AnyConnect安全移動連線錯誤："VPN客戶端無法設定IP過濾"

目錄

簡介

本文檔介紹在輸入此Cisco AnyConnect安全移動客戶端VPN使用者消息時應執行的操作：

```
The VPN client was unable to setup IP filtering.
A VPN connection will not be established.
```

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊僅基於Windows Vista和Windows 7作業系統。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

基本篩選引擎(BFE)服務

BFE是一項服務，用於管理防火牆和網際網路協定安全(IPsec)策略並實施使用者模式過濾。如果停止或禁用BFE服務，系統的安全性會顯著降低。它還會導致IPsec管理和防火牆應用中出現不可預測的行為。

這些系統元件取決於BFE服務：

- 網際網路金鑰交換(IKE)和驗證網際網路通訊協定(AuthIP)IPsec金鑰模組
- 網際網路連線共用(ICS)
- IPsec原則代理
- 路由和遠端訪問
- Windows防火牆

AnyConnect安全移動客戶端對主機進行路由和遠端訪問更改。IKEv2還依賴於IKE模組。這意味著，如果BFE服務停止，AnyConnect安全移動客戶端將無法安裝或用於建立安全套接字層(SSL)連線。

活動循環中存在一些威脅，它們會禁用和刪除BFE服務，以此作為感染過程中的第一步。

Win32/Sirefef(ZeroAccess)特洛伊木馬程式

Win32/Sirefef(ZeroAccess)特洛伊木馬程式是一個多元件惡意軟體系列，它使用隱藏功能來隱藏其在電腦中的存在。此威脅使攻擊者能夠完全訪問您的系統。由於其性質，負載可能因感染不同而有很大差異，但常見行為包括：

- 下載和執行任意檔案。
- 遠端主機的聯絡。
- 禁用安全功能。

沒有與此威脅相關的常見症狀。來自已安裝防病毒軟體的警報通知可能是唯一的症狀。

Win32/Sirefef(ZeroAccess)特洛伊木馬程式嘗試停止和刪除以下與安全相關的服務：

- Windows Defender服務(windefense)
- IP協助程式服務(iphlpsvc)
- Windows安全中心服務(wscsvc)
- Windows防火牆服務(mpsvc)
- 基本篩選引擎服務(bfe)

> **注意**：Win32/Sirefef(ZeroAccess)特洛伊木馬是一種使用高級隱藏技術來阻止其檢測和刪除的危險威脅。由於感染此威脅，您可能需要修復並重新配置某些Windows安全功能。

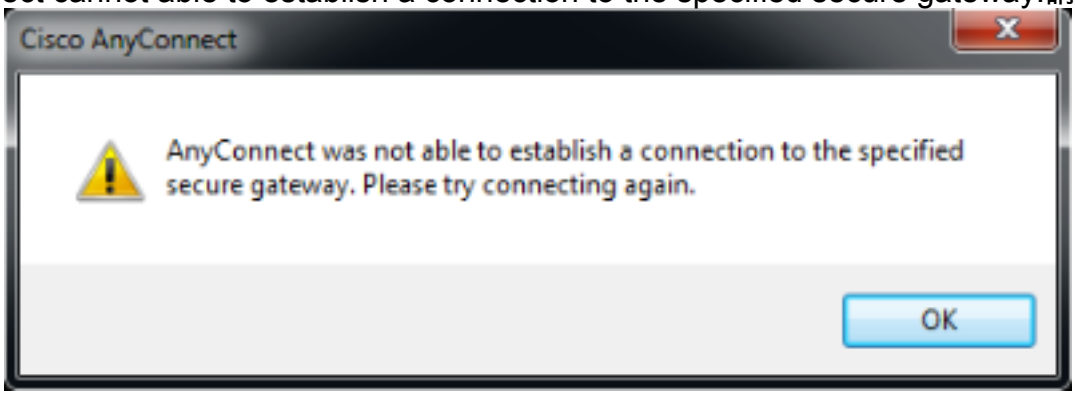
問題

方案如下：

- 使用者無法安裝AnyConnect安全移動客戶端，並收到錯誤消息「VPN客戶端無法設定IP過濾。

將不會建立VPN連線。」

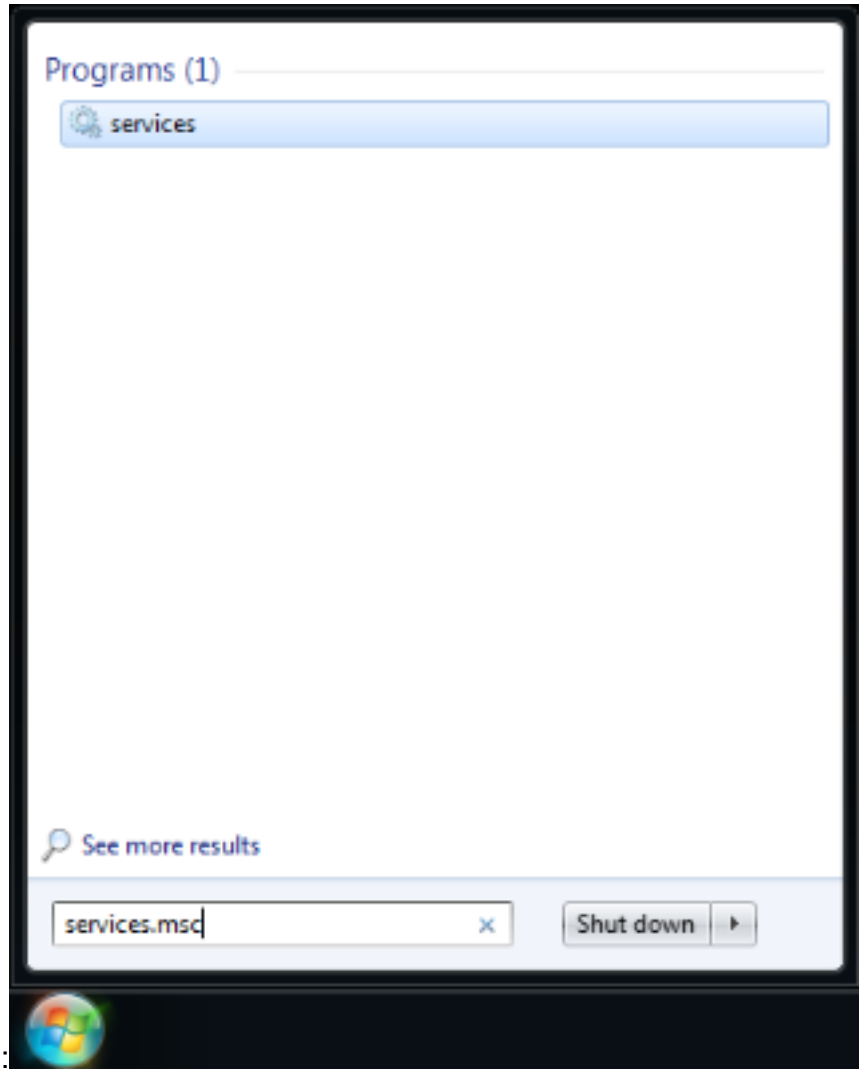
- AnyConnect安全移動客戶端最初工作正常。但是；終端使用者無法再建立連線並收到錯誤消息「Anyconnect cannot able to establish a connection to the specified secure gateway.請再次嘗試連線。」



解決方案

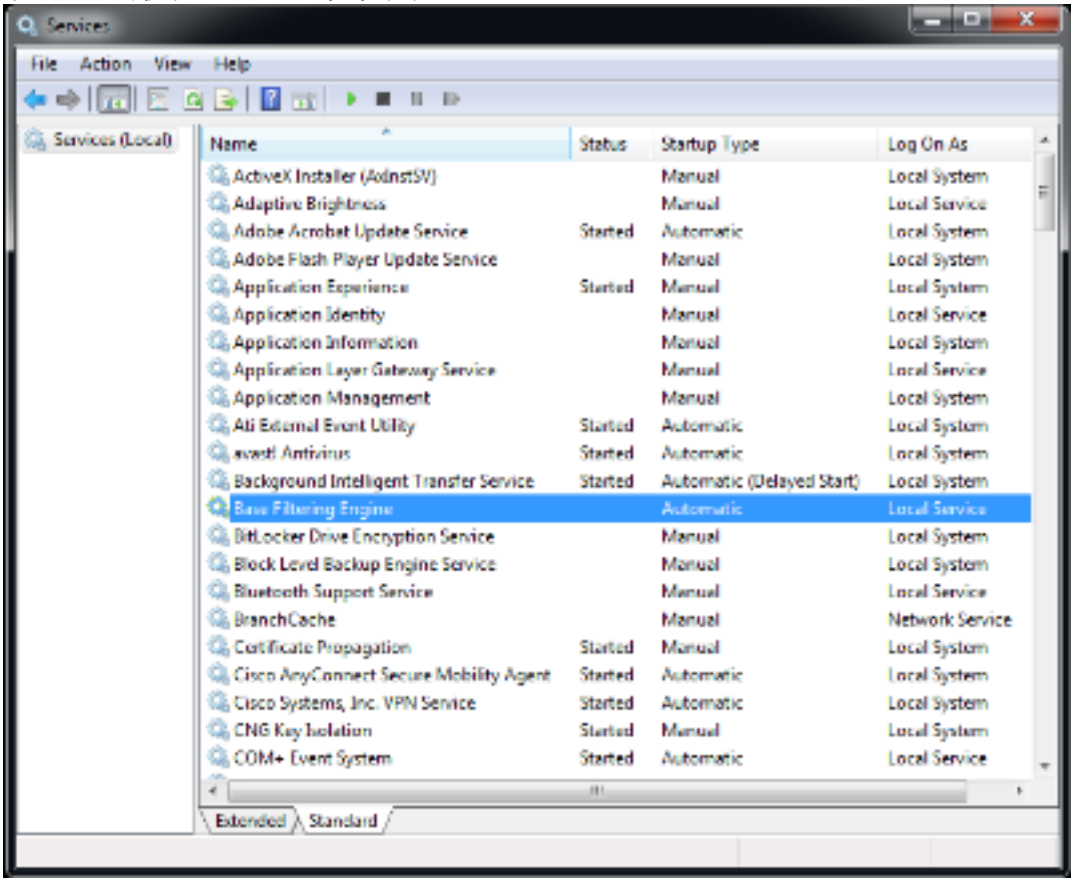
看到這些錯誤消息時，必須確認BFE是否實際被禁用/丟失，或者客戶端是否能夠識別它。若要疑難排解，請完成以下步驟：

1. 從Windows選單訪問服務控制管理器



(SCM):

2. 搜尋BFE服務以確認其存在與否。



如果服務運行，則狀態顯示為**Started**。如果該列中有任何其他內容，則說明該服務有問題。但是

，如果狀態顯示為「已啟動」，則客戶端顯然無法與服務通訊，並且可能存在錯誤。

如果服務已禁用或未啟動，可能的原因包括：

- 如前所述，惡意軟體會首先禁用此服務。
- 電腦上的登錄檔損壞。

修復程式

第一步是使用防病毒軟體掃描您的系統並進行消毒。如果BFE服務將被Win32/Sirefef(ZeroAccess)特洛伊木馬程式再次刪除，則不應恢復該服務。從此網頁下載ESET SirefefCleaner工具，並將其儲存到您的案頭。

以下影片介紹移除Win32/Sirefef(ZeroAccess)特洛伊木馬程式的步驟：

如何刪除Win32/Sirefef(ZeroAccess)特洛伊木馬程式？

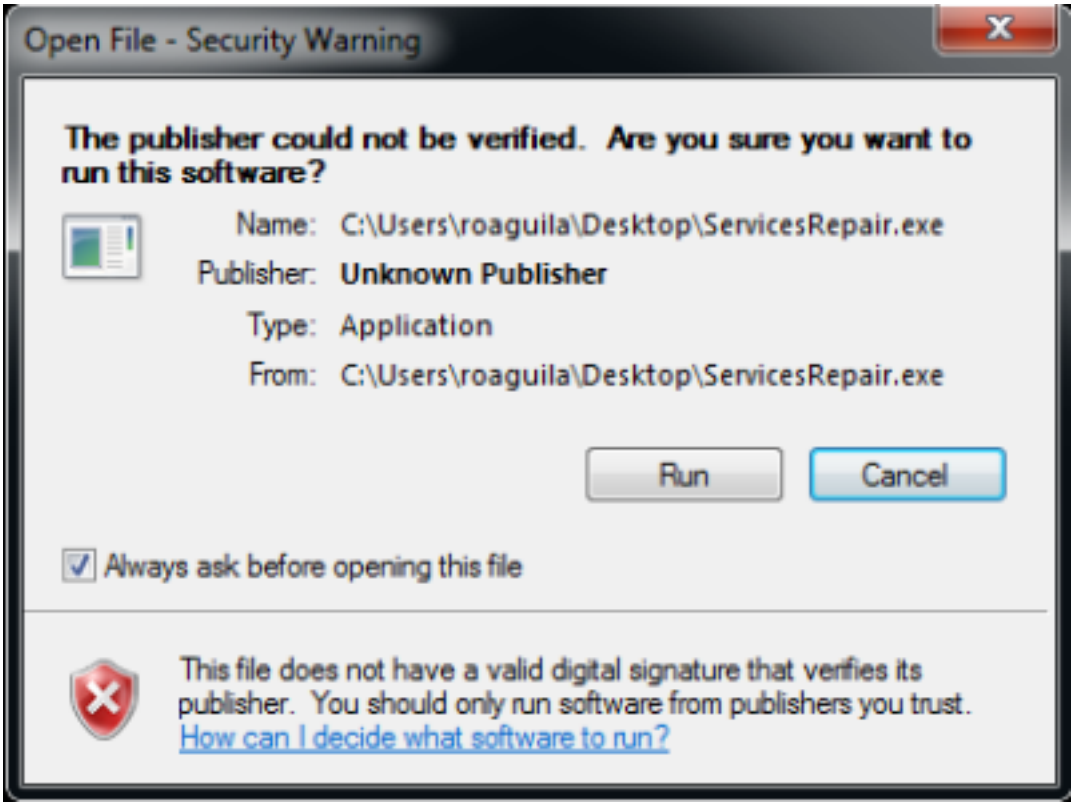
刪除Win32/Sirefef(ZeroAccess)特洛伊木馬程式後，驗證BFE服務是否可以正常啟動並保持活動狀態。為此：

1. 啟動SCM並選擇**Extended(擴展)選項**卡，而不是**Standard（標準）**。
2. 選擇BFE服務。
3. 選擇左側的**Start**選項。

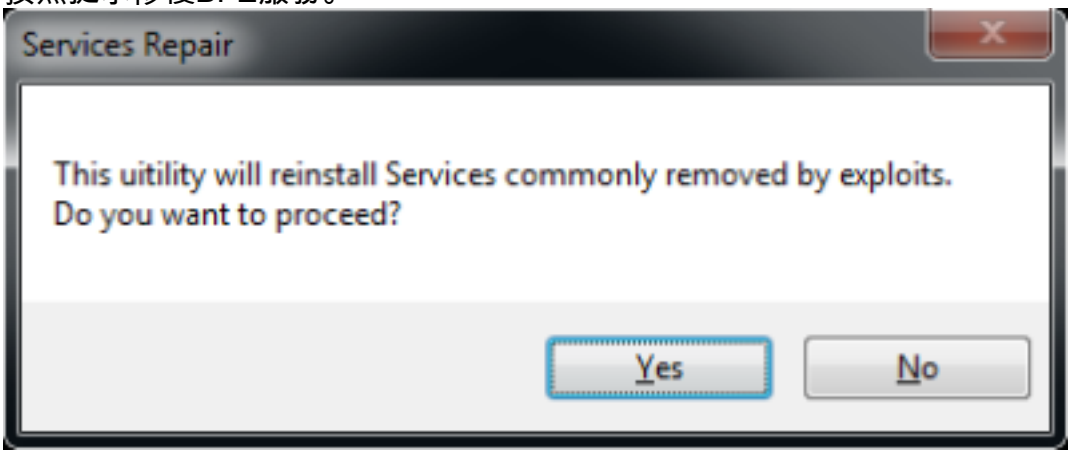
   注意：在嘗試此程式之前，最好先備份您的檔案。本文中的所有資訊均按原樣提供，對其準確性、完整性或適用於特定用途不作任何明示或暗示的擔保。

如果此過程不起作用，請完成以下步驟：

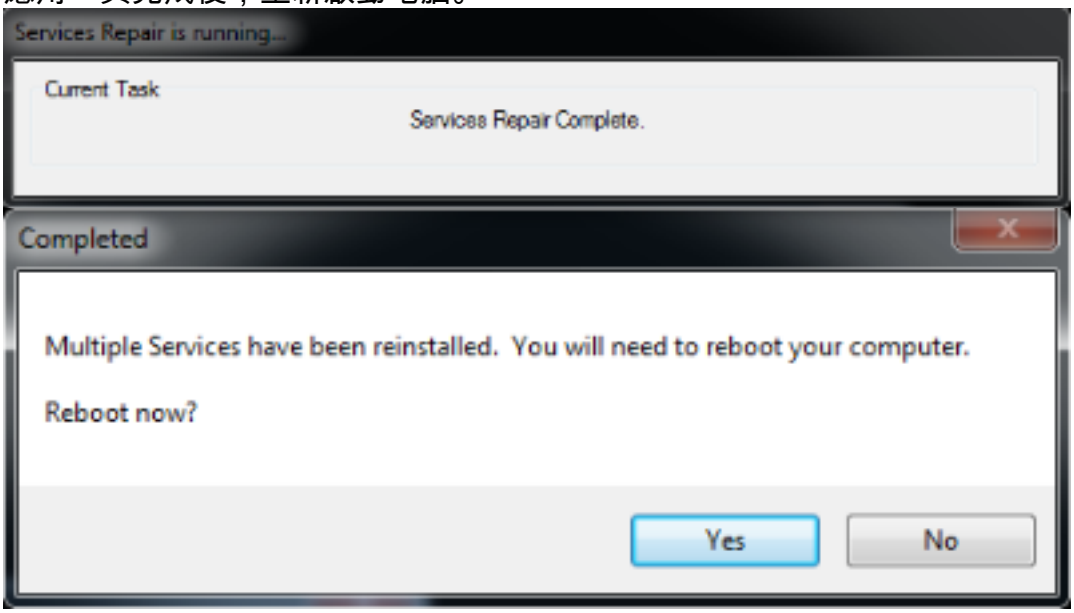
1. 從該網頁下載ESET ServicesRepair實用程序，並將其儲存到您的案頭。
2. 執行ESET ServicesRepair實用程式。



3. 按照提示修復BFE服務。



4. 應用工具完成後，重新啟動電腦。



5. 電腦重新啟動後，請再次安裝或執行AnyConnect安全移動客戶端。

附註：測試表明該工具在多數登錄檔檔案損壞或服務損壞的情況下都能發揮作用。因此，如果

您遇到這些錯誤訊息，此工具也證明是有用的：
- VPN客戶端代理無法建立進程間通訊倉庫。
- VPN代理服務沒有響應。請在一分鐘後重新啟動此應用程式。
— 本地電腦上的Cisco Anyconnect安全移動代理服務已啟動和停止。如果某些服務未被其他服務或程式使用，則這些服務會自動停止。