Errore di AnyConnect Secure Mobility: "Il client VPN non è riuscito a configurare il filtro IP"

Sommario

Introduzione

Questo documento descrive cosa fare quando viene visualizzato questo messaggio utente Cisco AnyConnect Secure Mobility Client VPN:

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

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano solo sui sistemi operativi Windows Vista e Windows 7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Servizio BFE (Base Filtering Engine)

BFE è un servizio che gestisce i criteri firewall e IPsec (Internet Protocol Security) e implementa il filtro in modalità utente. Se si arresta o si disabilita il servizio BFE, la sicurezza del sistema risulta notevolmente ridotta. e determina inoltre comportamenti imprevedibili nelle applicazioni di gestione IPSec e firewall.

Questi componenti di sistema dipendono dal servizio BFE:

- Moduli di impostazione chiavi IPSec IKE (Internet Key Exchange) e AuthIP (Authenticated Internet Protocol)
- Condivisione connessione Internet
- Agente criteri IPSec
- Routing e Accesso remoto
- Windows Firewall

AnyConnect Secure Mobility Client apporta al computer host modifiche sia al routing sia all'accesso remoto. IKEv2 dipende anche dai moduli IKE. Ciò significa che, se il servizio BFE viene arrestato, non è possibile installare o utilizzare AnyConnect Secure Mobility Client per stabilire una connessione SSL (Secure Sockets Layer).

Vi sono minacce in circolazione che disabilitano e rimuovono il servizio BFE come primo passo nel processo di infezione.

Trojan Win32/Sirefef (ZeroAccess)

Il trojan Win32/Sirefef (ZeroAccess) è una famiglia di malware a più componenti che utilizza lo stealth per nascondere la propria presenza nel computer. Questa minaccia fornisce agli aggressori accesso completo al sistema. A causa della sua natura, il payload può variare notevolmente da un'infezione all'altra, anche se il comportamento comune include:

- Scaricare ed eseguire file arbitrari.
- Contatto degli host remoti.
- Disabilitazione delle funzionalità di protezione.

Non ci sono sintomi comuni associati a questa minaccia. Gli unici sintomi potrebbero essere le notifiche di avviso del software antivirus installato.

Il trojan Win32/Sirefef (ZeroAccess) tenta di arrestare ed eliminare i seguenti servizi relativi alla sicurezza:

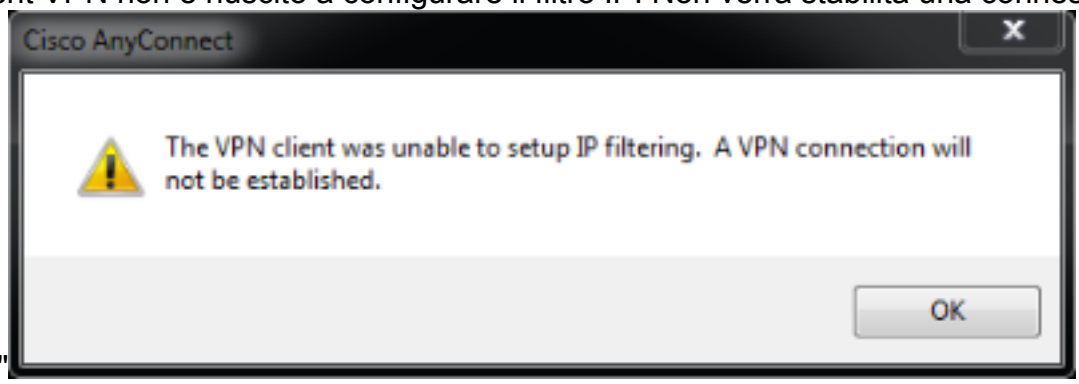
- Servizio Windows Defender (windefense)
- Servizio helper IP (iphlpsvc)
- Servizio Centro sicurezza PC Windows (wscsvc)
- Servizio Windows Firewall (mpssvc)
- Servizio BFE (Base Filtering Engine)

Attenzione: Il trojan Win32/Sirefef (ZeroAccess) è una minaccia pericolosa che utilizza tecniche avanzate di stealth per impedirne il rilevamento e la rimozione. Di conseguenza, potrebbe essere necessario ripristinare e riconfigurare alcune funzionalità di protezione di Windows.

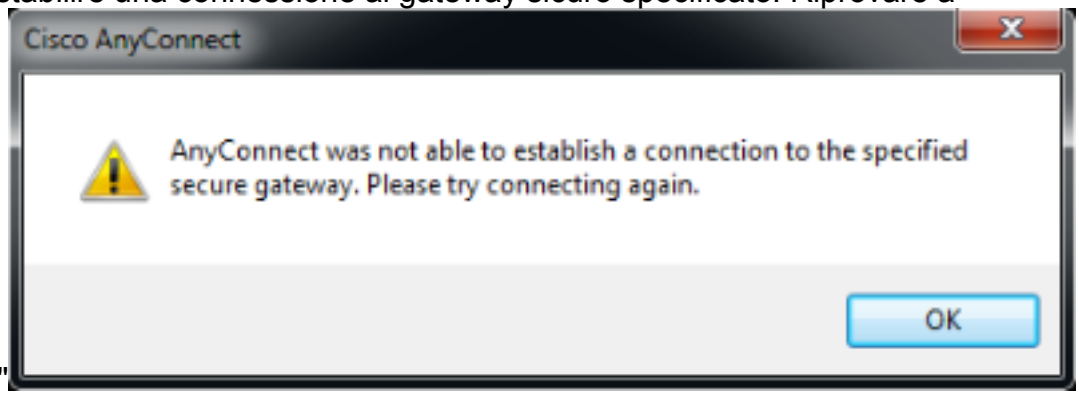
Problema

Gli scenari sono:

- L'utente non può installare AnyConnect Secure Mobility Client e riceve il messaggio di errore "Il client VPN non è riuscito a configurare il filtro IP. Non verrà stabilita una connessione VPN."



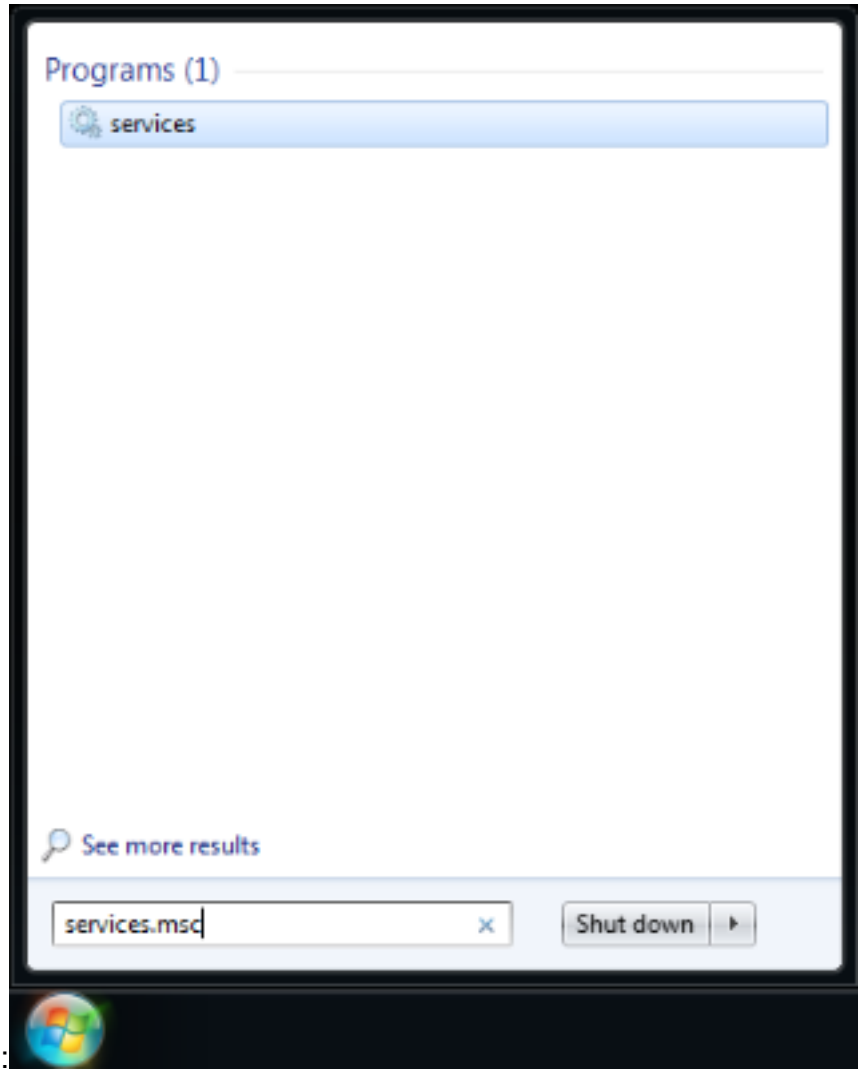
- AnyConnect Secure Mobility Client ha funzionato correttamente all'inizio. Tuttavia, l'utente finale non può più stabilire una connessione e riceve il messaggio di errore "Anyconnect non è riuscita a stabilire una connessione al gateway sicuro specificato. Riprovare a connettersi."

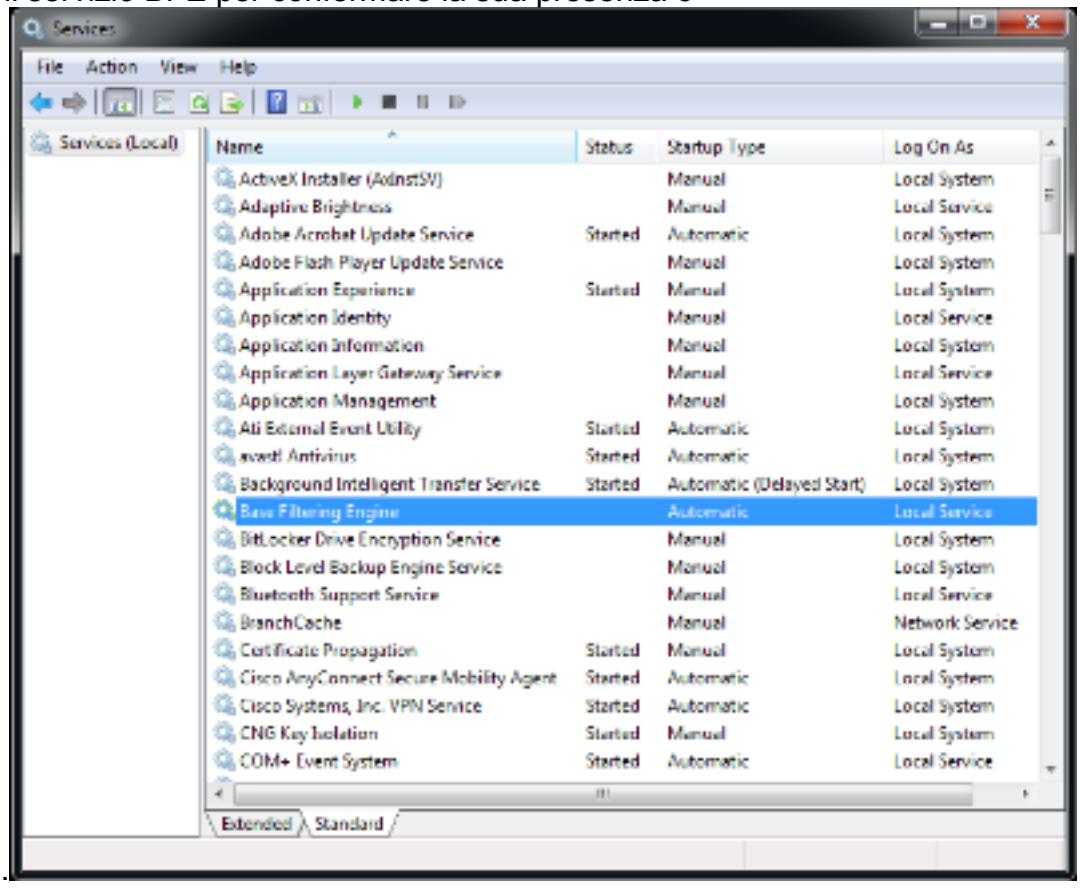


Soluzione

Quando vengono visualizzati questi messaggi di errore, è importante verificare se l'elemento BFE è effettivamente disabilitato/mancante o se il client non è in grado di riconoscerlo. Per risolvere il problema, procedere come segue:

1. Accedere a Gestione controllo servizi (SCM) dal menu

Windows: 

2. Cercare il servizio BFE per confermare la sua presenza o assenza. 

Se il servizio funziona, lo stato viene visualizzato come **Avviato**. Se nella colonna è presente altro,

è presente un problema relativo al servizio. Tuttavia, se lo stato è Started (Avviato), il client non sarà in grado di comunicare con il servizio ed è possibile che si sia verificato un bug.

Se il servizio è disabilitato o non avviato, è possibile che si verifichino le seguenti cause:

- Come spiegato in precedenza, il malware disabilita questo servizio come primo passo.
- Registro di sistema danneggiato nel computer.

Procedura di riparazione

Il primo passaggio consiste nell'analizzare e disinfettare il sistema con un software antivirus. Non ripristinare il servizio BFE se verrà eliminato nuovamente dal trojan Win32/Sirefef (ZeroAccess). Scaricare lo strumento ESET SirefefCleaner da questa pagina Web e salvarlo sul desktop.

In questo video viene illustrata la procedura per rimuovere il trojan Win32/Sirefef (ZeroAccess):.

Come rimuovere il trojan Win32/Sirefef (ZeroAccess)?

Dopo aver rimosso il trojan Win32/Sirefef (ZeroAccess), verificare che il servizio BFE possa essere avviato e mantenuto attivo con i mezzi normali. A tal fine:

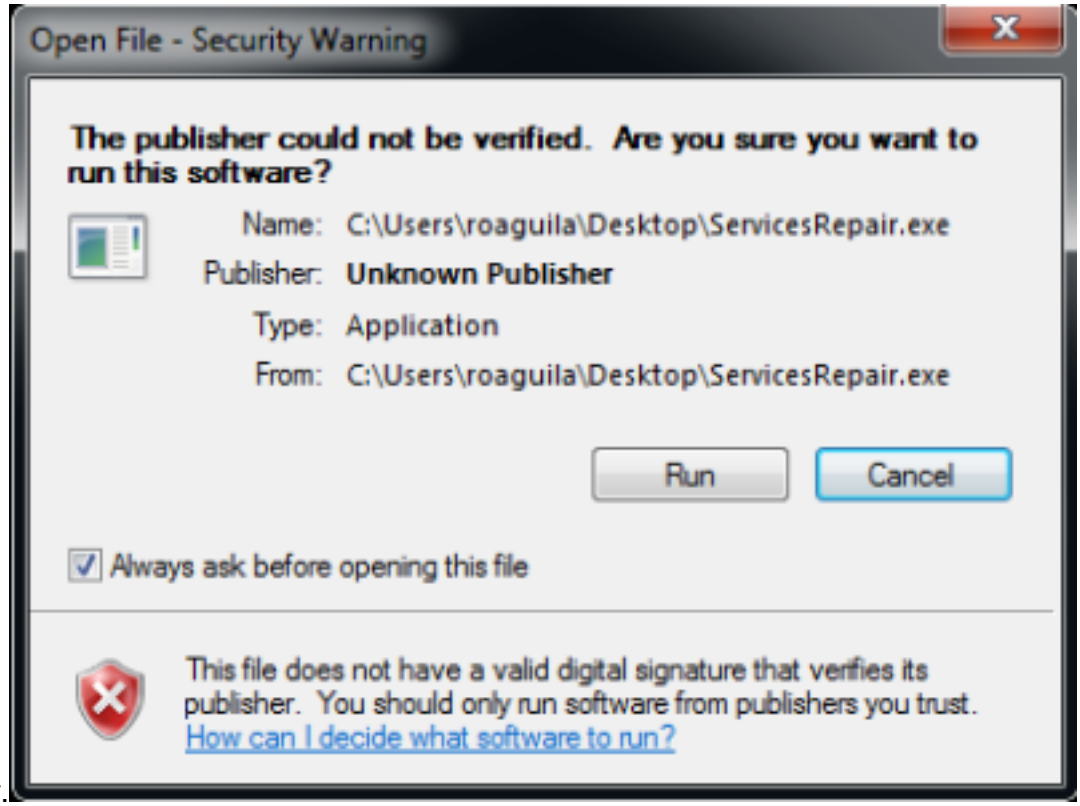
1. Avviare SCM e scegliere la scheda **Extended** anziché la scheda **Standard**.
2. Scegliere il servizio BFE.
3. Scegliere l'opzione **Start** a sinistra.

   Attenzione: È buona norma eseguire il backup dei file prima di eseguire questa procedura. Tutte le informazioni contenute in questo articolo vengono fornite così come sono, senza alcuna garanzia, espressa o implicita, di accuratezza, completezza o idoneità per uno scopo particolare.

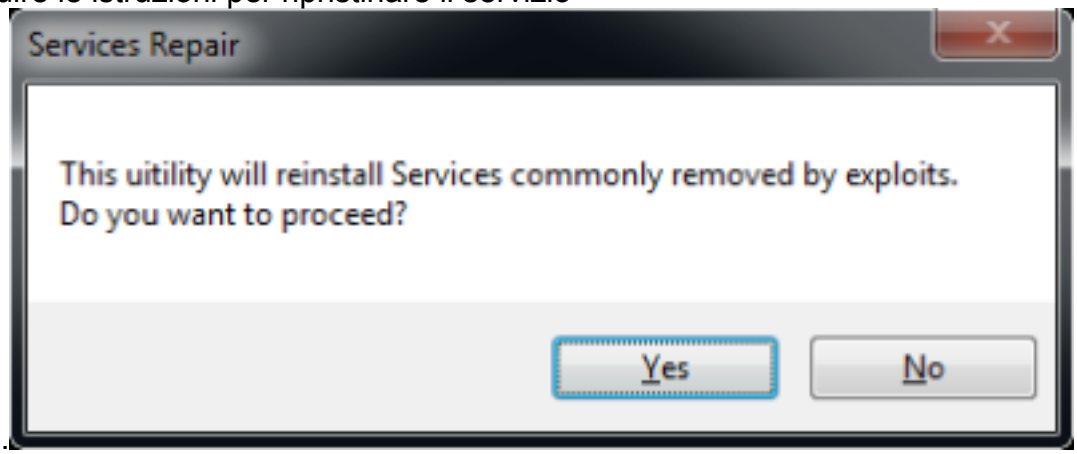
Se questa procedura non funziona, attenersi alla seguente procedura:

1. Scaricare l'utilità ESET ServicesRepair da questa pagina Web e salvarla sul desktop.
2. Eseguire l'utilità ESET

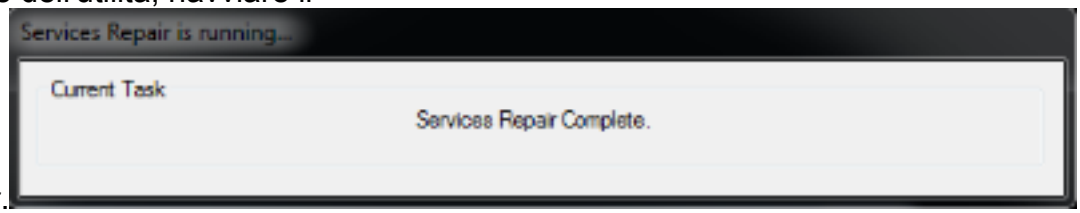
ServicesRepair.

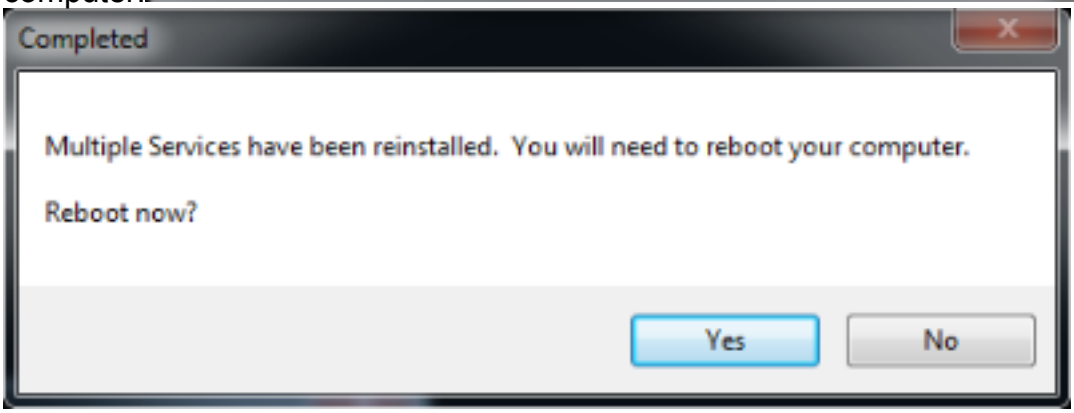


3. Seguire le istruzioni per ripristinare il servizio BFE.



4. Al termine dell'utilità, riavviare il computer.





5. Una volta riavviato il computer, installare o eseguire nuovamente AnyConnect Secure Mobility Client.

Nota: I test hanno dimostrato che questo strumento è utile nella maggior parte dei casi in cui i file del Registro di sistema sono danneggiati o i servizi sono danneggiati. Pertanto, se si incontrano questi messaggi di errore, questo strumento si rivela utile anche:
- L'agente client VPN non è riuscito a creare il deposito comunicazioni tra processi.
- Il servizio agente VPN non risponde. Riavvia l'applicazione tra un minuto.
- Il servizio Cisco Anyconnect Secure Mobility Agent sul computer locale è stato avviato e arrestato. Alcuni servizi vengono arrestati automaticamente se non sono utilizzati da altri servizi o programmi.