Erro de conexão seguro da mobilidade de AnyConnect: “O cliente VPN era incapaz de setup a filtração IP”

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[O serviço de filtração baixo do motor (BFE)](#)
[Trojan (ZeroAccess) Win32/Sirefef](#)
[Problema](#)
[Solução](#)
[Procedimento de reparo](#)

Introdução

Este documento descreve o que fazer quando você enounter esta mensagem do usuário do Cliente de mobilidade Cisco AnyConnect Secure VPN:

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

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em sistemas operacionais de Windows Vista e de Windows 7 somente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O serviço de filtração baixo do motor (BFE)

BFE é um serviço que controle o Firewall e as políticas da segurança de protocolo do Internet (IPsec) e execute a filtração USER-MODE. A Segurança do sistema é reduzida significativamente se você para ou desabilita o serviço BFE. Igualmente conduz ao comportamento imprevisível em aplicativos do Gerenciamento e do Firewall do IPsec.

Estes componentes de sistema dependem do serviço BFE:

- Internet Key Exchange (IKE) e IPsec autenticado do protocolo de internet (AuthIP) que fecham os módulos
- Internet Connection Sharing (ICS)
- Agente da política de IPsec
- Roteamento e Acesso remoto
- Windows Firewall

O cliente seguro da mobilidade de AnyConnect faz mudanças do roteamento e do Acesso remoto à máquina host. O IKEv2 é igualmente dependente dos módulos IKE. Isto significa que, se o serviço BFE é parado, o cliente seguro da mobilidade de AnyConnect não pode ser instalado ou usado para estabelecer uma conexão do secure sockets layer (SSL).

Há as ameaças na circulação ativa que desabilitam e removem o serviço BFE em primeiro no processo da infecção.

Trojan (ZeroAccess) Win32/Sirefef

O Trojan (ZeroAccess) Win32/Sirefef é uma família do multi-componente do malware que usa o discrição para esconder sua presença em seu computador. Esta ameaça dá a atacantes o acesso direto a seu sistema. Devido a sua natureza, o payload pôde variar extremamente de uma infecção a outra, embora o comportamento comum incluísse:

- Transferência e execução de arquivos arbitrários.
- Contato dos host remotos.
- Incapacidade dos recursos de segurança.

Não há nenhum sintoma comum associado com esta ameaça. As notificações de alerta do antivírus instalado puderam ser os únicos sintomas.

O Trojan (ZeroAccess) Win32/Sirefef tenta parar e suprimir destes serviços relacionado à segurança:

- Serviço de Windows Defender (windefend)
- Serviço do ajudante de IP (iphlpsvc)
- Serviço de Windows Security Center (wscsvc)

- Serviço do Windows Firewall (mpssvc)
- Serviço de filtração baixo do motor (bfe)

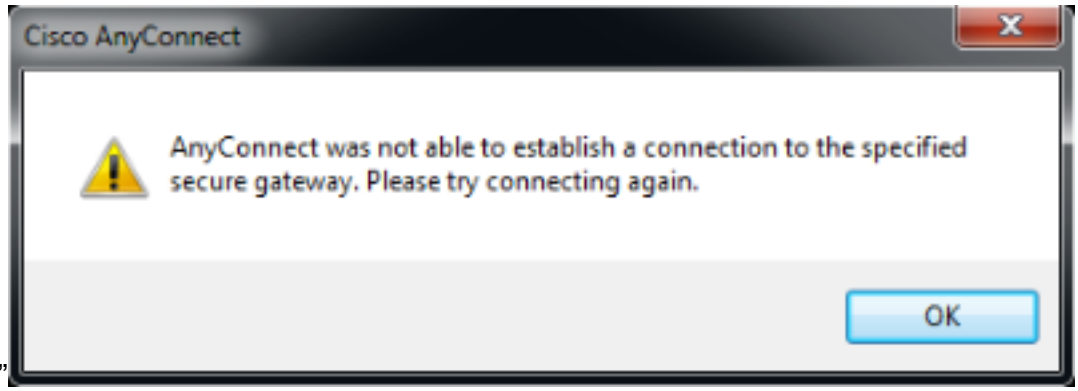
Caution: O Trojan (ZeroAccess) Win32/Sirefef é uma ameaça perigosa que use técnicas avançadas do discrição a fim impedir suas detecção e remoção. Consequentemente infecção com esta ameaça, você pode precisar de reparar e reconfigurar alguns recursos de segurança de Windows.

Problema

As encenações são:

- O usuário não pode instalar o cliente seguro da mobilidade de AnyConnnect e recebe o Mensagem de Erro, “o cliente VPN era incapaz de setup a filtração IP. Uma conexão de VPN não será estabelecida.”

- O cliente seguro da mobilidade de AnyConnect trabalhou muito bem inicialmente. Contudo; o utilizador final pode já não estabelecer uma conexão e recebe o Mensagem de Erro, “Anyconnect não podia estabelecer um connectoin ao especificado fixa o gateway. Tente por favor conectar outra vez.”

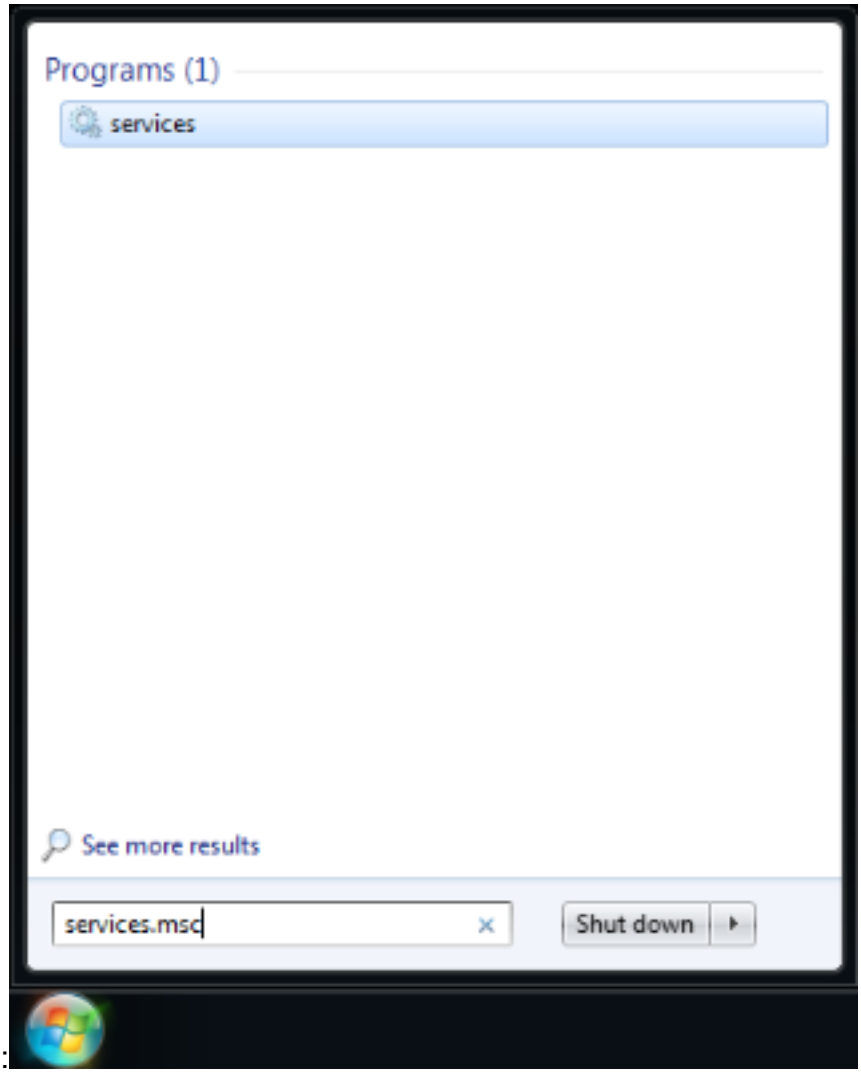


Solução

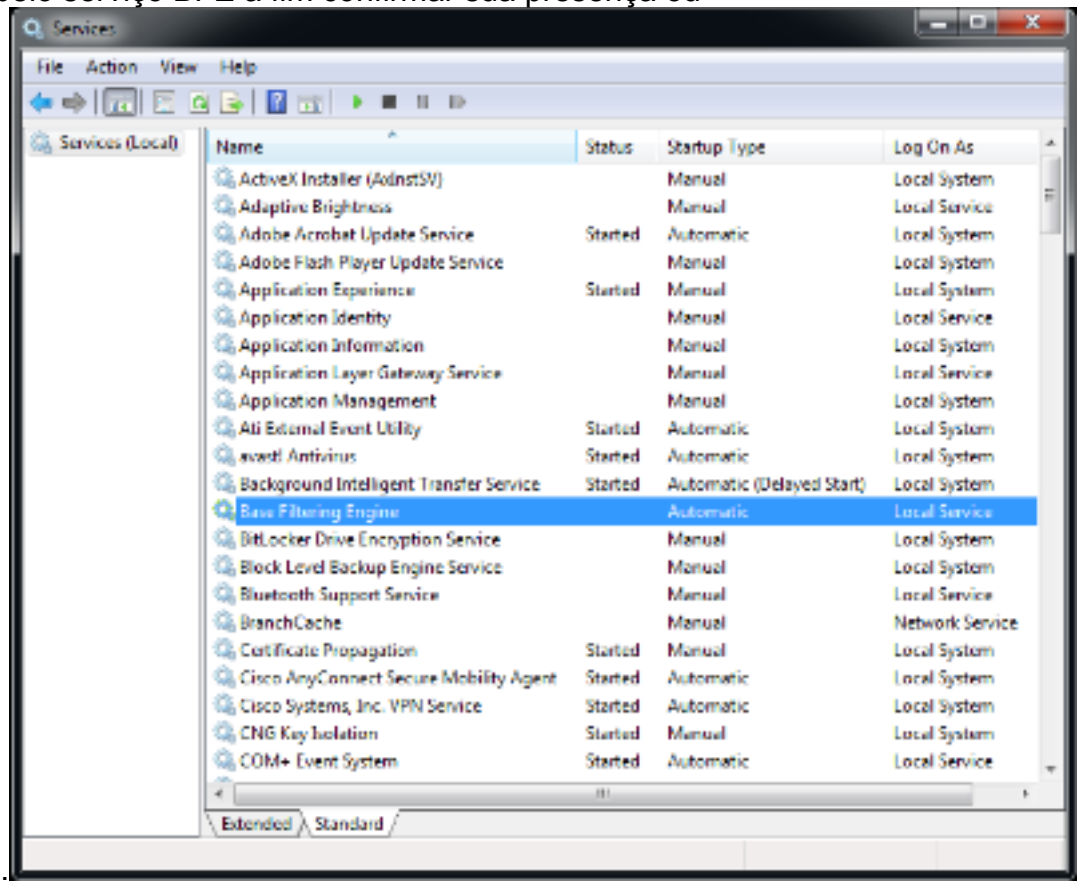
Quando estes Mensagens de Erro são considerados, é importante confirmar se o BFE está desabilitado realmente/faltando ou se o cliente não pode o reconhecer. O troublehoot, termina estas etapas:

1. Alcance o gerente do controle de serviço (SCM) do menu de

Windows:



2. Procure pelo serviço BFE a fim confirmar sua presença ou ausência.



Se o serviço trabalha, as exibições de status como **começadas**. Se há qualquer outra coisa nessa

coluna, há um problema com o serviço. Contudo, se as exibições de status como começadas, o cliente não podem claramente se comunicar com o serviço, e ele há possível está um erro.

Se o serviço é desabilitado ou não começado, algumas razões possíveis são:

- O malware, como explicado previamente, desabilita este serviço em primeiro.
- Corrupção do registro na máquina.

Procedimento de reparo

A primeira etapa é fazer a varredura e desinfetar de seu sistema com um antivírus. Você não deve restaurar o serviço BFE se será suprimido outra vez pelo Trojan (ZeroAccess) Win32/Sirefef. Transfira a ferramenta ESET SirefefCleaner deste página da web, e salvar à seu desktop.

Este vídeo explica o procedimento para remover o Trojan (ZeroAccess) Win32/Sirefef:.

Como eu removo o Trojan (ZeroAccess) Win32/Sirefef?

Uma vez que você removeu o Trojan (ZeroAccess) Win32/Sirefef, verifique que o serviço BFE pode ser começado e active mantido por meios normais. Para fazer isso:

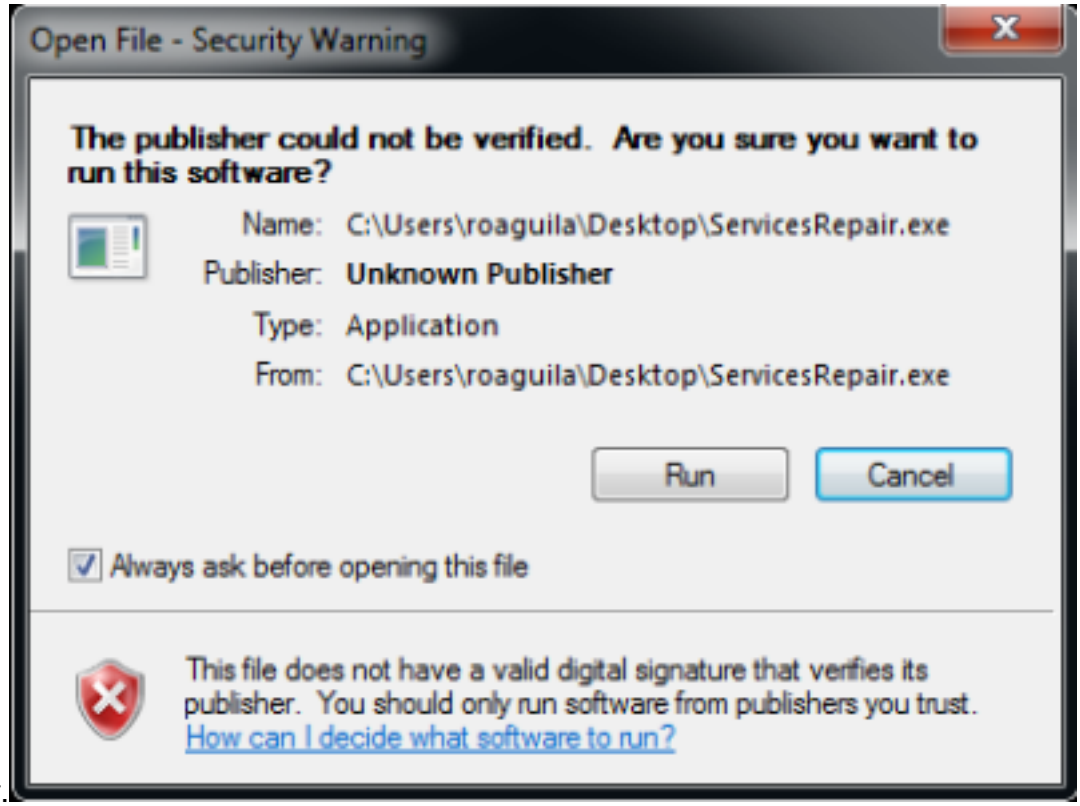
1. Comece o SCM e escolha a aba **prolongada** em vez do **padrão**.
2. Escolha o serviço BFE.
3. Escolha a opção de **começo** à esquerda.

   Caution: É uma boa prática suportar seus arquivos antes que você tente este procedimento. Toda a informação neste artigo é fornecida como é, sem nenhuma garantia, se expresso ou implicado, de sua precisão, integralidade, ou aptidão para uma finalidade particular.

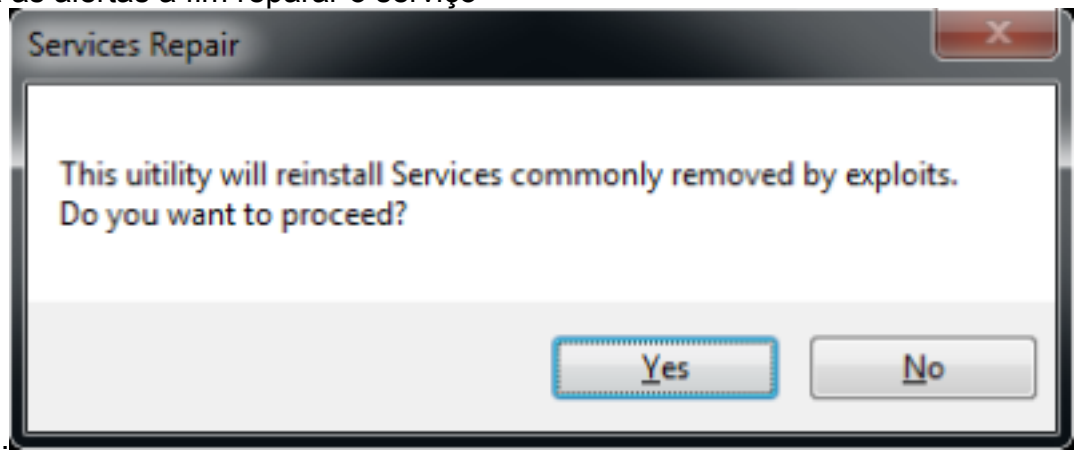
Se este procedimento não trabalha, termine estas etapas:

1. Transfira a utilidade ESET ServicesRepair deste página da web, e salvar à seu desktop.
2. Execute a utilidade ESET

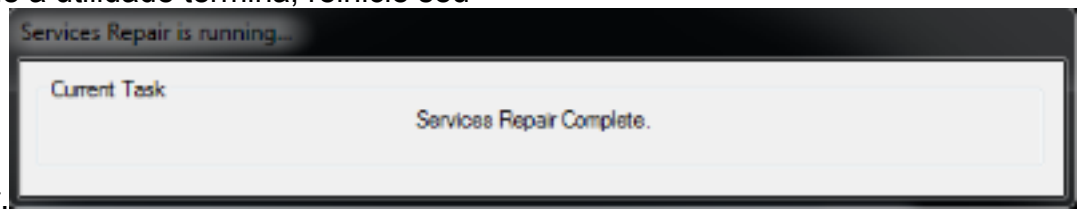
ServicesRepair.

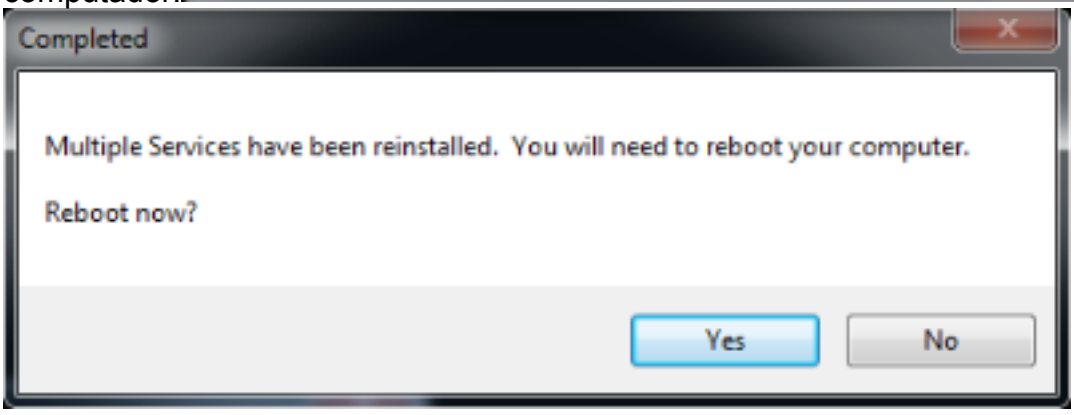


3. Siga as alertas a fim reparar o serviço BFE.



4. Uma vez que a utilidade termina, reinicie seu computador.





5. Uma vez que seu computador reinicia, instale ou execute o cliente seguro da mobilidade de AnyConnect outra vez.

Note: Os testes mostraram que esta ferramenta ajuda na maioria dos casos onde os arquivos de registro são corrompidos ou os serviços são danificados. Consequentemente, se você encontra estes Mensagens de Erro, esta ferramenta prova útil demasiado:
- O agente do cliente VPN era incapaz de criar o depósito de uma comunicação entre processos.
- O serviço do agente VPN não está respondendo. Reinicie por favor este aplicativo após um minuto.
- O serviço seguro do agente da mobilidade de Cisco Anyconnect no computador local ligado e parado. Alguns serviços param automaticamente se não são dentro uso por outros serviços ou programas.