Secure Client VPN Disconnects with Termination Reason Code 7 on Ubuntu 24.04

Contents

Issue

Cisco Secure Client on Ubuntu 24.04 successfully establishes a VPN connection but disconnects within seconds. The disconnection is consistently accompanied by termination reason code 7 and crashes involving libvpnapi.so, preventing stable VPN connectivity required for normal business access.

The connection sequence shows the client reaching "Connected" state but then immediately transitioning back to **Disconnected** state when checking the status. The VPN client displays "Termination reason code 7: The agent has been stopped" in the logs, along with tunnel state change entries and messages indicating DTLS/SSL connections being torn down with "close notify" alerts.

This command sequence demonstrates the issue:

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

Connection output shows successful establishment:

```
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
```

However, when checking the status immediately after connection:

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

The client shows disconnected state:

```
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>
```

Environment

- Operating System: Ubuntu 24.04
- Cisco Secure Client Version: 5.1.12.146
- Authentication Method: Client certificate authentication
- Virtual Interface: cscotun0 (or similar Cisco Secure Client virtual interface)
- Environment includes automation scripts for system management

Resolution

The issue was resolved by identifying and correcting an automation script that was incorrectly identifying the Cisco Secure Client virtual interface (cscotun0) as a new physical device and applying HTTP/transparent proxy configuration to it. These next steps outline the resolution process.

Step 1: Collect Diagnostic Information

Generate DART (Diagnostic and Reporting Tool) bundles from the affected endpoint to capture detailed VPN client logs and system information:

```
Generate DART bundle from Cisco Secure Client interface or command line
```

The DART bundles contain VPN agent log entries showing interface and profile configuration steps, including DNS settings for interface cscotun0, VPN adapter configuration, and routing table changes.

```
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.
```

Step 2: Analyze Automation Script Behavior

Investigate local automation scripts that manage network interfaces and proxy configurations. Look for scripts that automatically detect new network interfaces and apply configuration policies.

Step 3: Identify Proxy Assignment Issue

Determine if automation scripts are treating the Cisco Secure Client virtual interface as a new physical device and applying inappropriate proxy settings. The virtual interface (cscotun0 or similar) cannot have HTTP/transparent proxy configuration applied to it.

Step 4: Remove Proxy Configuration from Virtual Interface

Remove or correct the proxy assignment that was automatically applied to the Cisco Secure Client virtual interface by the automation script. This prevents the proxy from interfering with VPN traffic flow.

Step 5: Update Automation Script Logic

Modify the automation script to exclude Cisco Secure Client virtual interfaces (typically named cscotun0, cscotun1) from automatic proxy configuration policies. Add logic to identify and skip VPN virtual interfaces during automated network configuration processes.

Step 6: Verify VPN Connectivity

Test VPN connectivity after removing the proxy configuration to confirm stable connection:

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

Verify the connection remains stable by checking status after connection establishment:

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

Alternative Troubleshooting Steps

If the issue persists or occurs in similar environments, consider these additional troubleshooting approaches:

- Test the Cisco Secure Client on a fresh Linux endpoint without automation scripts
- Temporarily disable third-party services that can interfere with libvpnapi or the VPN agent
- Upgrade Cisco Secure Client to the latest available version
- Review system logs for conflicts with VPN virtual interface creation and configuration

Cause

The root cause was an in-house automation script that incorrectly identified the Cisco Secure Client virtual interface (cscotun0 or similar) as a new physical network device. The script automatically applied HTTP/transparent proxy configuration to this virtual interface, which interfered with VPN traffic flow and caused the connection to terminate with reason code 7.

When the VPN client establishes a connection, it creates a virtual network interface to handle encrypted traffic. The automation script detected this interface creation as a new network device joining the system and applied standard proxy policies intended for physical network interfaces. This proxy configuration disrupted the ability of the VPN tunnel to properly route encrypted traffic, leading to immediate disconnection after successful connection establishment.

The termination reason code 7 ("The agent has been stopped") and libvpnapi.so crashes were symptoms of the underlying proxy interference rather than direct VPN client software issues.

Related Content

- Cisco Technical Support & Downloads