Erreur sécurisée de connexion de mobilité d'AnyConnect : « Le client vpn ne pouvait pas installer le filtrage IP »

Contenu

Introduction

Ce document décrit quoi faire quand vous enounter ce message d'utilisateur du Client à mobilité sécurisé Cisco AnyConnect VPN :

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

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations dans ce document sont basées sur des systèmes d'exploitation de Windows Vista et de Windows 7 seulement.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le service de filtrage de base d'engine (BFE)

Le BFE est un service qui gère le Pare-feu et les stratégies d'IPSec (IPsec) et implémente le filtrage de mode utilisateur. La Sécurité du système est sensiblement réduite si vous arrêtez ou désactivez le service de BFE. Il a également comme conséquence le comportement imprévisible dans des applications de Gestion et de Pare-feu d'IPsec.

Ces composants système dépendent du service de BFE :

- Échange de clés Internet (IKE) et Internet Protocol authentifié (AuthIP) IPsec introduisant des modules
- Partage de connexion internet (ICS)
- Agent de stratégie d'IPsec
- Routage et Accès à distance
- Pare-feu Windows

Le client sécurisé de mobilité d'AnyConnect apporte des modifications de routage et d'Accès à distance à l'ordinateur hôte. L'IKEv2 dépend également des modules d'IKE. Ceci signifie que, si le service de BFE est arrêté, le client sécurisé de mobilité d'AnyConnect ne peut pas être installé ou utilisé pour établir une connexion de Secure Sockets Layer (SSL).

Il y a des menaces dans la circulation monétaire qui désactivent et enlèvent le service de BFE dans un premier temps dans le procédé d'infection.

Cheval de Troie (à temps d'attente nul) Win32/Sirefef

Cheval de Troie (à temps d'attente nul) Win32/Sirefef est une famille à plusieurs éléments du malware qui emploie le stealth pour masquer sa présence sur votre ordinateur. Cette menace donne à des attaquants l'accès complet à votre système. En raison de sa nature, la charge utile pourrait varier considérablement d'une infection à l'autre, bien que le comportement commun inclue :

- Téléchargement et exécution des fichiers arbitraires.
- Contact des serveurs distants.
- Désactivation des fonctionnalités de sécurité.

Il n'y a aucun symptôme commun associé avec cette menace. Les notifications vigilantes du logiciel anti-virus installé pourraient être les seuls symptômes.

Tentatives (à temps d'attente nul) de cheval de Troie Win32/Sirefef d'arrêter et supprimer ces services liés à la sécurité :

- Service de Windows Defender (windefend)
- Service d'aide IP (iphlpsvc)
- Service de Windows Security Center (wscsvc)

- Service de pare-feu Windows (mpssvc)
- Service de filtrage de base d'engine (bfe)

Attention : Cheval de Troie (à temps d'attente nul) Win32/Sirefef est une menace dangereuse qui emploie des techniques avancées de stealth afin de gêner sa détection et suppression. Par conséquent infection avec cette menace, vous pouvez devoir réparer et modifier quelques caractéristiques de protection windows.

Problème

Les scénarios sont :

- L'utilisateur ne peut pas installer le client sécurisé de mobilité d'AnyConnnect et reçoit le message d'erreur, « le client vpn ne pouvait pas installer le filtrage IP. Une connexion VPN ne sera pas établie. »
- Le client sécurisé de mobilité d'AnyConnect fonctionné bien au commencement. Cependant ; l'utilisateur final peut plus n'établir une connexion et reçoit le message d'erreur, « Anyconnect ne pouvait pas établir un connectoin au spécifié sécurisent la passerelle. Veuillez essayer se connecter de nouveau. »

Solution

Quand ces messages d'erreur sont vus, il est important de confirmer si le BFE est désactivé réellement/manquant ou si le client ne peut pas l'identifier. Le troublehoot, se terminent ces étapes :

1. Accédez au gestionnaire de contrôle des services (SCM) du menu de Windows :
2. Recherchez le service de BFE afin de confirmer sa présence ou absence.

Si le service fonctionne, les affichages d'état comme **commencés**. S'il y a toute autre chose dans cette colonne, il y a un problème avec le service. Cependant, si les affichages d'état comme commencés, le client ne peut clairement pas communiquer avec le service, et lui y a possible il est une bogue.

Si le service est désactivé ou pas commencé, quelques possibles raison sont :

- Le malware, comme précédemment expliqué, désactive ce service dans un premier temps.
- Corruption de registre sur l'ordinateur.

Procédure de réparation

La première étape est de balayer et désinfecter votre système avec un logiciel anti-virus. Vous ne devriez pas restaurer le service de BFE s'il sera supprimé de nouveau par cheval de Troie (à temps d'attente nul) Win32/Sirefef. Téléchargez l'outil ESET SirefefCleaner de cette page Web, et sauvegardez-le à votre appareil de bureau.

Ce vidéo explique la procédure pour retirer cheval de Troie (à temps d'attente nul) Win32/Sirefef :.

Comment est-ce que je retire cheval de Troie (à temps d'attente nul) Win32/Sirefef ?

Une fois que vous avez retiré cheval de Troie (à temps d'attente nul) Win32/Sirefef, vérifiez que le service de BFE peut être commencé et active gardé par des moyens normaux. Afin de faire ceci :

1. Commencez le SCM et choisissez l'onglet **étendu** au lieu de la **norme**.
2. Choisissez le service de BFE.
3. Choisissez l'**option Start** du côté gauche.

   Attention : L'il est conseillé de sauvegardent vos fichiers avant que vous tentiez cette procédure. Toute l'information dans l'article est fournie comme est, sans n'importe quelle garantie, si exprès ou implicite, de sa précision, exhaustivité, ou adéquation pour un usage particulier.

Si cette procédure ne fonctionne pas, terminez-vous ces étapes :

1. Téléchargez l'utilitaire ESET ServicesRepair de cette page Web, et sauvegardez-le à votre appareil de bureau.
2. Exécutez l'utilitaire ESET ServicesRepair.
3. Suivez les demandes afin de réparer le service de BFE.
4. Une fois que l'utilitaire termine, redémarrez votre ordinateur.
5. Une fois que vos redémarrages de l'ordinateur, installent ou exécutent le client sécurisé de mobilité d'AnyConnect de nouveau.

   Remarque: Les tests ont prouvé que cet outil aide dans la plupart des cas où les fichiers du registre sont corrompus ou des services sont endommagés. Par conséquent, si vous rencontrez ces messages d'erreur, cet outil s'avère utile trop :
   - L'agent de client vpn ne pouvait pas créer le dépôt de communication entre processus.
   - Le service d'agent VPN ne répond pas. Veuillez redémarrer cette application après une minute.
   - Le service sécurisé d'agent de mobilité de Cisco Anyconnect sur l'ordinateur local démarré et arrêté. Un certain arrêt de services automatiquement s'ils sont non utilisables par d'autres services ou programmes.