

在安全客户端中禁用VPN模块

目录

[简介](#)

[安全客户端中VPN模块的要求](#)

[禁用VPN功能的方法](#)

[在安装期间禁用VPN模块](#)

[Windows 窗口版本](#)

[macOS](#)

[安装后禁用VPN模块](#)

[确认](#)

简介

本文档介绍如何在确保DNS流量拦截继续正常工作的同时禁用安全客户端中的VPN模块。

安全客户端中VPN模块的要求

VPN模块是安全客户端的必需组件，即使AnyConnect不用于VPN访问。Umbrella依靠共享安全客户端驱动程序来拦截和管理DNS流量。虽然必须安装VPN模块，但您可以完全禁用VPN功能。

禁用VPN功能的方法

可以通过禁用安全客户端禁用VPN功能：

- 在安装期间使用安装参数(Windows)或修改安装包(OSX)。
- 安装后，将配置配置文件部署到终端（可通过编程方式部署）。

在安装期间禁用VPN模块

Windows 窗口版本

1. 在安装期间，使PRE_DEPLOY_DISABLE_VPN=1用MSI参数禁用VPN功能。
2. 有关详细信息，请参阅[自定义Cisco安全客户端的Windows安装](#)。

macOS

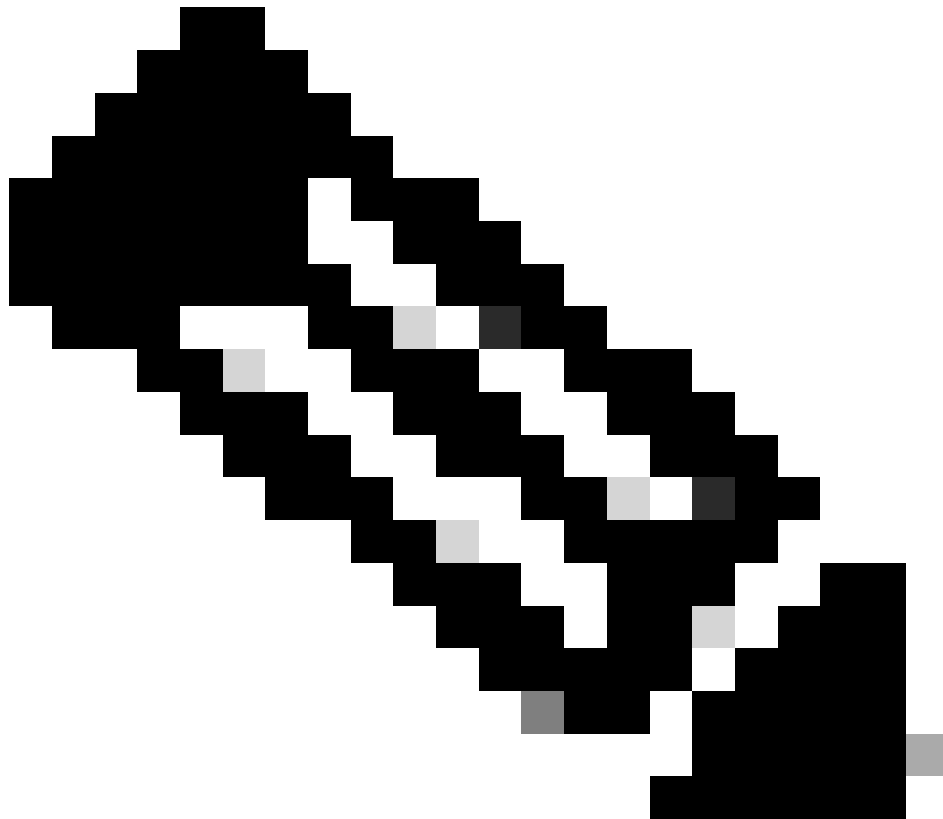
1. 使用控制VPN功能启用的文件自ACTransforms.xml定义安装包(.DMG)。
2. 有关详细信息，请参阅[自定义Cisco安全客户端的MacOS安装](#)。

安装后禁用VPN模块

1. 导航到终端上的配置文件目录：

- Windows 窗口版本:

C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile\



注意：默认情况下，ProgramData文件夹在Windows中处于隐藏状态。如果需要，直接在Windows资源管理器中键入路径。

- macOS:

/opt/cisco/secureclient/vpn/profile/

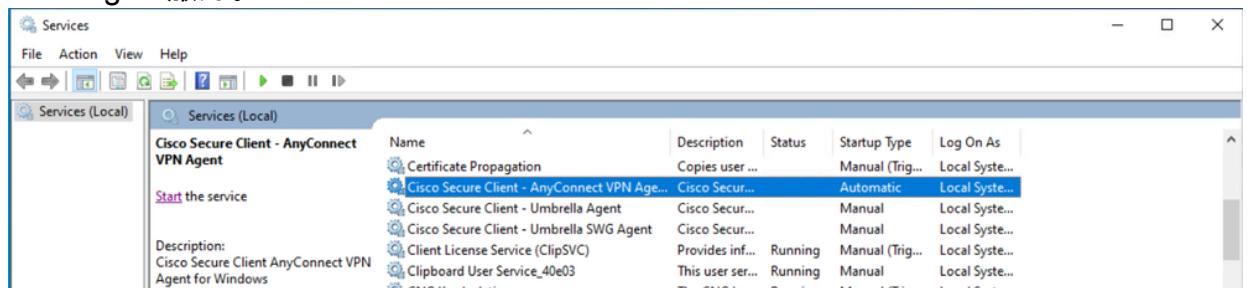
2. 创建新的空白文本文档。

3. 将提供的XML内容复制到文档中，并将其保存为 VPNDisable_ServiceProfile.xml“配置文件”文件夹中的：

true

4. 在配置文件文VPNDisable_ServiceProfile.xml 文件夹中保存文件后，重新启动计算机。

- 在Windows上，您也可以使用Windows服务重新启动Cisco Secure Client - AnyConnect VPN Agent服务。



18212956792980

确认

重新启动后，启动Secure Client图形用户界面(GUI)以验证VPN模块是否已禁用。



18212229472020

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。