AnyConnect Secure Mobility Connection Error: "The VPN client was unable to setup IP filtering"

Document ID: 116347

Contributed by Carlos Alberto Chaves Morales, Juan Gabriel Zuniga Segura, and Atri Basu, Cisco TAC Engineers.

Jul 29, 2013

Contents

Introduction

This document describes what to do when you enounter this Cisco AnyConnect Secure Mobility Client VPN User Message:

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

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Windows Vista and Windows 7 operating systems only.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The Base Filtering Engine (BFE) Service

BFE is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user−mode filtering. The security of the system is significantly reduced if you stop or disable the BFE service.

It also results in unpredictable behavior in IPsec management and firewall applications.

These system components depend on the BFE service:

- Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) IPsec Keying Modules
- Internet Connection Sharing (ICS)
- IPsec Policy Agent
- Routing and Remote Access
- Windows Firewall

The AnyConnect Secure Mobility Client makes both routing and remote access changes to the host machine. The IKEv2 is also dependent on the IKE modules. This means that, if the BFE service is stopped, The AnyConnect Secure Mobility Client cannot be installed or used to establish a Secure Sockets Layer (SSL) connection.

There are threats in active circulation that disable and remove the BFE service as a first step in the infection process.

Win32/Sirefef (ZeroAccess) Trojan

Win32/Sirefef (ZeroAccess) trojan is a multi−component family of malware that uses stealth to hide its presence on your computer. This threat gives attackers full access to your system. Due to its nature, the payload might vary greatly from one infection to another, although common behavior includes:

- Download and execution of arbitrary files.
- Contact of remote hosts.
- Disablement of security features.

There are no common symptoms associated with this threat. Alert notifications from installed antivirus software might be the only symptoms.

Win32/Sirefef (ZeroAccess) trojan attempts to stop and delete these security−related services:

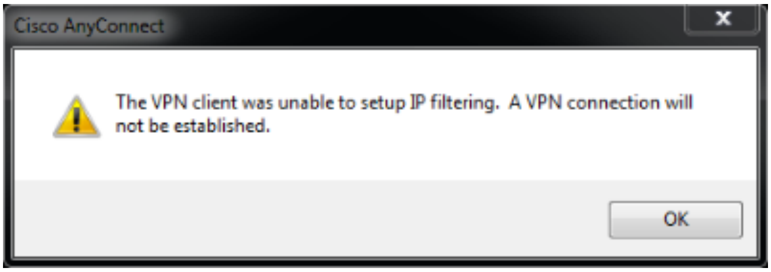
- Windows Defender Service (windefend)
- IP Helper Service (iphlpsvc)
- Windows Security Center Service (wscsvc)
- Windows Firewall Service (mpssvc)
- Base Filtering Engine Service (bfe)

Caution: Win32/Sirefef (ZeroAccess) trojan is a dangerous threat that uses advanced stealth techniques in order to hinder its detection and removal. As a consequence infection with this threat, you may need to repair and reconfigure some Windows security features.

Problem

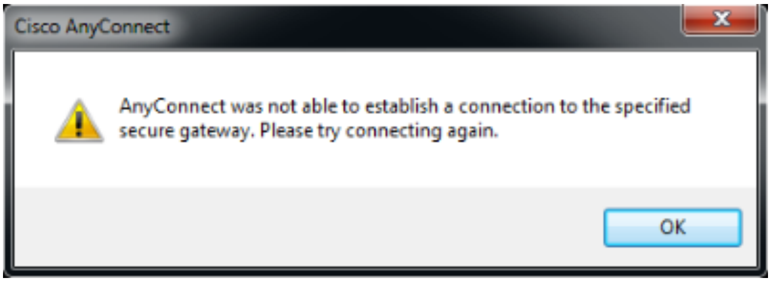
The scenarios are:

- The user cannot install the AnyConnnect Secure Mobility Client and receives the error message, "The VPN client was unable to setup IP filtering. A VPN connection will not be established."



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

- The AnyConnect Secure Mobility Client worked fine initially. However; the end user can no longer establish a connection and receives the error message, "Anyconnect was not able to establish a connectoin to the specified secure gateway. Please try connecting again."

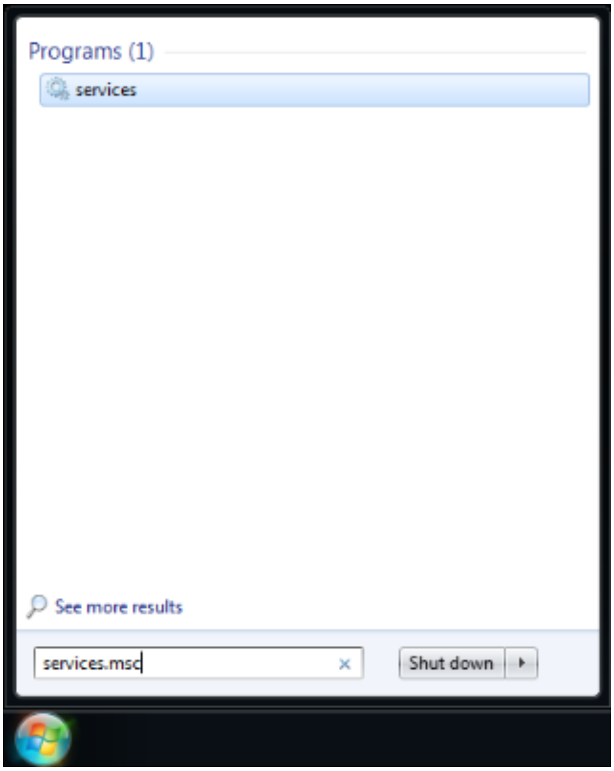


AnyConnect was not able to establish a connection to the specified secure gateway. Please try connecting again.

Solution

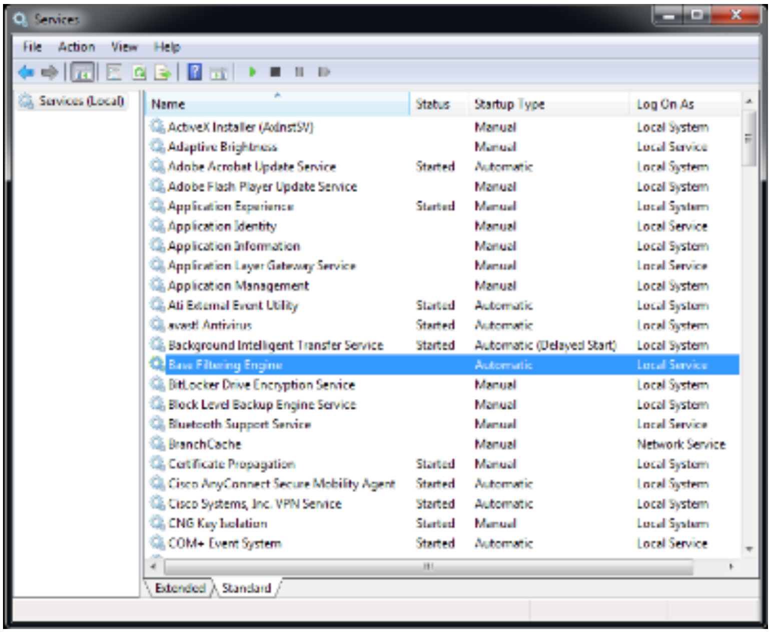
When these error messages are seen, it is important to confirm whether the BFE is actually disabled/missing or if the client is not able to recognize it. In order to troublehoot, complete these steps:

1. Access the Service Control Manager (SCM) from the Windows menu:



services.msc

2. Search for the BFE service in order to confirm its presence or absence.



Name	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)		Manual	Local System
Adaptive Brightness		Manual	Local Service
Adobe Acrobat Update Service	Started	Automatic	Local System
Adobe Flash Player Update Service		Manual	Local System
Application Experience	Started	Manual	Local System
Application Identity		Manual	Local Service
Application Information		Manual	Local System
Application Layer Gateway Service		Manual	Local Service
Application Management		Manual	Local System
Ati External Event Utility	Started	Automatic	Local System
avast! Antivirus	Started	Automatic	Local System
Background Intelligent Transfer Service	Started	Automatic (Delayed Start)	Local System
Base Filtering Engine		Automatic	Local Service
BitLocker Drive Encryption Service		Manual	Local System
Block Level Backup Engine Service		Manual	Local System
Bluetooth Support Service		Manual	Local Service
BranchCache		Manual	Network Service
Certificate Propagation	Started	Manual	Local System
Cisco AnyConnect Secure Mobility Agent	Started	Automatic	Local System
Cisco Systems, Inc. VPN Service	Started	Automatic	Local System
CNG Key Isolation	Started	Manual	Local System
COM+ Event System	Started	Automatic	Local Service

If the service works, the status displays as ***Started***. If there is anything else in that column, there is a problem with the service. However, if the status displays as started, the client is clearly not able to communicate with the service, and it is possible there is a bug.

If the service is disabled or not started, some possible reasons are:

- Malware, as previously explained, disables this service as a first step.
- Registry corruption on the machine.

Repair Procedure

The first step is to scan and disinfect your system with an antivirus software. You should not restore the BFE service if it will be deleted again by Win32/Sirefef (ZeroAccess) trojan. Download the ESET SirefefCleaner tool from this web page, and save it to your desktop.

This video explains the procedure to remove the Win32/Sirefef (ZeroAccess) trojan:.

How do I remove Win32/Sirefef (ZeroAccess) trojan?

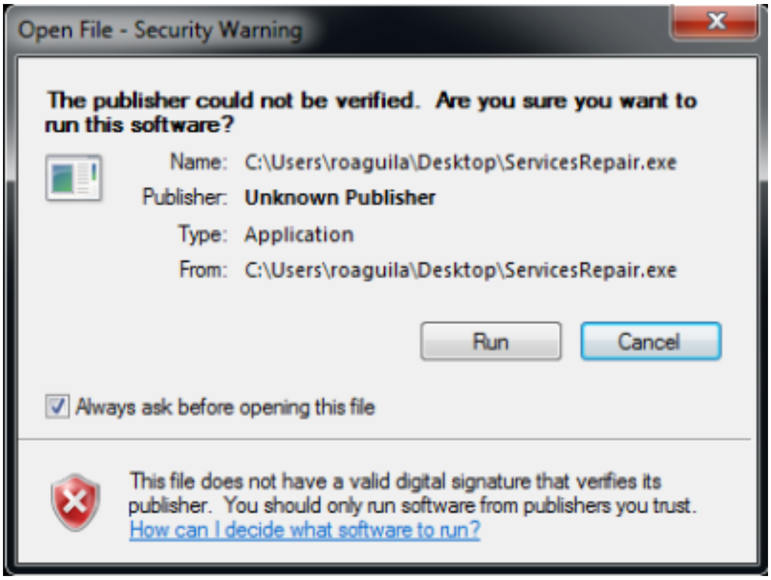
Once you have removed Win32/Sirefef (ZeroAccess) trojan, verify that the BFE service can be started and kept active by normal means. In order to do this:

1. Start SCM and choose the ***Extended*** tab instead of the ***Standard***.
2. Choose the BFE service.
3. Choose the ***Start*** option on the left.

Caution: It is a good practice to back up your files before you attempt this procedure. All information in this article is provided as is, without any warranty, whether express or implied, of its accuracy, completeness, or fitness for a particular purpose.

If this procedure does not work, complete these steps:

1. Download the ESET ServicesRepair utility from this web page, and save it to your desktop.
2. Execute the ESET ServicesRepair utility.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\roaguila\Desktop\ServicesRepair.exe

Publisher: **Unknown Publisher**

Type: Application

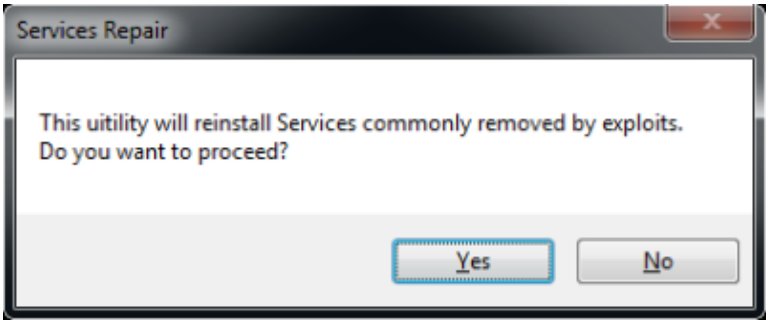
From: C:\Users\roaguila\Desktop\ServicesRepair.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verfies its publisher. You should only run software from publishers you trust.

How can I decide what software to run?

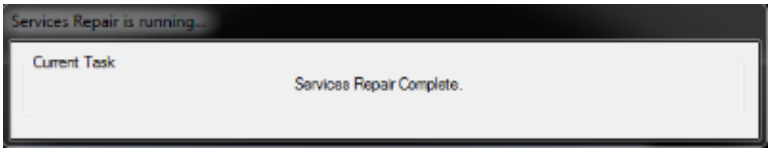
3. Follow the prompts in order to repair the BFE service.



Services Repair

This uitility will reinstall Services commonly removed by exploits.
Do you want to proceed?

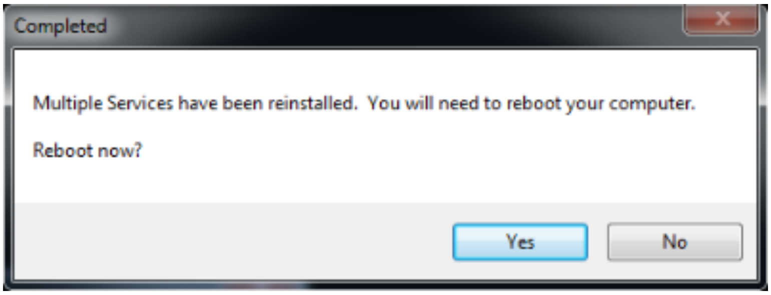
4. Once the utility finishes, restart your computer.



Services Repair is running...

Current Task

Services Repair Complete.



Completed

Multiple Services have been reinstalled. You will need to reboot your computer.

Reboot now?

5. Once your computer restarts, install or execute The AnyConnect Secure Mobility Client again.

Note: Tests have shown that this tool helps in most cases where the registry files are corrupt or services are damaged. Therefore, if you encounter these error messages, this tool proves useful too:
− The VPN client agent was unable to create the interprocess communication depot.
− The VPN agent service is not responding. Please restart this application after a minute.
− The Cisco Anyconnect Secure Mobility Agent service on Local Computer started and stopped. Some services stop automatically if they are not in use by other services or programs.

Updated: Jul 29, 2013 Document ID: 116347