

Ubuntu 24.04でSecure Client VPNが終了理由コード7で切断

内容

お問い合わせ内容

Ubuntu 24.04上のCisco Secure ClientはVPN接続を正常に確立しますが、数秒以内に切断されます。この切断には常に終了理由コード7とlibvnpapi.soに関連するクラッシュが伴い、通常のビジネスアクセスに必要な安定したVPN接続が妨げられます。

接続シーケンスでは、クライアントが「Connected」状態に達したにもかかわらず、ステータスを確認するとすぐにDisconnected状態に遷移することが示されています。VPN Clientのログには「Termination reason code 7: The agent has been stopped」と表示され、トンネル状態の変更エントリと、「close notify」アラートによってDTLS/SSL接続が解除されていることを示すメッセージも記録されます。

次のコマンドシーケンスは、この問題を示しています。

```
/opt/cisco/secureclient/bin/vpn connect
```

接続の出力は、正常な確立を示しています。

```
Cisco Secure Client (version 5.1.12.146) release.
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.
>> state: Unknown
>> state: Disconnected
>> state: Disconnected
>> notice: Ready to connect.
>> registered with local VPN subsystem.
>> contacting host (vpn.sse.cisco.com) for login information...
>> notice: Contacting vpn.sse.cisco.com.
>> Your client certificate will be used for authentication
Group:
>> state: Connecting
>> notice: Establishing VPN session...
The Cisco Secure Client - Downloader is analyzing this computer. Please wait...
Initializing the Cisco Secure Client - Downloader...
The Cisco Secure Client - Downloader is performing update checks...
```

```
The Cisco Secure Client - Downloader update checks have been completed.
>> notice: The Cisco Secure Client - Downloader is performing update checks...
>> notice: Checking for profile updates...
>> notice: Checking for customization updates...
>> notice: Performing any required updates...
>> notice: The Cisco Secure Client - Downloader update checks have been completed.
Please wait while the VPN connection is established...
>> state: Connecting
>> notice: Establishing VPN session...
>> notice: Establishing VPN - Initiating connection...
>> notice: Establishing VPN - Examining system...
>> notice: Establishing VPN - Activating VPN adapter...
>> notice: Establishing VPN - Configuring system...
>> notice: Establishing VPN...
>> state: Connected
```

ただし、接続直後にステータスを確認する場合は、次の手順を実行します。

```
/opt/cisco/secureclient/bin/vpn status
```

クライアントにdisconnected状態が表示されます。

```
Cisco Secure Client (version 5.1.12.146) release.
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.
>> state: Unknown
>> state: Disconnected
>> state: Disconnected
>> state: Disconnected
>> notice: Ready to connect.
>> registered with local VPN subsystem.
VPN>
```

環境

- オペレーティングシステム : Ubuntu 24.04
- Cisco Secure Clientバージョン : 5.1.12.146
- 認証方式 : クライアント証明書認証
- 仮想インターフェイス : cscotun0 (または同様のCisco Secure Client仮想インターフェイス)
- 環境には、システム管理用の自動化スクリプトが含まれる

解決策

この問題は、Cisco Secure Client仮想インターフェイス(cscotun0)を新しい物理デバイスとして誤って識別していた自動化スクリプトを識別して修正し、HTTP/トランスペアレントプロキシ設定を適用することで解決されました。次の手順では、解決プロセスの概要を説明します。

ステップ1：診断情報の収集

影響を受けるエンドポイントからDART(Diagnostic and Reporting Tool)バンドルを生成し、VPNクライアントの詳細なログとシステム情報を取得します。

Generate DART bundle from Cisco Secure Client interface or command line

DARTバンドルには、インターフェイスcscotun0のDNS設定、VPNアダプタ設定、ルーティングテーブルの変更など、インターフェイスとプロファイルの設定手順を示すVPNエージェントログエントリが含まれています。

```
Mar 13 16:41:08 Message type information sent to
> the user: Contacting vpn.sse.cisco.com.
> Mar 13 16:41:08 : VPN SESSION START: Initiating
> VPN connection to the secure gateway hvpn.sse.cisco.com
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy server configuration from
> the operating system: http://x.x.x.x:3128/
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy exception list from the
> operating system: localhost,127.0.0.0/8,:::1
> Mar 13 16:41:11 Termination reason code 7: The
> agent has been stopped.
```

手順2：自動化スクリプトの動作の分析

ネットワークインターフェイスとプロキシ設定を管理するローカル自動化スクリプトを調査します。新しいネットワークインターフェイスを自動的に検出し、設定ポリシーを適用するスクリプトを探します。

ステップ3：プロキシ割り当ての問題の特定

自動化スクリプトがCisco Secure Client仮想インターフェイスを新しい物理デバイスとして扱い、不適切なプロキシ設定を適用しているかどうかを判断します。仮想インターフェイス（cscotun0または同様のインターフェイス）にHTTP/トランスペアレントプロキシ設定を適用することはできません。

ステップ4：仮想インターフェイスからのプロキシ設定の削除

自動化スクリプトによってCisco Secure Client仮想インターフェイスに自動的に適用されたプロキシ割り当てを削除または修正します。これにより、プロキシがVPNトラフィックフローに干渉するのを防ぐことができます。

手順5：自動化スクリプトロジックの更新

自動プロキシ設定ポリシーからCisco Secure Client仮想インターフェイス（通常はcscotun0、cscotun1という名前）を除外するように、自動化スクリプトを変更します。自動化されたネットワーク設定プロセス中にVPN仮想インターフェイスを特定してスキップするロジックを追加します。

ステップ6:VPN接続の確認

プロキシ設定を削除した後にVPN接続をテストし、安定した接続であることを確認します。

```
/opt/cisco/secureclient/bin/vpn connect vpn.sse.cisco.com
```

接続確立後にステータスをチェックして、接続が安定していることを確認します。

```
/opt/cisco/secureclient/bin/vpn status
```

別のトラブルシューティング手順

問題が同様の環境で引き続き発生する場合、または同様の環境で発生する場合は、次の追加のトラブルシューティング方法を検討してください。

- 自動化スクリプトを使用せずに、新しいLinuxエンドポイントでCisco Secure Clientをテストする
- libvpnapiまたはVPNエージェントと干渉する可能性があるサードパーティサービスを一時的に無効にします
- Cisco Secure Clientを入手可能な最新バージョンにアップグレードする
- システムログでVPN仮想インターフェイスの作成と設定に関する競合を確認する

原因

根本原因は、Cisco Secure Client仮想インターフェイス (cscotun0または類似) を新しい物理ネットワークデバイスとして誤って特定した社内自動化スクリプトにあります。スクリプトによって、この仮想インターフェイスにHTTP/Transparentプロキシ設定が自動的に適用されました。これにより、VPNトラフィックフローが干渉され、理由コード7で接続が終了しました。

VPNクライアントが接続を確立すると、暗号化されたトラフィックを処理するための仮想ネットワークインターフェイスが作成されます。自動化スクリプトは、このインターフェイスの作成をシステムに参加する新しいネットワークデバイスとして検出し、物理ネットワークインターフェイス用の標準プロキシポリシーを適用しました。このプロキシ設定により、暗号化されたトラフィックを適切にルーティングするVPNトンネルの機能が中断され、接続が正常に確立された後、ただちに接続解除されます。

終了理由コード7(「The agent has been stopped」)およびlibvpnapi.soのクラッシュは、直接のVPNクライアントソフトウェアの問題ではなく、基盤となるプロキシ干渉の症状でした。

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。