害が発生する。

環境

- テクノロジー：Cisco Secure Access - Secure Client Remote Access（VPN、ポスチャ、プライベートリソース）
- 製品ファミリ：SECACCS
- オペレーティングシステム：macOS（/Users/admin/workspace/secure-client-macos_Raccoon_MR15/を示すログファイルパスに基づく）
- サードパーティソフトウェア：クライアントシステムにインストールされたZscaler
- VPNプロトコル：CSTP(Cisco SSL Tunnel Protocol)
- TLSバージョン：暗号TLS_AES_256_GCM_SHA384を使用するTLS 1.3

解決策

この問題を解決するには、Cisco Secure ClientとZscalerのSSL/TLS復号化機能の間の競合を特定して対処する必要があります。

ステップ1：ログの分析と診断

Cisco Secure Client DARTログをキャプチャして分析し、接続障害パターンを特定します。ログ

には、TLSセッションが正常に確立されたことが示された後、接続がただちにリセットされます。

ログの主要な診断インジケータ：

- 暗号TLS_AES_256_GCM_SHA384によるTLS 1.3接続の確立
- MTU計算とHTTPネゴシエーションが正常に進行
- ソケット読み取り操作中のピアエラーによる接続リセット（リターンコード： 54）

TLS 1.3セッションは暗号TLS_AES_256_GCM_SHA384を使用して正常に確立されますが、セッションの確立直後に、接続を終了するリセットパケットが送信され、その結果VPNトンネルが切断されます。ログに記録された特定のエラーには、ソケット読み取り操作中の「Connection reset by peer」とリターンコード54(0x00000036)が示されています。

接続の試行中に次のエラー・シーケンスが発生します。

```
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
```

ステップ2：サードパーティソフトウェアの識別

クライアントシステムでSSL/TLS検査または復号化を実行している可能性があるサードパーティ製セキュリティソフトウェアの存在を調査します。この場合、Zscalerが干渉アプリケーションとして識別されています。

ステップ3:SSL/TLS復号化の競合の解決

Cisco Secure Client VPNトラフィックとZscalerのSSL/TLS復号化機能の間の競合に対処します。VPNトラフィックはZscalerによってSSL/TLS復号化されているように見えます。これによりVPNトンネルの確立が妨げられ、接続がリセットされます。

考えられる解決方法は次のとおりです。

- SSL/TLSインスペクションからCisco Secure Client VPNトラフィックを除外するようにZscalerを設定する
- ZscalerでVPNサーバエンドポイント用のバイパスルールを作成する
- VPN接続テスト中にZscalerを一時的に無効にして、競合を確認します。
- ネットワークセキュリティチームと連携して適切な除外を確立

原因

この問題の根本原因は、Cisco Secure Client VPNトラフィックとZscalerのSSL/TLS復号化機能の間の競合です。ZscalerがVPNのTLSトラフィックを復号化または検査しようとすると、セキュアトンネルの確立プロセスに干渉します。この干渉は、TLSセッションが確立された直後に接続がリセットされ、VPNトンネルがネゴシエーションフェーズを完了できなくなるという形で現れます。リセットパケットのタイミング（TLSの確立に成功した直後で、トンネルが完了する前に発生）は、セキュリティアプライアンスまたはソフトウェアからのSSL/TLSインスペクション干渉の特性です。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。