AnyConnect Secure Mobility 연결 오류:"VPN 클라이언트가 IP 필터링을 설정할 수 없습니다."

목차

소개

이 문서에서는 Cisco AnyConnect Secure Mobility Client VPN 사용자 메시지를 입력할 때 수행할 작업에 대해 설명합니다.

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

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Windows Vista 및 Windows 7 운영 체제만을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

기본 필터링 엔진(BFE) 서비스

BFE는 방화벽 및 IPsec(Internet Protocol Security) 정책을 관리하고 사용자 모드 필터링을 구현하는 서비스입니다.BFE 서비스를 중지하거나 비활성화하면 시스템 보안이 크게 줄어듭니다.또한 IPsec 관리 및 방화벽 애플리케이션에서 예측할 수 없는 동작이 발생합니다.

이러한 시스템 구성 요소는 BFE 서비스에 따라 다릅니다.

- IKE(Internet Key Exchange) 및 AuthIP(Authenticated Internet Protocol) IPsec Keying Module
- 인터넷 연결 공유(ICS)
- IPsec 정책 에이전트
- 라우팅 및 원격 액세스
- Windows 방화벽

AnyConnect Secure Mobility Client는 호스트 시스템에 대한 라우팅 및 원격 액세스를 모두 변경합니다.IKEv2는 IKE 모듈에도 종속됩니다.즉, BFE 서비스가 중지되면 AnyConnect Secure Mobility Client를 설치하거나 사용하여 SSL(Secure Sockets Layer) 연결을 설정할 수 없습니다.

감염 프로세스의 첫 번째 단계로 BFE 서비스를 비활성화하고 제거하는 활성 순환에 위협이 있습니다.

Win32/Sireef(ZeroAccess) 트로이 목마

Win32/Sireef(ZeroAccess) 트로이 목마는 숨김을 사용하여 컴퓨터에 있는 존재를 숨기는 다중 구성 요소 악성코드 제품군입니다.이 위협은 공격자가 시스템에 대한 모든 액세스를 제공합니다.이러한 특성 때문에 일반적인 동작에는 다음이 포함되지만, 페이로드의 감염에서 다른 감염으로 크게 달라질 수 있습니다.

- 임의의 파일 다운로드 및 실행
- 원격 호스트의 연락처
- 보안 기능의 비활성화

이 위협과 관련된 일반적인 증상은 없습니다.설치된 안티바이러스 소프트웨어의 경고 알림만 나타날 수 있습니다.

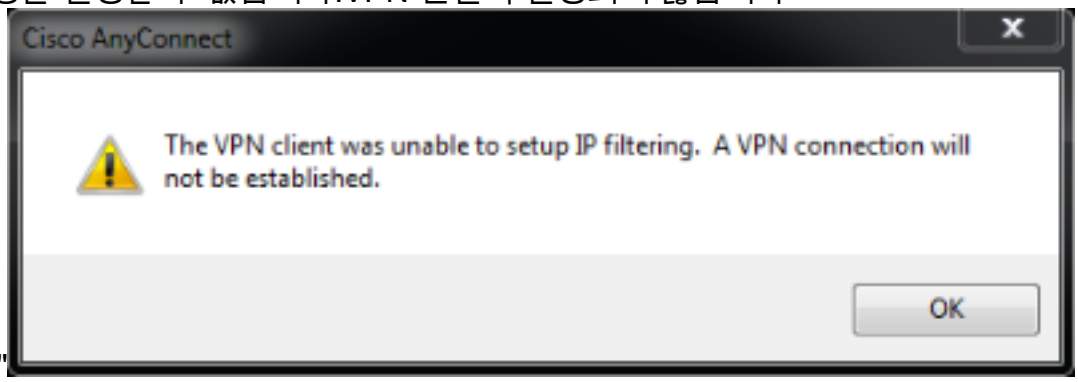
Win32/Sireef(ZeroAccess) 트로이 목마는 다음과 같은 보안 관련 서비스를 중지하고 삭제하려고 시도합니다.

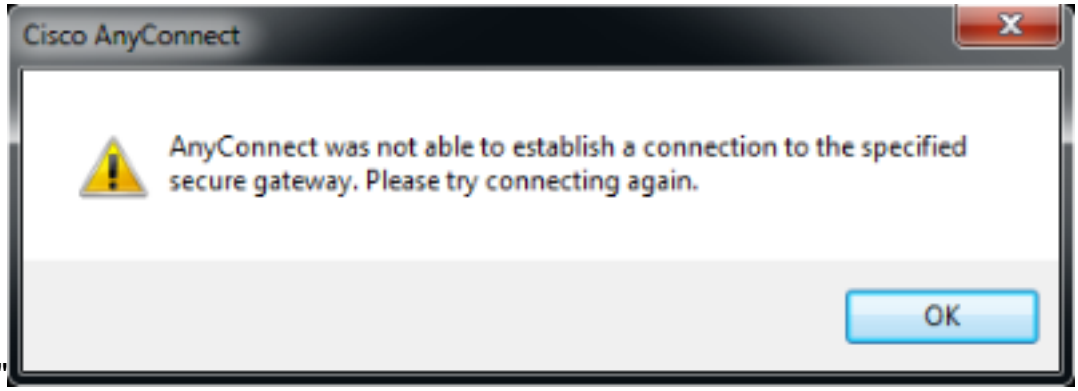
- Windows Defender 서비스(windefense)
- IP 도우미 서비스(iphlpsvc)
- Windows 보안 센터 서비스(wscsvc)
- Windows 방화벽 서비스(mpssvc)
- 기본 필터링 엔진 서비스(bfe)

  주의: Win32/Sireef(ZeroAccess) 트로이 목마는 탐지 및 제거를 방해하기 위해 고급 스텔스 기술을 사용하는 위험한 위협입니다.이 위협으로 인한 감염으로 인해 일부 Windows 보안 기능을 복구 및 재구성해야 할 수 있습니다.

문제

시나리오는 다음과 같습니다.

- 사용자는 AnyConnect Secure Mobility Client를 설치할 수 없으며 "VPN 클라이언트가 IP 필터링을 설정할 수 없습니다.VPN 연결이 설정되지 않습니다


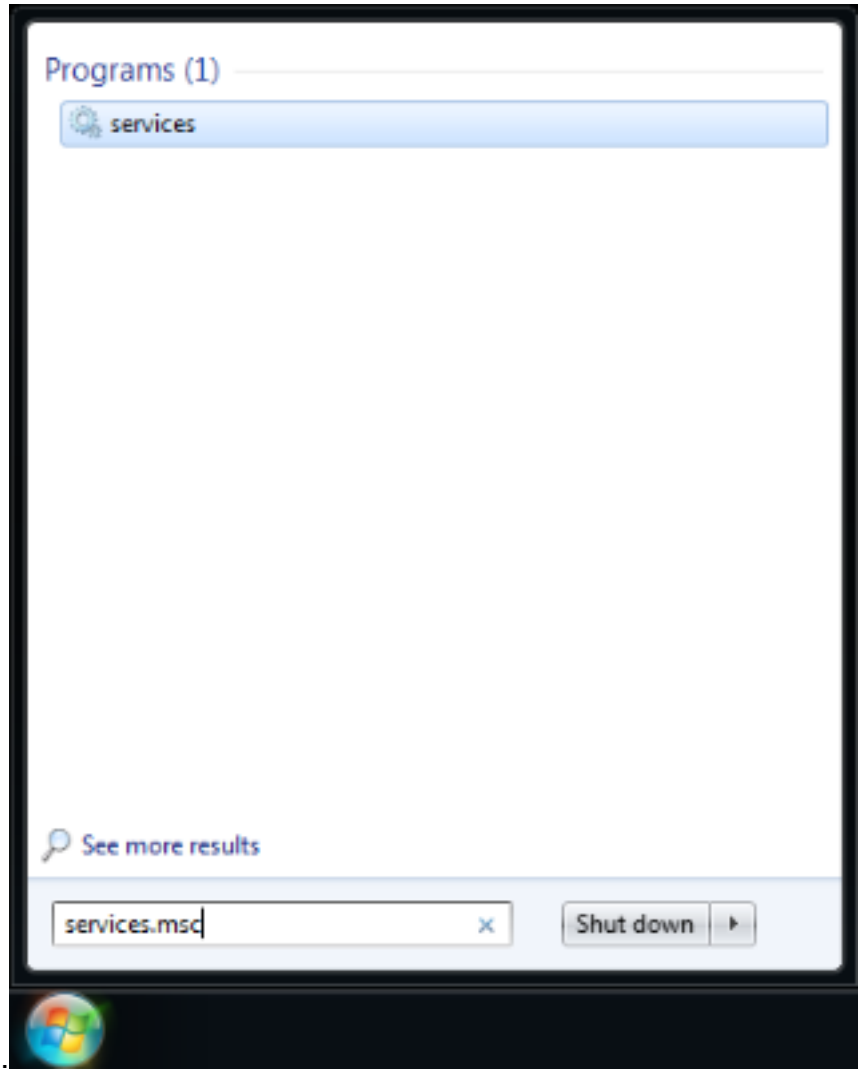
."
- 처음에는 AnyConnect Secure Mobility Client가 정상적으로 작동했습니다.그러나최종 사용자는 더 이상 연결을 설정할 수 없으며 "AnyConnect가 지정된 보안 게이트웨이에 대한 연결을 설정할 수 없습니다.다시 연결해 보십시오


."

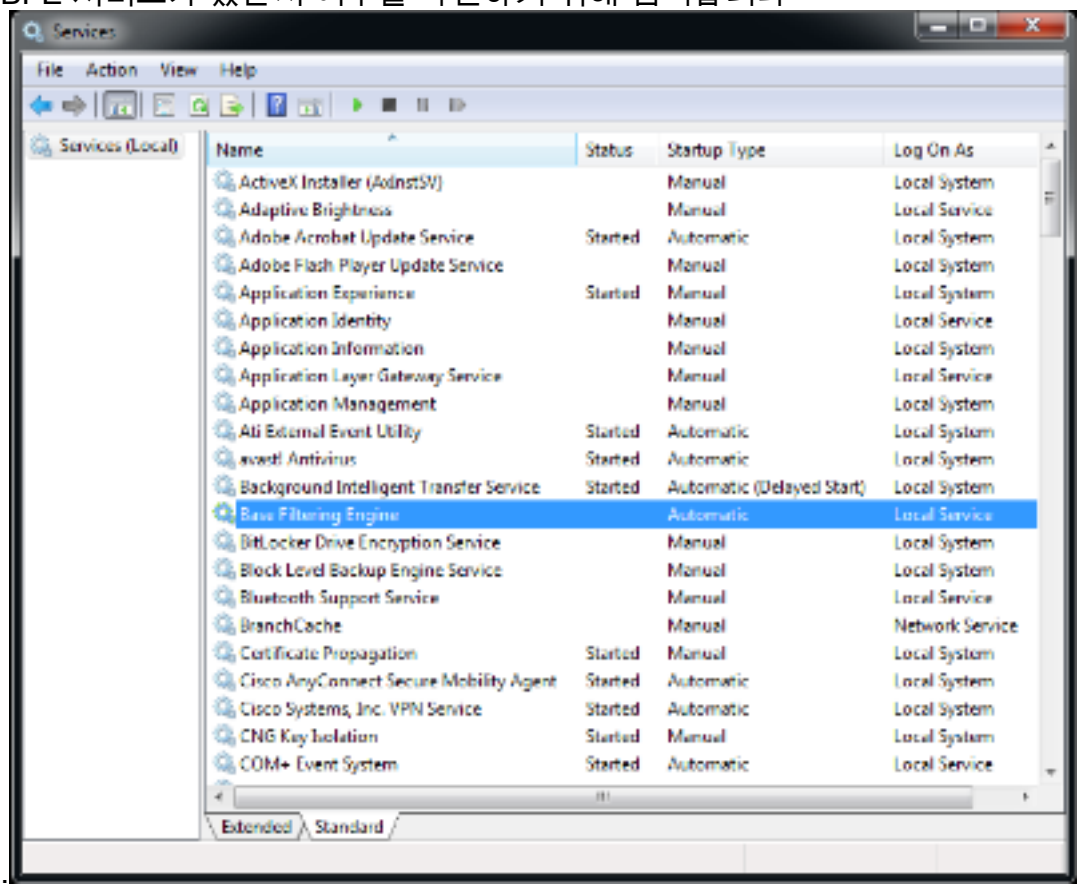
솔루션

이러한 오류 메시지가 표시되면 BFE가 실제로 비활성화되었는지/누락되었는지 또는 클라이언트가 이를 인식할 수 없는지 확인하는 것이 중요합니다.문제를 해결하려면 다음 단계를 완료하십시오.

1. Windows 메뉴에서 SCM(서비스 제어 관리자)에 액세스합니다



2. BFE 서비스가 있는지 여부를 확인하기 위해 검색합니다



서비스가 작동하면 상태가 **시작됨**으로 **표시됩니다**.해당 열에 다른 내용이 있는 경우 서비스에 문제

가 있습니다.그러나 상태가 시작됨으로 표시되면 클라이언트가 서비스와 통신할 수 없는 것이 분명하며 버그가 있을 수 있습니다.

서비스가 비활성화되었거나 시작되지 않은 경우 가능한 원인은 다음과 같습니다.

- 앞서 설명한 것처럼 악성코드는 이 서비스를 첫 번째 단계로 비활성화합니다.
- 컴퓨터의 레지스트리가 손상되었습니다.

복구 절차

첫 번째 단계는 바이러스 백신 소프트웨어로 시스템을 검사하고 소독하는 것입니다 .Win32/Sireef(ZeroAccess) 트로이 목마에 의해 다시 삭제될 경우 BFE 서비스를 복원해서는 안 됩니다.이 웹 페이지에서 ESET SirefCleaner 도구를 다운로드하고 데스크톱에 저장합니다.

이 비디오에서는 Win32/Sireef(ZeroAccess) 트로이 목마를 제거하는 절차에 대해 설명합니다.

Win32/Sireef(ZeroAccess) 트로이 목마를 제거하려면 어떻게 합니까?

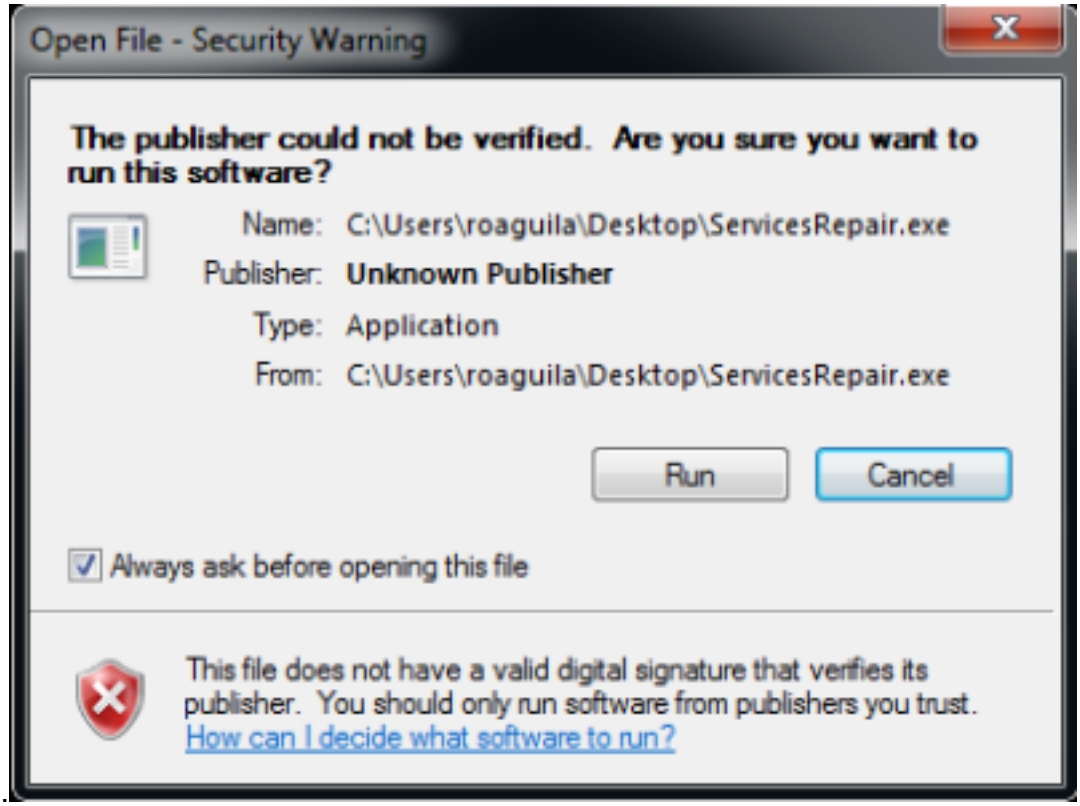
Win32/Sireef(ZeroAccess) 트로이 목마를 제거한 후 BFE 서비스를 시작할 수 있으며 정상적으로 활성 상태로 유지할 수 있는지 확인하십시오.이를 위해 다음을 수행합니다.

1. SCM을 시작하고 **표준** 대신 **확장** 탭을 선택합니다.
2. BFE 서비스를 선택합니다.
3. 왼쪽에서 **시작** 옵션을 선택합니다.

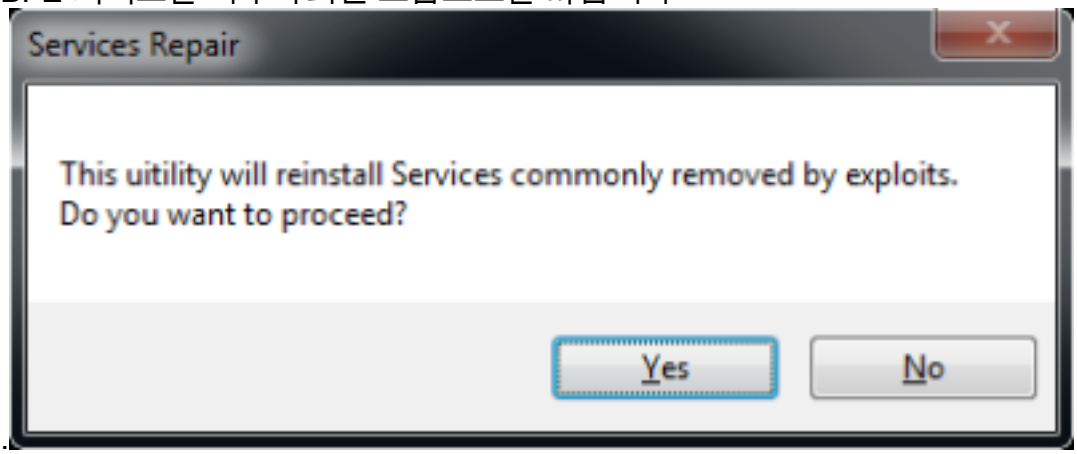
   주의:이 절차를 시도하기 전에 파일을 백업하는 것이 좋습니다.이 문서의 모든 정보는 특정 목적에 대한 정확성, 완전성 또는 적합성에 대한 어떠한 명시적 또는 묵시적 보증도 없이 그대로 제공됩니다.

이 절차가 작동하지 않으면 다음 단계를 완료합니다.

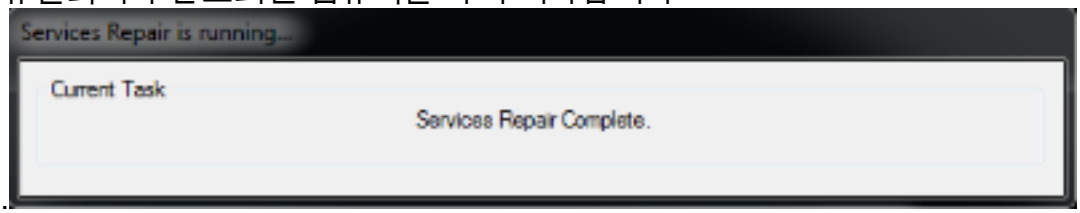
1. 이 웹 페이지에서 ESET 서비스복구 유틸리티를 다운로드하여 데스크톱에 저장합니다.
2. ESET 서비스복구 유틸리티를 실행합니다

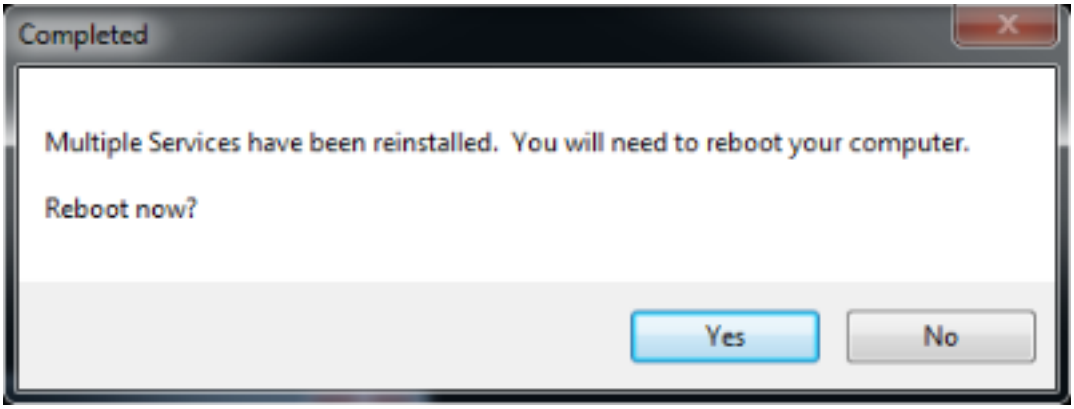


3. BFE 서비스를 복구하려면 프롬프트를 따릅니다



4. 유틸리티가 완료되면 컴퓨터를 다시 시작합니다





5. 컴퓨터가 다시 시작되면 AnyConnect Secure Mobility Client를 다시 설치하거나 실행합니다.

참고:이 도구는 레지스트리 파일이 손상되거나 서비스가 손상된 대부분의 경우에 도움이 됩니

다.따라서 이러한 오류 메시지가 나타나면 이 툴도 유용합니다.
- VPN 클라이언트 에이전트가 프로세스 간 통신 저장소를 만들 수 없습니다.
- VPN 에이전트 서비스가 응답하지 않습니다.1분 후에 이 응용 프로그램을 다시 시작하십시오.
- 로컬 컴퓨터의 Cisco Anyconnect Secure Mobility Agent 서비스가 시작되어 중지되었습니다.일부 서비스는 다른 서비스 또는 프로그램에서 사용하지 않는 경우 자동으로 중지됩니다.