

Problema con el cliente VPN Anyconnect de Cisco. Servicio BFE dañado.

Síntomas.

El problema que vamos a intentar resolver puede aparecer al instalar por primera vez el cliente Anyconnect o bien, una vez instalado, porque ha dejado de funcionar.

- Cuando no se deja instalar. Aparece este mensaje:

```
There is a problem with the Windows Installer package.
A program run as a part of the setup did not finish as
expected. Contact your support personnel or package
vendor.
```

- Cuando ya está instalado y deja de funcionar. Pueden aparecer dos posibles mensajes. Uno de ellos es:

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

Y el otro es:

```
Anyconnect was not able to establish a connection to the specified
Secure gateway. Please try connecting again.
```

- Lo que aquí se describe sirve también para aquellos casos en los que aparecen los siguientes mensajes de error.

```
- 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.
```

Causa.

El problema lo ha producido un virus (Win32/Sirefef (ZeroAccess) trojan family) que deshabilitado un servicio de seguridad e IPSec del ordenador. Este servicio es el que gestiona, entre otras cosas, el firewall de Windows, y es un servicio de Windows que el cliente Anyconnect necesita para funcionar.

También podría ser que, simplemente, el registro del sistema esté corrupto.

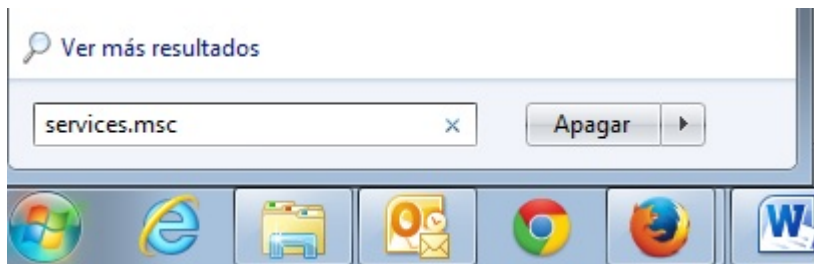
Comprobación.

Lo realmente esencial no es si el Firewall está funcionando o no. Cualquier administrador del equipo podría parar el firewall si así lo desea y eso no produciría ningún problema.

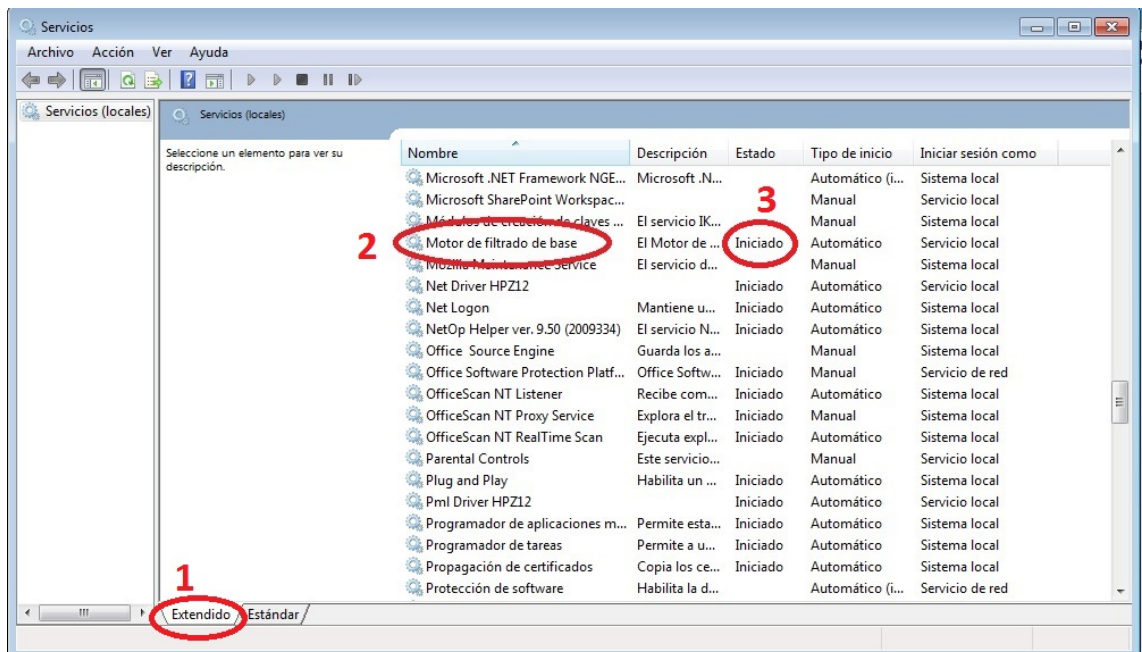
Lo importante aquí es que el firewall de Windows no se puede activar porque se ha deshabilitado y se ha “estropeado” el servicio que le hace funcionar. Es ese servicio el que se necesita.

Pasos de la comprobación.

1. Pulsar en el botón de Inicio de Windows y escribir services.msc en el cuadrado. Luego, pulsar Intro. Vea la imagen.



2. En la ventana resultante, pulse en la pestaña *Extendido*. Baje con la barra de desplazamiento y al llegar a la M, fíjese en el estado del servicio *Motor de filtrado de base*.



El servicio debería aparecer como *Iniciado*.

Si aparece de cualquier otra forma tenemos un problema.

Reparación.

1. Limpieza. Antes que nada, debemos asegurarnos que el posible virus no sigue en el ordenador. No sirve de nada reparar el servicio si el virus vuelve a estropear el servicio.

Aunque usted tenga antivirus, es necesario que ejecute alguna de estas dos herramientas para asegurar que elimina el virus problemático.

- Primera opción. Limpiar solo el virus Win32/Sirefef. Siga las instrucciones de este enlace:

http://kb.eset.com/esetkb/index?page=content&id=SOLN2895&viewlocale=es_ES

- Segunda opción. Hacer una limpieza en profundidad de un montón de posibles virus, no solo Win32/Sirefef.

Descargue, y más tarde instale, la VERSIÓN GRATUITA de la utilidad Malware Bytes (<http://es.malwarebytes.org/>). Vea la imagen siguiente.

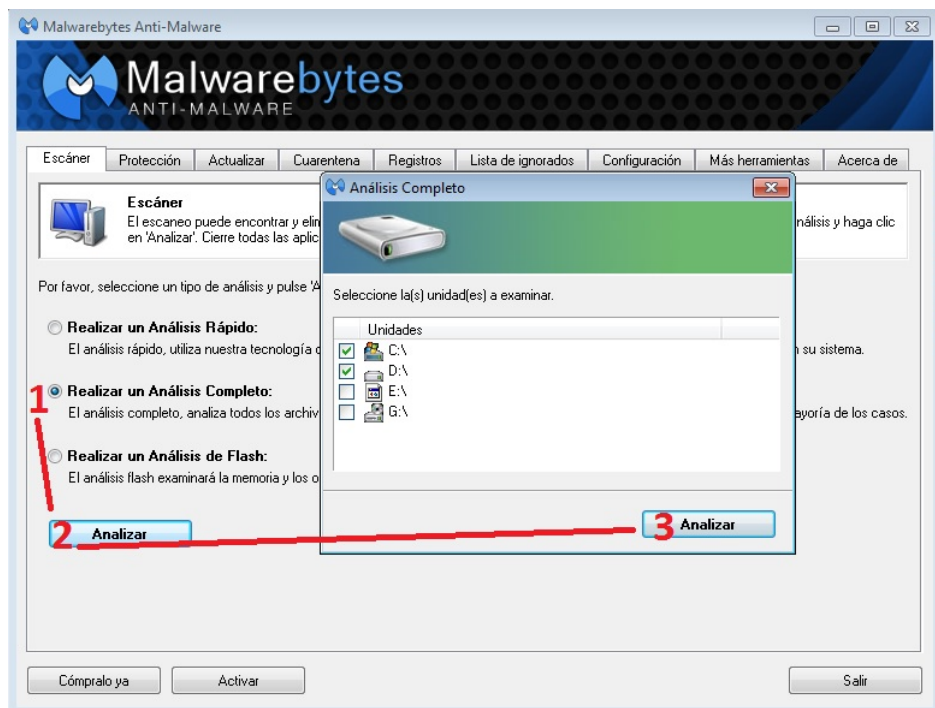


Hay una ventana en la que le propone probar la versión de pago. Haga lo que le parezca. Nosotros recomendamos quedarse en la opción gratuita.

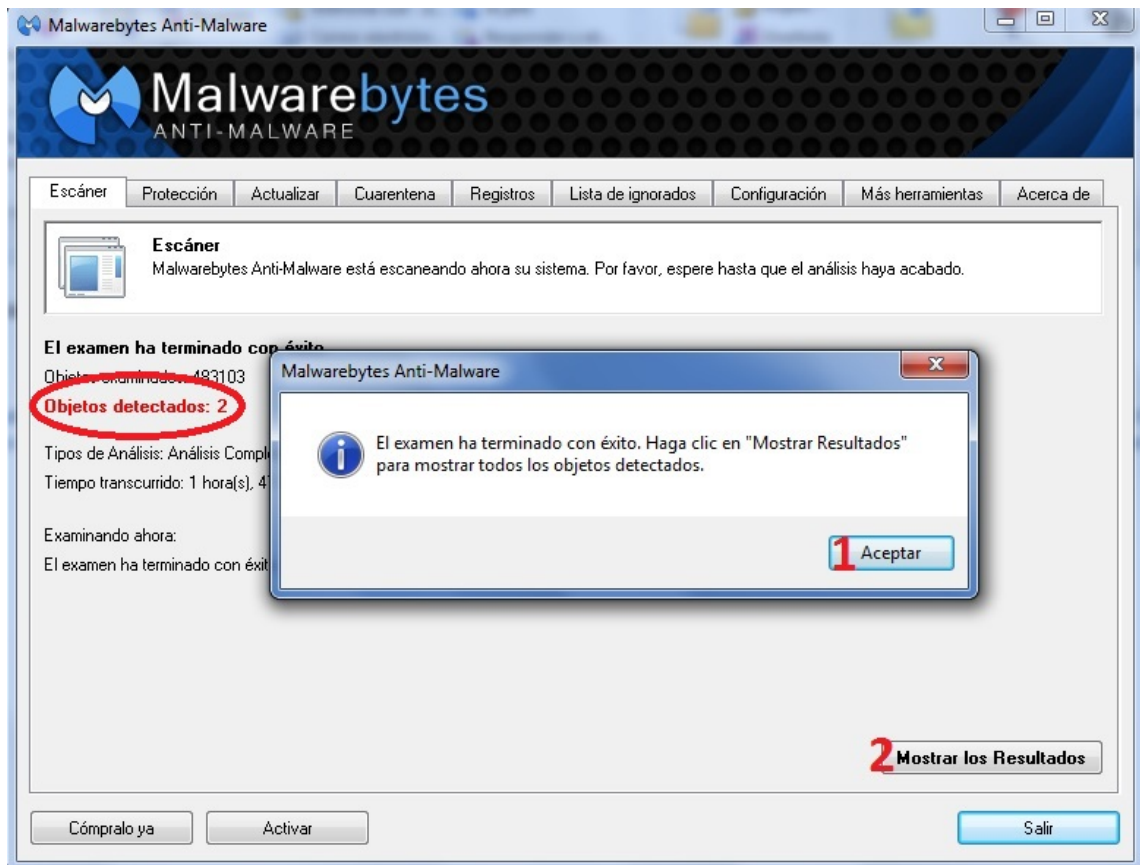
Deje activadas las opciones de actualización y de ejecución al acabar la instalación.



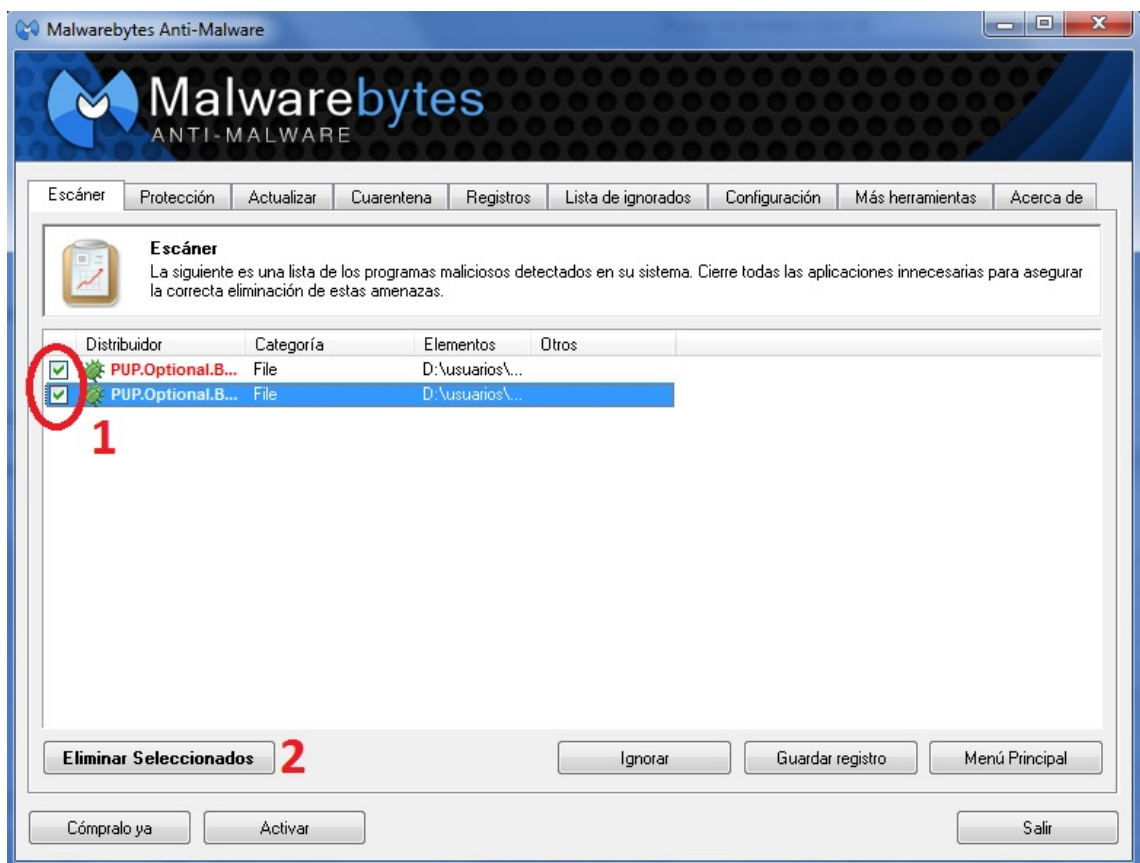
Después haga un escaneo de todo el pc (1). Incluya todos los discos del ordenador (2 y 3). Vea los pasos en la imagen siguiente.



Tardará bastante tiempo, dependiendo del ordenador en cuestión. Una vez termine, debe limpiar las infecciones.



En la siguiente ventana, se mostrarán todas las infecciones detectadas. Selecciónelas todas (1) y pulse en Eliminar Seleccionados (2).

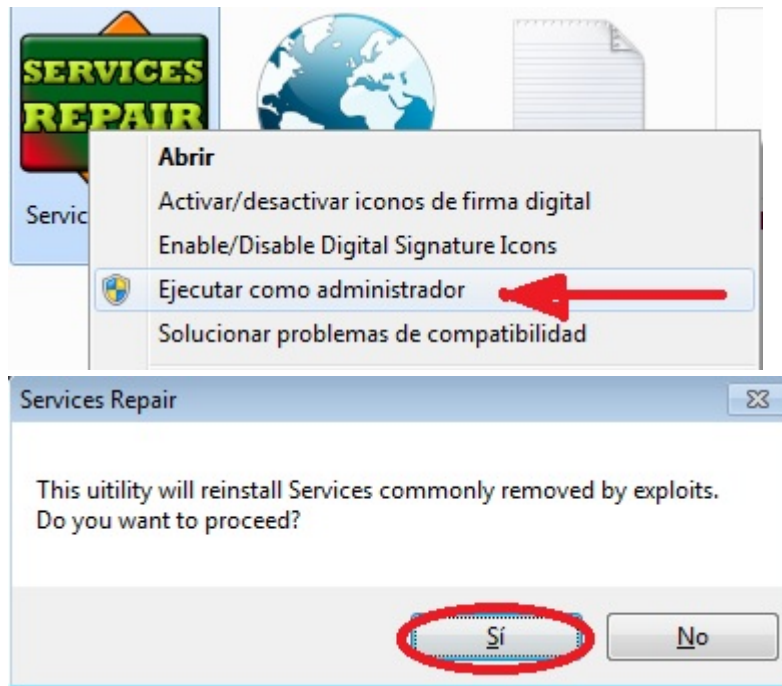


Vaya aceptando y al acabar, siga las indicaciones. Seguramente le pedirá reiniciar.

2. Una vez limpio el ordenador, hay que reparar los servicios que estaban dañados.

Descargue la herramienta de reparación de servicios de ESET (<http://kb.eset.com/library/ESET/KB%20Team%20Only/Malware/ServicesRepair.exe>)

Una vez descargada, ejecútela. Con estas viñetas le indicamos como hacerlo correctamente.



Reinicie el equipo para aplicar cambios. Después del arranque el Anyconnect debería funcionar o bien, debería dejarse instalar.

Referencias.

<http://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116347-technote-anyconnect-00.html>

<http://www.wintips.org/how-to-restore-windows-services-to-their-default-state/>