AnyConnect Secure Mobility Connection-Fehler: "Der VPN-Client konnte keine IP-Filterung einrichten."

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie vorgehen müssen, wenn Sie diese Cisco AnyConnect Secure Mobility Client VPN-Benutzermeldung verwenden:

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

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren nur auf Windows Vista- und Windows 7-Betriebssystemen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der Dienst Base Filtering Engine (BFE)

BFE ist ein Dienst, der Firewall- und IPsec-Sicherheitsrichtlinien verwaltet und die Benutzermodusfilterung implementiert. Die Sicherheit des Systems wird erheblich reduziert, wenn Sie den BFE-Dienst beenden oder deaktivieren. Dies führt auch zu unvorhersehbarem Verhalten bei IPsec-Verwaltungs- und Firewall-Anwendungen.

Diese Systemkomponenten hängen vom BFE-Service ab:

- Internet Key Exchange (IKE) und Authentifizierte Internet Protocol (AuthIP) IPsec-Schlüsselmodule
- Internet Connection Sharing (ICS)
- IPsec Policy Agent
- Routing und Remote-Zugriff
- Windows-Firewall

Der AnyConnect Secure Mobility Client ändert sowohl das Routing als auch den Remote-Zugriff auf den Host-Computer. IKEv2 ist ebenfalls von den IKE-Modulen abhängig. Das bedeutet, dass der AnyConnect Secure Mobility Client nicht installiert oder zum Herstellen einer SSL-Verbindung (Secure Sockets Layer) verwendet werden kann, wenn der BFE-Dienst beendet wird.

Im aktiven Umlauf befinden sich Bedrohungen, die den BFE-Dienst als ersten Schritt im Infektionsprozess deaktivieren und entfernen.

Win32/Sirefef (ZeroAccess)-Trojaner

Der Win32/Sirefef-Trojaner (ZeroAccess) ist eine aus mehreren Komponenten bestehende Familie von Malware, die sich versteckt auf Ihrem Computer befindet. Diese Bedrohung bietet Angreifern vollständigen Zugriff auf Ihr System. Aufgrund ihrer Art kann die Payload von einer Infektion zur anderen stark variieren, obwohl das häufige Verhalten Folgendes umfasst:

- Herunterladen und Ausführen beliebiger Dateien.
- Kontakt der Remote-Hosts.
- Deaktivieren von Sicherheitsfunktionen.

Es gibt keine häufigen Symptome, die mit dieser Bedrohung verbunden sind. Warnmeldungen von installierter Virenschutzsoftware können die einzigen Symptome sein.

Der Win32/Sirefef (ZeroAccess)-Trojaner versucht, diese sicherheitsrelevanten Services zu stoppen und zu löschen:

- Windows Defender-Dienst (winDefence)
- IP Helper Service (iphlpsvc)
- Windows Security Center Service (wscsvc)

- Windows-Firewall-Service (mpssvc)
- Base Filtering Engine Service (bfe)

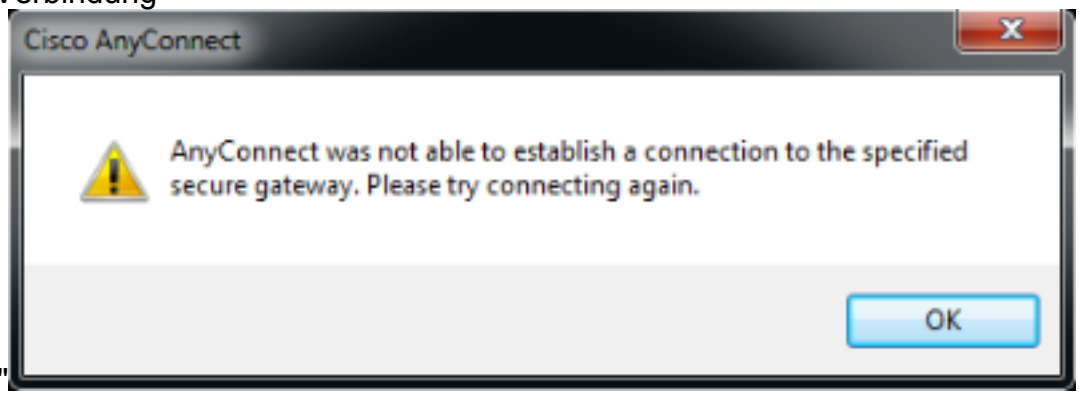
Vorsicht: Der Win32/Sirefef-Trojaner (ZeroAccess) ist eine gefährliche Bedrohung, die fortschrittliche Tarntechniken einsetzt, um seine Erkennung und Entfernung zu verhindern. Als Folge einer Infektion mit dieser Bedrohung müssen Sie möglicherweise einige Windows-Sicherheitsfunktionen reparieren und neu konfigurieren.

Problem

Folgende Szenarien sind möglich:

- Der Benutzer kann den AnyConnect Secure Mobility Client nicht installieren und erhält die Fehlermeldung "Der VPN-Client konnte keine IP-Filterung einrichten. Es wird keine VPN-Verbindung hergestellt."

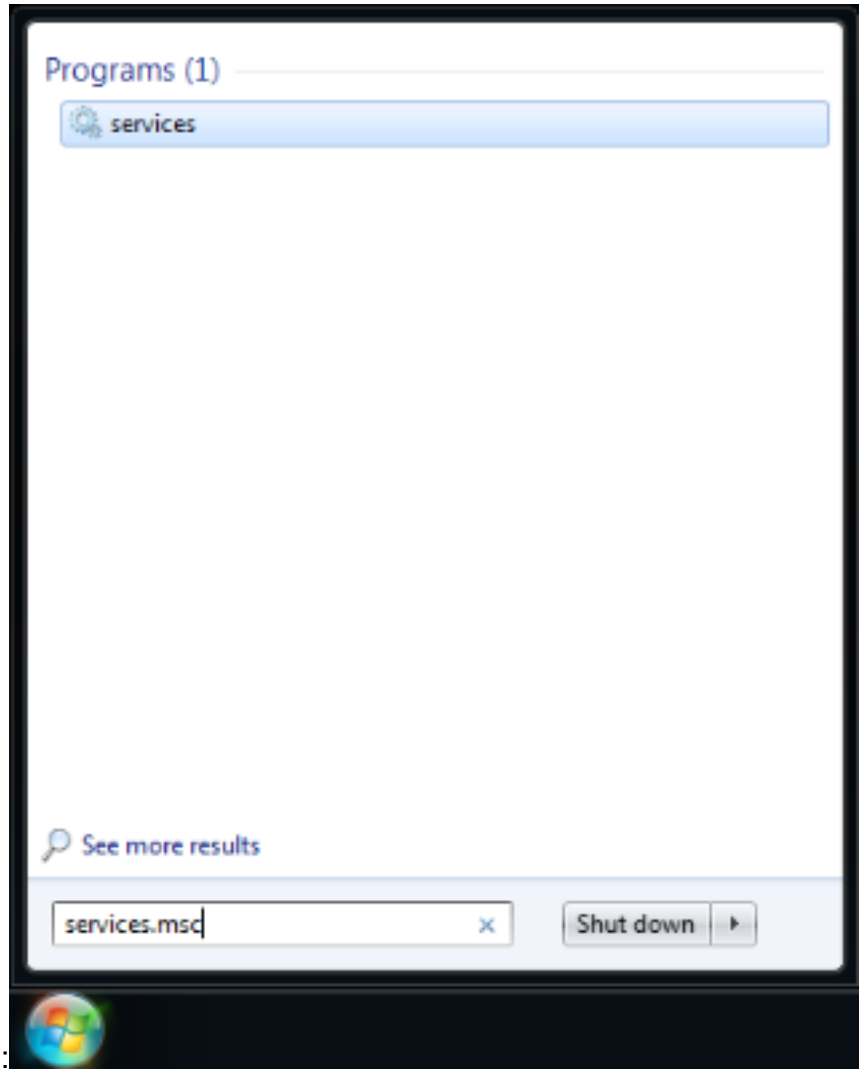
- Der AnyConnect Secure Mobility Client hat anfangs gut funktioniert. Jedoch Der Endbenutzer kann keine Verbindung mehr herstellen und erhält die Fehlermeldung "AnyConnect konnte keine Verbindung zum angegebenen sicheren Gateway herstellen. Versuchen Sie bitte erneut, eine Verbindung herzustellen."

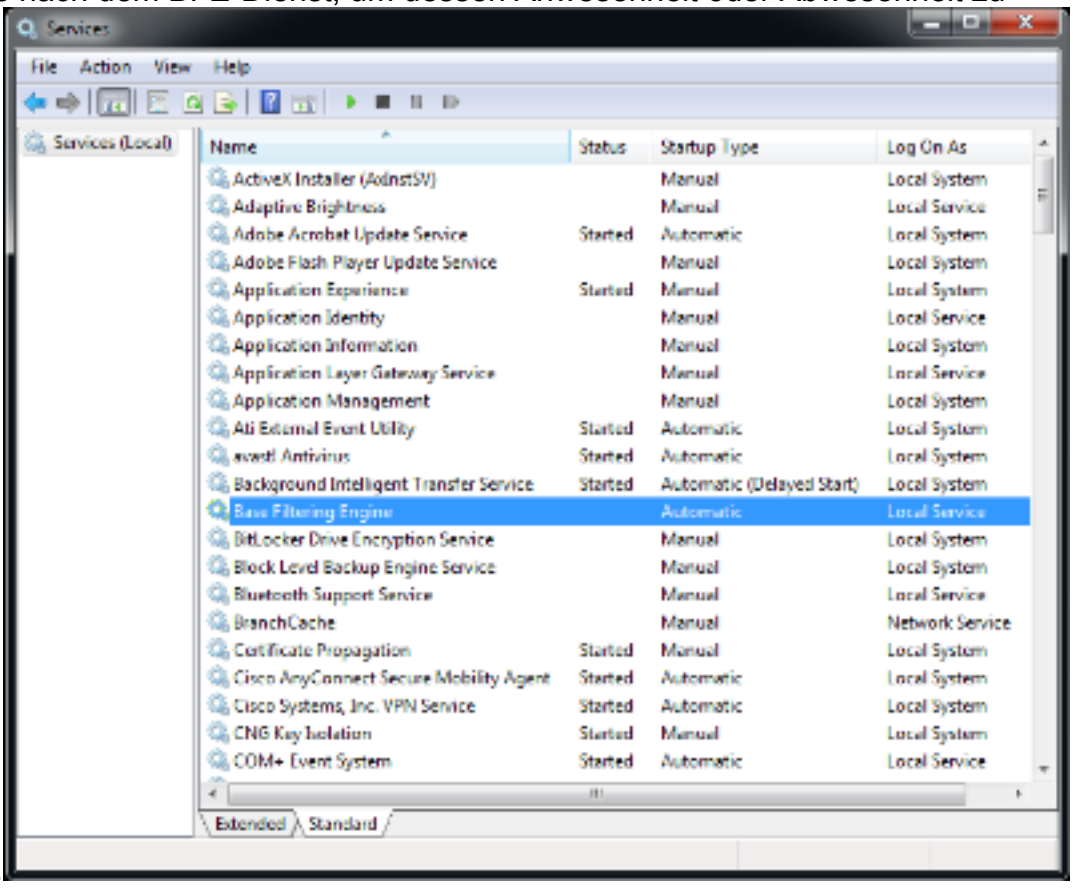


Lösung

Wenn diese Fehlermeldungen angezeigt werden, muss überprüft werden, ob die BFE tatsächlich deaktiviert/fehlt oder der Client sie nicht erkennen kann. Gehen Sie wie folgt vor, um eine Fehlerbehebung durchzuführen:

1. Öffnen Sie im Windows-Menü den Service Control Manager

(SCM): 

2. Suchen Sie nach dem BFE-Dienst, um dessen Anwesenheit oder Abwesenheit zu bestätigen. 

Wenn der Dienst funktioniert, wird der Status als **Gestartet** angezeigt. Wenn sich in dieser Spalte

noch etwas Anderes befindet, liegt ein Problem mit dem Dienst vor. Wenn der Status jedoch wie gestartet angezeigt wird, kann der Client mit dem Dienst nicht kommunizieren, und es ist möglich, dass ein Fehler vorliegt.

Wenn der Dienst deaktiviert ist oder nicht gestartet wird, können folgende Gründe vorliegen:

- Wie bereits erläutert, deaktiviert Malware diesen Dienst als ersten Schritt.
- Beschädigung der Registrierung auf dem Computer.

Reparaturverfahren

Der erste Schritt besteht darin, Ihr System mit einer Antivirus-Software zu scannen und zu desinfizieren. Sie sollten den BFE-Dienst nicht wiederherstellen, wenn er durch den Trojaner Win32/Sirefef (ZeroAccess) erneut gelöscht wird. Laden Sie das ESET SirefefCleaner-Tool von dieser Webseite herunter und speichern Sie es auf Ihrem Desktop.

In diesem Video wird das Verfahren zum Entfernen des Win32/Sirefef (ZeroAccess)-Trojaners beschrieben:.

Wie entferne ich den Win32/Sirefef-Trojaner (ZeroAccess)?

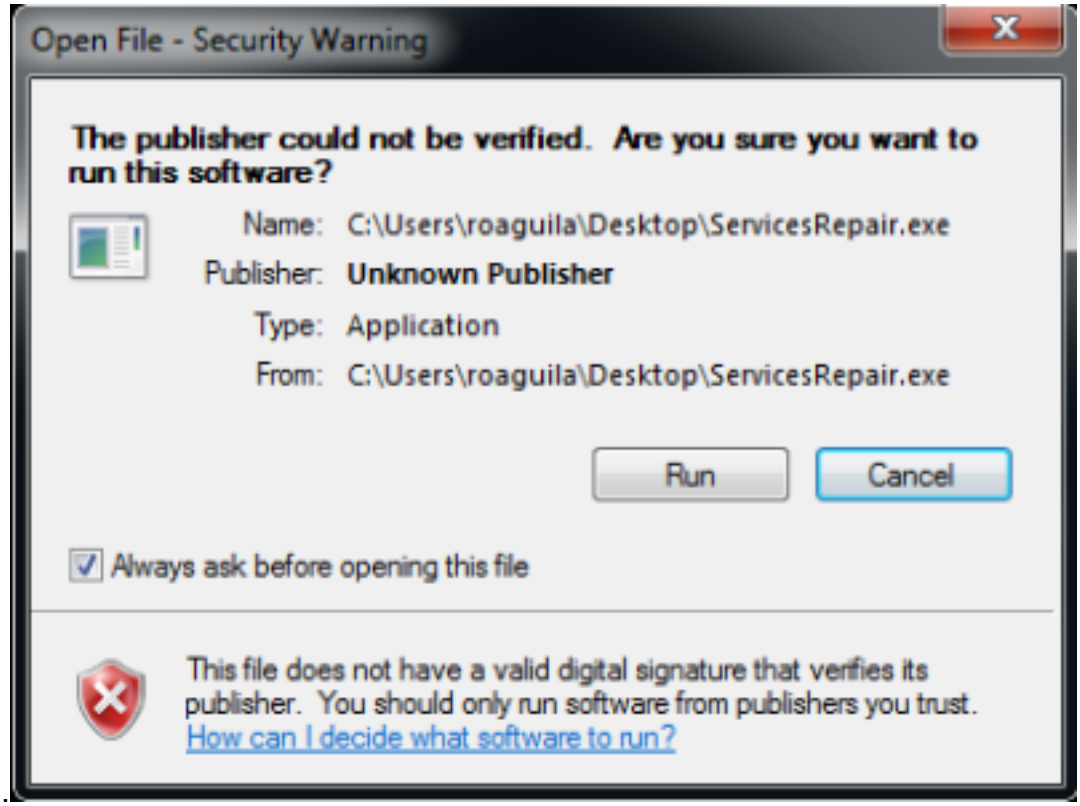
Nachdem Sie den Win32/Sirefef-Trojaner (ZeroAccess) entfernt haben, stellen Sie sicher, dass der BFE-Dienst gestartet und auf normale Weise aktiv bleiben kann. Gehen Sie wie folgt vor:

1. Starten Sie SCM, und wählen Sie die Registerkarte **Erweitert** statt **Standard**.
2. Wählen Sie den BFE-Service aus.
3. Wählen Sie links die **Start**-Option aus.

   Vorsicht: Es empfiehlt sich, Ihre Dateien zu sichern, bevor Sie dieses Verfahren durchführen. Alle Informationen in diesem Artikel werden ohne Mängelgewähr, sei es ausdrücklich oder stillschweigend, auf ihre Richtigkeit, Vollständigkeit oder Eignung für einen bestimmten Zweck bereitgestellt.

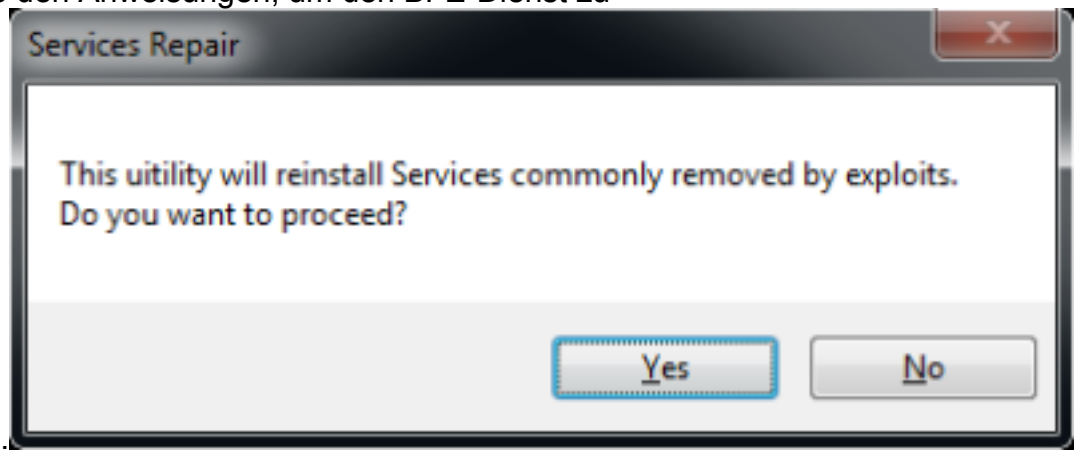
Wenn dieses Verfahren nicht funktioniert, gehen Sie wie folgt vor:

1. Laden Sie das ESET ServicesRepair-Dienstprogramm von dieser Webseite herunter, und speichern Sie es auf Ihrem Desktop.
2. Führen Sie das Dienstprogramm ESET ServicesRepair



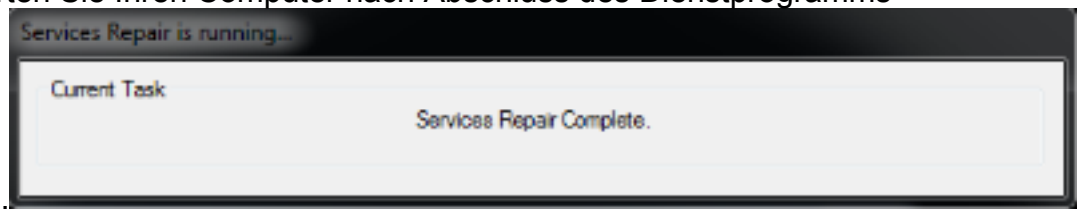
aus.

3. Folgen Sie den Anweisungen, um den BFE-Dienst zu

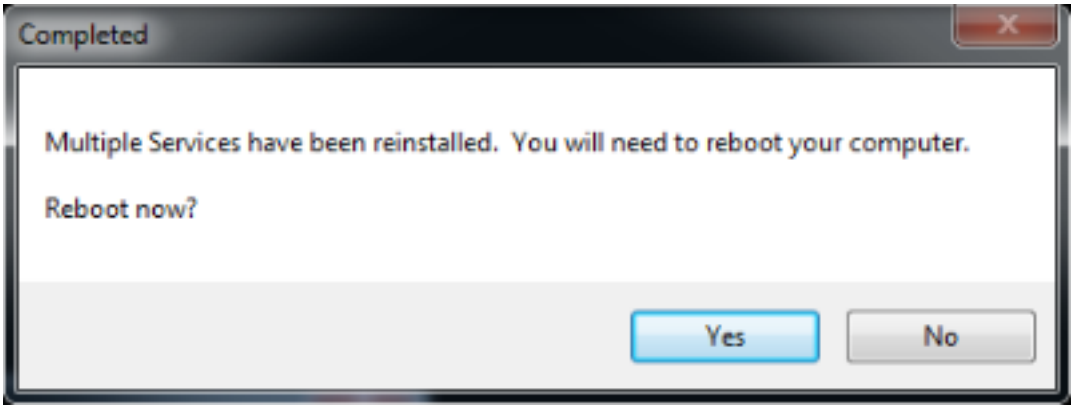


reparieren.

4. Starten Sie Ihren Computer nach Abschluss des Dienstprogramms



neu.



5. Sobald Ihr Computer neu startet, installieren oder führen Sie den AnyConnect Secure Mobility Client erneut aus.

Hinweis: Tests haben gezeigt, dass dieses Tool in den meisten Fällen hilft, wenn die Registrierungsdateien beschädigt sind oder Dienste beschädigt sind. Wenn Sie also auf diese Fehlermeldungen stoßen, erweist sich dieses Tool auch als nützlich:
- Der VPN-Client-Agent konnte das Interprocess Communication Depot nicht erstellen.
- Der VPN-Agent-Service reagiert nicht. Bitte starten Sie diese Anwendung nach einer Minute neu.
- Der Cisco AnyConnect Secure Mobility Agent-Dienst auf dem lokalen Computer wurde gestartet und beendet. Einige Dienste werden automatisch beendet, wenn sie nicht von anderen Diensten oder Programmen verwendet werden.