أطخ AnyConnect Secure Mobility Connection: "تعذر على عميل VPN إعداد تصفية IP"

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
خدمة محرك التصفية الأساسي (BFE)
نظام التشغيل Win32/Sirefef (ZeroAccess) Trojan
المشكلة
الحل
إجراء الإصلاح

المقدمة

يصف هذا وثيقة ماذا أن يفعل عندما يعين أنت هذا cisco AnyConnect يأمن حركية زبون VPN مستعمل رسالة:

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

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى نظامي التشغيل Windows Vista و Windows 7 فقط.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

خدمة محرك التصفية الأساسي (BFE)

BFE هي خدمة تقوم بإدارة جدار الحماية ونهج أمان بروتوكول الإنترنت (IPsec) وتنفيذ تصفية وضع المستخدم. يتم تقليل أمان النظام بشكل ملحوظ إذا قمت بإيقاف خدمة BFE أو تعطيلها. كما يؤدي إلى سلوك غير متوقع في تطبيقات إدارة IPsec وجدار الحماية.

تعتمد مكونات النظام هذه على خدمة BFE:

- وحدات تضمين IPsec الخاصة بتبادل مفتاح الإنترنت (IKE) وبروتوكول الإنترنت المعتمد (AuthIP)
- مشاركة اتصال الإنترنت (ICS)
- وكيل سياسة IPsec
- التوجيه والوصول عن بعد
- جدار حماية Windows

يجري AnyConnect Secure Mobility Client تغييرات في كل من التوجيه والوصول عن بعد للجهاز المضيف. ويعتمد IKEv2 أيضا على وحدات IKE. وهذا يعني أنه في حالة إيقاف خدمة BFE، لا يمكن تثبيت AnyConnect Secure Mobility Client أو إستخدامه لإنشاء اتصال طبقة مآخذ التوصيل الآمنة (SSL).

هناك تهديدات في التداول النشط تقوم بتعطيل خدمة BFE وإزالتها كخطوة أولى في عملية العدوى.

نظام التشغيل Win32/Sirefef (ZeroAccess) Trojan

يعد Win32/Sirefef (ZeroAccess) طروادة مجموعة متعددة المكونات من البرامج الضارة التي تستخدم التسلل لإخفاء وجودها على الكمبيوتر. يتيح هذا التهديد للمهاجمين الوصول الكامل إلى النظام الذي بحوزتك. ونظرا لطبيعة الحمولة فقد تختلف كثيرا من عدوى إلى أخرى، على الرغم من أن السلوك الشائع يشمل:

- تنزيل الملفات العشوائية وتنفيذها.
- جهة اتصال البيئات المضيفة البعيدة.
- تعطيل ميزات الأمان.

لا توجد أعراض شائعة مرتبطة بهذا التهديد. قد تكون إعلامات التنبيه من برنامج مكافحة الفيروسات المثبت هي الأعراض الوحيدة.

يحاول طروادة Win32/Sirefef (ZeroAccess) إيقاف هذه الخدمات المتعلقة بالأمان وحذفها:

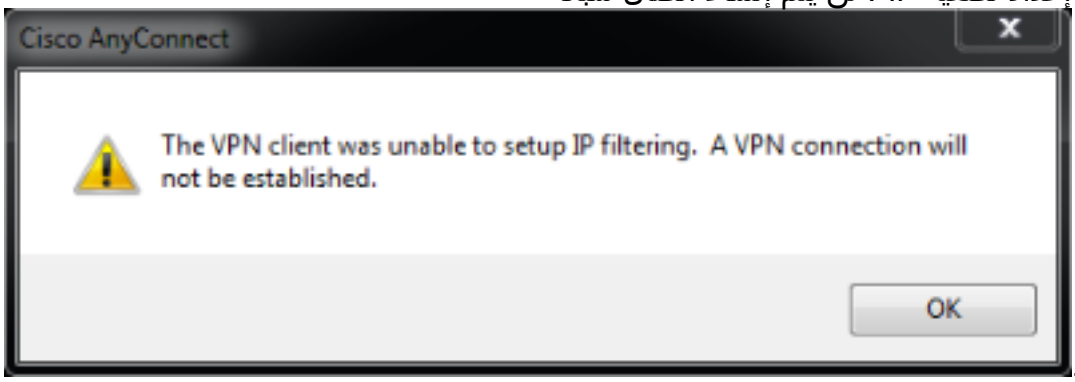
- خدمة WinDefense) Windows Defender)
- خدمة مساعد iPHLPSVC) IP)
- خدمة مركز أمان WSCSVC) Windows)
- خدمة جدار حماية mpssvc) Windows)
- خدمة محرك التصفية الأساسي (BFE)

تحذير: يشكل فيروس Win32/Sirefef (ZeroAccess) تهديدا خطيرا يستخدم تقنيات التخفي المتقدمة لإعاقة اكتشافه وإزالته. نتيجة للإصابة بهذا التهديد، قد تحتاج إلى إصلاح بعض ميزات أمان Windows وإعادة تكوينها.

المشكلة

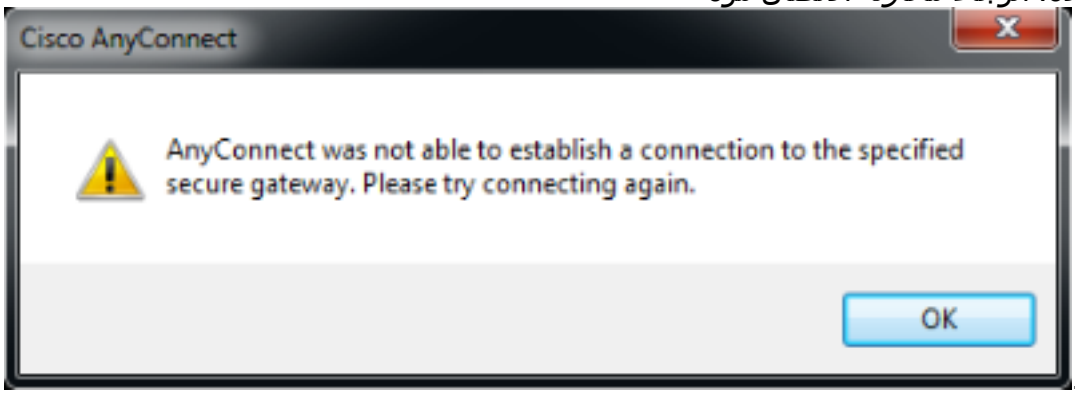
السيناريوهات هي:

- يتعذر على المستخدم تثبيت AnyConnect Secure Mobility Client واستلام رسالة الخطأ، "تعذر على عميل VPN إعداد تصفية IP". لن يتم إنشاء اتصال شبكة



VPN.

- عمل AnyConnect Secure Mobility Client بشكل جيد في البداية. ومع ذلك، لم يعد بإمكان المستخدم النهائي إنشاء اتصال ويستلم رسالة الخطأ، لم يكن AnyConnect قادرا على إنشاء اتصال بالبوابة الآمنة المحددة. الرجاء محاولة الاتصال مرة

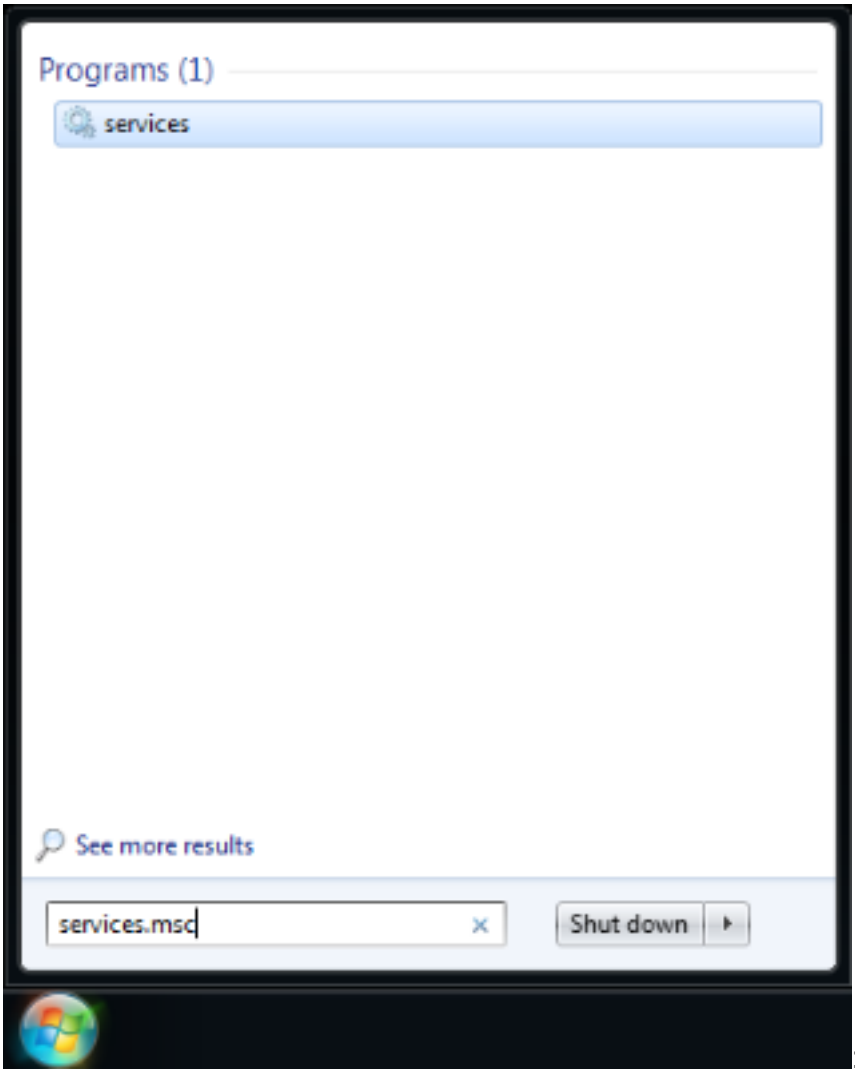


أخرى.

الحل

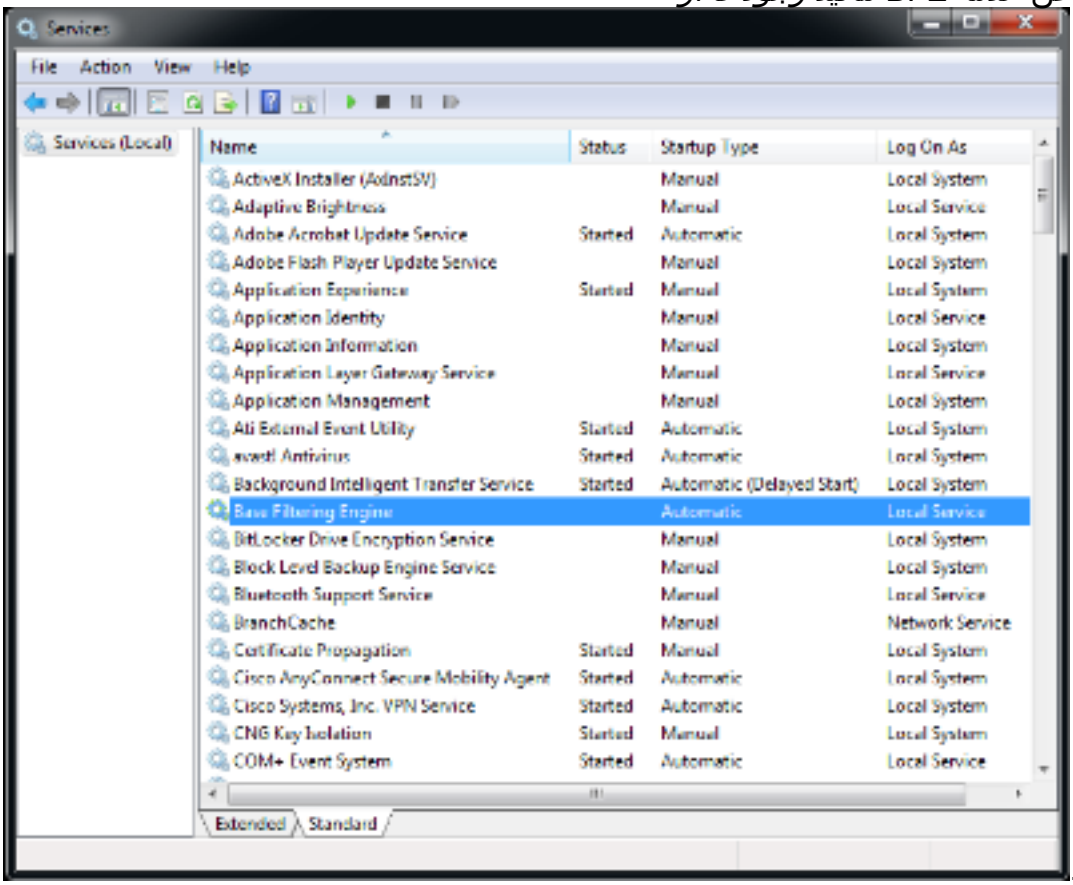
عند رؤية رسائل الخطأ هذه، من المهم تأكيد ما إذا كان BFE معطلا/مفقودا بالفعل أو ما إذا كان العميل غير قادر على التعرف عليه. أتمت in order to أعجزت، هذا steps:

1. الوصول إلى مدير التحكم في الخدمة (SCM) من قائمة



Windows:

2. ابحث عن خدمة BFE لتأكيد وجودها أو



غيابها.

إذا كانت الخدمة تعمل، فإن الحالة تعرض **كتم البدء**. إذا كان هناك أي شيء آخر في هذا العمود، فتوجد مشكلة في

الخدمة. ومع ذلك، إذا كانت الحالة تعرض كما بدأت، فمن الواضح أن العميل غير قادر على الاتصال بالخدمة، ومن المحتمل أن يكون هناك خطأ.

في حالة تعطيل الخدمة أو عدم بدئها، تكون بعض الأسباب المحتملة هي:

- تقوم البرامج الضارة، كما تم توضيحه مسبقا، بتعطيل هذه الخدمة كخطوة أولى.
- تلف التسجيل على الجهاز.

إجراء الإصلاح

تتمثل الخطوة الأولى في فحص النظام لديك وتطهيره باستخدام برنامج لمكافحة الفيروسات. لا يجب إستعادة خدمة BFE إذا كانت سيتم حذفها مرة أخرى بواسطة Win32/Sirefef (ZeroAccess). قم بتنزيل أداة ESET SirefefCleanTool من صفحة الويب هذه واحفظها على سطح المكتب.

يشرح هذا الفيديو إجراء إزالة تروجان Win32/Sirefef (ZeroAccess):.

كيف يمكنني إزالة طروادة Win32/Sirefef (ZeroAccess)؟

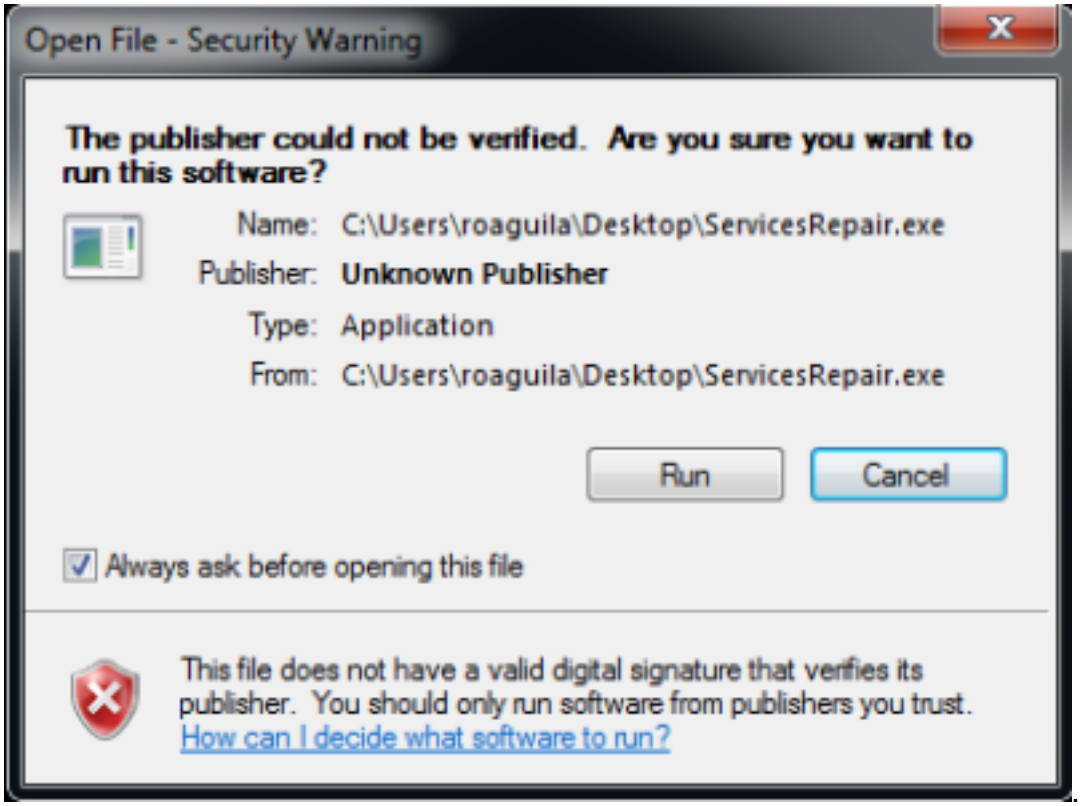
بمجرد إزالة تروبان Win32/Sirefef (ZeroAccess)، تحقق من إمكانية بدء خدمة BFE وإبقائها نشطة بالوسائل العادية. للقيام بذلك:

1. قم بتشغيل SCM واختر علامة التبويب **الموسعة** بدلا من **القياسي**.
2. أختر خدمة BFE.
3. أختر خيار **البدء** الموجود على اليسار.

تحذير: من الممارسات الجيدة نسخ ملفاتك إحتياطيا قبل محاولة إجراء هذا الإجراء. يتم توفير جميع المعلومات الواردة في هذه المادة كما هي، دون أي ضمان، سواء كان صريحا أو ضمنيا، بدقتها أو اكتمالها أو ملاءمتها لغرض معين.

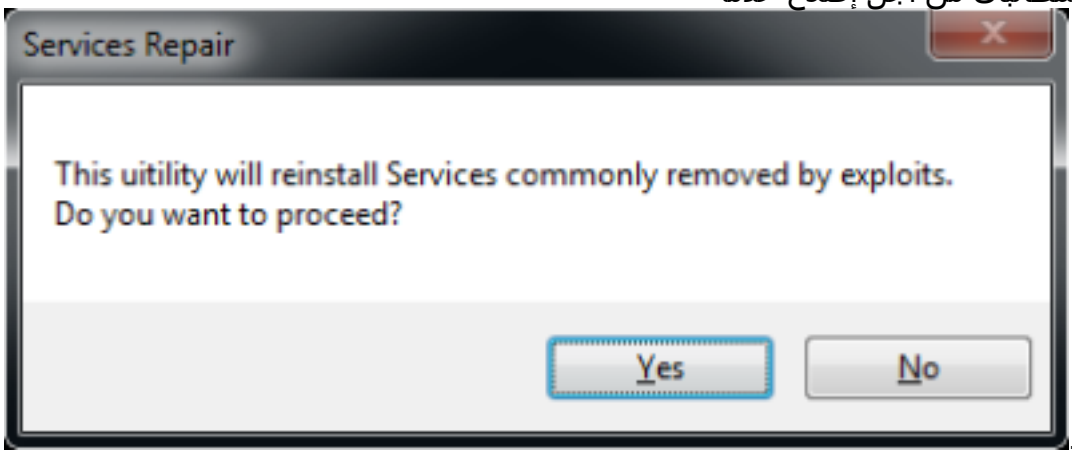
إذا لم ينجح هذا الإجراء، أكمل الخطوات التالية:

1. قم بتنزيل أداة ESET ServicesRepair المساعدة من صفحة الويب هذه واحفظها على سطح المكتب.
2. تنفيذ أداة إصلاح خدمات



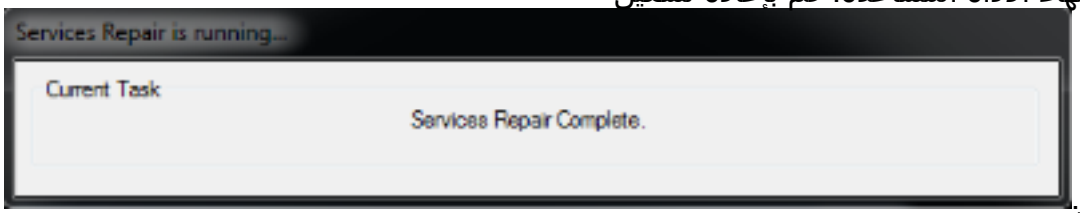
.ESET

3. اتبع المطالبات من أجل إصلاح خدمة

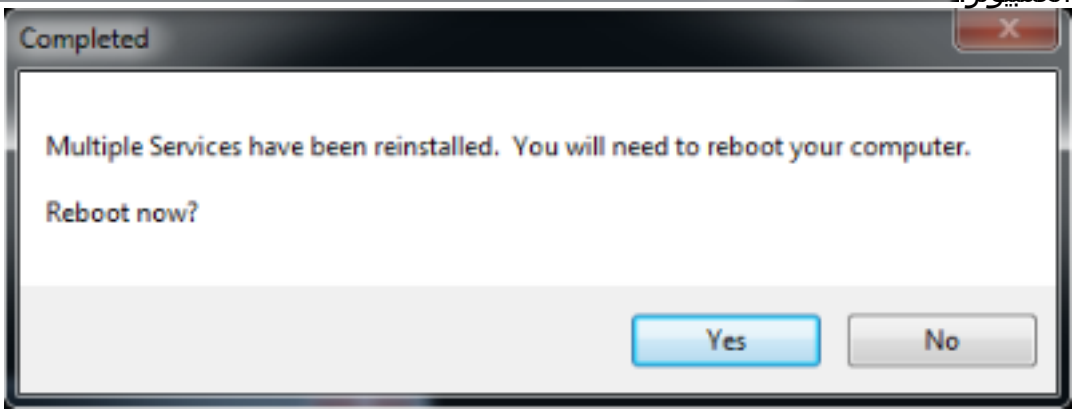


.BFE

4. بمجرد انتهاء الأداة المساعدة، قم بإعادة تشغيل



الكمبيوتر.



5. بمجرد إعادة تشغيل الكمبيوتر، قم بتثبيت AnyConnect Secure Mobility Client أو تنفيذه مرة أخرى.

ملاحظة: أظهرت الاختبارات أن هذه الأداة تساعد في معظم الحالات التي تكون فيها ملفات السجل تالفة أو

الخدمات تالفة. لذلك، إذا واجهت رسائل الخطأ هذه، فإن هذه الأداة تثبت أنها مفيدة أيضا:
- تعذر على عميل شبكة VPN إنشاء مستودع إتصالات العملية البينية.
- لا تستجيب خدمة وكيل الشبكة الخاصة الظاهرية (VPN). الرجاء إعادة تشغيل هذا التطبيق بعد دقيقة.
- تم بدء خدمة Cisco AnyConnect Secure Mobility Agent على الكمبيوتر المحلي وإيقافها. تتوقف بعض الخدمات تلقائيا إذا لم تكن قيد الاستخدام من قبل خدمات أو برامج أخرى.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).