AnyConnect Secure Mobility Connection-fout: "De VPN-client is niet in staat IP-filtering in te stellen"

Inhoud

Inleiding

Dit document beschrijft wat u moet doen wanneer u dit Cisco AnyConnect Secure Mobility Client VPN-gebruikersbericht invoert:

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

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is alleen gebaseerd op Windows Vista- en Windows 7-besturingssystemen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De Base Filtering Engine (BFE) service

BFE is een service die firewalls en IPsec-beleid (Internet Protocol Security) beheert en gebruikersmode-filtering implementeert. De beveiliging van het systeem is aanzienlijk verminderd als u de BFE-service stopt of uitschakelt. Het resulteert ook in onvoorspelbaar gedrag in IPsec beheer en firewalltoepassingen.

Deze systeemonderdelen zijn afhankelijk van de BFE-service:

- Internet Key Exchange (IKE) en Veriated Internet Protocol (AuthIP) IPsec-testmodules
- Internet Connection Sharing (ICS)
- IPsec-beleidsagent
- Routing- en externe toegang
- Windows Firewall

De AnyConnect Secure Mobility Client brengt zowel een routing als een externe toegang tot wijziging in de host-machine. De IKEv2 is ook afhankelijk van de IKE-modules. Dit betekent dat, als de BFE-service wordt stopgezet, de AnyConnect Secure Mobility Client niet kan worden geïnstalleerd of gebruikt om een Secure Socket Layer (SSL)-verbinding op te zetten.

Er zijn bedreigingen in actieve circulatie die de BFE-dienst uitschakelen en verwijderen als eerste stap in het infectieproces.

Win32/Sirefef (nultoegang) Trojan

De Win32/Sirefef (ZeroAccess)-trojan is een uit meerdere componenten bestaande serie malware die heimelijk gebruikt om zijn aanwezigheid op uw computer te verbergen. Deze dreiging geeft aanvallers volledige toegang tot uw systeem. Gezien de aard ervan kan de lading van infectie tot infectie sterk variëren, hoewel algemeen gedrag:

- Downloaden en uitvoeren van willekeurige bestanden.
- Contact van verafgelegen hosts.
- Uitschakeling van beveiligingsfuncties.

Er zijn geen vaak voorkomende symptomen geassocieerd met deze dreiging. Waarschuwingen van geïnstalleerde antivirussoftware kunnen de enige symptomen zijn.

Een trojka van Win32/Sirefef (ZeroAccess) probeert deze security-gerelateerde services te stoppen en te verwijderen:

- Windows Defender Service (winsverdediging)
- IP-Helper-service (iphlpv)
- Windows Security Center Service (WSC)
- Windows Firewall-service (MSFC)

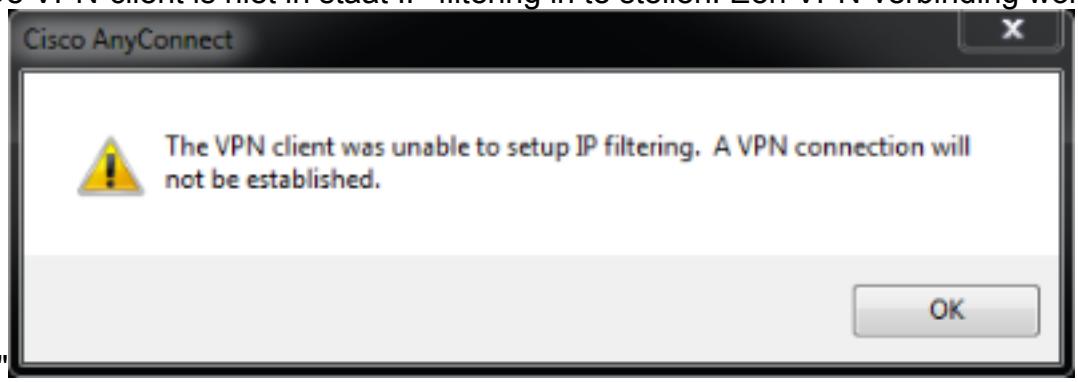
- Base Filtering Engine Service (SFE)

  Voorzichtig: De Win32/Sirefef (ZeroAccess)-trojan is een gevaarlijke dreiging die gebruik maakt van geavanceerde onzichtbare technieken om de detectie en verwijdering ervan te belemmeren. Als gevolg van een infectie met deze dreiging moet u mogelijk bepaalde beveiligingsfuncties van Windows repareren en opnieuw configureren.

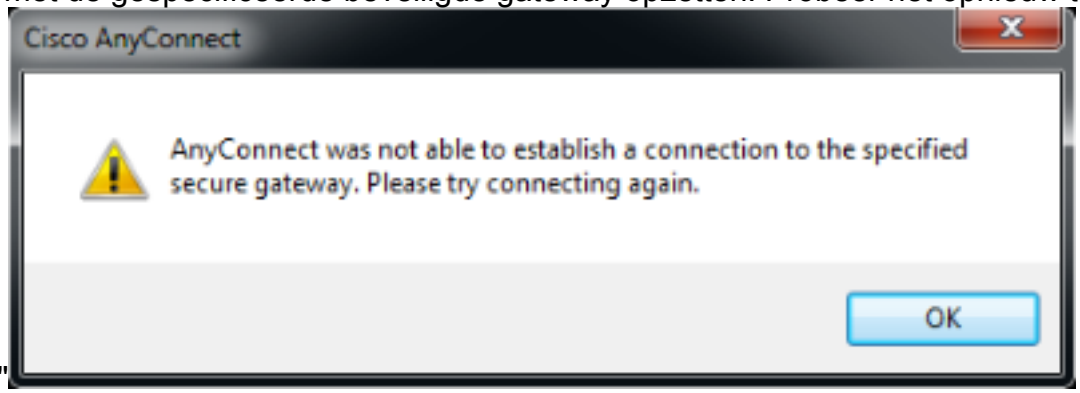
Probleem

De scenario's zijn:

- De gebruiker kan de AnyConnect Secure Mobility Client niet installeren en de foutmelding ontvangen: "De VPN-client is niet in staat IP-filtering in te stellen. Een VPN-verbinding wordt niet gemaakt."



- De AnyConnect Secure Mobility Client werkte aanvankelijk goed. Echter; De eindgebruiker kan geen verbinding meer maken en ontvangt het foutbericht, "AnyConnect kon geen verbinding met de gespecificeerde beveiligde gateway opzetten. Probeer het opnieuw te verbinden."

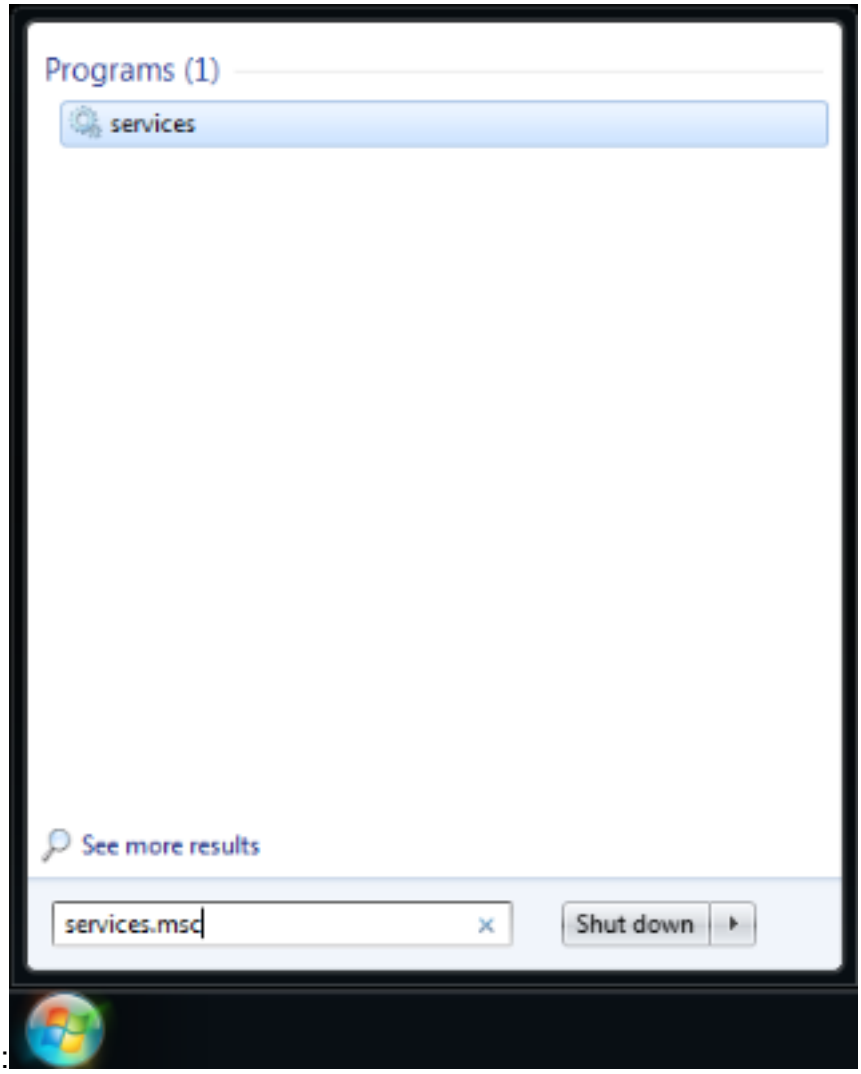


Oplossing

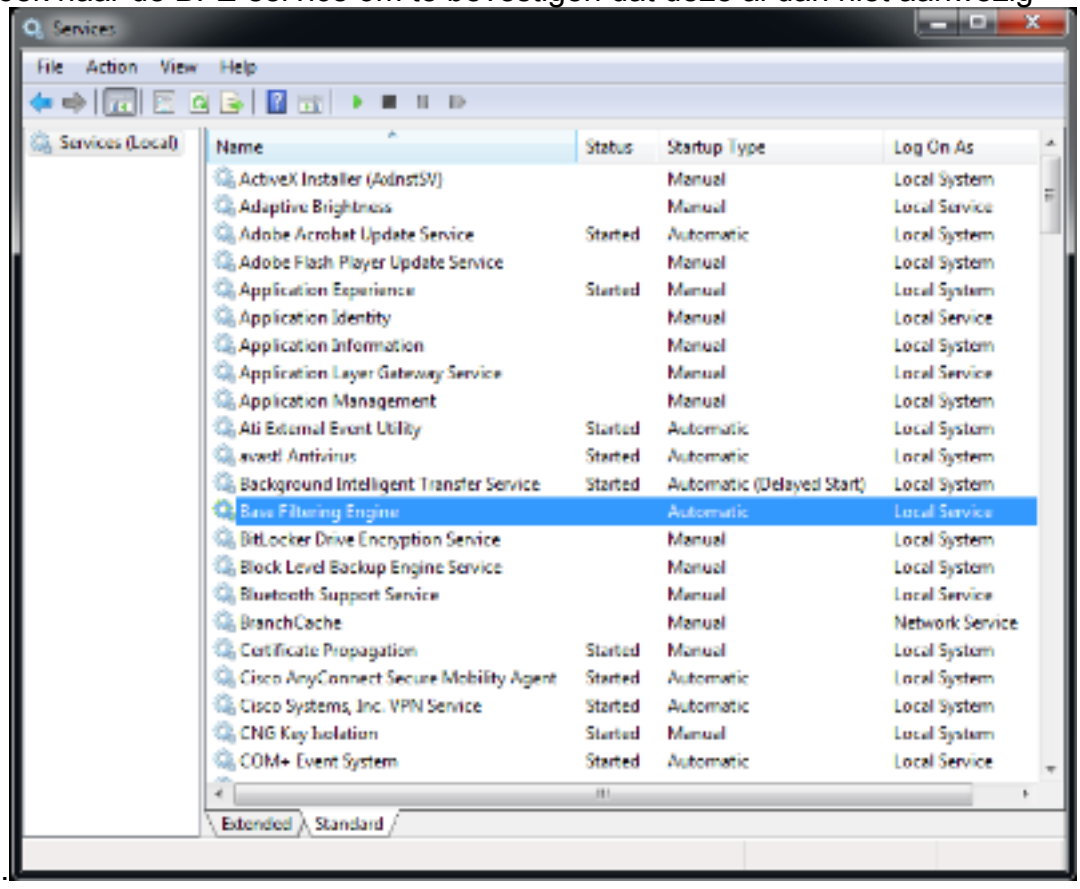
Wanneer deze foutmeldingen worden gezien, is het van belang te bevestigen of de BFE daadwerkelijk uitgeschakeld/ontbrekende is of dat de cliënt deze niet kan herkennen. Voltooi de volgende stappen om een probleem op te lossen:

1. Toegang tot Service Control Manager (SCM) in het menu

Windows:



2. Zoek naar de BFE-service om te bevestigen dat deze al dan niet aanwezig is.



Als de service werkt, wordt de status weergegeven als **gestart**. Als er iets anders in die kolom

staat, is er een probleem met de service. Als de status echter wordt weergegeven zoals is gestart, kan de klant duidelijk niet met de service communiceren en is het mogelijk dat er een bug is.

Als de service uitgeschakeld of niet gestart is, zijn de volgende redenen:

- Malware, zoals eerder uitgelegd, schakelt deze service als een eerste stap uit.
- Griffie corruptie op de machine.

reparatieprocedure

De eerste stap is het scannen en desinfecteren van uw systeem met antivirussoftware. U dient de BFE-service niet te herstellen indien deze opnieuw wordt verwijderd door een Win32/Sirefef (ZeroAccess)-trojan. Download het ESET SirefefCleaner gereedschap van deze webpagina en bewaar het op uw desktop.

Deze video legt de procedure uit om de Win32/Sirefef (ZeroAccess)-trojan te verwijderen:

Hoe verwijder ik de Win32/Sirefef (ZeroAccess)-trojan?

Controleer na het verwijderen van de Win32/Sirefef (ZeroAccess)-trojaan of de BFE-service kan worden gestart en actief gehouden op normale wijze. Dit doet u zo:

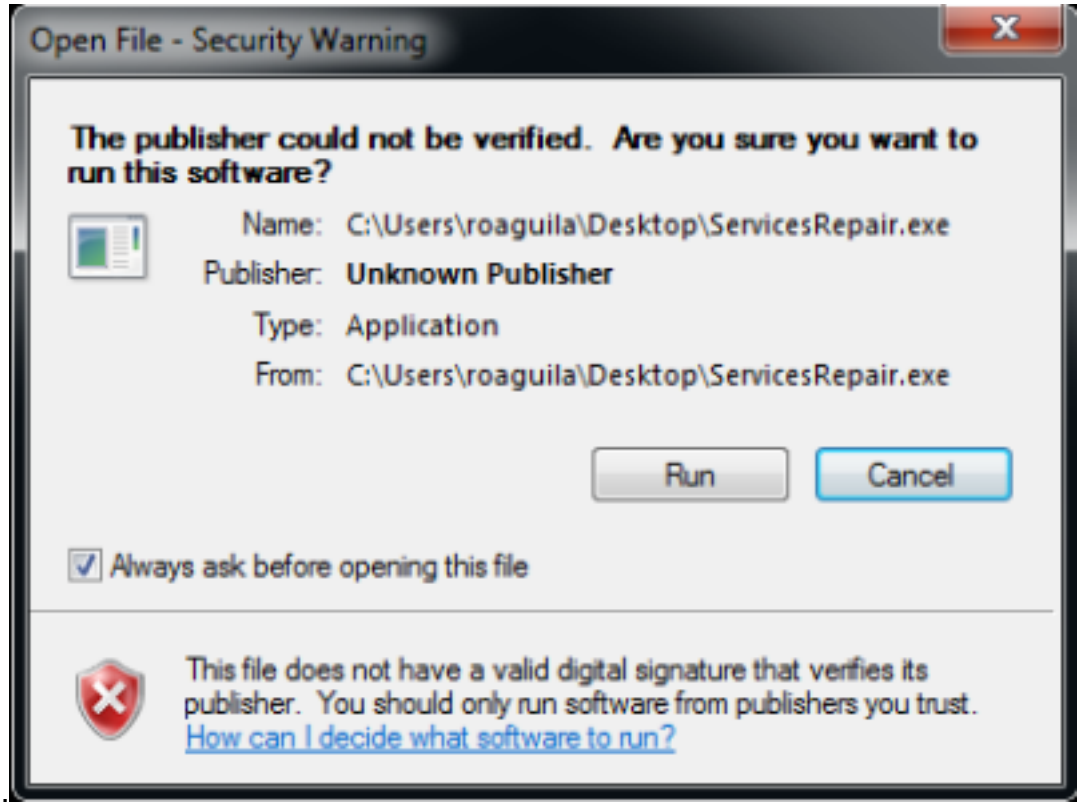
1. Start SCM en kies het **tabblad Uitgebreid** in plaats van de **standaard**.
2. Kies de BFE-service.
3. Selecteer de optie **Start** links.

   Voorzichtig: Het is een goede praktijk om uw dossiers te steunen voordat u deze procedure probeert. Alle informatie in dit artikel wordt geleverd zoals het is, zonder garantie, expliciet of impliciet, van de nauwkeurigheid, volledigheid of geschiktheid voor een bepaald doel.

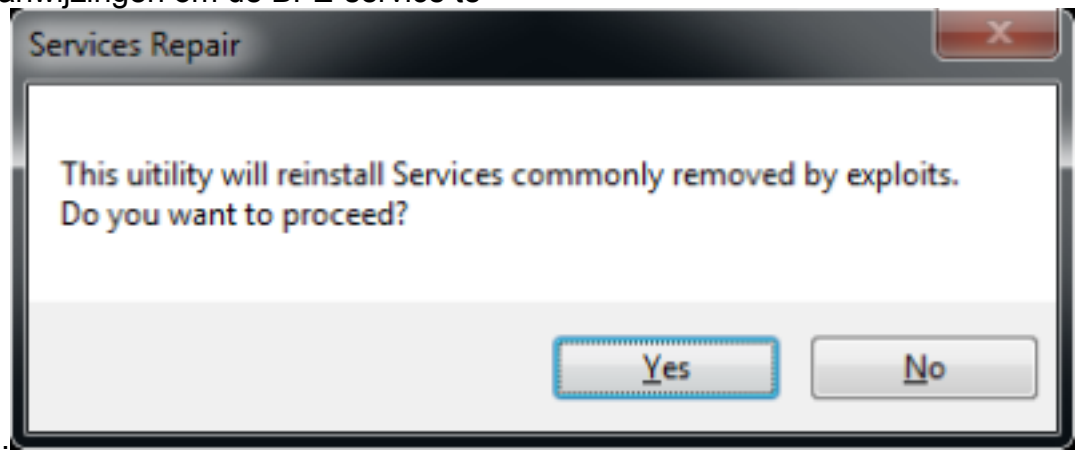
Als deze procedure niet werkt, voert u de volgende stappen uit:

1. Download het ESET ServicesReader-hulpprogramma van deze webpagina en bewaar het op uw bureaublad.
2. Uitvoeren van het ESET Services Repair

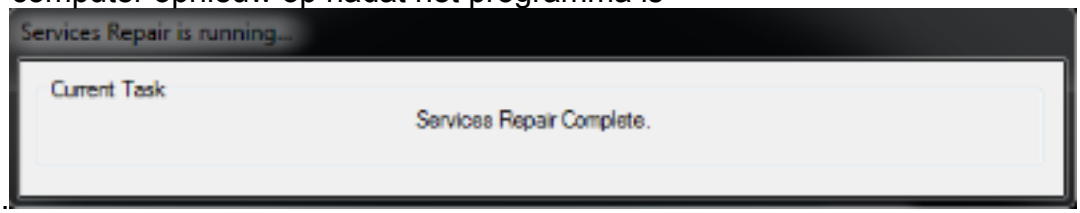
Hulpprogramma.

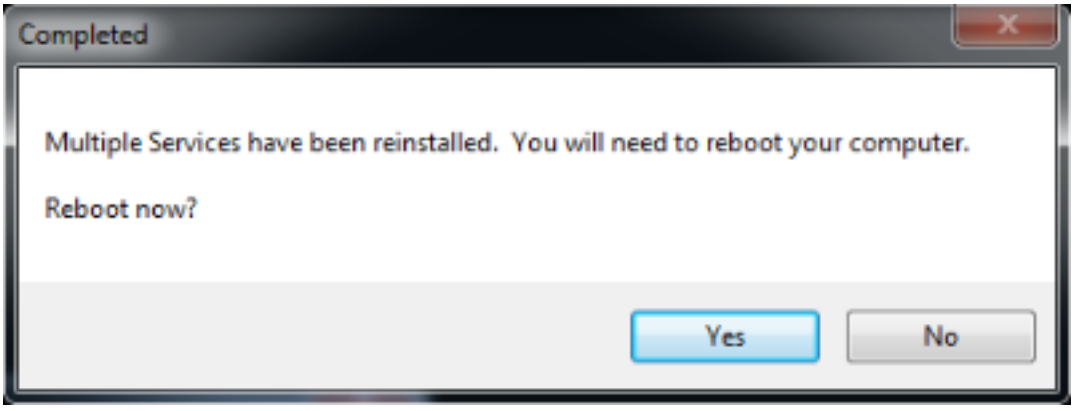


3. Volg de aanwijzingen om de BFE-service te repareren.



4. Start de computer opnieuw op nadat het programma is voltooid.





5. Nadat de computer is opgestart, installeert of voert u de AnyConnect Secure Mobility Client opnieuw uit.

Opmerking: Tests hebben aangetoond dat dit gereedschap helpt in de meeste gevallen waar de registratiebestanden beschadigd zijn of waar de services beschadigd zijn. Daarom, als u deze foutmeldingen tegenkomt, blijkt dit gereedschap ook handig:
- De VPN-client-agent kon het communicatieplatform tussen processen niet maken.
- De VPN-agent reageert niet. Start deze applicatie na een minuut opnieuw.
- De Cisco AnyConnect Secure Mobility Agent op lokale computer gestart en stopgezet.
Sommige diensten stoppen automatisch als ze niet door andere diensten of programma's worden gebruikt.