AnyConnect セキュア モビリティの接続エラー：「VPN Client は IP フィルタリングをセットアップできませんでした」

目次

概要

このドキュメントでは、次の Cisco AnyConnect セキュア モビリティ クライアント VPN ユーザ メッセージが表示された場合の対処方法を説明します。

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

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Windows Vista および Windows 7 オペレーティング システムのみに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

背景説明

ベース フィルタ エンジン（BFE）サービス

BFE は、ファイアウォールおよびインターネット プロトコル セキュリティ（IPsec）のポリシーを管理し、ユーザ モード フィルタリングを実装するサービスです。 BFE サービスを停止または無効化すると、システムのセキュリティが大幅に低下します。 また、IPSec の管理およびファイアウォール アプリケーションの予測できない動作が発生します。

次のシステム コンポーネントは BFE サービスに依存します。

- インターネット キー交換（IKE）および認証済みインターネット プロトコル（AuthIP）IPsec のキー モジュール
- インターネット接続共有（ICS）
- IPsec ポリシー エージェント
- ルーティングとリモート アクセス
- Windows ファイアウォール

AnyConnect セキュア モビリティ クライアントは、ホスト マシンのルーティングとリモート アクセスを変更します。 IKEv2 も IKE モジュールに依存します。 つまり、BFE サービスが停止すると、AnyConnect セキュア モビリティ クライアントをインストールできないか、AnyConnect セキュア モビリティ クライアントを使用してセキュア ソケット レイヤ（SSL）接続を確立できません。

感染プロセスの最初のステップとして BFE サービスを無効化および削除する脅威が活発になっています。

Win32/Sirefef（ZeroAccess）（トロイの木馬）

Win32/Sirefef（ZeroAccess）はトロイの木馬であり、ステルス技術を使用して自身の存在をコンピュータから隠すマルチコンポーネント マルウェア ファミリです。 この脅威が発生すると、攻撃者がシステムに対する完全なアクセス権を取得できる可能性があります。 その特性のため、感染の種類に応じてペイロードが大きく異なることがあります。感染した場合の一般的な動作は次のとおりです。

- 任意のファイルをダウンロードして実行する。
- リモート ホストに接続する。
- セキュリティ機能を無効化する。

この脅威に関連する一般的な症状はありません。 インストールされているアンチウイルス ソフトウェアからのアラート通知が唯一の症状になる場合があります。

Win32/Sirefef（ZeroAccess）は、次のようなセキュリティ関連のサービスを停止および削除しようとします。

- Windows Defender サービス（windefend）
- IP Helper Service（iphlpsvc）

- Windows セキュリティ センター サービス (wscsvc)
- Windows ファイアウォール サービス (mpssvc)
- ベース フィルタ エンジン サービス (bfe)

注意： Win32/Sirefef (ZeroAccess) は、高度なステルス技術を使用して自身の検知と削除を妨げる危険な脅威です。 この脅威からの感染の結果、一部の Windows セキュリティ機能の修復と再設定が必要になる場合があります。

問題

シナリオは次のとおりです。

- AnyConnect セキュア モビリティ クライアントがインストールされず、次のエラー メッセージが表示されました。「The VPN client was unable to setup IP filtering. A VPN connection will not be established.」
- 最初は AnyConnect セキュア モビリティ クライアントが正常に動作していました。 一方、エンド ユーザが接続を確立できなくなり、次のエラー メッセージを受け取りました。「Anyconnect was not able to establish a connectoin to the specified secure gateway. Please try connecting again.」

解決策

これらのエラー メッセージが表示された場合、BFE が実際に無効化されていたり欠落したりしているのか、またはクライアントが BFE を認識できないのかを確認することが重要です。 トラブルシューティングを行うために、次の手順を実行します。

1. Windows メニューからサービス コントロール マネージャ (SCM) にアクセスします。
2. BFE サービスを探して、BFE サービスがあるかどうかを確認します。

BFE サービスが動作している場合、そのステータスは [Started] と表示されます。 それ以外のステータスになっている場合は、BFE サービスに問題があります。 ただし、ステータスが [Started] と表示されていて、クライアントが BFE サービスと通信できない場合は、バグがある可能性があります。

BFE サービスが無効化されているか、開始されていない場合は、次の原因が考えられます。

- 前述したように、マルウェアが最初のステップとして BFE サービスを無効化している。
- マシンのレジストリが破損している。

修復手順

最初に、アンチウイルス ソフトウェアでシステムをスキャンし、感染を除去します。 Win32/Sirefef (ZeroAccess) によって BFE サービスが再度削除された場合は、BFE サービスを修復できません。 この Web ページから ESET SirefefCleaner ツールをダウンロードし、デスクトップに保存します。

次のビデオは、Win32/Sirefef (ZeroAccess) を削除する手順を説明しています。

How do I remove Win32/Sirefef (ZeroAccess) trojan?

Win32/Sirefef (ZeroAccess) を削除したら、BFE サービスを開始することができて、通常の方法でアクティブな状態に保持できることを確認します。 確認するには、次の手順を実行します。

1. SCM を起動し、[Standard] タブではなく、[Extended] タブを選択します。
2. BFE サービスを選択します。
3. 左側にある [Start] オプションを選択します。

   注意： この手順を実行する前に、ファイルをバックアップすることを推奨します。 このドキュメントのすべての情報は現状のままで提供され、明示的または暗示的にかかわらず、正確性、完全性、または特定目的への適合性を保証するものではありません。

上記の手順で上手くいかない場合は、次の手順を実行してください。

1. この Web ページから ESET ServicesRepair ユーティリティをダウンロードし、デスクトップに保存します。
2. ESET ServicesRepair ユーティリティを実行します。
3. プロンプトに従って、BFE サービスを修復します。
4. このユーティリティを使った修復が完了したら、コンピュータを再起動します。
5. コンピュータが再起動したら、AnyConnect セキュア モビリティ クライアントを再インストールするか、再実行します。

   注: レジストリ ファイルが破損していたり、サービスが動作しないなどのほとんどのケースで、このツールが役立つことが証明されています。 したがって、次のような エラー メッセージが表示された場合でも、このツールが役立ちます。
   - The VPN client agent was unable to create the interprocess communication depot.
   - The VPN agent service is not responding. Please restart this application after a minute.
   - The Cisco Anyconnect Secure Mobility Agent service on Local Computer started and stopped. Some services stop automatically if they are not in use by other services or programs.