

# Ubuntu 24.04上安全客戶端VPN斷開與終止原因代碼7

## 目錄

---

---

## 問題

Ubuntu 24.04上的Cisco安全客戶端成功建立VPN連線，但將在幾秒鐘內斷開連線。斷開連線時始終伴隨有終止原因代碼7和涉及libvpnapl.so的崩潰，從而阻止正常業務訪問所需的穩定VPN連線。

連線序列顯示客戶端到達「已連線」狀態，但在檢查狀態時立即轉換回Disconnected狀態。VPN客戶端顯示「終止原因代碼7:代理已停止」，同時還有隧道狀態更改條目和消息，這些消息指示使用「關閉通知」警報關閉的DTLS/SSL連線。

此命令序列可演示問題：

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

連線輸出顯示成功建立：

```
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
```

但是，在連線後立即檢查狀態時：

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

客戶端顯示斷開連線狀態：

```
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

- 作業系統：烏本圖24.04
- Cisco Secure Client版本：5.1.12.146
- 身份驗證方法：客戶端證書身份驗證
- 虛擬介面：cscotun0 (或類似的思科安全客戶端虛擬介面)
- 環境包括用於系統管理的自動化指令碼

# 解析

通過識別並更正自動指令碼(該指令碼錯誤地將Cisco Secure Client虛擬介面(cscotun0)標識為新的物理裝置並應用HTTP/透明代理配置)解決了此問題。接下來的步驟將概述解析過程。

## 步驟 1:收集診斷資訊

從受影響的終端生成DART ( 診斷和報告工具 ) 捆綁包，以捕獲詳細的VPN客戶端日誌和系統資訊：

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

DART捆綁包包含VPN代理日誌條目，其中顯示介面和配置檔案配置步驟，包括介面配置0、VPN介面卡配置和路由表更改的DNS設定。

```
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.
```

## 步驟 2:分析自動化指令碼行為

調查管理網路介面和代理配置的本地自動化指令碼。查詢自動檢測新網路介面並應用配置策略的指令碼。

## 步驟 3:確定代理分配問題

確定自動化指令碼是否將Cisco Secure Client虛擬介面視為新的物理裝置並應用不適當的代理設定。虛擬介面 ( cscotun0或類似介面 ) 不能應用HTTP/透明代理配置。

#### 步驟 4:從虛擬介面刪除代理配置

刪除或更正由自動化指令碼自動應用於Cisco Secure Client虛擬介面的代理分配。這可防止Proxy干擾VPN流量。

#### 步驟 5:更新自動化指令碼邏輯

修改自動化指令碼以從自動代理配置策略中排除Cisco安全客戶端虛擬介面 ( 通常名稱為cscotun0、cscotun1 ) 。新增邏輯以在自動網路配置過程中識別和跳過VPN虛擬介面。

#### 步驟 6:驗證VPN連線

刪除代理配置後測試VPN連線以確認穩定連線：

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

建立連線後，通過檢查狀態來驗證連線是否保持穩定：

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

#### 其他故障排除步驟

如果問題仍然存在，或發生在類似環境中，請考慮以下其他故障排除方法：

- 在沒有自動化指令碼的全新Linux終端上測試Cisco Secure Client

- 暫時禁用可能干擾libvpnapi或VPN代理的第三方服務
- 將Cisco Secure Client升級到最新可用版本
- 檢視與VPN虛擬介面建立和配置衝突的系統日誌

## 原因

根本原因是內部自動化指令碼錯誤地將Cisco Secure Client虛擬介面（cscotun0或類似）標識為新的物理網路裝置。指令碼自動將HTTP/透明代理配置應用到此虛擬介面，這干擾了VPN流量並導致連線終止，原因代碼為7。

當VPN客戶端建立連線時，它會建立一個虛擬網路介面來處理加密流量。自動化指令碼檢測到該介面建立為加入系統的新網路裝置並應用了用於物理網路介面的標準代理策略。此代理配置破壞了VPN隧道正確路由加密流量的能力，導致在成功建立連線後立即斷開。

終止原因代碼7（「代理已停止」）和libvpnapi.so崩潰是基礎代理干擾的症狀，而不是直接VPN客戶端軟體問題。

## 相關內容

- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。