McAfee®

PC Protection Plus 2007

VirusScan Plus, Backup & Restore

Guía del usuario

Contenido

CAPÍTULO 1

Introducción

McAfee PC Protection Plus Suite protege su equipo contra virus, software espía y piratas informáticos. Podrá navegar y descargar archivos con seguridad y confianza con McAfee siempre activado, actualizándose y protegiéndolo. La protección de confianza de McAfee ofrece copias de seguridad automatizadas que restauran fotos, música, vídeos y otros archivos importantes con un clic. Con McAfee es muy sencillo ver su estado de seguridad, detectar virus y software espía, y asegurar la actualización de los productos con el nuevo McAfee SecurityCenter. Además, recibirá automáticamente el último software y actualizaciones de McAfee con su suscripción.

PC Protection Plus incluye los programas siguientes:

- SecurityCenter
- VirusScan
- Personal Firewall
- Data Backup
- Network Manager
- EasyNetwork (sólo licencia para 3 usuarios)
- SiteAdvisor

CAPÍTULO 2

McAfee SecurityCenter

McAfee SecurityCenter es un entorno de fácil utilización en el que los usuarios de McAfee pueden ejecutar, gestionar y configurar sus suscripciones de seguridad.

SecurityCenter actúa también como fuente de información sobre alertas de virus, información de productos, soporte, información sobre suscripciones y acceso rápido a las herramientas y noticias del sitio Web de McAfee.

En este capítulo

Características

McAfee SecurityCenter ofrece las siguientes funciones y ventajas nuevas:

Estado de protección rediseñado

Facilita la comprobación del estado de seguridad de su equipo, la verificación de actualizaciones y la solución de problemas de seguridad potenciales.

Actualizaciones y mejores continuas

Instalar automáticamente las actualizaciones diarias. Cuando una nueva versión de McAfee está disponible, se obtiene automáticamente sin cargo durante el período que dura la suscripción, garantizando así que siempre tenga una protección actualizada.

Alertas en tiempo real

Las alertas de seguridad indican la aparición de emergencias de virus y amenazas contra la seguridad y ofrecen opciones de respuesta para eliminar la amenaza, neutralizarla u obtener más información sobre ella.

Protección adecuada

Una variedad de opciones nuevas le ayudan a mantener al día su protección con McAfee.

Herramientas de rendimiento

Elimine los archivos no utilizados, los archivos utilizados desfragmentados y utilice la restauración del sistema para que su equipo siga funcionando al máximo rendimiento.

Ayuda online real

Obtenga asistencia por parte de los expertos en seguridad informática de McAfee, a través de chat por Internet, correo electrónico y teléfono.

Protección de navegación segura

Si está instalado, el complemento del navegador de McAfee SiteAdvisor le protege contra software espía, correo basura, virus y fraudes de Internet mediante la clasificación de los sitios Web que visita o que aparecen en los resultados de búsqueda en Internet. Puede visualizar las clasificaciones de seguridad detalladas, que muestran la manera cómo se comprueba un sitio en busca de prácticas de correo electrónico, descargas, afiliaciones en línea y molestias como las ventanas emergentes y las cookies de rastreo de otras personas.

CAPÍTULO 3

Uso de SecurityCenter

Ejecute SecurityCenter desde el icono McAfee SecurityCenter en el área de notificación de Windows que se encuentra en el extremo derecho de la barra de tareas, o bien desde su escritorio de Windows.

Al abrir SecurityCenter, el panel Inicio muestra el estado de seguridad de su equipo y proporciona un acceso rápido a actualizaciones, análisis (si McAfee VirusScan está instalado) y otras tareas comunes:

Encabezado

Ayuda

Ver el archivo de ayuda del programa.

Columna izquierda

Actualizar

Actualice el producto para asegurarse de que está protegido contra las últimas amenazas.

Analizar

Si McAfee VirusScan está instalado, puede realizar un análisis manual de su equipo.

Tareas comunes

Realice tareas comunes, desde volver al panel Inicio, ver los eventos recientes y gestionar su red (si su equipo dispone de capacidad de gestión para esta red) hasta proteger su equipo. Si McAfee Data Backup está instalado, también puede realizar la copia de seguridad de sus datos.

Componentes instalados

Consulte de un vistazo los servicios de seguridad que están protegiendo el equipo.

Panel principal

Estado de protección

En **¿Estoy protegido?** puede consultar el nivel general del estado de protección del equipo. Debajo de éste puede ver un desglose de los estados por categoría y tipo de protección.

Información de SecurityCenter

Consulte en qué momento se realizó la última actualización del equipo y cuándo se ejecutó el último análisis (si McAfee VirusScan está instalado), así como en qué fecha caduca su suscripción.

En este capítulo

Descripción de los iconos de SecurityCenter

Los iconos de SecurityCenter aparecen en el área de notificación de Windows, en el extremo derecho de la barra de tareas. Utilícelos para ver si el equipo está completamente protegido, visualizar el estado de un análisis en curso (si McAfee VirusScan está instalado), comprobar actualizaciones, ver eventos recientes, mantener el equipo y obtener asistencia desde el sitio Web de McAfee.

Abrir SecurityCenter y utilizar las características adicionales

Mientras se está ejecutando SecurityCenter, el icono M de SecurityCenter aparece en el área de notificación de Windows, en el extremo derecho de la barra de tareas.

Para abrir SecurityCenter o utilizar las características adicionales:

- Haga clic con el botón derecho del ratón en el icono principal SecurityCenter y haga clic en una de las siguientes opciones:
  - Abrir SecurityCenter
  - Actualizaciones
  - Vínculos rápidos

    El submenú contiene vínculos a Inicio, Ver eventos recientes, Gestionar red, Mantener equipo y Data Backup (si está instalado).
  - Verificar suscripción

    (Este elemento aparece cuando ha caducado al menos una suscripción de producto.)
  - Centro de actualizaciones
  - Atención al cliente

Comprobar el estado de protección

Si el equipo no está completamente protegido, el icono de estado de protección aparece en el área de notificación de Windows, en el extremo derecho de la barra de estado. El icono puede ser rojo o amarillo, en función del estado de protección.

Para comprobar su estado de protección:

- Haga clic en el icono de estado de protección para abrir SecurityCenter y resolver los problemas que pueda haber.

Comprobar el estado de las actualizaciones

Si está comprobando las actualizaciones, el icono Actualizaciones  aparece en el área de notificación de Windows, en el extremo derecho de la barra de tareas.

Para comprobar el estado de las actualizaciones:

- Seleccione el icono Actualizaciones para ver el estado de las actualizaciones en una breve descripción.

Descripción del estado de protección

El estado de protección de seguridad general de su equipo se muestra en **¿Estoy protegido?** en SecurityCenter.

El estado de protección le notifica si su equipo está completamente protegido contra las últimas amenazas de seguridad o si los problemas requieren de su atención y cómo puede resolverlos. Cuando un problema afecta a más de una categoría de protección, es posible que, al resolverlo, muchas categorías vuelvan al estado de protección total.

Algunos de los factores que influyen en el estado de protección de su equipo son los siguientes: amenazas externas para la seguridad, los productos de seguridad que tenga instalados, productos que acceden a Internet y la configuración de esos productos de seguridad y de Internet.

De forma predeterminada, si la Protección contra correo basura o el Bloqueo de contenido no está instalado, estos problemas de protección no críticos se omiten automáticamente y no se les realiza ningún seguimiento en el estado de protección general. De todos modos, si un problema de protección va seguido de un vínculo **Omitir**, puede elegir la opción de omitir el problema si está seguro de que no desea solucionarlo.

¿Estoy protegido?

Consulte el nivel general del estado de protección de su equipo en **¿Estoy protegido?** en SecurityCenter:

- **Sí** aparece si su equipo está totalmente protegido (verde).
- **No** aparece cuando su equipo está parcialmente protegido (amarillo) o en absoluto protegido (rojo).

Para solucionar la mayoría de los problemas de protección de manera automática, haga clic en **Solucionar** junto al estado de protección. Si a pesar de ello, uno o más problemas persisten y requieren una respuesta de su parte, haga clic en el vínculo que aparece después del problema para realizar la operación sugerida.

Descripción de las categorías y tipos de protección

En **¿Estoy protegido?**, en SecurityCenter, puede ver un desglose de los estados que consiste en estas categorías y tipos de protección:

- Equipo y archivos
- Internet y redes
- Correo electrónico e IM
- Controles paternos

Los tipos de protección mostrados en SecurityCenter dependen de los productos en los que están instalados. Por ejemplo, el tipo de protección de salud del PC aparece si está instalado el software Data Backup de McAfee.

Si una categoría no tiene ningún problema de protección, su estado será Verde. Si hace clic en una categoría verde, aparecerá una lista de tipos de protección habilitados a la derecha y, a continuación, otra lista de los problemas ya omitidos. Si no existe ningún problema, aparece un aviso de virus en lugar de un problema. También puede hacer clic en **Configurar** para cambiar las opciones de esta categoría.

Si todos los tipos de protección dentro de una categoría tienen un estado Verde, entonces el estado de la categoría también es Verde. Y por consiguiente, si todas las categorías de protección tienen un estado Verde, entonces el Estado de protección general también será Verde.

Si alguna categoría de protección tiene un estado Amarillo o Rojo, puede resolver los problemas de protección solucionándolos u omitiéndolos y eso cambiará su estado a Verde.

Descripción de la protección del equipo y los archivos

La categoría de protección del equipo y los archivos consiste en los tipos de protección siguientes:

- **Protección antivirus**: La protección en tiempo real defiende a su equipo de virus, gusanos, troyanos, secuencias de comandos sospechosas, ataques híbridos y otras amenazas. Analiza e intenta limpiar automáticamente los archivos (archivos .exe comprimidos, archivos del sector de arranque, memoria y archivos importantes) cuando el usuario o el equipo acceden a ellos.
- **Protección contra software espía**: La protección contra software espía detecta, bloquea y elimina rápidamente software espía, software publicitario y otros tipos de software potencialmente peligrosos que obtienen y transmiten datos privados sin su autorización.
- **Guardianes del sistema**: Los guardianes del sistema detectan cualquier cambio en el equipo y le alertarán cuando se realice uno. Posteriormente, usted podrá repasar dichos cambios y decidir si desea permitirlos.
- **Protección de Windows**: La protección de Windows proporciona el estado de Windows Update del equipo. Si McAfee VirusScan está instalado, la protección contra desbordamiento de búfer también está disponible.

Uno de los factores que influye en esta protección del equipo y los archivos son las amenazas de virus externos. Por ejemplo, si aparece un brote de virus, ¿la protección antivirus le protege? Asimismo, existen otros factores, como la configuración del software antivirus y el hecho de si éste se actualiza continuamente con los últimos archivos de definiciones para proteger el equipo contra nuevas amenazas.

Abra el panel de configuración de Equipo y archivos

Si no existe ningún problema en **Equipo y archivos**, puede abrir el panel de configuración desde el panel de información

Para abrir el panel de configuración de Equipo y archivos:

1. En el panel Inicio, haga clic en **Equipo y archivos**.
2. En el panel de la derecha, haga clic en **Configurar**.

Descripción de la protección de Internet y redes

La categoría de protección de Internet y redes consiste en los tipos de protección siguientes:

- **Protección por cortafuegos**: La protección por cortafuegos defiende al equipo de intrusiones y tráfico de red no deseado. También le ayuda a gestionar las conexiones de Internet entrantes y salientes.
- **Protección inalámbrica**: La protección inalámbrica defiende a su red inalámbrica doméstica de intrusiones e intercepción de datos. No obstante, si está conectado actualmente a una red inalámbrica externa, su protección variará en función del nivel de seguridad de esa red.
- **Protección para navegación en Internet**: Esta protección oculta los anuncios, ventanas emergentes y microespías mientras navega por Internet en su equipo.
- **Protección contra phishing**: La protección contra phishing ayuda a bloquear los sitios Web fraudulentos que solicitan información personal a través de hipervínculos en el correo electrónico, mensajes instantáneos, ventanas emergentes y otras fuentes.
- **Protección de información personal**: La protección de información personal bloquea la difusión de información confidencial y comprometedora a través de Internet.

Abrir el panel de configuración de Internet y redes

Si no existe ningún problema en **Internet y redes**, puede abrir el panel de configuración desde el panel de información

Para abrir el panel de configuración de Internet y redes:

1. En el panel Inicio, haga clic en **Internet y redes**.
2. En el panel de la derecha, haga clic en **Configurar**.

Descripción de la protección de correo electrónico y de IM

La categoría de protección de correo electrónico y de IM consiste en los tipos de protección siguientes:

- **Protección de correo electrónico**: La protección de correo electrónico analiza y trata de eliminar automáticamente los virus, el software espía y las potenciales amenazas de los mensajes de correo y los archivos adjuntos, tanto entrantes como salientes.
- **Protección contra correo basura**: La protección contra correo basura permite bloquear los mensajes de correo no deseados para que no entren en su Buzón de entrada.
- **Protección de IM**: La protección de mensajes instantáneos (IM) escanea y trata de limpiar automáticamente los archivos adjuntos de los mensajes instantáneos de virus, software espía y amenazas potenciales. También impide que los clientes de mensajería instantánea intercambien contenidos o información personal a través de Internet.
- **Protección de navegación segura**: Si está instalado, el complemento del navegador de McAfee SiteAdvisor le protege contra software espía, correo basura, virus y fraudes de Internet mediante la clasificación de los sitios Web que visita o que aparecen en los resultados de búsqueda en Internet. Puede visualizar las clasificaciones de seguridad detalladas, que muestran la manera cómo se comprueba un sitio en busca de prácticas de correo electrónico, descargas, afiliaciones en línea y molestias como las ventanas emergentes y las cookies de rastreo de otras personas.

Abrir el panel de configuración de Correo electrónico e IM

Si no existe ningún problema en **Correo electrónico e IM**, puede abrir el panel de configuración desde el panel de información

Para abrir el panel de configuración de Correo electrónico e IM

1. En el panel Inicio, haga clic en **Correo electrónico e IM**.
2. En el panel de la derecha, haga clic en **Configurar**.

Descripción de la protección Controles paternos

La categoría de protección Controles paternos consiste en este tipo de protección:

- **Controles paternos**: El Bloqueo de contenido impide a los usuarios visualizar contenido de Internet no deseado mediante el bloqueo de sitios Web potencialmente peligrosos. La actividad y el uso de Internet por parte de los usuarios también se puede controlar y limitar.

Abrir el panel de configuración de Controles paternos

Si no existe ningún problema en **Controles paternos**, puede abrir el panel de configuración desde el panel de información.

Para abrir el panel de configuración de Controles paternos:

1. En el panel Inicio, haga clic en **Controles paternos**.
2. En el panel de la derecha, haga clic en **Configurar**.

Solución de problemas de protección

La mayoría de problemas de protección se pueden solucionar de manera automática. De todos modos, si uno o más problemas persisten, es necesario que los solucione por sí mismo.

Solucionar problemas de protección automáticamente

La mayoría de problemas de protección se pueden solucionar de manera automática.

Para solucionar problemas de protección automáticamente:

- Haga clic en **Solucionar**, que aparece junto al estado de protección.

Solucionar problemas de protección manualmente

Si uno o más problemas de protección no se solucionan automáticamente, haga clic en el vínculo que aparece después del problema para realizar la operación sugerida.

Para solucionar problemas de protección manualmente:

- Siga uno de estos procedimientos:
  - Si no se ha realizado un análisis completo del equipo durante los 30 últimos días, haga clic en **Analizar** a la izquierda del estado de protección principal para realizar el análisis manual. (Este elemento aparece si McAfee VirusScan está instalado.)
  - Si los archivos de definiciones (DAT) no están actualizados, haga clic en **Actualizar**, a la izquierda del estado de protección principal, para actualizar la protección.
  - Si hay un programa sin instalar, haga clic en **Obtener protección total** para instalarlo.
  - Si a un programa le faltan componentes, reinstálelo.
  - Si es necesario registrar un programa para que reciba protección total, haga clic en **Registrar ahora** para registrarlo. (Este elemento aparece si uno o más programas están caducados.)
  - Si ha caducado un programa, haga clic en **Verificar mi suscripción ahora** para comprobar el estado de su cuenta. (Este elemento aparece si uno o más programas están caducados.)

Ver la información de SecurityCenter

En la parte inferior del panel del estado de protección, Información de SecurityCenter proporciona acceso a opciones de SecurityCenter y muestra información relativa a la última actualización, el último análisis (si McAfee VirusScan está instalado) y la caducidad de la suscripción de los productos McAfee de su equipo.

Abrir el panel de configuración de SecurityCenter

Para su mayor comodidad, puede abrir el panel de configuración de SecurityCenter para cambiar las opciones desde el panel Inicio.

Para abrir el panel de configuración de SecurityCenter:

- En el panel Inicio, en **Información de SecurityCenter,** haga clic en **Configurar**.

Ver información del producto instalada

Puede ver una lista de los productos instalados que incluye el número de versión del producto y el momento en que se actualizó por última vez.

Para ver la información de su producto McAfee:

- En el panel Inicio, en **Información de SecurityCenter,** haga clic en **Ver detalles** para abrir la ventana de información del producto.

Uso del menú Avanzado

Cuando abra SecurityCenter por primera vez, el menú Básico aparecerá en la columna de la izquierda. Si es usted un usuario avanzado, puede hacer clic en **Menú Avanzado** para abrir otro menú de comandos más detallado en su lugar. Para su mayor comodidad, el último menú que utilice será el que aparezca la próxima vez que abra SecurityCenter.

El menú Avanzado se compone de los elementos siguientes:

- Inicio
- Informes y registros (incluye la lista Eventos recientes y los registros por tipo de los últimos 30, 60 y 90 días)
- Configurar
- Restaurar
- Herramientas

CAPÍTULO 4

Configuración de las opciones de SecurityCenter

SecurityCenter le muestra el estado de protección de seguridad general del equipo, le permite crear cuentas de usuario McAfee, instala automáticamente las últimas actualizaciones del producto y le informa, mediante alertas y sonidos también automáticos, de la existencia de brotes de virus públicos, amenazas para la seguridad y actualizaciones del producto.

En el panel Configuración de SecurityCenter, puede cambiar las opciones de SecurityCenter por estas características:

- Estado de protección
- Usuarios
- Actualizaciones automáticas
- Acerca de las alertas

En este capítulo

Configuración del estado de protección

El estado de protección de seguridad general de su equipo se muestra en **¿Estoy protegido?** en SecurityCenter.

El estado de protección le notifica si su equipo está completamente protegido contra las últimas amenazas de seguridad o si los problemas requieren de su atención y cómo puede resolverlos.

De forma predeterminada, si la Protección contra correo basura o el Bloqueo de contenido no está instalado, estos problemas de protección no críticos se omiten automáticamente y no se les realiza ningún seguimiento en el estado de protección general. De todos modos, si un problema de protección va seguido de un vínculo **Omitir**, puede elegir la opción de omitir el problema si está seguro de que no desea solucionarlo. Si más adelante decide solucionar un problema previamente omitido, puede incluirlo en el estado de protección para que se le realice un seguimiento.

Configurar problemas omitidos

Puede incluir o excluir problemas del seguimiento como parte del estado de protección general de su equipo. Si un problema de protección va seguido de un vínculo **Omitir**, puede elegir la opción de omitir el problema si está seguro de que no desea solucionarlo. Si más adelante decide solucionar un problema previamente omitido, puede incluirlo en el estado de protección para que se le realice un seguimiento.

Para configurar problemas omitidos:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto a **Estado de protección** para ampliar el panel y después en **Avanzado**.
3. Realice una de las siguientes acciones en el panel Problemas omitidos:
   - Para incluir en el estado de protección los problemas omitidos anteriormente, quite la selección de sus casillas respectivas.
   - Para excluir problemas del estado de protección, seleccione sus casillas respectivas.
4. Haga clic en **Aceptar**.

Configuración de las opciones de usuario

Si ejecuta programas McAfee que requieren permisos de usuario, estos permisos corresponden de forma predeterminada a las cuentas de usuario de Windows de este equipo. Para facilitar la gestión de los usuarios para estos programas, puede pasar a utilizar las cuentas de usuario McAfee en cualquier momento.

Si cambia y utiliza las cuentas de usuario McAfee, se importarán automáticamente del programa Controles paternos todos los nombres de usuario y permisos que pueda haber. De todos modos, la primera vez que cambie de cuentas deberá crear una cuenta de Administrador. Después ya podrá crear y configurar otras cuentas de usuario de McAfee.

Cambiar a las cuentas de usuario de McAfee

De forma predeterminada, se utilizan las cuentas de usuario de Windows. Pero para cambiar a cuentas de usuario de McAfee no es necesario crear cuentas de usuario de Windows adicionales.

Para cambiar a las cuentas de usuario de McAfee:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto a **Usuarios** para ampliar el panel y después en **Avanzados**.
3. Para utilizar las cuentas de usuario de McAfee, haga clic en **Cambiar**.

Si es la primera vez que cambia a cuentas de usuario de McAfee, deberá crear una cuenta de Administrador (página 23).

Crear una cuenta de Administrador

La primera vez que pase a utilizar usuarios de McAfee, se le pedirá que cree una cuenta de Administrador.

Para crear una cuenta de Administrador:

1. Escriba una contraseña en el cuadro **Contraseña** y vuelva a escribirla en el cuadro **Confirmar contraseña**.
2. Seleccione de la lista una pregunta para la recuperación de la contraseña y escriba la respuesta a la pregunta secreta en el cuadro **Respuesta**.
3. Haga clic en **Aplicar**.

   Cuando haya terminado, el tipo de cuenta de usuario estará actualizado en el panel con los nombres de usuario y los permisos ya existentes del programa Controles paternos, en el caso de que hubiera alguno. Si ésta es la primera vez que

configura cuentas de usuario, aparecerá el panel Gestión de usuarios.

Configurar las opciones de usuario

Si cambia y utiliza las cuentas de usuario McAfee, se importarán automáticamente del programa Controles paternos todos los nombres de usuario y permisos que pueda haber. De todos modos, la primera vez que cambie de cuentas deberá crear una cuenta de Administrador. Después ya podrá crear y configurar otras cuentas de usuario de McAfee.

Para configurar las opciones de usuario:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto a **Usuarios** para ampliar el panel y después en **Avanzados**.
3. En **Cuentas de usuario**, haga clic en **Agregar**.
4. Escriba un nombre en el cuadro **Nombre de usuario**.
5. Escriba una contraseña en el cuadro **Contraseña** y vuelva a escribirla en el cuadro **Confirmar contraseña**.
6. Active la casilla de verificación **Usuario de inicio**, si desea que sea este usuario el que inicie automáticamente la sesión cuando se inicie SecurityCenter.
7. En **Tipos de cuentas de usuario**, seleccione un tipo de cuenta para este usuario y después haga clic en **Crear**.

   Nota: una vez creada la cuenta de usuario, deberá configurar un Usuario restringido en Controles paternos.

8. Para editar la contraseña, el inicio de sesión automático o el tipo de cuenta de un usuario, seleccione el nombre de usuario de la lista y haga clic en **Editar**.
9. Cuando haya terminado, haga clic en **Aplicar**.

Recuperar la contraseña del Administrador

Si olvida la contraseña del Administrador, no podrá recuperarla.

Para recuperar la contraseña del Administrador:

1. Haga clic con el botón derecho del ratón en el icono M de SecurityCenter y, a continuación, haga clic en **Cambiar usuario**.
2. En la lista **Nombre de usuario**, seleccione **Administrador** y, a continuación, haga clic en **¿Olvidó su contraseña?**
3. Escriba la respuesta a la pregunta secreta que seleccionó cuando creó la cuenta de Administrador.
4. Haga clic en **Enviar**.

   Aparecerá su contraseña de Administrador olvidada.

Cambiar la contraseña del Administrador

Si no consigue recordar la contraseña del Administrador o sospecha que puede no ser segura, puede modificarla.

Para modificar la contraseña del Administrador:

1. Haga clic con el botón derecho del ratón en el icono M de SecurityCenter y, a continuación, haga clic en **Cambiar usuario**.
2. En la lista **Nombre de usuario**, seleccione **Administrador** y, a continuación, haga clic en **Cambiar contraseña.**
3. Escriba su contraseña actual en el cuadro **Contraseña antigua**.
4. Escriba su nueva contraseña en el cuadro **Contraseña** y vuelva a escribirla en el cuadro **Confirmar contraseña**.
5. Haga clic en **Aceptar**.

Configuración de las opciones de actualización

SecurityCenter comprueba automáticamente las actualizaciones de todos sus servicios McAfee cada cuatro horas mientras está conectado a Internet y después instala también automáticamente las últimas actualizaciones del producto. A pesar de ello, también puede comprobar las actualizaciones manualmente y en cualquier momento mediante el icono de SecurityCenter que aparece en el extremo derecho de la barra de tareas.

Comprobar si hay actualizaciones automáticamente

SecurityCenter comprueba automáticamente las actualizaciones cada cuatro horas si está conectado a Internet. Pero también puede configurar SecurityCenter para que le avise siempre antes de descargar o instalar actualizaciones.

Para comprobar si hay actualizaciones automáticamente:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto al estado **Las actualizaciones automáticas están activadas** para ampliar el panel y después en **Avanzadas**.
3. Seleccione una de las siguientes opciones en el panel Opciones de actualización:
   - Instalar actualizaciones automáticamente y notificarme cuando el producto esté actualizado (recomendado) (página 27)
   - Descargar actualizaciones automáticamente y notificarme cuando estén listas para su instalación (página 28)
   - Notificarme antes de descargar cualquier actualización (página 28)
4. Haga clic en **Aceptar**.

Nota: para disfrutar de una protección máxima, McAfee recomienda que permita que SecurityCenter compruebe e instale automáticamente las actualizaciones existentes. Sin embargo, si sólo desea actualizar manualmente los servicios de seguridad, puede desactivar la actualización automática (página 29).

Descargar e instalar las actualizaciones automáticamente

Si selecciona **Instalar actualizaciones automáticamente y notificarme cuando los servicios estén actualizados (recomendado)** en el cuadro de diálogo Opciones de actualización de SecurityCenter, éste descargará e instalará de manera automática las actualizaciones.

Descargar las actualizaciones automáticamente

Si selecciona **Descargar actualizaciones automáticamente y notificarme cuando estén listas para su instalación** en las Opciones de actualización, SecurityCenter descargará las actualizaciones de manera automática y, a continuación, le notificará cuando estén listas. A continuación, puede decidir si instalar la actualización o posponerla (página 29).

Para instalar una actualización descargada automáticamente:

1. Haga clic en **Actualizar mis productos ahora** en la alerta y después en **Aceptar**.

   Puede que necesite iniciar una sesión en el sitio Web para verificar su suscripción antes de iniciar la descarga.

2. Tras verificar su suscripción, haga clic en **Actualizar** en el panel Actualizaciones para descargar la actualización e instalarla. Si su suscripción ha caducado, haga clic en **Renovar mi suscripción** en la alerta y siga las instrucciones que se muestran en los mensajes.

Nota: en algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Guarde su trabajo y cierre todos los programas antes de reiniciar el equipo.

Notificar antes de descargar actualizaciones

Si selecciona **Notificarme antes de descargar cualquier actualización** en el panel Opciones de actualización, SecurityCenter le notificará antes de descargar las actualizaciones. A continuación, puede optar descargar e instalar una actualización para los servicios seguridad y eliminar la amenaza de que se produzca cualquier ataque.

Para descargar e instalar una actualización:

1. Seleccione **Actualizar mis productos ahora** en la alerta y después haga clic en **Aceptar**.
2. Inicie sesión en el sitio Web si así se le pide.

   La actualización se descargará automáticamente.

3. Haga clic en **Aceptar** en la alerta, cuando la actualización haya terminado de instalarse.

Nota: en algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Guarde su trabajo y cierre todos los programas antes de reiniciar el equipo.

Desactivar la actualización automática

Para disfrutar de una protección máxima, McAfee recomienda que permita que SecurityCenter compruebe e instale automáticamente las actualizaciones existentes. No obstante, si desea realizar las actualizaciones de sus servicios de seguridad manualmente, puede desactivar la actualización automática.

Nota: No olvide comprobar manualmente la existencia de actualizaciones (página 30) al menos una vez por semana. Si no comprueba la existencia de actualizaciones, el equipo no estará protegido con las actualizaciones de seguridad más recientes.

Para desactivar la función de actualización automática:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto al estado **Las actualizaciones automáticas están activadas** para ampliar el panel.
3. Haga clic en **Desactivar**.
4. Haga clic en **Sí** para confirmar el cambio.

   El estado aparece actualizado en el encabezado.

Si no se ha realizado la comprobación manual de las actualizaciones en siete días, una alerta recuerda al usuario que debe comprobar las actualizaciones.

Posponer las actualizaciones

Si está demasiado ocupado para actualizar sus servicios de seguridad cuando aparezca una alerta, puede optar por activar un aviso para que se lo recuerde más tarde o ignorar la alerta.

Para posponer una actualización:

- Siga uno de estos procedimientos:
  - Seleccione **Recordármelo más tarde** en la alerta y haga clic en **Aceptar**.
  - Seleccione **Cerrar esta alerta** y haga clic en **Aceptar** para cerrar la alerta sin realizar ninguna operación.

Comprobar si hay actualizaciones de forma manual

SecurityCenter comprueba automáticamente si hay actualizaciones cada cuatro horas mientras está conectado a Internet y después instala, también automáticamente, las últimas actualizaciones del producto. A pesar de ello, también se pueden comprobar las actualizaciones manualmente y en cualquier momento mediante el icono de SecurityCenter que aparece en el área de notificación de Windows, en el extremo derecho de la barra de tareas.

Nota: para disfrutar de una protección máxima, McAfee le recomienda que permita a SecurityCenter comprobar e instalar automáticamente las actualizaciones existentes. Sin embargo, si sólo desea actualizar manualmente los servicios de seguridad, puede desactivar la actualización automática (página 29).

Para comprobar manualmente si hay actualizaciones:

1. Asegúrese de que su equipo está conectado a Internet.
2. Haga clic con el botón derecho del ratón en el icono M de SecurityCenter que aparece en el área de notificación de Windows, en el extremo derecho de la barra de tareas y, a continuación, haga clic en **Actualizaciones**.

   Mientras SecurityCenter comprueba si hay actualizaciones, puede seguir realizando otras tareas con este programa.

   Para su comodidad, aparece un icono animado en el área de notificación de Windows, en la parte derecha más alejada de la barra de herramientas. Cuando SecurityCenter finalice, el icono desaparece automáticamente.
3. Inicie sesión en el sitio Web si así se le pide, para comprobar su suscripción.

Nota: en algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Guarde su trabajo y cierre todos los programas antes de reiniciar el equipo.

Configuración de las opciones de alerta

SecurityCenter notifica automáticamente al usuario con alertas y sonidos de los nuevos virus públicos, las amenazas contra la seguridad y las actualizaciones de los productos. De todos modos, es posible configurar SecurityCenter para que muestre sólo aquellas alertas que requieren una atención inmediata.

Configurar las opciones de alerta

SecurityCenter notifica automáticamente al usuario con alertas y sonidos de los nuevos virus públicos, las amenazas contra la seguridad y las actualizaciones de los productos. De todos modos, es posible configurar SecurityCenter para que muestre sólo aquellas alertas que requieren una atención inmediata.

Para configurar las opciones de alerta:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto a **Alertas** para ampliar el panel y después en **Avanzadas**.
3. Seleccione una de las siguientes opciones en el panel Opciones de alerta:
   - **Avisarme cuando se produzca un brote de virus público o una amenaza para la seguridad.**
   - **Mostrar alertas informativas cuando se detecte el modo de juegos**
   - **Reproducir un sonido cuando se produzca una alerta**
   - **Mostrar pantalla de bienvenida de McAfee al iniciar Windows**
4. Haga clic en **Aceptar**.

Nota: Para deshabilitar futuras alertas informativas desde la alerta misma, active la casilla de verificación **No volver a mostrar esta alerta**. Puede volver a habilitarlas más tarde en el panel Alertas informativas.

Configurar alertas informativas

Las alertas informativas le notifican de cuándo se producen eventos que no requieren de su respuesta inmediata. Si deshabilita futuras alertas informativas desde la alerta misma, puede volver a habilitarlas más tarde en el panel Alertas informativas.

Para configurar las alertas informativas:

1. En **Información de SecurityCenter**, haga clic en **Configurar**.
2. Haga clic en la flecha situada junto a **Alertas** para ampliar el panel y después en **Avanzadas**.
3. En **Configuración de SecurityCenter**, haga clic en **Alertas informativas**.
4. Desactive la casilla **Ocultar alertas informativas** y después desactive las casillas de verificación de las alertas de la lista que desee mostrar.
5. Haga clic en **Aceptar**.

CAPÍTULO 5

Realización de tareas comunes

Realice tareas comunes, desde volver al panel Inicio, ver los eventos recientes y gestionar la red (si su equipo dispone de capacidad de gestión para esta red) hasta mantener el equipo. Si McAfee Data Backup está instalado, también puede realizar la copia de seguridad de sus datos.

En este capítulo

Realizar tareas comunes

Realice tareas comunes, desde volver al panel Inicio, ver los eventos recientes, mantener el equipo y gestionar la red (si su equipo dispone de capacidad de gestión para esta red), hasta realizar la copia de seguridad de sus datos (si tiene instalado Data Backup de McAfee).

Para realizar tareas comunes:

- En **Tareas comunes**, en el menú Básico, realice una de las siguientes operaciones:
  - Para volver al panel Inicio, haga clic en **Inicio**.
  - Para ver los eventos recientes que han sido detectados por su software de seguridad, haga clic en **Eventos recientes**.
  - Para eliminar los archivos no utilizados, desfragmentar los datos y restaurar la configuración anterior de su equipo, haga clic en **Mantener equipo**.
  - Para gestionar su red, haga clic en **Gestionar red** en un equipo que tenga capacidad de gestión para la misma.

    El Gestor de red supervisa los equipos que están conectados a su red en busca de puntos débiles en cuanto a seguridad, con el fin de facilitarle la identificación de los problemas de seguridad de la red.
  - Para crear copias de seguridad de sus archivos, haga clic en **Data Backup**, si tiene instalado McAfee Data Backup.

Las copias de seguridad automatizadas guardan copias de los archivos más valiosos siempre que lo desee, cifrando y almacenando los archivos en una unidad de CD/DVD, USB, externa o de red.

Sugerencia: Para su comodidad, también puede realizar tareas comunes desde dos ubicaciones más (en **Inicio** en el menú Avanzado, y en el menú **Vínculos rápidos** del icono M de SecurityCenter que aparece en el extremo derecho de la barra de tareas). También puede ver los eventos recientes y registros completos por tipos en **Informes y registros** en el menú Avanzado.

Ver eventos recientes

Los eventos recientes se registran cuando se realizan cambios en su equipo. Como por ejemplo cuando se habilita o deshabilita un tipo de protección, cuando se elimina una amenaza o cuando se bloquea un intento de conexión a Internet. Puede visualizar los 20 eventos más recientes y sus detalles.

Consulte el archivo de ayuda del producto para obtener información acerca de los eventos correspondientes.

Para visualizar eventos recientes:

1. Haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos,** y, a continuación, haga clic en **Ver eventos recientes**.

   En la lista aparecen todos los eventos más recientes, junto con la fecha y una breve descripción.

2. En **Eventos recientes**, seleccione un evento para ver información adicional en el panel Detalles.

   En **Deseo**, aparecen todas las acciones disponibles.

3. Para ver una lista más completa de eventos, haga clic en **Ver registro**.

Mantener el equipo de manera automática

Para liberar espacio en disco y optimizar el rendimiento del equipo, puede planificar las tareas de QuickClean o del Desfragmentador de disco para que se ejecuten a intervalos regulares. Dichas tareas incluyen eliminar, destruir y desfragmentar archivos y carpetas.

Para mantener el equipo de manera automática:

1. Haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos,** y a continuación, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.
3. De la lista de operaciones, seleccione **QuickClean** o **Desfragmentador de disco**.
4. Siga uno de estos procedimientos:
   - Para modificar una tarea existente, selecciónela y después haga clic en **Modificar**. Siga las instrucciones que aparecen en pantalla.
   - Para crear una tarea nueva, escriba el nombre en el cuadro **Nombre de la tarea** y, a continuación, haga clic en **Crear**. Siga las instrucciones que aparecen en pantalla.
   - Para suprimir una tarea, selecciónela y, a continuación, haga clic en **Eliminar**.
5. En **Resumen de la tarea**, puede ver cuándo se ejecutó una tarea por última vez, cuándo se volverá a ejecutar y su estado actual.

Mantener el equipo manualmente

Puede realizar tareas de mantenimiento manuales para eliminar archivos sin usar, desfragmentar sus datos o restaurar la configuración previa del equipo.

Para mantener el equipo manualmente:

- Siga uno de estos procedimientos:
  - Para utilizar QuickClean, haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos**, haga clic en **Mantener equipo** y después en **Inicio**.
  - Para utilizar el Desfragmentador de disco, haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos**, haga clic en **Mantener equipo** y después en **Analizar**.
  - Para utilizar Restaurar sistema, en el menú Avanzado haga clic en **Herramientas**, en **Restaurar sistema** y después en **Inicio**.

Eliminar archivos y carpetas no utilizados

Utilice QuickClean para liberar espacio en disco y optimizar el rendimiento de su equipo.

Para eliminar archivos y carpetas no utilizados:

1. Haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos,** y a continuación, haga clic en **Mantener equipo**.
2. En **QuickClean**, haga clic en **Inicio**.
3. Siga las instrucciones que aparecen en pantalla.

Desfragmentar archivos y carpetas

La fragmentación de disco se realiza cuando se eliminan archivos y carpetas, y cuando se agregan archivos nuevos. La fragmentación ralentiza el acceso al disco duro y reduce el rendimiento general del equipo, aunque normalmente no ocurre de manera excesiva.

Utilice la desfragmentación para reescribir partes de un archivo en sectores contiguos de un disco duro con el fin de aumentar la velocidad de acceso y recuperación.

Para desfragmentar archivos y carpetas:

1. Haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos** y, a continuación, haga clic en **Mantener equipo**.
2. En **Desfragmentador de disco**, haga clic en **Analizar**.
3. Siga las instrucciones que aparecen en pantalla.

Restaurar la configuración previa del equipo

Los puntos de restauración son instantáneas del equipo que Windows guarda de forma periódica y siempre que ocurre un evento relevante (como cuando se instala un programa o un controlador). No obstante, también puede crear y nombrar sus propios puntos de restauración en cualquier momento.

Utilice los puntos de restauración para deshacer cambios peligrosos realizados en su equipo y volver a la configuración anterior.

Para restaurar la configuración anterior del equipo:

1. En el menú Avanzado, haga clic en **Herramientas** y después en **Restaurar sistema**.
2. En **Restaurar sistema**, haga clic en **Inicio**.
3. Siga las instrucciones que aparecen en pantalla.

Gestionar la red

Si su equipo dispone de capacidad de gestión para la red, utilice el Gestor de red para supervisar los equipos que estén conectados a la suya y buscar los puntos débiles en cuanto a seguridad; de este modo, podrá identificar fácilmente los problemas.

Si el estado de protección de su equipo no está siendo controlado en esta red significa que o bien su equipo no forma parte de ella, o bien es un miembro no gestionado de la misma. Para más información, consulte el archivo de ayuda del Gestor de red.

Para gestionar su red:

1. Haga clic con el botón derecho del ratón en el icono principal de SecurityCenter, seleccione **Vínculos rápidos,** y a continuación, haga clic en **Gestionar red**.
2. Haga clic en el icono que representa este equipo en el mapa de la red.
3. En **Deseo**, haga clic en **Supervisar este equipo**.

Obtener más información sobre virus

Utilice la Biblioteca de información de virus y el Mapa de virus para realizar la siguiente operación:

- Conozca más información acerca de los últimos virus, amenazas falsas de virus por correo electrónico y otras amenazas.
- Obtenga herramientas de eliminación de virus gratuitas para ayudar a reparar el equipo.
- Eche un vistazo en tiempo real a los lugares del mundo en los que los últimos virus estén infectando equipos.

Para obtener más información sobre virus:

1. En el menú Avanzado, haga clic en **Herramientas** y después en **Información de virus**.
2. Siga uno de estos procedimientos:
   - Busque virus mediante la Biblioteca de información de virus gratuita de McAfee.
   - Busque virus mediante el World Virus Map que aparece en el sitio Web de McAfee.

CAPÍTULO 6

McAfee QuickClean

Cuando navega por Internet, el desorden va aumentando rápidamente en el equipo. Proteja su privacidad y elimine toda la basura de Internet y del correo electrónico con QuickClean. QuickClean identifica y quita los archivos que se acumulan al navegar, incluidas las cookies, los mensajes de correo electrónico, las descargas y el historial (datos que contienen información personal sobre el usuario). QuickClean protege su privacidad y permite eliminar de manera eficaz esta información confidencial.

QuickClean también elimina los programas no deseados. Especifique los archivos que desea eliminar y limpie el desorden sin eliminar información esencial.

En este capítulo

Descripción de las características de QuickClean

En esta sección se describen las características de QuickClean.

Características

QuickClean proporciona un conjunto de herramientas de gran eficacia y sencillez que eliminan eficazmente los desechos digitales. Ahora puede liberar espacio en disco y optimizar el rendimiento del equipo.

CAPÍTULO 7

Limpiando el equipo

QuickClean le permite eliminar eficazmente archivos y carpetas.

Cuando navega por Internet, el explorador copia todas las páginas de Internet y sus gráficos en una carpeta de la caché del disco. De este modo, el navegador puede cargar rápidamente la página cuando vuelve a acceder a ella. Los archivos almacenados en caché resultan útiles cuando se visitan repetidamente las mismas páginas de Internet y su contenido no cambia con frecuencia. La mayor parte de las veces, sin embargo, los archivos de la caché no resultan útiles y pueden eliminarse.

Con los limpiadores siguientes puede eliminar distintos elementos.

- Limpiador de la Papelera de reciclaje: Limpia la Papelera de reciclaje de Windows.
- Limpiador de archivos temporales: Elimina los archivos almacenados en las carpetas temporales.
- Limpiador de accesos directos: Elimina los accesos directos deshabilitados o aquellos que no tienen un programa asociado.
- Limpiador de fragmentos de archivos perdidos: Elimina del equipo los fragmentos de archivos perdidos.
- Limpiador del Registro: Elimina la información de los programas que ya no están en el equipo del Registro de Windows.
- Limpiador de caché: Elimina los archivos de la caché que se almacenan mientras navega por Internet. Los archivos de este tipo se guardan por lo general como archivos temporales de Internet.
- Limpiador de cookies: Elimina las cookies. Los archivos de este tipo se guardan por lo general como archivos temporales de Internet.
  Las cookies son archivos pequeños que el navegador guarda en el equipo a petición de un servidor Web. Cada vez que consulte una página de dicho servidor Web, el navegador enviará la cookie de vuelta al servidor. Estas cookies pueden funcionar como una etiqueta que permite al servidor Web realizar un seguimiento de las páginas que usted visita y la frecuencia con la que lo hace.
- Limpiador del historial del navegador: Elimina el historial del navegador.
- Limpiador de correo de Outlook Express y Outlook para elementos eliminados y enviados: Elimina el correo de las

carpetas Elementos enviados y Elementos eliminados de Outlook.

- Limpiador utilizado recientemente: Elimina los elementos utilizados recientemente almacenados en el equipo, como los documentos de Microsoft Office.
- Limpiador de ActiveX y complementos: Elimina los complementos y los controles de ActiveX.
  ActiveX es una tecnología que se utiliza para implementar controles en un programa. Un control de ActiveX puede agregar un botón a la interfaz de un programa. La mayoría de estos controles son inofensivos; sin embargo, la tecnología ActiveX puede utilizarse para obtener información del equipo. Los complementos son pequeños programas de software que se adhieren a aplicaciones más grandes para proporcionar una funcionalidad adicional. Los complementos permiten que el navegador Web acceda a archivos que están incorporados en documentos HTML y que tienen formatos que normalmente no podría reconocer (por ejemplo, archivos de animación, vídeo y audio) y le permite ejecutarlos.
- Limpiador de puntos de restauración del sistema: Elimina los puntos antiguos de restauración del sistema del equipo.

En este capítulo

Utilización de QuickClean

En esta sección se describe cómo se utiliza QuickClean.

Limpieza del equipo

Puede eliminar los archivos y las carpetas que no utiliza, liberar espacio en disco y mejorar el rendimiento del equipo.

Para limpiar el equipo:

1. En el menú avanzado, haga clic en **Herramientas**.
2. Haga clic en **Mantener el equipo** y, a continuación, debajo de **McAfee QuickClean**, en **Iniciar**.
3. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar los limpiadores predeterminados de la lista.
   - Active o desactive los limpiadores correspondientes y haga clic en **Siguiente.** En el limpiador utilizado recientemente, puede hacer clic en **Propiedades** para desactivar los programas cuyas listas no desea limpiar.
   - Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente.**
4. Una vez completado el análisis, haga clic en **Siguiente** para confirmar la eliminación de los archivos. Puede expandir esta lista para ver los archivos que se van a limpiar y su ubicación.
5. Haga clic en **Siguiente**.
6. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
   - Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos** y especifique el número de veces que se ejecutará el proceso. Los archivos eliminados con Shredder no se pueden recuperar.
7. Haga clic en **Finalizar**.
8. En **Resumen de QuickClean**, consulte el número de archivos del Registro que se han eliminado y el volumen de espacio en disco recuperado tras efectuar la limpieza del disco e Internet.

CAPÍTULO 8

McAfee Shredder

Los archivos eliminados se pueden recuperar de su equipo incluso después de haber vaciado la Papelera de reciclaje. Cuando se elimina un archivo, Windows sólo marca ese espacio en la unidad de disco como espacio que ya no está en uso, pero el archivo sigue ahí. A través de herramientas forenses informáticas, se pueden recuperar registros fiscales, currículos y otros documentos que se hayan borrado. Shredder protege su privacidad al eliminar de forma eficaz y definitiva los archivos no deseados.

Para eliminar permanentemente un archivo, deberá sobrescribir varias veces el archivo existente con datos nuevos. Microsoft® Windows no elimina los archivos definitivamente porque cada operación de borrado requeriría demasiado tiempo. La purga de un documento mediante Shredder no siempre evita que se recupere, ya que algunos programas crean copias temporales ocultas de los documentos abiertos. Si sólo purga los documentos que se ven en el Explorador de Windows®, es posible que aún existan copias temporales de estos documentos.

Nota: no se realizan copias de seguridad de los archivos purgados. Los archivos eliminados mediante Shredder no se pueden restaurar.

En este capítulo

Descripción de las características de Shredder

En esta sección se describen las características de Shredder.

Características

Shredder permite borrar el contenido de la Papelera de reciclaje, los archivos temporales de Internet, el historial de sitios Web, los archivos, las carpetas y los discos.

CAPÍTULO 9

Eliminar archivos no deseados con Shredder

Shredder protege su privacidad al eliminar de forma eficaz y definitiva los archivos no deseados, como el contenido de la Papelera de reciclaje, los archivos temporales de Internet o el historial de sitios Web. Puede seleccionar los archivos y las carpetas que desea purgar o buscarlos en el equipo.

En este capítulo

Uso de Shredder

En esta sección se describe cómo se utiliza Shredder.

Purgar archivos, carpetas y discos

Los archivos pueden permanecer en el equipo incluso después de vaciar la Papelera de reciclaje. Sin embargo, cuando se purgan los archivos, los datos se suprimen definitivamente y los piratas informáticos no pueden acceder a ellos.

Para purgar archivos, carpetas y discos:

1. En el menú avanzado, haga clic en **Herramientas** y, a continuación, en **Shredder**.
2. Siga uno de estos procedimientos:
   - Haga clic en **Borrar archivos y carpetas** si desea purgar archivos y carpetas.
   - Haga clic en **Borrar un disco entero** si desea purgar un disco**.**
3. Seleccione uno de los niveles siguientes:
   - **Rápido**: Purga una vez los elementos seleccionados.
   - **Exhaustivo**: Purga siete veces los elementos seleccionados.
   - **Personalizado**: Purga los elementos seleccionados un máximo de diez veces. Cuanto mayor sea al número de veces que se realiza esta operación, más eficaz será la eliminación del archivo.
4. Haga clic en **Siguiente**.
5. Siga uno de estos procedimientos:
   - Si desea purgar archivos, haga clic en **Contenido de la Papelera de reciclaje**, **Archivos temporales de Internet** o **Historial de sitios Web** en la lista **Seleccionar archivos a purgar**. Si desea purgar un disco, haga clic en el disco.
   - Haga clic en **Examinar**, acceda a los archivos que desea depurar y selecciónelos.
   - Escriba la ruta de los archivos que desea purgar en la lista **Seleccionar archivos a purgar**.
6. Haga clic en **Siguiente**.
7. Haga clic en **Finalizar** para completar la operación.
8. Haga clic en **Listo**.

CAPÍTULO 10

McAfee Network Manager

McAfee® Network Manager ofrece una representación gráfica de los equipos y componentes que forman una red doméstica. Con Network Manager podrá supervisar de forma remota el estado de protección de cada uno de los equipos gestionados en la red, así como reparar también de forma remota todas las vulnerabilidades de seguridad que se hayan registrado en cualquiera de esos equipos.

Antes de empezar a utilizar Network Manager, familiarícese primero con algunas de sus funciones más conocidas. En la ayuda de Network Manager hallará toda la información acerca de cómo configurar y utilizar dichas funciones.

En este capítulo

Funciones

Network Manager ofrece las siguientes funciones:

Mapa de la red gráfica

El mapa de la red de Network Manager ofrece una visión general gráfica del estado de la seguridad de los equipos y componentes que forman su red doméstica. Cuando realice cambios en su red (por ejemplo, cuando agregue un equipo), el mapa de la red reconoce estos cambios. Puede actualizar el mapa de la red, cambiar el nombre de la red, y mostrar u ocultar componentes del mapa de la red para personalizar su vista. También puede ver los detalles asociados con cualquiera de los componentes mostrados en el mapa de la red.

Gestión remota

Utilice el mapa de la red de Network Manager para gestionar el estado de seguridad de los equipos que forman su red doméstica. Puede invitar a un equipo a conectarse a la red gestionada, controlar el estado de protección del equipo gestionado y solucionar vulnerabilidades de seguridad conocidas desde un equipo remoto de la red.

Descripción de los iconos de Network Manager

La siguiente tabla describe los iconos que más se utilizan en el mapa de la red de Network Manager.

Icono	Descripción
	Representa un equipo gestionado, en línea
	Representa un equipo gestionado, sin conexión
	Representa un equipo no gestionado que tiene instalado el software de seguridad McAfee 2007
	Representa un equipo no gestionado y sin conexión
	Representa un equipo en línea que no tiene instalado el software de seguridad McAfee 2007, o un dispositivo de red desconocido
	Representa un equipo sin conexión que no tiene instalado el software de seguridad McAfee 2007, o bien un dispositivo de red desconocido y sin conexión
	Indica que el elemento correspondiente está protegido y conectado
	Indica que el elemento correspondiente requiere su atención
	Indica que el elemento correspondiente requiere su atención y está desconectado
	Representa un enrutador doméstico inalámbrico
	Representa un enrutador doméstico estándar
	Representa Internet cuando está conectado
	Representa Internet cuando está desconectado

CAPÍTULO 11

Configuración de una red gestionada

Para configurar una red gestionada, debe trabajar con los elementos del mapa de la red y agregar miembros (equipos) a la misma.

En este capítulo

Trabajar con el mapa de la red

Cada vez que conecte un equipo a la red, Network Manager analizará el estado de la red para determinar si existen miembros (gestionados o no), los atributos del enrutador y el estado de Internet. Si no encuentra a ningún miembro, Network Manager supone que el equipo conectado actualmente es el primer equipo de la red y, automáticamente, lo trata como a un miembro gestionado con permisos de administración. De forma predeterminada, el nombre de la red incluye el grupo de trabajo o el nombre de dominio del primer equipo que se conecta a la red con el software de seguridad McAfee 2007 instalado; de todos modos, puede cambiar el nombre de la red en cualquier momento.

Siempre que realice cambios en la red (por ejemplo, cuando agregue un equipo), puede personalizar el mapa de la red. Por ejemplo, puede actualizar el mapa de la red, cambiar el nombre de la red y mostrar u ocultar componentes del mapa de la red para personalizar su vista. También puede ver los detalles asociados con cualquiera de los componentes mostrados en el mapa de la red.

Acceder al mapa de la red

Para acceder al mapa de la red, inicie el Network Manager desde la lista de tareas comunes de SecurityCenter. El mapa de la red le ofrece una representación gráfica de los equipos y componentes que forman su red doméstica.

Para acceder al mapa de la red:

- En el menú Básico o Avanzado, haga clic en **Gestionar red**. El mapa de la red aparecerá en el panel de la derecha.

Nota: La primera vez que accede al mapa de la red, se le pide que confíe en los otros equipos de esta red antes de que aparezca dicho mapa.

Actualizar el mapa de la red

El mapa de la red se puede actualizar en cualquier momento; por ejemplo, después de que se haya incorporado otro equipo a la red gestionada.

Para actualizar el mapa de la red:

1. En el menú Básico o Avanzado, haga clic en **Gestionar red**. El mapa de la red aparecerá en el panel de la derecha.
2. Haga clic en **Actualizar el mapa de la red** en **Deseo**.

Nota: El enlace **Actualizar el mapa de la red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para deseleccionar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el grupo de trabajo o el nombre de dominio del primer equipo que se conecta a la red con el software de seguridad McAfee 2007 instalado. Si no le parece un nombre adecuado, lo puede cambiar.

Para cambiar el nombre de la red:

1. En el menú Básico o Avanzado, haga clic en **Gestionar red**. El mapa de la red aparecerá en el panel de la derecha.
2. Haga clic en **Cambiar nombre de red** en **Deseo**.
3. Escriba el nombre de la red en el cuadro **Cambiar nombre de red**.
4. Haga clic en **Aceptar**.

Nota: El enlace **Cambiar nombre de red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para deseleccionar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Mostrar u ocultar elementos en el mapa de la red

De forma predeterminada, el mapa de la red muestra todos los equipos y componentes de su red doméstica. Si tiene elementos ocultos, puede volver a mostrarlos en cualquier momento. Sólo se pueden ocultar los elementos no gestionados, los equipos gestionados no se pueden ocultar.

Para...	En el menú Básico o Avanzado, haga clic en **Gestionar red** y luego haga lo siguiente:
Ocultar un elemento en el mapa de la red	Haga clic en un elemento del mapa de la red y otro clic en **Ocultar este elemento** en **Deseo**. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
Mostrar elementos ocultos en el mapa de la red	En **Deseo**, haga clic en **Mostrar elementos ocultos**.

Visualizar detalles de un elemento

Para visualizar información detallada acerca de un componente de la red, seleccione el componente en cuestión en el mapa de la red. Dicha información incluye el nombre del componente, su estado de protección y demás información necesaria para gestionar el componente.

Para visualizar los detalles de un elemento:

1. Haga clic en el icono del elemento en el mapa de la red.
2. En **Detalles**, visualice la información sobre el elemento.

Incorporación a la red gestionada

Es preciso que un equipo se convierta primero en miembro de confianza de la red antes de poder gestionarlo de forma remota o antes de concederle el permiso para que gestione otros equipos de la red de forma remota. Los miembros (equipos) ya existentes en la red que poseen permisos de administración son los que conceden el título de miembro de la red a los equipos nuevos. Para asegurar que sólo los equipos de confianza se incorporan a la red, tanto los usuarios de los equipos que conceden el permiso como los de los equipos que se incorporan tienen que autenticarse.

Cuando un equipo se incorpora a la red, se le pide que exponga su estado de protección McAfee a los demás equipos de la red. Si el equipo accede a exponer su estado de protección, se convierte en miembro *gestionado* de la red. Si el equipo se niega a exponer su estado de protección, se convierte en miembro *no gestionado* de la red. Los miembros no gestionados de la red suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, al uso compartido de archivos o impresoras).

Nota: Tras incorporarse a la red, y en el caso de que tenga instalados otros programas de redes McAfee (por ejemplo, McAfee Wireless Network Security o EasyNetwork), esos programas también reconocerán al equipo como equipo gestionado. El nivel de permisos que se asigna a un equipo en Network Manager es aplicable al resto de programas de redes McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporarse a una red gestionada

Cuando reciba una invitación para incorporarse a una red gestionada, podrá aceptarla o rechazarla. También puede determinar si desea que éste y otros equipos de la red se supervisen entre ellos las configuraciones de seguridad (por ejemplo, si los servicios de protección antivirus de un equipo están actualizados o no).

Para incorporarse a una red gestionada:

1. En el cuadro de diálogo de la invitación, seleccione la casilla de activación **Permitir a este y a otros equipos supervisarse mutuamente las configuraciones de seguridad** para permitir que otros equipos de la red gestionada supervisen la configuración de seguridad de su equipo.
2. Haga clic en **Incorporar**.
   Al aceptar la invitación, se muestran dos tarjetas.
3. Confirme que se trata de las mismas tarjetas que se mostraron en el equipo que le invitó a incorporarse a la red gestionada.
4. Haga clic en **Confirmar**.

Nota: Si el equipo que le invitó a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. En ese caso, la incorporación a la red pondría en peligro a su equipo; por consiguiente, haga clic en **Rechazar** en el cuadro de diálogo de confirmación.

Invitar a un equipo a que se incorpore a la red gestionada

Si un equipo se agrega a la red gestionada, o bien existe un equipo no gestionado en la red, puede invitar a ese equipo a incorporarse a la red gestionada. Sólo los equipos con permisos de administración en la red pueden invitar a otros equipos a que se incorporen a ella. Al enviar la invitación se especifica también el nivel de permisos que se desea asignar al equipo que se incorpora.

Para invitar a un equipo a que se incorpore a la red gestionada

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Supervisar este equipo** en **Deseo**.
3. En el cuadro de diálogo Invitar a un equipo a incorporarse a esta red gestionada, haga clic en una de las siguientes opciones:
   - **Conceder acceso de invitado**
     El acceso de invitado permite que el equipo acceda a la red.
   - **Conceder acceso pleno a todas las aplicaciones de la red gestionada**
     El acceso pleno (al igual que el acceso de invitado) permite que el equipo acceda a la red.
   - **Conceder acceso de administración a todas las aplicaciones de la red gestionada**
     El acceso administrativo permite que el equipo acceda a la red con permisos de administración. Asimismo, permite que el equipo conceda acceso, a su vez, a otros equipos que desean incorporarse a la red gestionada.

4 Haga clic en **Invitar**.
El equipo recibe una invitación para incorporarse a la red gestionada. Cuando el equipo acepta la invitación, se muestran dos tarjetas.

5 Confirme que se trata de las mismas tarjetas que se muestran en el equipo que ha invitado a incorporarse a la red gestionada.

6 Haga clic en **Conceder acceso**.

Nota: Si el equipo que ha invitado a incorporarse a la red gestionada no está mostrando las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. Si permite que el equipo se incorpore a la red, puede poner en peligro a otros equipos; por consiguiente, haga clic en **Denegar acceso** en el cuadro de diálogo de confirmación de seguridad.

Dejar de confiar en los equipos de la red

Si ha accedido a confiar en otros equipos de la red por error, puede dejar de confiar en ellos.

Para dejar de confiar en los equipos de la red:

- Haga clic en **Dejar de confiar en los equipos de esta red**, en **Deseo**.

Nota: El enlace **Dejar de confiar en los equipos de esta red** sólo está disponible cuando no se ha incorporado ningún otro equipo gestionado a la red.

CAPÍTULO 12

Gestión remota de la red

Después de configurar su red gestionada, puede utilizar Network Manager para gestionar los equipos y componentes que forman la red de manera remota. Puede supervisar el estado y los niveles de permiso de los equipos y componentes, así como solucionar problemas de seguridad de forma remota.

En este capítulo

Supervisión de estados y permisos

Una red gestionada posee dos tipos de miembros: miembros gestionados y miembros no gestionados. Los miembros gestionados permiten que otros equipos de la red supervisen su estado de protección de McAfee; los miembros no gestionados no lo permiten. Los miembros no gestionados suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, al uso compartido de archivos o impresoras). Un equipo gestionado de la red puede invitar en cualquier momento a un equipo no gestionado a que se convierta en equipo gestionado. Asimismo, un equipo gestionado puede convertirse en no gestionado en cualquier momento.

Los equipos gestionados pueden tener permisos de administración, plenos o de invitado. Los permisos de administración permiten al equipo gestionado gestionar el estado de protección de todos los demás equipos gestionados de la red y conceder el título de miembro de la red a otros equipos. Los permisos pleno y de invitado sólo permiten al equipo acceder a la red. El nivel de permisos de un equipo se puede modificar en cualquier momento.

Network Manager también permite gestionar los dispositivos (por ejemplo, enrutadores) que conforman una red gestionada. Asimismo, es posible configurar y modificar las propiedades de visualización de un dispositivo en el mapa de la red.

Supervisar el estado de protección de un equipo

Si en la red no se supervisa el estado de protección de un equipo (ya sea porque el equipo no es un miembro de ésta o porque es un miembro no gestionado de la misma), se puede emitir una solicitud para hacerlo.

Para supervisar el estado de protección de un equipo:

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Controlar este equipo** en **Deseo**.

Interrumpir la supervisión del estado de protección de un equipo

Puede dejar de supervisar el estado de protección de un equipo gestionado en su red privada. Entonces el equipo pasa a ser un equipo no gestionado.

Para interrumpir la supervisión del estado de protección de un equipo:

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Interrumpir el control en este equipo** en **Deseo**.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Modificar los permisos de un equipo gestionado

Se pueden modificar los permisos de un equipo gestionado en cualquier momento. Esto permite delimitar los equipos que pueden supervisar el estado de protección (configuración de seguridad) de otros equipos de la red.

Para modificar los permisos de un equipo gestionado:

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Modificar los permisos para este equipo** en **Deseo**.
3. En el cuadro de diálogo de modificación de permisos, active o desactive la casilla para determinar si este y otros equipos de la red gestionada pueden supervisarse mutuamente el estado de protección.
4. Haga clic en **Aceptar**.

Gestionar un dispositivo

Puede gestionar un dispositivo accediendo a su página Web de administración desde Network Manager.

Para gestionar un dispositivo:

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Gestionar este dispositivo**, en **Deseo**.
   Se abrirá un navegador Web que mostrará la página Web de administración del dispositivo.
3. En su navegador Web, introduzca sus datos de inicio de sesión y configure la seguridad del dispositivo.

Nota: Si el dispositivo es un enrutador inalámbrico o un punto de acceso protegido por Wireless Network Security, deberá utilizar Wireless Network Security para configurar la seguridad del dispositivo.

Modificar las propiedades de visualización de un dispositivo

Al modificar las propiedades de visualización de un dispositivo, puede cambiar el nombre de visualización del mismo en el mapa de la red y especificar si se trata de un enrutador inalámbrico.

Para modificar las propiedades de visualización de un dispositivo:

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Modificar propiedades de dispositivos** en **Deseo**.
3. Para especificar el nombre de visualización de un dispositivo, escriba el nombre en el cuadro **Nombre**.
4. Para especificar el tipo de dispositivo, haga clic en una de las siguientes opciones:
   - **Enrutador**
     Representa un enrutador doméstico estándar.
   - **Enrutador inalámbrico**
     Representa un enrutador doméstico inalámbrico.
5. Haga clic en **Aceptar**.

Solución de vulnerabilidades de seguridad

Los equipos gestionados con permisos de administración pueden supervisar el estado de protección McAfee de otros equipos gestionados de la red, así como solucionar de forma remota cualquier tipo de vulnerabilidad de seguridad que se registre. Por ejemplo, si el estado de protección McAfee de un equipo gestionado indica que VirusScan está desactivado, otro equipo gestionado que posea permisos de administración puede *solucionar* esta vulnerabilidad de la seguridad activando VirusScan de forma remota.

Al solucionar vulnerabilidades de seguridad de forma remota, Network Manager repara automáticamente los problemas más habituales. No obstante, algunas vulnerabilidades de seguridad pueden precisar la intervención manual en el equipo local. En tal caso, Network Manager soluciona aquellos problemas que se pueden resolver de forma remota y luego le solicita que solucione los temas restantes iniciando la sesión en SecurityCenter desde el equipo vulnerable y siguiendo las recomendaciones propuestas. En algunos casos, la solución sugerida consiste en instalar el software de seguridad McAfee 2007 en el equipo o equipos remotos de la red.

Solucionar vulnerabilidades de seguridad

Puede utilizar Network Manager para solucionar de forma automática la mayoría de las vulnerabilidades de seguridad en equipos gestionados remotos. Por ejemplo, si VirusScan está desactivado en un equipo remoto, puede utilizar Network Manager para activarlo de forma automática.

Para solucionar vulnerabilidades de seguridad:

1. Haga clic en el icono del elemento en el mapa de la red.
2. Visualice el estado de protección de un elemento en **Detalles**.
3. Haga clic en **Solucionar vulnerabilidades de seguridad** en **Deseo**.
4. Una vez solucionados los problemas de seguridad, haga clic en **Aceptar**.

Nota: Si bien Network Manager soluciona automáticamente la mayoría de las vulnerabilidades de seguridad, algunas reparaciones pueden requerir que inicie SecurityCenter en el equipo vulnerable y siga las recomendaciones que aparecen.

Instalar el software de seguridad McAfee en equipos remotos

Si uno o más equipos de su red no tienen instalado el software de seguridad McAfee 2007, su estado de seguridad no se podrá supervisar de forma remota. Si desea supervisar estos equipos de forma remota, deberá ir a cada uno de ellos e instalar el software de seguridad McAfee 2007.

Para instalar el software de seguridad McAfee en un equipo remoto:

1. En un navegador del equipo remoto, vaya a http://download.mcafee.com/us/.
2. Siga las instrucciones que aparecen en la pantalla para instalar el software de seguridad McAfee 2007 en el equipo.

CAPÍTULO 13

McAfee VirusScan

VirusScan ofrece protección total, fiable y actualizada frente a los virus y el software espía. Mediante la galardonada tecnología de análisis de McAfee, VirusScan le protege contra virus, gusanos, archivos troyanos, secuencias de comandos sospechosas, kits de raíz, desbordamientos del búfer, ataques híbridos, software espía, programas no deseados y otras amenazas.

En este capítulo

Funciones

Esta versión de VirusScan incluye las siguientes funciones:

Protección antivirus

La protección en tiempo real analiza los archivos a los que accede el usuario o el equipo.

Analizar

Detecta la existencia de virus y otras amenazas en las unidades de disco duro, unidades de disquete y en cada una de las carpetas y archivos. También puede hacer clic con el botón derecho del ratón sobre un elemento para analizarlo.

Detección de software espía y software publicitario

VirusScan identifica y elimina software espía y publicitario, y otros programas que pueden poner en peligro su privacidad y reducir el rendimiento del equipo.

Actualizaciones automáticas

Las actualizaciones automáticas le protegen frente a las amenazas informáticas más recientes, identificadas y no identificadas.

Análisis rápido en segundo plano

Los análisis rápidos y discretos identifican y destruyen virus, troyanos, gusanos, software espía, publicitario y de marcación, y otras amenazas sin interrumpir el trabajo.

Alertas de seguridad en tiempo real

Las alertas de seguridad indican la aparición de emergencias de virus y amenazas contra la seguridad y ofrecen opciones de respuesta para eliminar la amenaza, neutralizarla u obtener más información sobre ella.

Detección y limpieza en varios puntos de entrada

VirusScan supervisa y limpia en los puntos de entrada clave del equipo: correo electrónico, archivos adjuntos de mensajes instantáneos y descargas de Internet.

Supervisión de las actividades características de los gusanos en el correo electrónico

WormStopper™ impide que los troyanos envíen gusanos a través del correo electrónico a otros equipos y pregunta al usuario antes de que programas de correo electrónico desconocidos envíen mensajes a otros equipos.

Supervisión de actividades características de los gusanos en las secuencias de comandos

ScriptStopper™ impide que se ejecuten secuencias de comandos dañinas en el equipo.

McAfee X-ray para Windows

McAfee X-ray detecta y elimina los kits de raíz y otros programas que están ocultos para Windows.

Protección contra desbordamientos del búfer

Esta protección impide que el búfer se desborde. Los desbordamientos del búfer pueden tener lugar si un programa o proceso sospechoso intenta guardar datos en el búfer (área de almacenamiento temporal de datos del equipo) por encima del límite, con lo que los datos de los búfers adyacentes se sobrescriben o se dañan.

McAfee SystemGuards

Los guardianes del sistema examinan el equipo en busca de determinados comportamientos que pudieran constituir una señal de actividad de virus, software espía o piratas informáticos.

CAPÍTULO 14

Gestión de la protección antivirus

Puede gestionar en tiempo real la protección antivirus, la protección de software espía, la protección de secuencias de comandos y los guardianes del sistema. Por ejemplo, puede deshabilitar análisis o especificar los elementos que desea analizar.

Sólo los usuarios con derechos de administrador pueden modificar las opciones avanzadas.

En este capítulo

Utilización de la protección antivirus

Cuando se inicia la protección antivirus (análisis en tiempo real), el equipo se supervisa ininterrumpidamente con el fin de detectar posibles actividades de los virus. El análisis en tiempo real examina los archivos cada vez que el usuario o el equipo accede a ellos. Cuando la protección antivirus detecta un archivo infectado, intenta limpiarlo y eliminar la infección. Si el archivo no se puede limpiar ni eliminar, aparece un mensaje de alerta en el que se solicita información sobre la acción que debe llevarse a cabo.

Temas relacionados

- Descripción de las alertas de seguridad (página 105)

Desactivar la protección antivirus

Si se desactiva la protección antivirus, el equipo no se supervisa continuamente para detectar posibles actividades de virus. Si necesita detener la protección antivirus, asegúrese de que la conexión a Internet está deshabilitada.

Nota: al desactivar la protección antivirus, también se desactiva la protección contra software espía, la protección de correo electrónico y de mensajería instantánea en tiempo real.

Para deshabilitar la protección antivirus:

1. En el menú avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección antivirus**, haga clic en **Desactivado**.
4. En el cuadro de diálogo de confirmación, realice una de las operaciones siguientes:
   - Para restablecer la protección antivirus después de un tiempo especificado, active la casilla **Volver a activar el análisis en tiempo real después de** y seleccione un período en el menú.
   - Para detener la protección antivirus tras iniciarla después de un tiempo especificado, desactive la casilla **Volver a activar la protección antivirus después de**.

5 Haga clic en **Aceptar**.

Si la protección en tiempo real se configura para que se inicie junto con Windows, el equipo estará protegido cuando reinicie el equipo.

Temas relacionados

- Configuración de la protección en tiempo real (página 76)

Activación de la protección antivirus

La protección antivirus supervisa la actividad de los virus del equipo.

Para habilitar la protección antivirus:

1 En el menú Avanzado, haga clic en **Configurar**.

2 En el panel Configurar, haga clic en **Equipo & Archivos**.

3 En **Protección antivirus**, haga clic en **Activado**.

Configuración de la protección en tiempo real

Puede modificar la protección antivirus en tiempo real. Es posible, por ejemplo, que sólo desee analizar documentos y archivos de programa o que desee desactivar el análisis en tiempo real al iniciar Windows (desaconsejado).

Configuración de la protección en tiempo real

Puede modificar la protección antivirus en tiempo real. Es posible, por ejemplo, que sólo desee analizar documentos y archivos de programa o que desee desactivar el análisis en tiempo real al iniciar Windows (desaconsejado).

Para configurar la protección en tiempo real:

1. En el menú avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección antivirus**, haga clic en **Opciones avanzadas**.
4. Active o desactive las casillas siguientes:
   - **Buscar virus nuevos desconocidos con la opción de heurística**: Los archivos se comparan con las firmas de virus conocidas para detectar indicios de virus no identificados. Esta opción proporciona el análisis más completo, pero suele resultar más lenta que un análisis normal.
   - **Analizar la unidad A al apagar el equipo**: Cuando se apaga el equipo, se analiza la unidad A.
   - **Buscar software espía y programas potencialmente no deseados**: El software espía, el software publicitario y otros programas que pueden recopilar y transmitir datos sin su permiso se detectan y eliminan.
   - **Analizar y eliminar las cookies de rastreo**: Se detectan y se eliminan las cookies que pueden recopilar y transmitir datos sin su permiso. Una cookie identifica a los usuarios cuando visitan una página Web.
   - **Analizar unidades de red**: Se analizan las unidades conectadas a la red.
   - **Activar protección contra desbordamiento de búfer**: Si se detecta actividad de desbordamiento del búfer, se bloquea y se alerta al usuario.
   - **Iniciar análisis en tiempo real al iniciar Windows (recomendado)**: La protección en tiempo real se activa cada vez que se inicia el equipo, incluso si se desactiva la protección durante una sesión.
5. Haga clic en uno de los botones siguientes:
   - **Todos los archivos (recomendado)**: Se analizan todos los archivos que utiliza el equipo. Utilice esta opción para obtener el máximo provecho posible del análisis.

- **Solamente archivos de programas y documentos**: Sólo se analizan los documentos y los archivos de programa.

6 Haga clic en **Aceptar**.

Utilización de la protección contra software espía

La protección contra software espía elimina el software espía, el software publicitario y cualquier otro programa no deseado que pudiera recopilar o transmitir información sin su permiso.

Desactivación de la protección contra software espía

Si desactiva la protección contra software espía, no se detectarán los programas no deseados que pueden recopilar y transmitir información sin su permiso.

Para deshabilitar la protección contra software espía:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección contra software espía**, haga clic en **Desactivado**.

Activación de la protección contra software espía

La protección contra software espía elimina el software espía, el software publicitario y cualquier otro programa no deseado que pudiera recopilar o transmitir información sin su permiso.

Para habilitar la protección contra software espía:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección contra software espía**, haga clic en **Activado**.

Utilización de los guardianes del sistema

Los guardianes del sistema detectan posibles cambios no autorizados en el equipo y alertan al usuario si estos cambios se producen. El usuario podrá revisar los cambios y decidir si desea admitirlos.

Los guardianes del sistema se clasifican como se describe a continuación.

Programa

Los guardianes del sistema de programas detectan los cambios en los archivos de inicio, las extensiones y los archivos de configuración.

Windows

Los guardianes del sistema de Windows detectan los cambios en la configuración de Internet Explorer, incluidos los atributos y los parámetros de seguridad del navegador.

Navegador

Los guardianes del sistema del navegador detectan los cambios en los servicios, los certificados y los archivos de configuración de Windows.

Desactivación de los guardianes del sistema

Si se desactivan los guardianes del sistema, no se detectarán los cambios no autorizados en el equipo.

Para deshabilitar todos los guardianes del sistema:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección del guardián del sistema**, haga clic en **Desactivado**.

Activación de los guardianes del sistema

Los guardianes del sistema detectan posibles cambios no autorizados en el equipo y alertan al usuario si estos cambios se producen.

Para habilitar los guardianes del sistema:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección del guardián del sistema**, haga clic en **Activado**.

Configuración de los guardianes del sistema

Los guardianes del sistema se pueden modificar. Cada vez que se detecta un cambio, el usuario puede decidir si desea que aparezca un aviso y que se registre el evento, si sólo desea que se registre el evento o si desea desactivar el guardián del sistema.

Configuración de los guardianes del sistema

Los guardianes del sistema se pueden modificar. Cada vez que se detecta un cambio, el usuario puede decidir si desea que aparezca un aviso y que se registre el evento, si sólo desea que se registre el evento o si desea desactivar el guardián del sistema.

Para configurar los guardianes del sistema:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección de guardianes del sistema**, haga clic en **Opciones avanzadas**.
4. En la lista de guardianes del sistema, haga clic en una categoría para ver un listado con los guardianes del sistema asociados y su estado.
5. Haga clic en el nombre de un guardián del sistema.
6. En **Detalles**, consulte la información sobre el guardián del sistema.
7. En **Deseo**, elija una de las siguientes opciones:
   - Haga clic en **Mostrar alertas** si desea que se emita un aviso cuando se produzca un cambio y se registre el evento.
   - Haga clic en **Sólo cambios de registro** si no desea que se lleve a cabo ninguna acción cuando se detecte un cambio. El cambio se incluye en el registro únicamente.
   - Haga clic en **Desactivar este guardián del sistema** para deshabilitar el guardián del sistema. No se emitirá ningún aviso cuando se produzca un cambio y no se registrará el evento.
8. Haga clic en **Aceptar**.

Descripción de los guardianes del sistema

Los guardianes del sistema detectan posibles cambios no autorizados en el equipo y alertan al usuario si estos cambios se producen. El usuario podrá revisar los cambios y decidir si desea admitirlos.

Los guardianes del sistema se clasifican como se describe a continuación.

Programa

Los guardianes del sistema de programas detectan los cambios en los archivos de inicio, las extensiones y los archivos de configuración.

Windows

Los guardianes del sistema de Windows detectan los cambios en la configuración de Internet Explorer, incluidos los atributos y los parámetros de seguridad del navegador.

Navegador

Los guardianes del sistema del navegador detectan los cambios en los servicios, los certificados y los archivos de configuración de Windows.

Acerca de los guardianes del sistema de programas

Los guardianes del sistema de programas detectan los elementos siguientes:

Instalaciones de ActiveX

Detectan programas ActiveX que se han descargado a través de Internet Explorer. Los programas ActiveX se descargan de sitios Web y se guardan en el equipo en C:\Windows\Downloaded Program Files o en C:\Windows\Temp\Archivos temporales de Internet. También se incluye una referencia en el registro mediante su CLSID (cadena numérica larga entre llaves).

Internet Explorer utiliza muchos programas ActiveX legítimos. Si tiene alguna duda sobre algún programa ActiveX, puede borrarlo sin problema, ya que no causará daño alguno al equipo. Si posteriormente necesita este programa, Internet Explorer lo descargará automáticamente la próxima vez que visite un sitio Web en el que sea necesario.

Elementos de inicio

Controlan los cambios realizados en las carpetas y las claves de registro de inicio. Las claves del registro de inicio del Registro de Windows y las carpetas de inicio del menú Inicio almacenan las rutas de los programas del equipo. Los programas que aparecen en estas ubicaciones se cargan cuando se inicia Windows. Algunas aplicaciones de software espía y programas no deseados intentan cargarse automáticamente al iniciar Windows.

Hooks de ejecución en Shell de Windows

Controlan los cambios realizados en la lista de programas que se cargan en explorer.exe. Un hook de ejecución en Shell es un programa que se carga en el shell de Windows (explorer.exe). Los programas de hook de ejecución en Shell reciben todos los comandos que se ejecutan en el equipo. Cualquier programa que se cargue en el shell explorer.exe puede realizar una tarea adicional antes de que otro programa se inicie realmente. Algunas aplicaciones de software espía y programas no deseados pueden utilizar hooks de ejecución en shell para impedir que se inicien los programas de seguridad.

Carga retrasada de objeto de servicio de Shell

Supervisan los cambios que se realizan en los archivos que aparecen en la carga retrasada de objeto de servicio de Shell. Estos archivos se cargan mediante explorer.exe cuando se inicia el equipo. Dado que explore.exe es el shell del equipo, se inicia siempre, y carga los archivos que figuren bajo esta clave. Dichos archivos se cargan al principio de la rutina de inicio, antes de que intervenga el usuario.

Acerca de los guardianes del sistema de Windows

Los guardianes del sistema de Windows detectan los elementos siguientes:

Identificadores de menús contextuales

Impiden que se realicen cambios no autorizados en los menús contextuales de Windows. Estos menús permiten hacer clic con el botón derecho del ratón en un archivo y llevar a cabo acciones específicas en dichos archivos.

AppInit DLLs

Impiden que se realicen cambios o se agreguen elementos no autorizados al valor AppInit.DLLs de Windows. El valor de registro AppInit_DLLs contiene una lista de archivos que se cargan cuando se carga el archivo user32.dll. Los archivos incluidos en el valor AppInit_DLLs se cargan al principio de la rutina de inicio de Windows, con lo que los archivos .DLL potencialmente dañinos se ocultan antes de que un usuario intervenga.

Archivo Hosts de Windows

Supervisan los cambios que se realizan en el archivo Hosts del equipo. Este archivo se utiliza para redirigir algunos nombres de dominio a determinadas direcciones IP. Por ejemplo, si visita www.example.com, su navegador buscará en el archivo Hosts y, si ve una entrada que corresponda a example.com, se dirigirá a la dirección IP de dicho dominio. Algunos programas de software espía intentan modificar el archivo Hosts para redirigir la navegación a otro sitio o para impedir la correcta actualización del software.

Shell Winlogon

Controlan el Shell Winlogon. Este Shell se carga cuando un usuario inicia sesión en Windows. El Shell es la interfaz de usuario (IU) principal que se utiliza para administrar Windows y suele ser el Explorador de Windows (explore.exe). Sin embargo, el Shell de Windows puede modificarse fácilmente para que apunte a otro programa. Si se hace, se utilizará un programa diferente al Shell de Windows cada vez que un usuario inicie sesión.

Winlogon User Init

Controlan los cambios que tienen lugar en la configuración de inicio de sesión de Windows. La clave HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit establece qué programa se va a ejecutar después de que el usuario inicie sesión en Windows. El programa predeterminado restablece el perfil, las fuentes, los colores y otras opciones del nombre de usuario. El software espía y otros programas no deseados pueden intentar ejecutarse incluyéndose ellos mismos en esta clave.

Protocolos Windows

Controlan los cambios realizados en los protocolos de red. Algunas aplicaciones de software espía y otros programas no deseados toman control de ciertos métodos mediante los cuales el equipo envía y recibe información. Para ello, utilizan filtros e identificadores de protocolos de Windows.

Proveedores de servicios por niveles de Winsock

Controlan los proveedores de servicios por niveles (LSP), que pueden interceptar los datos en la red, modificarlos o redirigirlos. Los LSP legítimos incluyen software de control paterno, cortafuegos y otros programas de seguridad. El software espía puede utilizar los LSP para controlar la actividad de Internet y modificar los datos del usuario. Si no desea instalar de nuevo el sistema operativo, utilice los programas de McAfee para que eliminen automáticamente el software espía y los LSP comprometidos.

Comandos de apertura de Shell de Windows

Impiden que se realicen cambios en los comandos de apertura del Shell de Windows (explorer.exe). Los comandos de apertura del Shell hacen que, cada vez que se abra un tipo de archivo, se abra siempre el mismo programa concreto. Por ejemplo, los gusanos pueden intentar ejecutarse cada vez que se abre una aplicación .exe.

Planificador de tareas compartidas

Supervisan la clave de registro SharedTaskScheduler (planificador de tareas compartidas), que contiene una lista de programas que se ejecutan al iniciar Windows. Algunas aplicaciones de software espía y otros programas potencialmente no deseados modifican esta clave y se agregan a la lista sin permiso del usuario.

Windows Messenger Service

Controlan Windows Messenger Service, una función sin documentar de Windows Messenger que permite a los usuarios enviar mensajes instantáneos. Algunas aplicaciones de software espía y otros programas no deseados intentan activar el servicio y enviar anuncios no solicitados. El servicio puede utilizarse igualmente mediante una vulnerabilidad conocida para ejecutar código de forma remota.

Archivo Win.ini de Windows

Win.ini es un archivo basado en texto que proporciona la lista de programas que se deben ejecutar cuando se inicia Windows. La sintaxis para cargar estos programas se encuentra en el archivo que se utiliza para admitir las versiones anteriores de Windows. La mayor parte de los programas no utilizan el archivo win.ini para cargar los programas; sin embargo, algunas aplicaciones de software espía y otros programas no deseados están diseñados para aprovechar esta sintaxis y cargarse durante el inicio de Windows.

Acerca de los guardianes del sistema del navegador

Los guardianes del sistema del navegador detectan los elementos siguientes:

Objetos de ayuda del navegador

Controlan los contenidos que se agregan a los objetos de ayuda del navegador (BHO). Los BHO son programas que funcionan como complementos de Internet Explorer. Los programas de software espía y los secuestradores del navegador suelen utilizar los BHO para mostrar anuncios o realizar un seguimiento de los hábitos de navegación del usuario. Muchos programas legítimos, como las barras de herramientas de búsqueda, utilizan BHO.

Barras de Internet Explorer

Controlan los cambios que se efectúan en la lista de programas de las barras de Internet Explorer. La barra de un explorador es un panel, como Búsqueda, Favoritos o Historial, que se ve en Internet Explorer (IE) o en el Explorador de Windows.

Complementos de Internet Explorer

Impiden que se instale software espía desde los complementos de Internet Explorer. Los complementos de Internet Explorer son elementos de software complementarios que se cargan cuando se inicia Internet Explorer. El software espía utiliza, por lo general, los complementos de Internet Explorer para mostrar anuncios o hacer un seguimiento de los hábitos de navegación del usuario. Los complementos legítimos agregan funcionalidad a Internet Explorer.

ShellBrowser de Internet Explorer

Supervisan los cambios que se producen en la instancia ShellBrowser de Internet Explorer. El ShellBrowser de Internet Explorer contiene información y parámetros sobre una instancia de Internet Explorer. Si se cambian esos parámetros o se agrega un nuevo ShellBrowser, dicho ShellBrowser tomará el control absoluto sobre Internet Explorer y agregará diferentes funciones, como barras de herramientas, menús y botones.

WebBrowser de Internet Explorer

Supervisan los cambios que se producen en la instancia WebBrowser de Internet Explorer. El WebBrowser de Internet Explorer contiene información y parámetros sobre una instancia de Internet Explorer. Si se cambian esos parámetros o se agrega un nuevo WebBrowser, dicho WebBrowser tomará el control absoluto sobre Internet Explorer y agregará diferentes funciones, como barras de herramientas, menús y botones.

Hook de búsqueda de direcciones URL de Internet Explorer

Controlan los cambios realizados en el hook de búsqueda de direcciones URL de Internet Explorer. Los hooks de búsqueda de direcciones URL se utilizan al escribir una dirección en la barra de direcciones del navegador sin especificar el protocolo, como http:// o ftp://. Al escribir dicha dirección, el navegador puede utilizar el hook de búsqueda de direcciones URL para buscar en Internet la ubicación especificada.

Direcciones URL de Internet Explorer

Controla los cambios realizados en las URL predefinidas de Internet Explorer. Esto evita que las aplicaciones de software espía y otros programas no deseados puedan modificar los parámetros de configuración del navegador sin su permiso.

Restricciones de Internet Explorer

Supervisan las restricciones de Internet Explorer, lo que permite al administrador del equipo impedir que un usuario cambie la página de inicio u otras opciones de Internet Explorer. Dichas opciones sólo aparecerán si el administrador así lo especifica.

Zonas de seguridad de Internet Explorer

Supervisan las zonas de seguridad de Internet Explorer. Internet Explorer tiene cuatro zonas de seguridad predefinidas: Internet, Intranet local, Sitios de confianza y Sitios restringidos. Cada zona de seguridad tiene su propia configuración, que puede ser predefinida o personalizada. Las zonas de seguridad son uno de los objetivos de algunas aplicaciones de software espía y otros programas no deseados, ya que la reducción del nivel de seguridad permite que dichos programas burlen las alertas de seguridad y actúen sin que sea posible detectarlos.

Sitios de confianza de Internet Explorer

Supervisan los sitios de confianza de Internet Explorer. La lista de sitios de confianza es un directorio de los sitios Web que se han definido como fiables. Algunas aplicaciones de software espía y otros programas no deseados se dirigen a esta lista, ya que ofrece un método para establecer como fiables sitios sospechosos sin el conocimiento del usuario.

Directiva de Internet Explorer

Supervisan las directivas de Internet Explorer. Los administradores de sistema son los que modifican estas configuraciones de directivas, pero es posible que el software espía también las utilice y aproveche. Las modificaciones pueden impedirle que defina una Página de inicio distinta o pueden ocultar etiquetas de su vista en el cuadro de diálogo Opciones de Internet del menú Herramientas.

Utilización del análisis de secuencias de comandos

Una secuencia de comandos puede crear, copiar o eliminar archivos. También puede abrir el Registro de Windows.

El análisis de secuencias de comandos impide que se ejecuten secuencias de comandos dañinas conocidas en el equipo.

Desactivación del análisis de secuencias de comandos

Si se desactiva el análisis de secuencias de comandos, no se detectará la ejecución de secuencias de comandos sospechosas.

Para deshabilitar el análisis de secuencias de comandos:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección de análisis de secuencias de comandos**, haga clic en **Desactivado**.

Activación del análisis de secuencias de comandos

El análisis de secuencias de comandos avisa si la ejecución de una secuencia de comandos produce la creación, copia o eliminación de archivos, o bien la apertura del Registro de Windows.

Para habilitar el análisis de secuencias de comandos:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección de análisis de secuencias de comandos**, haga clic en **Activado**.

Utilización de la protección de correo electrónico

La protección de correo electrónico detecta y bloquea las amenazas de los mensajes de correo entrantes (POP3) y salientes (SMTP), y de los archivos adjuntos, incluidos los virus, troyanos, gusanos, software espía, software publicitario y otras amenazas.

Desactivación de la protección de correo electrónico

Si desactiva la protección de correo electrónico, no se detectarán las amenazas potenciales de los mensajes de correo electrónico entrantes (POP3) y salientes (SMTP) ni de los archivos adjuntos.

Para deshabilitar la protección de correo electrónico

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico & MI**.
3. En **Protección de correo electrónico**, haga clic en **Desactivado**.

Activación de la protección de correo electrónico

La protección de correo electrónico detecta amenazas en los mensajes de correo electrónico entrantes (POP3) y salientes (SMTP) y los archivos adjuntos.

Para habilitar la protección de correo electrónico

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico & MI**.
3. En **Protección de correo electrónico**, haga clic en **Activado**.

Configuración de la protección de correo electrónico

Las opciones de protección de correo electrónico permiten analizar los mensajes de correo electrónico entrantes y salientes, y los gusanos. Los gusanos replican y consumen los recursos del sistema, reducen su rendimiento o interrumpen tareas. Los gusanos pueden enviar copias de sí mismos a través de los mensajes de correo electrónico. Por ejemplo, pueden intentar reenviar mensajes de correo electrónico a los contactos de la libreta de direcciones.

Configuración de la protección de correo electrónico

Las opciones de protección de correo electrónico permiten analizar los mensajes de correo electrónico entrantes y salientes, y los gusanos.

Para configurar la protección de correo electrónico:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico & MI**.
3. En **Protección de correo electrónico**, haga clic en **Opciones avanzadas**.
4. Active o desactive las casillas siguientes:
   - **Analizar mensajes de correo electrónicos entrantes**: Los mensajes entrantes (POP3) se analizan en busca de amenazas potenciales.
   - **Analizar mensajes de correo electrónico salientes**: Los mensajes salientes (SMTP) se analizan en busca de amenazas potenciales.
   - **Activar WormStopper**: WormStopper bloquea los gusanos de los mensajes de correo electrónico.
5. Haga clic en **Aceptar**.

Utilización de la protección de mensajería instantánea

La protección de mensajería instantánea detecta amenazas en los archivos adjuntos a los mensajes instantáneos entrantes.

Desactivación de la protección de mensajería instantánea

Si desactiva la protección de mensajería instantánea, no se detectarán las amenazas de los archivos adjuntos a los mensajes instantáneos entrantes.

Para deshabilitar la protección de mensajería instantánea:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico & MI**.
3. En **Protección para mensajería instantánea**, haga clic en **Desactivado**.

Activación de la protección de mensajería instantánea

La protección para mensajería instantánea detecta amenazas en los archivos adjuntos a los mensajes instantáneos entrantes.

Para habilitar la protección para mensajería instantánea:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico & MI**.
3. En **Protección para mensajería instantánea**, haga clic en **Activado**.

CAPÍTULO 15

Análisis manual del equipo

Puede buscar virus y otras amenazas en las unidades de disco duro, unidades de disquete y en cada carpeta y archivo. Cuando VirusScan localiza un archivo sospechoso, intenta limpiarlo, a menos que se trate de un programa potencialmente no deseado. Si VirusScan no puede limpiar el archivo, el usuario puede ponerlo en cuarentena o eliminarlo.

En este capítulo

Análisis manual

Puede realizar análisis manuales en todo momento. Por ejemplo, si acaba de instalar VirusScan, puede realizar un análisis para comprobar que el equipo no tiene virus ni otras amenazas. Asimismo, si ha desactivado el análisis en tiempo real, puede realizar un análisis para comprobar que el equipo sigue protegido.

Realizar un análisis con las opciones de análisis manual

En este tipo de análisis se utilizan las opciones de análisis manual definidas por el usuario. VirusScan analiza los archivos comprimidos (.zip, .cab, etc.), aunque contabiliza cada archivo comprimido como un solo archivo. Además, el número de archivos analizados puede variar si se han eliminado los archivos temporales de Internet desde el último análisis.

Para realizar análisis utilizando las opciones de análisis manual:

1. En el menú Básico, haga clic en **Analizar**. Una vez que haya finalizado el análisis, se mostrará un resumen con el número de elementos examinados y detectados, el número de elementos limpiados y la fecha del último análisis.
2. Haga clic en **Finalizar**.

Temas relacionados

- Configuración de análisis manuales (página 96)

Realizar un análisis sin utilizar las opciones de análisis manual

En este tipo de análisis no se utilizan las opciones de análisis manual que define el usuario. VirusScan analiza los archivos comprimidos (.zip, .cab, etc.), aunque contabiliza cada archivo comprimido como un solo archivo. Además, el número de archivos analizados puede variar si se han eliminado los archivos temporales de Internet desde el último análisis.

Para realizar un análisis sin utilizar las opciones de análisis manual:

1. En el menú Avanzado, haga clic en **Inicio**.
2. En el panel Inicio, haga clic en **Analizar**.
3. En **Ubicaciones para el análisis**, active las casillas situadas junto a los archivos, carpetas y unidades que desea analizar.
4. En **Opciones**, active las casillas situadas junto al tipo de archivos que desea analizar.
5. Haga clic en **Analizar ahora**. Una vez que haya finalizado el análisis, se mostrará un resumen con el número de elementos examinados y detectados, el número de elementos limpiados y la fecha del último análisis.
6. Haga clic en **Finalizar**.

Nota: estas opciones no se guardan.

Realizar un análisis en el Explorador de Windows

Puede buscar virus y otras amenazas en los archivos, las carpetas o las unidades seleccionadas en el Explorador de Windows.

Para analizar archivos en el Explorador de Windows:

1. Abra el Explorador de Windows.
2. Haga clic con el botón derecho del ratón en la unidad, la carpeta o el archivo que desea analizar y, a continuación, haga clic en **Analizar**. Todas las opciones predeterminadas de análisis estarán seleccionadas para proporcionar un análisis exhaustivo.

Configuración de análisis manuales

Cuando se realiza un análisis manual o programado, se puede especificar el tipo de archivos y las ubicaciones que se van a analizar, así como el momento en que se ejecutará dicho análisis.

Configuración del tipo de archivos que se va a analizar

Puede configurar el tipo de archivos que desea analizar.

Para configurar el tipo de archivos que se va a analizar:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección antivirus**, haga clic en **Opciones avanzadas**.
4. En el panel Protección antivirus, haga clic en **Análisis manual**.
5. Active o desactive las casillas siguientes:
   - **Buscar virus nuevos desconocidos con la opción de heurística**: Los archivos se comparan con las firmas de virus conocidas para detectar indicios de virus no identificados. Esta opción proporciona el análisis más completo, pero suele resultar más lenta que un análisis normal.
   - **Buscar en archivos .zip y otros archivos de almacenamiento**: Detecta y elimina los virus de los archivos .zip y otros archivos de almacenamiento. En ocasiones, los creadores de virus colocan virus en un archivo .zip y, a su vez, insertan este archivo .zip dentro de otro archivo .zip con el objeto de intentar eludir la acción de los analizadores antivirus.
   - **Buscar software espía y programas potencialmente no deseados**: El software espía, el software publicitario y otros programas que pueden recopilar y transmitir datos sin su permiso se detectan y eliminan.
   - **Analizar y eliminar las cookies de rastreo**: Se detectan y se eliminan las cookies que pueden recopilar y transmitir datos sin su permiso. Una cookie identifica a los usuarios cuando visitan una página Web.
   - **Buscar kits de raíz y otros programas furtivos**: Detecta y elimina todos los kits de raíz y otros programas ocultos de Windows.
6. Haga clic en uno de los botones siguientes:
   - **Todos los archivos (recomendado)**: Se analizan todos los archivos que utiliza el equipo. Utilice esta opción para obtener el máximo provecho posible del análisis.
   - **Solamente archivos de programas y documentos**: Sólo se analizan los documentos y los archivos de programa.

7 Haga clic en **Aceptar**.

Configuración de las ubicaciones que se van a analizar

Puede configurar análisis manuales o programados en las ubicaciones que desea examinar.

Para configurar las ubicaciones que se van a analizar:

1 En el menú Avanzado, haga clic en **Configurar**.

2 En el panel Configurar, haga clic en **Equipo & Archivos**.

3 En **Protección antivirus**, haga clic en **Opciones avanzadas**.

4 En el panel Protección antivirus, haga clic en **Análisis manual**.

5 En **Ubicación predeterminada para el análisis**, seleccione los archivos, las carpetas y las unidades que desea analizar.

Para obtener el máximo provecho del análisis, asegúrese de que ha seleccionado **Archivos importantes**.

6 Haga clic en **Aceptar**.

Análisis programados

Puede programar los análisis para examinar exhaustivamente el equipo en busca de virus y otras amenazas en los intervalos que especifique.

Para programar un análisis:

1 En el menú Avanzado, haga clic en **Configurar**.

2 En el panel Configurar, haga clic en **Equipo & Archivos**.

3 En **Protección antivirus**, haga clic en **Opciones avanzadas**.

4 En el panel Protección antivirus, haga clic en **Análisis programado**.

5 Asegúrese de que la opción **Activar análisis programado** está seleccionada.

6 Active la casilla de selección situada junto al día de la semana en que se va a efectuar el análisis.

7 Haga clic en los valores de las listas de hora de inicio para especificar una hora de inicio.

8 Haga clic en **Aceptar**.

Sugerencia: Para utilizar una programación predeterminada, haga clic en **Restablecer**.

CAPÍTULO 16

Administración de VirusScan

Puede eliminar elementos de las listas de confianza, gestionar los programas, las cookies y los archivos que están en cuarentena, consultar eventos y registros y notificar cualquier actividad sospechosa a McAfee.

En este capítulo

Gestión de listas de confianza

Cuando un guardián del sistema, programa, desbordamiento del búfer o programa de correo electrónico son de confianza, se incluyen en una lista de confianza para que no se detecten nunca más.

Si, por error, la lista incluye un programa que desea que se detecte, debe eliminarlo de dicha lista.

Gestión de listas de confianza

Cuando un guardián del sistema, programa, desbordamiento del búfer o programa de correo electrónico son de confianza, se incluyen en una lista de confianza para que no se detecten nunca más.

Si, por error, la lista incluye un programa que desea que se detecte, debe eliminarlo de dicha lista.

Para eliminar elementos de las listas de confianza:

1. En el menú Avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Equipo & Archivos**.
3. En **Protección antivirus**, haga clic en **Opciones avanzadas**.
4. En el panel Protección antivirus, haga clic en **Listas de confianza**.
5. En la lista seleccione un guardián de sistema, un programa, un desbordamiento del búfer o un programa de correo electrónico para consultar sus elementos y su estado de confianza.
6. En **Detalles**, consulte la información sobre el elemento.
7. En **Deseo**, haga clic en una acción.
8. Haga clic en **Aceptar**.

Gestión de programas, cookies y archivos en cuarentena

Los programas, las cookies y los archivos en cuarentena se pueden restaurar, suprimir o enviar a McAfee para su análisis.

Restauración de programas, cookies y archivos en cuarentena

Si procede, puede restaurar programas, cookies y archivos que estén en cuarentena.

Para restaurar programas, cookies y archivos en cuarentena:

1. En el menú Avanzado, haga clic en **Restaurar**.
2. En el panel de restauración, haga clic en **Programas y cookies** o en **Archivos**, según corresponda.
3. Seleccione los programas, las cookies o los archivos en cuarentena que desea restaurar.
4. Para obtener más información acerca del virus que está en cuarentena, haga clic en su nombre de detección, en **Detalles**. Se abrirá la Biblioteca de información sobre virus con la descripción del virus.
5. En **Deseo**, haga clic en **Restaurar**.

Eliminación de programas, cookies y archivos en cuarentena

Puede eliminar programas, cookies y archivos en cuarentena.

Para eliminar programas, cookies y archivos en cuarentena:

1. En el menú Avanzado, haga clic en **Restaurar**.
2. En el panel de restauración, haga clic en **Programas y cookies** o en **Archivos**, según corresponda.
3. Seleccione los programas, las cookies o los archivos en cuarentena que desea restaurar.
4. Para obtener más información acerca del virus que está en cuarentena, haga clic en su nombre de detección, en **Detalles**. Se abrirá la Biblioteca de información sobre virus con la descripción del virus.
5. En **Deseo**, haga clic en **Eliminar**.

Envío de programas, cookies y archivos en cuarentena a McAfee

Puede enviar programas, cookies y archivos en cuarentena a McAfee para que los analice.

Nota: Si el archivo en cuarentena que desea enviar supera un tamaño máximo, podría ser rechazado. No obstante, esto no ocurre casi nunca.

Para enviar programas o archivos en cuarentena a McAfee:

1. En el menú Avanzado, haga clic en **Restaurar**.
2. En el panel de restauración, haga clic en **Programas y cookies** o en **Archivos**, según corresponda.
3. Seleccione los programas, cookies o archivos en cuarentena que desea enviar a McAfee.
4. Para obtener más información acerca del virus que está en cuarentena, haga clic en su nombre de detección, en **Detalles**. Se abrirá la Biblioteca de información sobre virus con la descripción del virus.
5. En **Deseo**, haga clic en **Enviar a McAfee**.

Consulta de eventos y registros recientes

Los eventos y los registros recientes muestran las incidencias de todos los productos de McAfee instalados.

En Eventos recientes, podrá ver los últimos 30 eventos importantes que han tenido lugar en su equipo. Puede restaurar programas bloqueados, reactivar el análisis en tiempo real y confiar en desbordamientos del búfer.

También puede consultar los registros, en los que figura cada uno de los eventos que se ha producido durante los últimos 30 días.

Visualización de eventos

En Eventos recientes, podrá ver los últimos 30 eventos importantes que han tenido lugar en su equipo. Puede restaurar programas bloqueados, reactivar el análisis en tiempo real y confiar en desbordamientos del búfer.

Para consultar los eventos:

1. En el menú Avanzado, haga clic en **Informes & registros**.
2. En el panel Informes & registros, haga clic en **Eventos recientes**.
3. Seleccione el evento que desea consultar.
4. En **Detalles**, consulte la información sobre el evento.
5. En **Deseo**, haga clic en una acción.

Consulta de registros

Los registros recogen todos los eventos que se han producido durante los últimos 30 días.

Para consultar los registros:

1. En el menú Avanzado, haga clic en **Informes & registros**.
2. En el panel Informes & registros, haga clic en **Eventos recientes**.
3. En el panel Eventos recientes, haga clic en **Ver registro**.
4. Seleccione el tipo de registro que desea consultar y, a continuación, seleccione un registro.
5. En **Detalles**, consulte la información sobre el registro.

Notificación automática de información anónima

Puede enviar virus, programas no deseados e información de rastreo de piratas informáticos de forma anónima a McAfee. Esta opción sólo está disponible durante la instalación.

No se recopila información personal que pueda identificar al usuario.

Notificar a McAfee

Puede enviar virus, programas no deseados e información de rastreo de piratas informáticos a McAfee. Esta opción sólo está disponible durante la instalación.

Para enviar automáticamente información anónima:

1. Durante la instalación de VirusScan, acepte la opción predeterminada **Enviar información anónima**.
2. Haga clic en **Siguiente**.

Descripción de las alertas de seguridad

Si el análisis en tiempo real detecta una amenaza, se mostrará una alerta. El análisis en tiempo real intenta limpiar automáticamente la mayor parte de los virus, troyanos, secuencias de comandos y gusanos y alertar al usuario. En los programas no deseados y en los guardianes del sistema, el análisis en tiempo real detecta el archivo o una modificación que se haya producido y envía una alerta. Por lo que respecta al desbordamiento del búfer, las cookies de rastreo y la actividad de secuencias de comandos, el análisis en tiempo real bloquea automáticamente la actividad y alerta al usuario.

Las alertas se agrupan en tres tipos básicos.

- Alerta roja
- Alerta amarilla
- Alerta verde

Puede seleccionar el modo en que desea gestionar los archivos y los correos detectados, las secuencias de comandos sospechosas, los posibles gusanos, los programas no deseados, los guardianes del sistema o los desbordamientos del búfer.

Gestión de alertas

McAfee emplea todo un abanico de alertas para gestionar la seguridad con mayor facilidad. Las alertas se agrupan en tres tipos básicos.

- Alerta roja
- Alerta amarilla
- Alerta verde

Alerta roja

Una alerta roja requiere la respuesta del usuario. En algunos casos, McAfee no puede determinar automáticamente cómo debe responder ante una determinada actividad. En estos casos, la alerta roja describe la actividad en cuestión, y proporciona una o varias opciones para que el usuario elija.

Alerta amarilla

Una alerta amarilla es una notificación no crítica que normalmente requiere una respuesta del usuario. La alerta amarilla describe la actividad en cuestión, y proporciona una o varias opciones para que el usuario elija.

Alerta verde

En la mayoría de los casos, una alerta verde proporciona información básica acerca de un evento y no requiere ningún tipo de respuesta.

Configuración de las opciones de alerta

Si decide no mostrar de nuevo una alerta y posteriormente cambia de opinión, puede volver a atrás y configurarla para que aparezca de nuevo. Para obtener más información acerca de cómo configurar las opciones de alerta, consulte la documentación del centro de seguridad (SecurityCenter).

CAPÍTULO 17

Ayuda adicional

En este capítulo se incluyen preguntas frecuentes y escenarios de solución de problemas.

En este capítulo

Preguntas más frecuentes

En esta sección se da respuesta a las preguntas más frecuentes.

Se ha detectado una amenaza, ¿qué debo hacer?

McAfee utiliza alertas para ayudale a gestionar la seguridad. Las alertas se agrupan en tres tipos básicos.

- Alerta roja
- Alerta amarilla
- Alerta verde

Puede seleccionar el modo en que desea gestionar los archivos y los correos detectados, las secuencias de comandos sospechosas, los posibles gusanos, los programas no deseados, los guardianes del sistema o los desbordamientos del búfer.

Para obtener más información sobre la gestión de amenazas específicas, consulte la Biblioteca de información sobre virus en: http://us.mcafee.com/virusInfo/default.asp?affid=.

Temas relacionados

- Descripción de las alertas de seguridad (página 105)

¿Puedo utilizar VirusScan con los navegadores de Netscape, Firefox y Opera?

Puede utilizar Netscape, Firefox y Opera como navegador predeterminado de Internet, pero debe tener instalado Microsoft Internet Explorer 6.0 o una versión posterior en el equipo.

¿Es preciso estar conectado a Internet para ejecutar un análisis?

No es necesario tener conexión a Internet para ejecutar un análisis, aunque debe conectarse al menos una vez a la semana para recibir las actualizaciones de McAfee.

¿VirusScan analiza los archivos adjuntos del correo electrónico?

Si se ha activado el análisis en tiempo real y la protección de correo electrónico, se analizarán todos los archivos adjuntos cuando se reciban los mensajes de correo electrónico.

¿VirusScan analiza los archivos comprimidos?

VirusScan analiza los archivos .zip y otros archivos comprimidos.

¿Por qué se producen errores de análisis del correo electrónico saliente?

Cuando se analizan los mensajes de correo electrónico salientes pueden producirse los siguientes tipos de errores:

- Error de protocolo. El servidor de correo electrónico ha rechazado un mensaje de correo electrónico.
  Si se produce un error de protocolo o de sistema, los mensajes de correo electrónico restantes de esa sesión se procesarán y enviarán al servidor.
- Error de conexión. Se ha producido un error en una conexión con el servidor de correo electrónico.
  Si se produce un error de conexión, asegúrese de que el equipo está conectado a Internet y, a continuación, vuelva a intentar enviar el mensaje desde la lista de elementos **enviados** de su programa de correo electrónico.
- Error del sistema. Se ha producido un error de gestión de archivos u otro error del sistema.
- Error de conexión SMTP codificada. Se ha detectado una conexión SMTP codificada en su programa de correo electrónico.
  Si se produce una conexión SMTP codificada, deberá desconectar la conexión SMTP codificada en su programa de correo electrónico para asegurarse de que los mensajes de correo electrónico se analizan.

Si se agota el tiempo de espera mientras se envían mensajes de correo electrónico, desactive el análisis de mensajes de correo electrónico saliente o deshabilite la conexión SMTP codificada en el programa de correo electrónico.

Temas relacionados

- Configuración de la protección de correo electrónico (página 91)

Solución de problemas

En esta sección encontrará asistencia para los problemas generalas que pueda experimentar.

No es posible limpiar ni suprimir un virus

Con algunos virus, el equipo debe limpiarse manualmente. Intente reiniciar el equipo y vuelva a ejecutar el análisis.

Si no consigue limpiar o eliminar un virus, consulte la Biblioteca de información sobre virus en http://us.mcafee.com/virusInfo/default.asp?affid=.

Si necesita más ayuda, póngase en contacto con el servicio de atención de McAfee, en el sitio Web de McAfee.

Nota: No se pueden limpiar los virus de CD-ROM, DVD ni de unidades de disco protegidas contra escritura.

Después de reiniciar el equipo, hay un elemento que no se ha eliminado.

Tras analizar y eliminar elementos, algunas situaciones requieren que se reinicie el equipo.

Si el elemento no se elimina después de reinciar, envíe el archivo a McAfee.

Nota: No se pueden limpiar los virus de CD-ROM, DVD ni de unidades de disco protegidas contra escritura.

Temas relacionados

- Gestión de programas, cookies y archivos en cuarentena (página 101)

Componentes ausentes o dañados

Hay circunstancias que pueden impedir que VirusScan se instale correctamente:

- El equipo no dispone de suficiente memoria o espacio en disco. Compruebe que el equipo cumple los requisitos del sistema para ejecutar este software.
- El navegador de Internet no está configurado correctamente.
- La conexión a Internet falla. Compruebe la conexión o intente establecer una nueva más tarde.
- Faltan archivos o se han producido errores en la instalación.

La mejor solución consiste en resolver estos posibles problemas e instalar de nuevo VirusScan.

CAPÍTULO 18

McAfee Personal Firewall

Personal Firewall ofrece protección avanzada para su equipo y sus datos personales. Personal Firewall establece una barrera entre su equipo e Internet y supervisa en segundo plano si se realizan operaciones de tráfico de Internet que resulten sospechosas.

En este capítulo

Características

Personal Firewall proporciona protección completa de cortafuegos entrante y saliente y confía automáticamente en los programas inofensivos conocidos y le ayuda a bloquear el software espía, los troyanos y los registradores de claves. Este cortafuegos permite al usuario defenderse de programas y ataques de piratas informáticos, supervisa la actividad de Internet y de la red, alerta contra eventos hostiles o sospechosos, proporciona información detallada acerca del tráfico de Internet y complementa defensas antivirus.

Niveles de protección estándar y personalizada

Protéjase contra intrusiones y actividades sospechosas mediante la configuración de protección predeterminada de Firewall o personalice Firewall según sus propias necesidades de seguridad.

Recomendaciones en tiempo real

Reciba recomendaciones de forma dinámica para ayudarle a determinar si debe concederse acceso a Internet a los programas o si el tráfico de red es fiable.

Gestión de acceso inteligente para los programas

Gestione el acceso a Internet de programas, a través de alertas y registros de eventos, o configure permisos de acceso de programas específicos desde el panel Permisos de programas de Firewall.

Protección para juegos

Evite que las alertas de intentos de intrusión y actividades sospechosas le distraigan mientras juega a pantalla completa y configure Firewall para que muestre alertas una vez finalizado el juego de ordenador.

Protección al iniciar el equipo

Antes de que se abra Windows, Firewall protege su equipo contra intentos de intrusión y programas no deseados, así como el tráfico de red.

Control de puertos de servicio del sistema

Los puertos de servicio del sistema pueden proporcionar una puerta trasera para su equipo. Firewall permite crear y gestionar los puertos de servicio del sistema abiertos y cerrados que requieren algunos programas.

Gestión de conexiones de equipo

Defina como fiables y prohíba direcciones IP y conexiones remotas que puedan conectarse a su equipo.

Integración de la información de HackerWatch

HackerWatch es un eje de información de seguridad que rastrea patrones globales de intrusión y piratería informática, y también proporciona la información más actualizada sobre los programas de su equipo. Puede ver eventos de seguridad globales y estadísticas de puertos de Internet.

Firewall bloqueado

Bloquee instantáneamente todo el tráfico de red entrante y saliente entre el equipo e Internet.

Restaurar Firewall

Restaure instantáneamente la configuración original de protección de Firewall. Si Personal Firewall se comporta de modo distinto al deseado y no puede corregirlo, restaure la configuración predeterminada de Firewall.

Detección avanzada de troyanos

Firewall combina la gestión de conexión de los programas con una base de datos mejorada para detectar y bloquear aplicaciones potencialmente malintencionadas, como los troyanos, y evitar que accedan a Internet y puedan transmitir sus datos personales.

Registro de eventos

Especifique si desea habilitar o deshabilitar el registro y, en el caso de que lo habilite, qué tipos de evento desea registrar. El registro de eventos le permite ver los eventos entrantes y salientes más recientes. También puede ver los eventos detectados por intrusión.

Control del tráfico de Internet

Firewall revisa mapas gráficos de fácil lectura que muestran el origen de ataques y tráfico hostiles en todo el mundo. También localiza información detallada de propiedad y datos geográficos correspondientes a las direcciones IP de origen. Además, analiza el tráfico entrante y saliente, controla el ancho de banda del programa y la actividad del programa.

Prevención de intrusiones

Firewall protege la privacidad mediante la prevención de intrusiones de posibles amenazas de Internet. Gracias a la función heurística, McAfee proporciona un tercer nivel de protección mediante el bloqueo de los elementos que muestren indicios de ataque o intentos de piratería.

Análisis de tráfico sofisticado

Firewall revisa el tráfico entrante y saliente de Internet, así como las conexiones de programas, incluidas aquéllas que están "a la escucha" de conexiones abiertas. Esto permite a los usuarios ver los programas que pueden ser susceptibles de intrusión y actuar en consecuencia.

Iniciar el cortafuegos

Desde el mismo momento en que instala el cortafuegos, su equipo queda protegido contra las intrusiones y el tráfico de red no deseado. Por otra parte, ya puede responder a las alertas y gestionar el acceso entrante y saliente a Internet, tanto para programas conocidos como desconocidos. Las recomendaciones inteligentes y el nivel de seguridad Estándar se habilitan de manera automática.

Si bien puede deshabilitar el cortafuegos desde el panel Configuración de Internet y redes, su equipo ya no estará protegido contra intrusiones y tráfico de red no deseado; tampoco podrá gestionar de manera eficiente las conexiones de Internet entrantes y salientes. Si tiene que deshabilitar la protección del cortafuegos, hágalo de manera temporal y sólo cuando sea realmente necesario. También puede habilitar el cortafuegos desde el panel Configuración de Internet & redes.

El cortafuegos desactiva automáticamente el servidor de seguridad de Windows y se establece como cortafuegos predeterminado.

Nota: Para configurar el cortafuegos, abra el panel Configuración de Internet y redes.

Iniciar la protección de Firewall

Al habilitar la protección del cortafuegos, está defendiendo al equipo contra intrusiones y tráfico de red no deseado, y además le ayuda a gestionar las conexiones de Internet entrantes y salientes.

Para habilitar la protección del cortafuegos:

1. En el panel McAfee SecurityCenter, realice una de las siguientes acciones:
   - Haga clic en **Internet & redes**, y a continuación **Configurar**.
   - Haga clic en **Menú avanzado**, luego en **Configurar** en el panel **Inicio** y a continuación elija **Internet & redes**.
2. En el panel **Configuración de Internet & redes**, en **Protección por cortafuegos**, haga clic en **Activar**.

Detener la protección de Firewall

Al deshabilitar la protección del cortafuegos, su equipo queda totalmente vulnerable a las intrusiones y al tráfico de red no deseado. Sin la protección del cortafuegos habilitada no podrá gestionar las conexiones de Internet, ni entrantes ni salientes.

Para deshabilitar la protección del cortafuegos:

1. En el panel McAfee SecurityCenter, realice una de las siguientes acciones:
   - Haga clic en **Internet & redes**, y a continuación **Configurar**.
   - Haga clic en **Menú avanzado**, luego en **Configurar** en el panel **Inicio** y a continuación elija **Internet & redes**.
2. En el panel **Configuración de Internet & redes** en **Protección por cortafuegos**, haga clic en **Desactivar**.

Trabajar con alertas

El cortafuegos emplea todo un abanico de alertas para que gestione su seguridad con mayor facilidad. Las alertas se agrupan en cuatro tipos básicos.

- Alerta Troyano bloqueado
- Alerta roja
- Alerta amarilla
- Alerta verde

Las alertas también pueden contener información de ayuda para que el usuario pueda decidir mejor cómo ordenar las alertas o bien obtener información relativa a los programas que se ejecutan en su equipo.

Acerca de las alertas

El cortafuegos dispone de cuatro tipos de alerta básicos. A su vez, algunas alertas incluyen información relativa a los programas que se ejecutan en su equipo o sobre cómo obtener información.

Alerta Troyano bloqueado

Los troyanos tienen el aspecto de programas válidos, pero pueden trastornar o dañar los equipos, así como proporcionar acceso no autorizado a ellos. La alerta Troyano aparece cuando el cortafuegos detecta, y luego bloquea, un troyano en su equipo, y recomienda que analice el equipo en busca de más amenazas. Esta alerta funciona en todos los niveles de seguridad menos en Abierta o cuando Recomendaciones inteligentes está deshabilitada.

Alerta roja

Se trata del tipo de alerta más común y por lo general solicita una respuesta del usuario. En ocasiones, el cortafuegos no es capaz de determinar de forma automática la línea de actuación a seguir para la actividad de un programa o un evento de red. Entonces la alerta describe primero la actividad del programa o el evento de red en cuestión y ofrece una o más opciones, a las cuales debe responder el usuario. Si Recomendaciones inteligentes está habilitada, los programas se agregan al panel Permisos de programas.

Las descripciones de alerta siguientes son las que aparecen más a menudo:

- **El programa solicita acceso a Internet**: El cortafuegos detecta un programa que intenta acceder a Internet.
- **El programa ha sido modificado**: El cortafuegos detecta un programa que ha cambiado en algún aspecto, quizás como resultado de una actualización en línea.
- **Programa bloqueado**: El cortafuegos bloquea un programa porque aparece en la lista del panel Permisos de programas.

Según cuál sea su configuración y la actividad del programa o el evento de red, las opciones siguientes son las que encontrará más a menudo:

- **Conceder acceso**: Permite a un programa de su equipo que acceda a Internet. La regla se agrega a la página Permisos de programas.
- **Conceder acceso una vez**: Permite a un programa de su equipo que acceda a Internet de manera temporal. Por ejemplo, la instalación de un programa nuevo puede necesitar el acceso sólo una vez.

- **Bloquear acceso**: Impide que un programa acceda a Internet.
- **Permitir sólo acceso saliente**: Permite realizar sólo una conexión saliente a Internet. Esta alerta suele aparecer cuando los niveles de seguridad están definidos como Estricta y Furtiva.
- **Confiar en esta red**: Permite el tráfico entrante y saliente desde una red. La red se agrega a la sección de direcciones IP fiables.
- **No confiar en esta red en este momento**: Bloquea el tráfico entrante y saliente desde una red.

Alerta amarilla

La alerta amarilla es una notificación no crítica que le informa acerca de un evento de red que el cortafuegos ha detectado. Por ejemplo, la alerta **Nueva red detectada** aparece cuando el cortafuegos se ejecuta por primera vez o cuando un equipo con cortafuegos instalado se conecta a una red nueva. Puede elegir entre confiar o no confiar en la red. Si la red es fiable, el cortafuegos permite el tráfico desde cualquier otro equipo de la red y la agrega a las Direcciones IP fiables.

Alerta verde

En la mayoría de los casos, una alerta verde proporciona información básica acerca de un evento y no requiere ningún tipo de respuesta. Las alertas verdes suelen aparecer cuando los niveles de seguridad están definidos como Estándar, Estricta, Furtiva y Bloqueada. Las descripciones de la alerta verde son las siguientes:

- **El programa ha sido modificado**: Le informa de que un programa, al cual le había concedido acceso a Internet con anterioridad, ha sido modificado. Puede optar por bloquear el programa pero si no responde, la alerta desaparecerá del escritorio y el programa seguirá teniendo acceso.
- **Se ha concedido acceso a Internet a este programa**: Le notifica que se ha concedido acceso a Internet a un programa. Puede optar por bloquear el programa pero si no responde, la alerta desaparecerá y el programa seguirá teniendo acceso a Internet.

Ayuda al usuario

Muchas alertas del cortafuegos contienen información adicional para facilitarle la gestión de la seguridad de su equipo y consisten en lo siguiente:

- **Obtener más información sobre este programa**: Inicie el sitio Web de seguridad global de McAfee para obtener información acerca de un programa que el cortafuegos ha detectado en su equipo.
- **Notifique a McAfee la existencia de este programa**: Envíe información a McAfee acerca de un archivo desconocido que el cortafuegos ha detectado en su equipo.
- **Recomendaciones de McAfee**: Consejos sobre cómo gestionar las alertas. Por ejemplo, una alerta le puede recomendar que conceda acceso a un programa.

Gestionar las alertas informativas

El cortafuegos le permite mostrar u ocultar las alertas informativas durante ciertos eventos.

Mostrar las alertas mientras se juega

De forma predeterminada, el cortafuegos impide que las alertas informativas aparezcan mientras se juega en pantalla completa. No obstante, puede configurar el cortafuegos para que muestre las alertas informativas durante el juego, si el cortafuegos detecta intentos de intrusión o alguna actividad sospechosa.

Para mostrar las alertas durante el juego:

1. En el panel Tareas comunes, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, haga clic en **Alertas**.
4. Haga clic en **Avanzadas**.
5. En el panel **Opciones de alerta**, seleccione **Mostrar alertas informativas cuando se detecte el modo de juegos**.

Ocultar alertas informativas

Las alertas informativas le indican los eventos que no requieren de su respuesta inmediata.

Para ocultar las alertas informativas:

1. En el panel Tareas comunes, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, haga clic en **Alertas**.
4. Haga clic en **Avanzadas**.
5. En el panel **Configuración de SecurityCenter**, haga clic en **Alertas informativas**.
6. En el panel **Alertas informativas**, realice una de las siguientes operaciones:
   - Seleccione un tipo de alerta que desee ocultar.
   - Seleccione **Ocultar alertas informativas** para que se oculten todas las alertas informativas.

7 Haga clic en **Aceptar**.

CAPÍTULO 19

Configurar la protección del cortafuegos

El cortafuegos le ofrece varios métodos para gestionar su seguridad y personalizar su respuesta a las alertas y los eventos relacionados con la seguridad.

Cuando se instala el cortafuegos por primera vez, el nivel de protección queda definido como seguridad Estándar. Para la mayoría de la gente esta opción cubre todas sus necesidades en cuanto a seguridad. A pesar de ello, el cortafuegos proporciona otros niveles, desde el más restrictivo al más permisivo.

El cortafuegos también le ofrece la posibilidad de recibir recomendaciones sobre alertas y acceso a Internet para programas.

En este capítulo

Gestionar los niveles de seguridad del cortafuegos

Puede configurar los niveles de seguridad para controlar el grado con que desea gestionar y responder a las alertas que surjan cuando el cortafuegos detecte tráfico de red y conexiones de Internet entrantes y salientes no deseados. El nivel de seguridad que se habilita de forma predeterminada es el Estándar.

Si el nivel de seguridad Estándar está activado y las recomendaciones inteligentes habilitadas, las alertas rojas proporcionan las opciones para conceder o bloquear el acceso a los programas desconocidos o modificados. Cuando se detectan programas conocidos, aparecen alertas informativas de color verde y se les concede el acceso de forma automática. Conceder acceso a un programa significa permitirle establecer conexiones salientes y escuchar conexiones entrantes no solicitadas.

Por lo general, cuanto más restrictivo es un nivel de seguridad (Furtiva y Estricta), mayor es el número de opciones y alertas que se muestran y que, por consiguiente, deberá gestionar.

El cortafuegos emplea seis niveles de seguridad. Empezando por los más restrictivos, se incluyen los niveles siguientes:

- **Bloqueada**: Bloquea todas las conexiones de Internet.
- **Furtiva**: Bloquea todas las conexiones de Internet entrantes.
- **Estricta**: Las alertas requieren una respuesta a cada solicitud de conexión a Internet entrante y saliente.
- **Estándar**: Las alertas le notifican si un programa nuevo o desconocido solicita acceso a Internet.
- **Fiable**: Concede acceso a todas las conexiones de Internet entrantes y salientes, y luego las agrega automáticamente al panel Permisos de programas.
- **Abierta**: Concede acceso a todas las conexiones de Internet entrantes y salientes.

El cortafuegos también le permite restablecer de inmediato su nivel de seguridad al estándar desde el panel Restaurar valores predeterminados de protección del cortafuegos.

Definir el nivel de seguridad como Bloqueada

Al definir el nivel de seguridad del cortafuegos como Bloqueada, éste bloquea todas las conexiones de red entrantes y salientes, incluido el acceso a los sitios Web, al correo electrónico y a las actualizaciones de seguridad. Este nivel de seguridad da el mismo resultado que si eliminara su conexión de Internet. Puede utilizar esta opción para bloquear puertos que haya definido como abiertos en el panel Servicios del sistema. Durante el bloqueo pueden seguir apareciendo alertas que soliciten el bloqueo de programas.

Para definir el nivel de seguridad del cortafuegos como Bloqueada:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Bloqueada** como el nivel actual.
3. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Furtiva

Al definir el nivel de seguridad del cortafuegos como Furtiva, éste bloquea todas las conexiones de red entrantes a excepción de los puertos abiertos. Esta opción oculta por completo la presencia de su equipo en Internet. Cuando el nivel de seguridad está definido como Furtiva, el cortafuegos le avisa cuando hay programas nuevos que intentan conexiones salientes a Internet o reciben solicitudes de conexión entrantes. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.

Para definir el nivel de seguridad del cortafuegos como Furtiva:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Furtiva** como el nivel actual.
3. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Estricta

Cuando el nivel de seguridad está definido como Estricta, el cortafuegos le informa siempre que hay programas nuevos que intentan conexiones salientes a Internet o reciben solicitudes de conexión entrantes. Los programas bloqueados y agregados aparecen en el panel Permisos de programas. Si el nivel de seguridad está definido como Estricta, un programa sólo solicita el tipo de acceso que necesita en ese momento, por ejemplo acceso sólo saliente, que usted le puede conceder o bloquear. Más adelante, si el programa solicita tanto una conexión entrante como saliente, puede concederle acceso pleno desde el panel Permisos de programas.

Para definir el nivel de seguridad del cortafuegos como Estricta:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Estricta** como el nivel actual.
3. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Estándar

El nivel de seguridad recomendado y predeterminado es el Estándar.

Al definir el nivel de seguridad del cortafuegos como Estándar, el cortafuegos supervisa las conexiones entrantes y salientes, y le avisa cuando hay programas nuevos que intentan acceder a Internet. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.

Para definir el nivel de seguridad del cortafuegos como Estándar:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Estándar** como el nivel actual.
3. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Fiable

Al definir el nivel de seguridad del cortafuegos como Fiable, éste permite todas las conexiones entrantes y salientes. En la seguridad Fiable, el cortafuegos concede acceso a todos los programas de manera automática y los agrega a la lista de programas permitidos en el panel Permisos de programas.

Para definir el nivel de seguridad del cortafuegos como Fiable:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Fiable** como el nivel actual.
3. Haga clic en **Aceptar**.

Configurar Recomendaciones inteligentes para alertas

Puede configurar el cortafuegos para incluir, excluir o mostrar recomendaciones en alertas relativas a programas que intentan acceder a Internet.

Al habilitar Recomendaciones inteligentes obtendrá ayuda para decidir la manera cómo ordenar las alertas. Cuando Recomendaciones inteligentes está habilitada (y el nivel de seguridad es Estándar), el cortafuegos bloquea o concede acceso a programas conocidos de manera automática, y por otra parte le avisa y le recomienda una línea de actuación cuando detecta programas desconocidos y potencialmente peligrosos.

Cuando Recomendaciones inteligentes está deshabilitada, el cortafuegos ni bloquea o concede acceso a Internet de manera automática, ni recomienda ninguna línea de actuación.

Si el cortafuegos está configurado sólo para mostrar Recomendaciones inteligentes, una alerta le pedirá que conceda el acceso o lo bloquee pero le sugerirá una línea de actuación.

Habilitar Recomendaciones inteligentes

Al habilitar Recomendaciones inteligentes obtendrá ayuda para decidir la manera cómo ordenar las alertas. Cuando Recomendaciones inteligentes está habilitada, el cortafuegos bloquea los programas o les concede acceso de manera automática y le avisa de que hay programas no reconocidos que son potencialmente peligrosos.

Para habilitar Recomendaciones inteligentes:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Habilitar Recomendaciones inteligentes**.
3. Haga clic en **Aceptar**.

Deshabilitar Recomendaciones inteligentes

Si deshabilita Recomendaciones inteligentes, las alertas no incluyen la ayuda para ordenarlas y gestionar el acceso a los programas. Cuando Recomendaciones inteligentes está deshabilitada, el cortafuegos sigue bloqueando los programas o concediéndoles acceso y le avisa de que hay programas no reconocidos que son potencialmente peligrosos. Y si detecta un programa nuevo que parece sospechoso o que se sabe que puede ser una amenaza, el cortafuegos bloquea automáticamente el acceso a Internet a este programa.

Para deshabilitar Recomendaciones inteligentes:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Deshabilitar Recomendaciones inteligentes**.
3. Haga clic en **Aceptar**.

Mostrar sólo recomendaciones inteligentes

Al mostrar Recomendaciones inteligentes, obtendrá ayuda para decidir la manera cómo ordenar las alertas relativas a programas no reconocidos y potencialmente peligrosos. Cuando Recomendaciones inteligentes está definido como **Mostrar sólo**, se muestra información acerca de cómo ordenar las alertas, pero a diferencia de la opción **Habilitar Recomendaciones inteligentes**, las recomendaciones que se muestran no se aplican de manera automática como tampoco se concede o bloquea automáticamente el acceso a los programas. En este caso las alertas proporcionan recomendaciones que ayudan a decidir sobre si conceder acceso a los programas o bloquearlos.

Para sólo mostrar recomendaciones inteligentes:

1. Desde el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Mostrar sólo**.
3. Haga clic en **Aceptar**.

Optimizar la seguridad del cortafuegos

Existen muchas maneras de poner en peligro la seguridad de su equipo. Por ejemplo, algunos programas pueden intentar conectarse a Internet antes de que se inicie Windows®. Asimismo, otros usuarios informáticos pueden lograr una solicitud de ping en su equipo que les permita saber si está conectado a una red. El cortafuegos le permite defenderse contra estos dos tipos de intrusión porque le da la posibilidad de deshabilitar la protección durante el arranque y de bloquear las solicitudes de ping ICMP. La primera opción bloquea a los programas el acceso a Internet cuando Windows se inicia y la segunda bloquea las solicitudes de ping que permiten a otros usuarios detectar su equipo en una red.

La configuración de instalación estándar incluye una detección automática para los intentos de intrusión más comunes, como los ataques de denegación de servicio o vulnerabilidades. Al utilizar esta configuración se garantiza su protección contra estos ataques y análisis. No obstante, puede deshabilitar la detección automática de uno o varios ataques y análisis en el panel Detección de intrusiones.

Proteger su equipo durante el inicio

El cortafuegos puede proteger su equipo mientras se inicia Windows. La protección de tiempo de arranque bloquea todos los programas nuevos que solicitan acceso a Internet y a los que previamente no se les ha concedido. Tras lanzar el cortafuegos, éste muestra alertas para los programas que habían solicitado acceso a Internet durante el inicio, y que ahora puede conceder o bloquear. Para utilizar esta opción, su nivel de seguridad no debe estar definido como Abierta o Bloqueada.

Para proteger su equipo durante el inicio:

1. Desde el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, en Configuración de seguridad, seleccione **Habilitar protección durante el arranque**.
3. Haga clic en **Aceptar**.

Nota: Las conexiones e intrusiones bloqueadas no quedan registradas mientras la protección durante el arranque está habilitada.

Configurar solicitudes de ping

Los usuarios de otros equipos pueden utilizar una herramienta de ping, que manda y recibe mensajes de solicitud de eco IMCP, para determinar si cierto equipo está conectado a la red. Puede configurar el cortafuegos para prevenir o permitir que otros usuarios de equipos hagan una solicitud de ping a su equipo.

Para configurar su solicitud de ping ICMP:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, en **Configuración de seguridad**, realice una de las siguientes acciones:
   - Seleccione **Permitir solicitudes de ping ICMP** para permitir que se detecte su equipo en la red mediante solicitudes de ping.
   - Borre **Permitir solicitudes de ping ICMP** para impedir que se detecte su equipo en la red mediante solicitudes de ping.
3. Haga clic en **Aceptar**.

Configurar la detección de intrusiones

La detección de intrusiones (IDS) supervisa los paquetes de datos en busca de transferencias de datos o métodos de transferencia sospechosos. El IDS analiza el tráfico y los paquetes de datos en busca de patrones de tráfico específicos de los agresores. Por ejemplo, si el cortafuegos detecta paquetes de ICMP, los analiza en busca de patrones de tráfico sospechoso comparando el tráfico de ICMP con los patrones de los ataques conocidos. El cortafuegos compara los paquetes con la base de datos de firmas y, si resultan sospechosos o peligrosos, suelta los paquetes procedentes del equipo agresor y, opcionalmente, registra el evento.

La configuración de instalación estándar incluye una detección automática para los intentos de intrusión más comunes, como los ataques de denegación de servicio o vulnerabilidades. Al utilizar esta configuración se garantiza su protección contra estos ataques y análisis. No obstante, puede deshabilitar la detección automática de uno o varios ataques y análisis en el panel Detección de intrusiones.

Para configurar la detección de intrusiones:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Detección de intrusiones**.
3. En **Detectar intentos de intrusión**, realice una de las siguientes opciones:
   - Seleccione un nombre para detectar el ataque o el análisis de manera automática.
   - Borre un nombre para deshabilitar la detección automática del ataque o el análisis.
4. Haga clic en **Aceptar**.

Configurar los estados de protección del cortafuegos

SecurityCenter realiza el seguimiento de los problemas como parte del estado de protección general de su equipo. No obstante, se puede configurar el cortafuegos para que ignore ciertos problemas de su equipo que pueden afectar a su estado de protección. Puede configurar SecurityCenter para que ignore que el nivel de seguridad del cortafuegos está definido como Abierta, que el cortafuegos no se está ejecutando y que en su equipo no hay instalado ningún cortafuegos sólo saliente.

Para configurar los estados de protección del cortafuegos:

1. En el panel Tareas comunes, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, haga clic en **Alertas**.
4. Haga clic en **Avanzadas**.
5. En el panel Tareas comunes haga clic en **Menú avanzado**.
6. Haga clic en **Configurar**.
7. En el panel Configuración de SecurityCenter, haga clic en **Estado de protección**.
8. Haga clic en Avanzado.
9. En el panel Problemas omitidos, seleccione una o más de las opciones siguientes:
   - **El cortafuegos está configurado con nivel de seguridad Abierta.**
   - **El servicio de cortafuegos no está en funcionamiento.**
   - **El cortafuegos saliente no está instalado en este equipo.**
10. Haga clic en **Aceptar**.

Bloquear y restaurar el cortafuegos

Esta función resulta útil cuando se deben gestionar emergencias relacionadas con el equipo, para los usuarios que necesiten bloquear todo el tráfico con el fin de resolver un problema del equipo o para aquellos que no estén seguros, y deban estarlo, de cómo gestionar el acceso a Internet de un programa.

Bloquear el cortafuegos de manera instantánea

Al bloquear el cortafuegos se bloquea instantáneamente todo el tráfico de red entrante y saliente entre el equipo e Internet. Evita que todas las conexiones remotas accedan al equipo y que todos los programas del equipo accedan a Internet.

Para bloquear el cortafuegos instantáneamente y bloquear todo el tráfico de red:

1. En los paneles Inicio o Tareas comunes con el menú **Básico** o el **Menú Avanzado** habilitado, haga clic en **Bloquear cortafuegos**.
2. En el panel Bloquear cortafuegos haga clic en **Bloquear**.
3. En el cuadro de diálogo, haga clic en **Sí** para confirmar que desea bloquear de manera instantánea todo el tráfico entrante y saliente.

Desbloquear el cortafuegos de manera instantánea

Al bloquear el cortafuegos se bloquea instantáneamente todo el tráfico de red entrante y saliente entre el equipo e Internet. Evita que todas las conexiones remotas accedan al equipo y que todos los programas del equipo accedan a Internet. Después de haber bloqueado el cortafuegos, puede volver a desbloquearlo para permitir el tráfico de red.

Para desbloquear el cortafuegos instantáneamente y permitir el tráfico de red:

1. En los paneles Inicio o Tareas comunes con el menú **Básico** o el **Menú Avanzado** habilitado, haga clic en **Bloquear cortafuegos**.
2. En el panel Bloqueo activado, haga clic en **Desbloquear**.
3. En el cuadro de diálogo, haga clic en **Sí** para confirmar que desea desbloquear el cortafuegos y permitir el tráfico de red.

Restaurar la configuración del cortafuegos

Puede restaurar el cortafuegos con su configuración de protección original rápidamente. Define el nivel de seguridad como estándar, permite recomendaciones inteligentes, restablece direcciones IP fiables y no permitidas, y elimina todos los programas del panel Permisos de programas.

Para restaurar el cortafuegos con su configuración original:

1. En los paneles Inicio o Tareas comunes con el menú **Básico** o el **Menú Avanzado** habilitado, haga clic en **Restaurar valores predeterminados del cortafuegos**.
2. En el panel Restaurar valores predeterminados de protección del cortafuegos, haga clic en **Restaurar valores predeterminados**.
3. En el cuadro de diálogo Restaurar valores predeterminados de protección del cortafuegos, haga clic en **Sí** para confirmar que desea restaurar la configuración del cortafuegos con sus valores predeterminados.

Definir el nivel de seguridad como Abierta

Al definir el nivel de seguridad como Abierta, el cortafuegos puede conceder acceso a todas las conexiones de red entrantes y salientes. Para conceder acceso a los programas bloqueados previamente, utilice el panel Permisos de programas.

Para definir el nivel de seguridad del cortafuegos como Abierta:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Abierta** como el nivel actual.
3. Haga clic en **Aceptar**.

Nota: Las aplicaciones bloqueadas con anterioridad siguen bloqueadas cuando el nivel de seguridad del cortafuegos está definido como **Abierta**. Para evitar esto, puede cambiar la regla del programa por **Acceso pleno**.

CAPÍTULO 20

Gestionar programas y permisos

El cortafuegos le permite gestionar y crear permisos de acceso tanto para programas ya existentes como para programas nuevos que soliciten acceso a Internet entrante y saliente. El cortafuegos le permite conceder acceso pleno o sólo saliente a estos programas. Aunque también puede bloquearles el acceso.

En este capítulo

Conceder acceso a Internet a los programas

Algunos programas, como los navegadores de Internet, necesitan acceder a Internet para funcionar correctamente.

El cortafuegos le permite utilizar el panel Permisos de programas para:

- Conceder acceso a los programas
- Conceder a los programas sólo acceso saliente
- Bloquear el acceso a los programas

También puede conceder acceso pleno o sólo saliente desde el registro Eventos salientes y eventos recientes.

Conceder acceso pleno a un programa

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Personal Firewall incluye una lista de programas a los que se concede acceso pleno de forma automática, pero es posible modificar estos permisos.

Para conceder a un programa acceso pleno a Internet:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso sólo saliente**.
4. En **Acción**, haga clic en **Conceder acceso pleno**.
5. Haga clic en **Aceptar**.

Conceder acceso pleno a un programa nuevo

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. El cortafuegos incluye una lista de programas a los que se concede acceso pleno de manera automática, pero se puede agregar un programa nuevo y modificar sus permisos.

Para conceder a un programa nuevo acceso pleno a Internet:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel **Cortafuegos** haga clic en **Permisos de programas**.
3. En **Permisos de programas**, haga clic en **Agregar programa con permiso**.
4. En el cuadro de diálogo **Agregar programa** busque el programa que desea agregar y selecciónelo.
5. Haga clic en **Abrir**.
6. Haga clic en **Aceptar**.

   El programa recién agregado aparece en **Permisos de programas**.

Nota: Puede modificar los permisos de un programa recién agregado como lo haría con un programa ya existente, es decir, seleccionando el programa y haciendo clic en **Conceder sólo acceso saliente** o bien **Bloquear acceso** en **Acción**.

Conceder acceso pleno desde el registro Eventos recientes

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Puede seleccionar un programa desde el registro Eventos recientes y concederle acceso pleno a Internet.

Para conceder a un programa acceso pleno a Internet desde el registro Eventos recientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En Eventos recientes, seleccione la descripción del evento y luego haga clic en **Conceder acceso pleno**.
3. En el diálogo Permisos de programas, haga clic en **Sí** para confirmar que desea conceder al programa acceso pleno.

Temas relacionados

- Ver eventos salientes (página 170)

Conceder acceso pleno desde el registro Eventos salientes

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Puede seleccionar un programa desde el registro Eventos salientes y concederle acceso pleno a Internet.

Para conceder a un programa acceso pleno a Internet desde el registro Eventos salientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos salientes**.
4. En el panel Eventos salientes, seleccione una dirección IP de origen y luego haga clic en **Conceder acceso**.
5. En el diálogo Permisos de programas, haga clic en **Sí** para confirmar que desea conceder al programa acceso pleno a Internet.

Temas relacionados

- Ver eventos salientes (página 170)

Conceder a los programas sólo acceso saliente

Algunos programas de su equipo sólo requieren acceso saliente a Internet. El cortafuegos le permite conceder a los programas sólo acceso saliente a Internet.

Conceder a un programa sólo acceso saliente

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Personal Firewall incluye una lista de programas a los que se concede acceso pleno de forma automática, pero es posible modificar estos permisos.

Para conceder a un programa sólo acceso saliente:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso pleno**.
4. En **Acción**, haga clic en **Conceder sólo acceso saliente**.
5. Haga clic en **Aceptar**.

Conceder sólo acceso saliente desde el registro Eventos recientes

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Puede seleccionar un programa desde el registro Eventos recientes y concederle sólo acceso saliente a Internet.

Para conceder a un programa sólo acceso saliente a Internet desde el registro Eventos recientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En Eventos recientes, seleccione la descripción del evento y luego haga clic en **Conceder sólo acceso saliente**.
3. En el diálogo Permisos de programas, haga clic en **Sí** para confirmar que desea conceder al programa sólo acceso saliente a Internet.

Temas relacionados

- Ver eventos salientes (página 170)

Conceder sólo acceso saliente desde el registro Eventos salientes

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Puede seleccionar un programa desde el registro Eventos salientes y concederle sólo acceso saliente a Internet.

Para conceder a un programa sólo acceso saliente a Internet desde el registro Eventos salientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos salientes**.
4. En el panel Eventos salientes, seleccione una dirección IP de origen y luego haga clic en **Conceder sólo acceso saliente**.
5. En el diálogo Permisos de programas, haga clic en **Sí** para confirmar que desea conceder al programa sólo acceso saliente a Internet.

Temas relacionados

- Ver eventos salientes (página 170)

Bloquear el acceso a Internet a los programas

El cortafuegos le permite bloquear los programas para que no accedan a Internet. Asegúrese de que al bloquear un programa no se va a interrumpir su conexión a Internet o la de otro programa que necesite acceso a Internet para funcionar correctamente.

Bloquear el acceso a los programas

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Personal Firewall incluye una lista de programas a los que se concede acceso pleno de forma automática, pero es posible bloquear estos permisos.

Para bloquear el acceso a Internet a los programas:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, seleccione un programa con **Acceso pleno** o **Sólo acceso saliente**.
4. En **Acción**, haga clic en **Bloquear acceso**.
5. Haga clic en **Aceptar**.

Bloquear el acceso a un nuevo programa

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Personal Firewall incluye una lista de programas a los que se concede acceso pleno de manera automática, pero puede agregar un programa nuevo y luego bloquearle el acceso a Internet.

Para bloquear el acceso a Internet a un programa nuevo:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, haga clic en **Agregar programa bloqueado**.
4. En el cuadro de diálogo **Agregar programa** busque el programa que desea agregar y selecciónelo.
5. Haga clic en **Abrir**.
6. Haga clic en **Aceptar**.

   El programa recién agregado aparece en **Permisos de programas**.

Nota: Puede modificar los permisos de un programa recién agregado como lo haría con un programa ya existente, es decir, seleccionando el programa y haciendo clic en **Conceder sólo acceso saliente** o bien **Conceder acceso pleno** en **Acción**.

Bloquear el acceso desde el registro Eventos recientes

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. No obstante, también puede optar por bloquear los programas para que no accedan a Internet desde el registro Eventos recientes.

Para bloquear a un programa el acceso a Internet desde el registro Eventos recientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En Eventos recientes, seleccione la descripción del evento y luego haga clic en **Bloquear acceso**.
3. En el diálogo Permisos de programas, haga clic en **Sí** para confirmar que desea bloquear el programa.

Temas relacionados

- Ver eventos salientes (página 170)

Eliminar los permisos de acceso de los programas

Antes de eliminar un permiso de un programa, asegúrese de que su ausencia no afectará a la funcionalidad de su equipo o de su conexión a Internet.

Eliminar un permiso de programa

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. El cortafuegos incluye una lista de programas a los que se concede acceso pleno de manera automática, pero es posible eliminar programas que hayan sido agregados automática y manualmente.

Para eliminar un permiso de un programa nuevo:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, seleccione un programa.
4. En **Acción**, haga clic en **Eliminar permiso de programa**.
5. Haga clic en **Aceptar**.

   El programa se elimina del panel Permisos de programas.

Nota: El cortafuegos le impide modificar algunos programas mediante la atenuación y la deshabilitación.

Obtener información sobre los programas

Si no está seguro de qué permiso de programa debe aplicar, puede obtener información acerca del programa en el sitio Web McAfee's HackerWatch para decidirlo mejor.

Obtener información sobre un programa

Muchos programas de su equipo requieren acceso entrante y saliente a Internet. Personal Firewall incluye una lista de programas a los que se concede acceso pleno de forma automática, pero es posible modificar estos permisos.

El cortafuegos puede ayudarle a decidir si conceder acceso a Internet a un programa o bloqueárselo. Asegúrese de que está conectado a Internet para que su navegador pueda lanzar correctamente el sitio Web McAfee's HackerWatch; allí encontrará información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

Para obtener información sobre los programas:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Permisos de programas**.
3. En **Permisos de programas**, seleccione un programa.
4. En **Acción**, haga clic en **Más información**.

Obtener información sobre el programa desde el registro Eventos salientes

Personal Firewall le permite obtener información relativa a los programas que aparecen en el registro Eventos salientes.

Antes de obtener información sobre un programa, asegúrese de que dispone de conexión a Internet y de un navegador.

Para obtener información sobre el programa desde el registro Eventos salientes:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos salientes**.
4. En el panel Eventos salientes, seleccione una dirección IP de origen y luego haga clic en **Más información**.

   En el sitio Web HackerWatch también puede ver información relativa al programa. HackerWatch proporciona información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

Temas relacionados

- Ver eventos salientes (página 170)

CAPÍTULO 21

Gestionar los servicios del sistema

Para funcionar correctamente, algunos programas (incluidos los servidores Web o programas servidores de intercambio de archivos), deben aceptar conexiones no solicitadas procedentes de otros equipos a través de puertos de servicio de sistema designados. El cortafuegos suele cerrar estos puertos de servicio de sistema porque constituyen el origen más probable de las inseguridades en su sistema. Sin embargo, para aceptar conexiones procedentes de equipos remotos, los puertos de servicio de sistema deben estar abiertos.

Esta lista muestra los puertos estándar de servicios comunes.

- Protocolo de transferencia de archivos (FTP): puertos 20-21
- Servidor de correo (IMAP): puerto 143
- Servidor de correo (POP3): puerto 110
- Servidor de correo (SMTP): puerto 25
- Servidor de directorio de Microsoft (MSFT DS): puerto 445
- Microsoft SQL Server (MSFT SQL): puerto 1433
- Asistencia remota / Terminal Server (RDP): puerto 3389
- Llamadas a procedimientos remotos (RPC): puerto 135
- Servidor Web seguro (HTTPS): puerto 443
- Plug and Play universal (UPNP): puerto 5000
- Servidor Web (HTTP): puerto 80
- Archivos compartidos en Windows (NETBIOS): puertos 137-139

En este capítulo

Configurar puertos de servicio del sistema

Para permitir el acceso remoto a un servicio de su equipo, debe especificar el servicio y el puerto asociado para que se abran. Sólo seleccione un servicio y un puerto si está seguro de que debe abrirse. En raras ocasiones es necesario abrir un puerto.

Permitir el acceso a un puerto de servicio del sistema existente

Desde el panel Servicios del sistema, puede abrir o cerrar un puerto existente para permitir o denegar el acceso remoto a un servicio de red en el equipo. Un puerto de servicio del sistema abierto puede dejar a su equipo totalmente vulnerable ante las amenazas de seguridad de Internet, por lo que es mejor que sólo abra un puerto cuando sea necesario.

Para permitir el acceso a un puerto de servicio del sistema:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Servicios del sistema**.
3. En **Abrir puerto de servicio del sistema**, seleccione un servicio del sistema para que abra un puerto.
4. Haga clic en **Aceptar**.

Bloquear el acceso a un puerto de servicio del sistema existente

Desde el panel Servicios del sistema, puede abrir o cerrar un puerto existente para permitir o denegar el acceso remoto a un servicio de red en el equipo. Un puerto de servicio del sistema abierto puede dejar a su equipo totalmente vulnerable ante las amenazas de seguridad de Internet, por lo que es mejor que sólo abra un puerto cuando sea necesario.

Para bloquear el acceso a un puerto de servicio del sistema:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Servicios del sistema**.
3. En **Abrir puerto de servicio del sistema**, borre un servicio del sistema para que cierre un puerto.
4. Haga clic en **Aceptar**.

Configurar un puerto de servicio del sistema

Desde el panel Servicios del sistema, puede agregar un puerto de servicio nuevo que, a su vez, puede abrir o cerrar para permitir o denegar acceso remoto a un servicio de red de su equipo. Un puerto de servicio del sistema abierto puede dejar a su equipo totalmente vulnerable ante las amenazas de seguridad de Internet, por lo que es mejor que sólo abra un puerto cuando sea necesario.

Para crear y configurar un puerto de servicio del sistema:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Servicios del sistema**.
3. Haga clic en **Agregar**.
4. En **Agregar configuración de puerto**, especifique lo siguiente:
   - Nombre del programa
   - Puertos TCP/IP entrantes
   - Puertos TCP/IP salientes
   - Puertos UDP entrantes
   - Puertos UDP salientes
5. También puede introducir una descripción opcional para la nueva configuración.
6. Haga clic en **Aceptar**.

   El puerto de servicio del sistema recién configurado aparece en **Abrir puerto de servicio del sistema**.

Modificar un puerto de servicio del sistema

Un puerto abierto y cerrado permite y deniega el acceso a un servicio de red de su equipo. Desde el panel Servicios del sistema, puede modificar la información entrante y saliente para un puerto existente. Si la información del puerto está escrita de manera incorrecta, el servicio del sistema no funciona.

Para modificar un puerto de servicio del sistema:

1. Desde el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos haga clic en **Servicios del sistema**.
3. Seleccione un servicio del sistema y haga clic en **Editar**.
4. En **Agregar configuración de puerto**, especifique lo siguiente:
   - Nombre del programa

- Puertos TCP/IP entrantes
- Puertos TCP/IP salientes
- Puertos UDP entrantes
- Puertos UDP salientes

5 También puede introducir una descripción opcional para la configuración modificada.

6 Haga clic en **Aceptar**.

El puerto de servicio del sistema modificado aparece en **Abrir puerto de servicio del sistema**.

Eliminar un puerto de servicio del sistema

Un puerto abierto o cerrado permite o deniega el acceso a un servicio de red de su equipo. Desde el panel Servicios del sistema, puede eliminar un puerto existente y el servicio del sistema asociado. Tras haber eliminado un puerto y el servicio del sistema asociado desde el panel Servicios del sistema, los equipos remotos ya no pueden acceder al servicio de red de su equipo.

Para eliminar un puerto de servicio del sistema:

1 En el panel Configuración de Internet & redes, haga clic en **Avanzada**.

2 En el panel Cortafuegos haga clic en **Servicios del sistema**.

3 Seleccione un servicio del sistema y haga clic en **Eliminar**.

4 En el cuadro de diálogo **Servicios del sistema** haga clic en **Sí** para confirmar que desea eliminar el servicio del sistema.

El puerto de servicio del sistema ya no aparece en el panel Servicios del sistema.

CAPÍTULO 22

Gestionar conexiones de equipo

Puede configurar el cortafuegos para gestionar conexiones remotas específicas a su equipo mediante la creación de reglas, basadas en direcciones del protocolo de Internet (IP), que están asociadas a los equipos remotos. Los equipos que están asociados a direcciones IP fiables se pueden conectar a su equipo con confianza, mientras que a las IP que sean desconocidas, sospechosas o no sean fiables, se les puede prohibir que se conecten a su equipo.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo definido como fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que los equipos en los que confía estén protegidos por un cortafuegos y un programa antivirus actualizado. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP que están en la lista Direcciones IP fiables.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

En este capítulo

Definir conexiones de equipo como fiables

Puede agregar, editar y eliminar direcciones IP fiables desde el panel IP fiables y prohibidas, en **Direcciones IP fiables**.

La lista **Direcciones IP fiables** del panel Direcciones IP fiables y prohibidas se utiliza para permitir que todo el tráfico procedente de un equipo determinado acceda al equipo propio. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP que están en la lista **Direcciones IP fiables**.

El cortafuegos confía en cualquier dirección IP verificada que esté en la lista y siempre permite pasar a través suyo el tráfico procedente de una dirección IP fiable a cualquier puerto. El cortafuegos no registra los eventos de direcciones IP definidas como fiables. El cortafuegos no filtra ni analiza la actividad que pueda haber entre el equipo asociado a un dirección IP fiable y su equipo.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo definido como fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que los equipos en los que confía estén protegidos por un cortafuegos y un programa antivirus actualizado.

Agregar una conexión de equipo fiable

Puede utilizar el cortafuegos para agregar una conexión de equipo fiable y su dirección IP asociada.

La lista **Direcciones IP fiables** del panel Direcciones IP fiables y prohibidas se utiliza para permitir que todo el tráfico procedente de un equipo determinado acceda al equipo propio. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP que están en la lista **Direcciones IP fiables**.

Los equipos asociados con las direcciones IP fiables siempre se pueden conectar al equipo. Al agregar, editar o eliminar una dirección IP fiable, asegúrese de que se trata de una IP cuya comunicación o eliminación sea segura.

Para agregar una conexión de equipo fiable:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables**.
4. Haga clic en **Agregar**.
5. En **Agregar regla de direcciones IP fiables**, realice una de las acciones siguientes:
   - Seleccione una **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.
6. También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.
7. O también puede escribir una descripción para la regla.
8. Haga clic en **Aceptar**.
9. En el cuadro de diálogo Agregar regla de direcciones IP fiables, haga clic en **Sí** para confirmar que desea agregar la conexión de equipo fiable.

   La dirección IP recién agregada aparece en **Direcciones IP fiables**.

Agregar un equipo fiable desde el registro Eventos entrantes

Puede agregar una conexión de equipo fiable y su dirección IP asociada desde el registro Eventos entrantes.

Los equipos asociados con las direcciones IP fiables siempre se pueden conectar al equipo. Al agregar, editar o eliminar una dirección IP fiable, asegúrese de que se trata de una IP cuya comunicación o eliminación sea segura.

Para agregar un equipo fiable desde el registro Eventos entrantes:

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos entrantes**.
4. En el panel Eventos entrantes, seleccione una dirección IP de origen y luego haga clic en **Definir como IP fiable**.
5. En el cuadro de diálogo Agregar regla de direcciones IP fiables, haga clic en **Sí** para confirmar que desea agregar la conexión de equipo fiable.

   La dirección IP recién agregada aparece en **Direcciones IP fiables**.

Temas relacionados

- Registro de eventos (página 168)

Editar una conexión de equipo fiable

Puede utilizar el cortafuegos para editar una conexión de equipo fiable y su dirección IP asociada.

Los equipos asociados con las direcciones IP fiables siempre se pueden conectar al equipo. Al agregar, editar o eliminar una dirección IP fiable, asegúrese de que se trata de una IP cuya comunicación o eliminación sea segura.

Para editar una conexión de equipo fiable:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables**.
4. Seleccione una dirección IP y haga clic en **Editar**.
5. En **Agregar regla de direcciones IP fiables**, realice una de las acciones siguientes:
   - Seleccione una **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.
6. También tiene la opción de verificar **Regla caduca en** e introducir el número de días para aplicar la regla.
7. O también puede escribir una descripción para la regla.
8. Haga clic en **Aceptar**.

   La dirección IP modificada aparece en **Direcciones IP fiables**.

Eliminar una conexión de equipo fiable

Puede utilizar el cortafuegos para eliminar una conexión de equipo fiable y su dirección IP asociada.

Los equipos asociados con las direcciones IP fiables siempre se pueden conectar al equipo. Al agregar, editar o eliminar una dirección IP fiable, asegúrese de que se trata de una IP cuya comunicación o eliminación sea segura.

Para eliminar una conexión de equipo fiable:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables**.
4. Seleccione una dirección IP y haga clic en **Eliminar**.
5. En el cuadro de diálogo **Direcciones IP fiables y prohibidas**, haga clic en **Sí** para confirmar que desea eliminar la dirección IP fiable de **Direcciones IP fiables**.

Prohibir conexiones de equipo

Puede agregar, editar y eliminar direcciones IP fiables desde el panel IP fiables y prohibidas, en **Direcciones IP no permitidas**.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Agregar una conexión de equipo no permitida

Puede utilizar el cortafuegos para agregar una conexión de equipo no permitida y su dirección IP asociada.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Para agregar una conexión de equipo no permitida:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP no permitidas**.
4. Haga clic en **Agregar**.
5. En Agregar regla de direcciones IP prohibidas, realice una de las acciones siguientes:
   - Seleccione una **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los campos **Dirección IP inicial** y **Dirección IP final**.
6. También tiene la opción de verificar **Regla caduca en** e introducir el número de días para aplicar la regla.
7. O también puede escribir una descripción de la regla.
8. Haga clic en **Aceptar**.
9. En el cuadro de diálogo **Agregar regla de direcciones IP no permitidas**, haga clic en **Sí** para confirmar que desea agregar la conexión de equipo no permitida.

   La dirección IP recién agregada aparece en **Direcciones IP no permitidas**.

Editar una conexión de equipo no permitida

Puede utilizar el cortafuegos para editar una conexión de equipo no permitida y su dirección IP asociada.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Para editar una conexión de equipo no permitida:

1. Desde el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP no permitidas**.
4. Seleccione una dirección IP y haga clic en **Editar**.
5. En **Agregar regla de direcciones IP fiables**, realice una de las acciones siguientes:
   - Seleccione una **Dirección IP individual** y luego escriba la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego escriba las direcciones IP iniciales y finales en los campos **Dirección IP inicial** y **Dirección IP final**.
6. También tiene la opción de verificar **Regla caduca en** y escribir el número de días para aplicar la regla.
7. O también puede escribir una descripción de la regla.

   Haga clic en **Aceptar**. La dirección IP modificada aparece en **Direcciones IP no permitidas**.

Eliminar una conexión de equipo no permitida

Puede utilizar el cortafuegos para eliminar una conexión de equipo no permitida y su dirección IP asociada.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Para eliminar una conexión de equipo no permitida:

1. Desde el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
3. En el panel IP fiables y prohibidas, seleccione **Direcciones IP no permitidas**.
4. Seleccione una dirección IP y haga clic en **Eliminar**.
5. En el cuadro de diálogo **Direcciones IP fiables y no permitidas**, haga clic en **Sí** para confirmar que desea eliminar la dirección IP de **Direcciones IP no permitidas**.

Prohibir un equipo desde el registro Eventos entrantes

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos entrantes.

Las direcciones IP que aparecen en el registro Eventos entrantes están bloqueadas. Por consiguiente, aunque prohíba una dirección no ganará en protección, a menos que su equipo utilice puertos que estén abiertos de manera intencionada o a menos que su equipo incluya un programa al cual se ha concedido acceso a Internet.

Agregue una dirección IP a su lista de **Direcciones IP no permitidas** sólo si su equipo tiene uno o varios puertos abiertos intencionadamente y tiene razones para creer que debe bloquear el acceso a los puertos abiertos por parte de esa dirección.

Puede utilizar la página Eventos entrantes, que muestra las direcciones IP de todo el tráfico de Internet entrante, para prohibir una dirección IP que crea que es el origen de actividad de Internet no deseada o sospechosa.

Para prohibir un equipo fiable desde el registro Eventos entrantes:

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos entrantes**.
4. En el panel Eventos entrantes, seleccione una dirección IP de origen y luego haga clic en **Definir como IP no permitida**.
5. En el cuadro de diálogo **Agregar regla de direcciones IP no permitidas**, haga clic en **Sí** para confirmar que desea prohibir esta dirección IP.

   La dirección IP recién agregada aparece en **Direcciones IP no permitidas**.

Temas relacionados

- Registro de eventos (página 168)

Prohibir un equipo desde el registro Eventos de detección de intrusiones

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos de detección de intrusiones.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Para prohibir una conexión de equipo desde el registro Eventos de detección de intrusiones:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet & redes** y luego haga clic en **Eventos de detección de intrusiones**.
4. En el panel Eventos de detección de intrusiones, seleccione una dirección IP de origen y luego haga clic en **Definir como IP no permitida**.
5. En el cuadro de diálogo **Agregar regla de direcciones IP no permitidas**, haga clic en **Sí** para confirmar que desea prohibir esta dirección IP.

   La dirección IP recién agregada aparece en **Direcciones IP no permitidas**.

Temas relacionados

- Registro de eventos (página 168)

CAPÍTULO 23

Registro, supervisión y análisis

El cortafuegos proporciona el registro, supervisión y análisis de los eventos y el tráfico de Internet, los cuales resultan muy completos y de fácil lectura. El hecho de comprender mejor el tráfico y los eventos de Internet facilita la gestión de sus conexiones de Internet.

En este capítulo

Registro de eventos

El cortafuegos le permite especificar si desea habilitar o deshabilitar el registro y, en el caso de que lo habilite, qué tipos de evento desea registrar. El registro de eventos le permite ver los eventos entrantes y salientes más recientes. También puede ver los eventos detectados por intrusión.

Configurar un registro de eventos

Para realizar un seguimiento de los eventos y la actividad del cortafuegos, puede especificar y configurar los tipos de eventos que desea visualizar.

Para configurar el registro de eventos:

1. En el panel Configuración de Internet & redes, haga clic en **Avanzada**.
2. En el panel Cortafuegos, haga clic en **Configuración de registro de eventos**.
3. En el panel Configuración de registro de eventos, realice una de las siguientes acciones:
   - Seleccione **Registrar evento** para habilitar el registro de eventos.
   - Seleccione **No registrar evento** para deshabilitar el registro de eventos.
4. En **Configuración de registro de eventos**, especifique los tipos de evento que desea registrar. Existen los tipos de evento siguientes:
   - Pings ICMP
   - Tráfico de direcciones IP no permitidas
   - Eventos en puertos de servicio del sistema
   - Eventos en puertos desconocidos
   - Eventos de detección de intrusiones (IDS)
5. Para evitar el registro en algunos puertos específicos, seleccione **No registrar eventos en los puertos siguientes** e introduzca los números de puerto individuales separados por comas o series de puertos separados por guiones. Por ejemplo, `137-139, 445, 400-5000`.
6. Haga clic en **Aceptar**.

Ver eventos recientes

Si el registro está habilitado, podrá ver los eventos recientes. El panel Eventos recientes muestra la fecha y la descripción del evento. El panel Eventos recientes sólo muestra actividad para aquellos programas que han sido explícitamente bloqueados para que no accedan a Internet.

Para ver los eventos recientes del cortafuegos:

- En el **Menú avanzado**, en el panel Tareas comunes, haga clic en **Informes & Registros** o **Ver eventos recientes**. Como alternativa, haga clic en **Ver eventos recientes** en el panel Tareas comunes desde el Menú básico.

Ver eventos entrantes

Si el registro está habilitado, podrá ver y ordenar los eventos entrantes.

El registro Eventos entrantes incluye las siguientes categorías de registro:

- Fecha y hora
- Dirección IP de origen
- Nombre del servidor
- Información y tipo de evento

Para ver los eventos entrantes del cortafuegos:

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos entrantes**.

Nota: Puede definir una dirección IP como fiable o permitida, o bien rastrearla desde el registro Eventos entrantes.

Temas relacionados

- Agregar un equipo de confianza desde el registro Eventos entrantes (página 158)
- Prohibir un equipo desde el registro Eventos entrantes (página 165)
- Rastrear un equipo desde el registro Eventos entrantes (página 174)

Ver eventos salientes

Si el registro está habilitado, podrá ver los eventos salientes. Eventos salientes incluye el nombre del programa que intenta obtener acceso saliente, la fecha y la hora del evento, y la ubicación del programa en su equipo.

Para ver los eventos salientes del cortafuegos:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos salientes**.

Nota: Puede conceder acceso pleno y sólo saliente a un programa desde el registro Eventos salientes. También puede localizar información adicional sobre el programa.

Temas relacionados

- Conceder acceso pleno desde el registro Eventos salientes (página 142)
- Conceder sólo acceso saliente desde el registro Eventos salientes (página 144)
- Obtener información sobre el programa desde el registro Eventos salientes (página 149)

Ver eventos de detección de intrusiones

Si el registro está habilitado, podrá ver los eventos entrantes. Los eventos de detección de intrusiones muestran la fecha y la hora, la IP de origen y el nombre de host del evento. El registro también describe el tipo de evento.

Para ver sus eventos de detección de intrusiones:

1. En el panel Tareas comunes haga clic en **Informes & Registros**.
2. En Eventos recientes, haga clic en **Ver registro**.
3. Haga clic en **Internet & redes** y luego haga clic en **Eventos de detección de intrusiones**.

Nota: Puede prohibir y rastrear una dirección IP desde el registro Eventos de detección de intrusiones.

Temas relacionados

- Prohibir un equipo desde el registro Eventos de detección de intrusiones (página 166)
- Rastrear un equipo desde el registro Eventos de detección de intrusiones (página 175)

Trabajar con estadísticas

El cortafuegos aprovecha el sitio Web de seguridad McAfee's HackerWatch para proporcionarle estadísticas sobre los eventos de seguridad de Internet y la actividad de puertos en todo el mundo.

Visualizar las estadísticas globales de los eventos de seguridad

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información rastreada enumera los incidentes que ha recibido HackerWatch en las últimas 24 horas, 7 días y 30 días.

Para ver las estadísticas de seguridad globales:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. Visualice las estadísticas de eventos de seguridad en **Rastreo de eventos**.

Visualizar la actividad global de los puertos de Internet

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información que se muestra incluye los puertos de eventos principales que HackerWatch ha registrado durante los últimos siete días. La información que se muestra suele ser de puertos HTTP, TCP y UDP.

Para ver la actividad de puertos en todo el mundo:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. Visualice los eventos de los puertos principales en **Actividad de puertos reciente**.

Rastrear el tráfico de Internet

El cortafuegos ofrece varias opciones para rastrear el tráfico de Internet. Dichas opciones le permiten rastrear geográficamente un equipo de red, obtener información acerca del dominio y la red, y rastrear equipos desde los registros Eventos entrantes y Eventos de detección de intrusiones.

Rastrear un equipo de red geográficamente

Con Visual Tracer puede localizar geográficamente un equipo que esté conectado o esté intentado conectarse a su equipo, mediante su nombre o dirección IP. También puede acceder a información relativa a la red y al registro mediante Visual Tracer. Al ejecutar Visual Tracer aparece un mapamundi que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo.

Para localizar un equipo geográficamente:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de mapa**.

Nota: No se pueden rastrear eventos de direcciones IP de bucle de retorno, privadas o no válidas.

Obtener información de registro de los equipos

Mediante Visual Trace puede obtener información de registro de un equipo desde SecurityCenter. Dicha información incluye el nombre de dominio, el nombre y la dirección de la persona registrada, y el contacto administrativo.

Para obtener información acerca del dominio de un equipo:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de personas registradas**.

Obtener información de red de los equipos

Mediante Visual Trace puede obtener información de red de un equipo desde SecurityCenter. La información de red incluye detalles relativos a la red en la que reside el dominio.

Para obtener información acerca de la red de un equipo:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de red**.

Rastrear un equipo desde el registro Eventos entrantes

Desde el panel Eventos entrantes, se puede rastrear una dirección IP que aparezca en el registro Eventos entrantes.

Para rastrear una dirección IP de un equipo desde el registro Eventos entrantes:

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet** y **redes** y, a continuación, en **Eventos entrantes**.
4. En el panel Eventos entrantes, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta dirección**.
5. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
6. Haga clic en **Realizado**.

Temas relacionados

- Rastrear el tráfico de Internet (página 173)
- Ver eventos entrantes (página 169)

Rastrear un equipo desde el registro Eventos de detección de intrusiones

Desde el panel Eventos de detección de intrusiones, se puede rastrear una dirección IP que aparezca en el registro Eventos de detección de intrusiones.

Para rastrear una dirección IP de un equipo desde el registro Eventos de detección de intrusiones:

1. En el panel Tareas comunes haga clic en **Informes** y **Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet & redes** y luego haga clic en **Eventos de detección de intrusiones**. En el panel Eventos de detección de intrusiones, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta dirección**.
4. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
5. Haga clic en **Realizado**.

Temas relacionados

- Rastrear el tráfico de Internet (página 173)
- Registro, supervisión y análisis (página 167)

Rastrear una dirección IP supervisada

Puede rastrear una dirección IP supervisada para obtener una vista geográfica que muestre la ruta más probable que han seguido los datos desde el equipo de origen hasta el suyo. También puede obtener información de red y de registro sobre la dirección IP.

Para supervisar el ancho de banda de un programa utilice:

1. Asegúrese de que el Menú avanzado está habilitado y haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Seleccione un programa y luego la dirección IP que aparece debajo del nombre del programa.
5. En **Actividad del programa**, haga clic en **Rastrear esta IP**.
6. En **Visual Trace** aparece un mapa que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo. También puede obtener información de red y de registro sobre la dirección IP.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Visual Trace**.

Temas relacionados

- Supervisar el tráfico de Internet (página 177)

Supervisar el tráfico de Internet

El cortafuegos proporciona varios métodos para supervisar su tráfico de Internet, incluido lo siguiente:

- **Gráfico Análisis de tráfico**: Muestra el tráfico de Internet entrante y saliente más reciente.
- **Gráfico Uso del tráfico**: Muestra el porcentaje aproximado de ancho de banda que las aplicaciones más activas han utilizado durante las últimas 24 horas.
- **Programas activos**: Muestra aquellos programas que utilizan actualmente la mayoría de conexiones de Internet en su equipo, así como las direcciones IP a las que acceden dichos programas.

Acerca del gráfico Análisis del tráfico

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el control del tráfico muestra los programas que emplean un mayor número de conexiones de red en el equipo y las direcciones IP a las que acceden los programas.

Desde el panel Análisis de tráfico, se puede visualizar el tráfico de Internet entrante y saliente más reciente, así como las velocidades de transferencia actual, media y máxima. También puede visualizar el volumen de tráfico, incluida la cantidad de tráfico acumulada desde que inició el cortafuegos, y el tráfico total del mes actual o de los meses anteriores.

El panel Análisis de tráfico muestra la actividad de Internet en su equipo a tiempo real, incluidos el volumen y la velocidad del tráfico de Internet entrante y saliente más reciente de su equipo, la velocidad de conexión y el total de bytes transferidos a través de Internet.

La línea continua de color verde representa la velocidad actual de transferencia del tráfico entrante. La línea punteada de color verde representa la velocidad media de transferencia del tráfico entrante. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

La línea continua de color rojo representa la velocidad actual de transferencia del tráfico saliente. La línea punteada de color rojo representa la velocidad media de transferencia del tráfico saliente. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

Temas relacionados

- Analizar el tráfico entrante y saliente (página 179)

Analizar el tráfico entrante y saliente

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el control del tráfico muestra los programas que emplean un mayor número de conexiones de red en el equipo y las direcciones IP a las que acceden los programas.

Para analizar el tráfico entrante y saliente:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Análisis del tráfico**.

Sugerencia: Para ver las estadísticas más actualizadas, haga clic en **Actualizar** en **Análisis del tráfico**.

Temas relacionados

- Acerca del gráfico Análisis del tráfico (página 178)

Supervisar el ancho de banda de un programa

Puede visualizar el gráfico de sectores, que muestra el porcentaje aproximado del ancho de banda utilizado por los programas que han estado más activos en su equipo durante las últimas veinticuatro horas. El gráfico de sectores ofrece una representación visual de las cantidades relativas del ancho de banda utilizado por los programas.

Para supervisar el ancho de banda de un programa utilice:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Uso del tráfico**.

Sugerencia: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Uso del tráfico**.

Supervisar la actividad de un programa

Puede ver la actividad entrante y saliente del programa, que le muestra las conexiones y puertos del equipo.

Para supervisar el ancho de banda de un programa utilice:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Puede ver la información siguiente:
   - Gráfico de actividad del programa: Seleccione un programa para que muestre un gráfico de su actividad.
   - Conexión en escucha: Seleccione un elemento en escucha bajo el nombre del programa.
   - Conexión del equipo: Seleccione una dirección IP con el nombre del programa, proceso del sistema o servicio.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Programas activos**.

CAPÍTULO 24

Obtener más información sobre la seguridad en Internet

El cortafuegos aprovecha el sitio Web de seguridad de McAfee, HackerWatch, para proporcionarle información acerca de los programas y la actividad de Internet en todo el mundo. HackerWatch también pone a su disposición un tutorial HTML sobre el cortafuegos.

En este capítulo

Iniciar el tutorial de HackerWatch

Para obtener información sobre el cortafuegos, puede acceder al tutorial de HackerWatch desde SecurityCenter.

Para iniciar el tutorial de HackerWatch:

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. En **Recursos de HackerWatch**, haga clic en **Ver tutorial**.

CAPÍTULO 25

McAfee Data Backup

Utilice Data Backup para evitar la pérdida accidental de sus datos archivando sus archivos en CD, DVD, unidad USB, disco duro externo o unidad de red. El almacenamiento local le permite archivar (realizar una copia de seguridad) de sus datos personales en CD, DVD, unidad USB, disco duro externo o unidad de red. De este modo se crea una copia local de sus registros, documentos y demás material de interés personal en caso de pérdida accidental.

Antes de empezar a utilizar Data Backup, puede familiarizarse con algunas de las funciones más conocidas. Encontrará información más detallada sobre la configuración y uso de estas funciones en la ayuda de Data Backup. Después de consultar las funciones del programa, debe asegurarse de que cuenta con los soportes de archivo necesarios para realizar almacenamientos locales.

En este capítulo

Funciones

Data Backup ofrece las funciones siguientes para guardar y restaurar sus fotos, música y otros archivos importantes.

Archivo planificado local

Proteja sus datos archivando archivos y carpetas en CD, DVD, unidad USB, disco duro externo o unidad de red. Después de iniciar la primera operación de archivo, se realizarán operaciones de archivo incrementales automáticamente.

Restaurar con un clic

Si los archivos o carpetas se eliminan por error o se corrumpen en su equipo, puede recuperar las versiones más recientes archivadas desde el soporte de archivo utilizado.

Compresión y encriptación

De forma predeterminada, se comprimen los archivos archivados, de modo que se ahorra espacio en los soportes de archivo. Como medida de seguridad adicional, se encriptan los archivos de forma predeterminada.

CAPÍTULO 26

Cómo archivar archivos

Puede utilizar McAfee Data Backup para archivar una copia de los archivos de su equipo en CD, DVD, unidad USB, disco duro externo o unidad de red. Al archivar sus ficheros de esta manera, le resultará fácil recuperar la información en caso de pérdida o daño accidental de los datos.

Antes de empezar a archivar los archivos, debe seleccionar su ubicación predeterminada (CD, DVD, unidad USB, disco duro externo o unidad de red). McAfee ha preconfigurado algunos ajustes más; por ejemplo, las carpetas y los tipos de archivo que desea archivar, pero usted puede modificar estos ajustes.

Después de configurar las opciones del archivo local, puede modificar los ajustes predeterminados referentes a cada cuánto tiempo Data Backup ejecuta archivos rápidos o completos. Puede realizar archivos manuales en cualquier momento.

En este capítulo

Configuración de las opciones de archivo

Antes de empezar a archivar sus datos, debe configurar algunas opciones del archivo local. Por ejemplo, debe establecer las ubicaciones y los tipos de archivos observados. Las ubicaciones de observación son las carpetas de su equipo en las que Data Backup controla y busca nuevos archivos o cambios en éstos. Los tipos de archivos observados son los tipos de archivo (por ejemplo, .doc, .xls, etc.) que Data Backup archiva en las ubicaciones de observación. Por defecto, Data Backup observa todos los tipos de archivo almacenados en sus ubicaciones de observación.

Puede configurar dos tipos de ubicaciones de observación: ubicaciones de observación en profundidad y ubicaciones de observación superficial. Si se establece una ubicación de observación en profundidad, Data Backup archiva una copia de los tipos de archivos observados en dicha carpeta y sus subcarpetas. Si se establece una ubicación de observación superficial, Data Backup crea una copia de los tipos de archivos observados únicamente en dicha carpeta (no en sus subcarpetas). También puede identificar las ubicaciones que desea excluir del archivo local. Por defecto, el Escritorio de Windows y Mis documentos se configuran como ubicaciones de observación en profundidad.

Después de configurar los tipos de archivos y las ubicaciones de observación, debe seleccionar la ubicación del archivo (es decir, el CD, DVD, unidad USB, disco duro externo o unidad de red donde se almacenarán los datos archivados). Puede cambiar la ubicación del archivo en cualquier momento.

Por motivos de seguridad o problemas de tamaño, el cifrado y la compresión están habilitados por defecto para sus ficheros archivados. El contenido de los archivos cifrados se transforma de texto en código, de forma que la información queda oculta y resulta ilegible para aquellas personas que no saben cómo descifrarla. Los archivos comprimidos se comprimen en un formato que minimiza el espacio necesario para su almacenamiento y transmisión. Si bien McAfee no recomienda hacerlo, puede desactivar el cifrado o la compresión en cualquier momento.

Cómo incluir una ubicación en el archivo

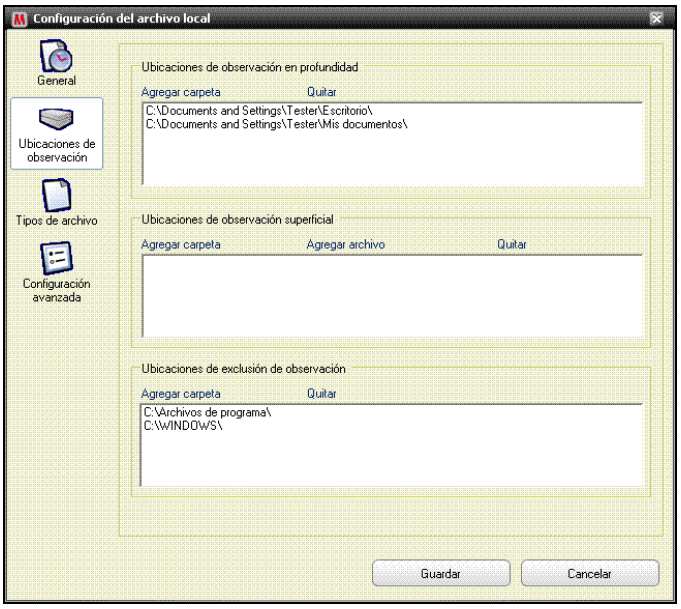
Puede configurar dos tipos de ubicaciones de observación para archivar: en profundidad y superficial. Si se establece una ubicación de observación en profundidad, Data Backup controla los cambios del contenido de dicha carpeta y sus subcarpetas. Si se establece una ubicación de observación superficial, Data Backup controla únicamente el contenido de dicha carpeta (no de sus subcarpetas).

Para incluir una ubicación en el archivo:

1 Haga clic en **Archivo local**.

2 En el panel izquierdo, haga clic en **Configuración**.

3 En el cuadro de diálogo Configuración del archivo local, haga clic en **Ubicaciones de observación**.



4 Siga uno de estos procedimientos:

- Para archivar el contenido de una carpeta, incluido el contenido de sus subcarpetas, haga clic en **Agregar carpeta** bajo **Ubicaciones de observación en profundidad**.
- Para archivar el contenido de una carpeta, pero no del contenido de sus subcarpetas, haga clic en **Agregar carpeta** bajo **Ubicaciones de observación superficial**.

5 En el cuadro de diálogo Buscar carpeta, acceda a la carpeta que desee observar y haga clic en **Aceptar**.

6 Haga clic en **Guardar**.

Sugerencia: Si desea que Data Backup observe una carpeta que aún no ha creado, puede hacer clic en **Crear nueva carpeta** en el cuadro de diálogo Buscar carpeta para agregar una carpeta y configurarla como ubicación de observación al mismo tiempo.

Configuración de los tipos de fichero del archivo

Puede especificar los tipos de ficheros archivados en las ubicaciones de observación en profundidad o superficial. Puede seleccionarlos de una lista de tipos de ficheros existente o agregar un nuevo tipo de fichero a la lista.

Para configurar los tipos de fichero del archivo:

1 Haga clic en **Archivo local**.

2 En el panel izquierdo, haga clic en **Configuración**.

3 En el cuadro de diálogo Configuración del archivo local, haga clic en **Tipos de archivo**.

4 Amplíe las listas de tipos de archivo y active las casillas situadas junto a los tipos de archivo que desea archivar.

5 Haga clic en **Guardar**.

Sugerencia: Para agregar un nuevo tipo de archivo a la lista **Tipos de archivo seleccionados**, escriba la extensión del archivo en el cuadro de diálogo **Agregar tipo de archivo personalizado a "Otros"** y haga clic en **Agregar**. El nuevo tipo de archivo se convierte automáticamente en un tipo de archivo de observación.

Cómo excluir una ubicación del archivo

Puede excluir una ubicación del archivo si desea evitar que dicha ubicación (carpeta) y su contenido se archiven.

Para excluir una ubicación del archivo:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. En el cuadro de diálogo Configuración del archivo local, haga clic en **Ubicaciones de observación**.
4. Haga clic en **Agregar carpeta** bajo **Ubicaciones de exclusión de observación**.
5. En el cuadro de diálogo Buscar carpeta, acceda a la carpeta que desee excluir, selecciónela y haga clic en **Aceptar**.
6. Haga clic en **Guardar**.

Sugerencia: Si desea que Data Backup excluya una carpeta que aún no ha creado, puede hacer clic en **Crear nueva carpeta** en el cuadro de diálogo Buscar carpeta para agregar una carpeta y excluirla al mismo tiempo.

Cómo cambiar la ubicación del archivo

Al cambiar la ubicación del archivo, los ficheros previamente archivados en una ubicación diferente aparecen como *Nunca archivado*.

Para cambiar la ubicación del archivo:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. Haga clic en **Cambiar ubicación de archivo**.
4. En el cuadro de diálogo Ubicación del archivo, realice una de las acciones siguientes:
   - Haga clic en **Seleccionar grabador de CD/DVD**, pulse la unidad de CD o DVD de se equipo en la lista **Grabador** y haga clic en **Guardar**.
   - Haga clic en **Seleccionar ubicación del disco**, vaya al disco USB, al disco local o al disco duro externo, selecciónelo y haga clic en **Aceptar**.
   - Haga clic en **Seleccionar ubicación de red**, vaya a la carpeta de red, selecciónela y haga clic en **Aceptar**.

5 Verifique la nueva ubicación del archivo en **Ubicación de archivo seleccionada** y haga clic en **Aceptar**.

6 En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

7 Haga clic en **Guardar**.

Desactivación del cifrado y la compresión de archivos

El cifrado de los ficheros archivados protege la confidencialidad de sus datos ocultando el contenido de los archivos para que sean ilegibles. La compresión de los ficheros archivados ayuda a minimizar el tamaño de los archivos. Por defecto, tanto el cifrado como la compresión están habilitados; sin embargo, puede desactivar estas opciones en cualquier momento.

Para desactivar el cifrado y la compresión de archivos:

1 Haga clic en **Archivo local**.

2 En el panel izquierdo, haga clic en **Configuración**.

3 En el cuadro de diálogo Configuración del archivo local, haga clic en **Configuración avanzada**.

4 Desactive la casilla **Activar cifrado para aumentar seguridad**.

5 Desactive la casilla **Activar compresión para reducir almacenamiento**.

6 Haga clic en **Guardar**.

Nota: McAfee le aconseja que no desactive el cifrado ni la compresión al archivar sus archivos.

Uso de archivos completos y rápidos

Puede utilizar dos tipos de archivo: completo o rápido. Al utilizar un archivo completo, se archiva un conjunto de datos completo basado en las ubicaciones y los tipos de archivos observados que haya configurado. Al utilizar un archivo rápido, archiva únicamente aquellos archivos observados que se han modificado desde la última operación de archivado rápido.

Por defecto, Data Backup está programado para realizar un archivado completo de los tipos de archivos observados en sus ubicaciones de observación los lunes a las 9:00 y un archivado rápido cada 48 horas después del último archivado completo o rápido. Esta programación garantiza que en todo momento se mantenga un archivo de sus archivos actualizado. Pese a ello, si no desea archivar cada 48 horas, puede ajustar la programación a sus necesidades.

Si desea archivar el contenido de sus ubicaciones de observación cuando lo solicite, puede hacerlo en todo momento. Por ejemplo, si desea modificar un archivo y archivarlo, pero Data Backup no está programado para realizar un archivado completo o rápido hasta dentro de 60 minutos, puede archivar los archivos de manera manual. Al archivar archivos manualmente, se restablece el intervalo configurado para los archivados automáticos.

También puede interrumpir un archivado automático o manual si se produce en un momento inadecuado. Por ejemplo, si está realizando una tarea que consume muchos recursos y se inicia un archivado automático, usted puede detenerlo. Al detener un archivado automático se restablece el intervalo configurado para los archivados automáticos.

Programación de los archivados automáticos

Puede configurar la frecuencia de los archivos rápidos y completos para asegurarse de que sus datos están permanentemente protegidos.

Para programar archivos automáticos:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. En el cuadro de diálogo Configuración del archivo local, haga clic en **General**.
4. Para realizar un archivo completo todos los días, semanas o meses, haga clic en lo siguiente bajo **Archivo completo cada**:
   - **Día**

- **Semana**
- **Mes**

5 Active la casilla situada junto al día en el que desea realizar el archivo completo.

6 Haga clic en un valor de la lista **A las** para especificar la hora en la que desea realizar el archivo completo.

7 Para realizar un archivo rápido diariamente, haga clic en lo siguiente bajo **Archivo rápido**:

- **Horas**
- **Días**

8 Escriba un número que represente la frecuencia en el cuadro **Archivo rápido cada**.

9 Haga clic en **Guardar**.

Interrupción de un archivo automático

Data Backup archiva automáticamente los archivos de sus ubicaciones de observación en función de la programación que usted defina. Sin embargo, si se está archivando automáticamente y desea interrumpir la operación, puede hacerlo en todo momento.

Para interrumpir un archivo automático:

1 En el panel izquierdo, haga clic en **Detener el archivado**.

2 En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Nota: El enlace **Detener el archivado** únicamente aparece cuando hay un archivado en progreso.

Ejecutar archivados manualmente

Pese a que los archivados automáticos se realizan en función de una programación predefinida, puede realizar archivados completos o rápidos de manera manual en cualquier momento. Un archivado rápido archiva únicamente aquellos archivos que se han modificado desde la última operación de archivado rápido o completo. Un archivo completo archiva los tipos de archivos observados de todas las ubicaciones de observación.

Para ejecutar un archivo rápido o completo manualmente:

1. Haga clic en **Archivo local**.
2. Para ejecutar un archivo rápido, haga clic en **Archivo rápido** en el panel de la izquierda.
3. Para ejecutar un archivo completo, haga clic en **Archivo completo** en el panel de la izquierda.
4. En el cuadro de diálogo Listo para iniciar el proceso de archivo, verifique su espacio de almacenamiento y su configuración y haga clic en **Continuar**.

CAPÍTULO 27

Cómo trabajar con archivos archivados

Después de archivar algunos archivos, puede utilizar Data Backup para trabajar con ellos. Los archivos archivados se presentan en la vista tradicional del navegador, lo que le permite localizarlos fácilmente. A medida que su archivo aumenta, es posible que desee ordenar los archivos o buscarlos. También puede abrir los archivos directamente en la vista del navegador para examinar el contenido sin tener que recuperar los archivos.

Puede recuperar los archivos de un archivo si la copia local del mismo no está actualizada, se daña o falta. Data Backup también le ofrece la información necesaria para gestionar sus archivos locales y su espacio de almacenamiento.

En este capítulo

Uso del navegador del archivo local

El navegador del archivo local le permite visualizar y manipular los archivos que ha archivado localmente. Puede ver el nombre, tipo, ubicación, tamaño, estado (archivado, no archivado o archivo en progreso) y la fecha en la que cada archivo se archivó por última vez. También puede ordenar los archivos por cualquiera de estos criterios.

Si tiene un archivo grande, puede encontrar un archivo rápidamente al buscarlo. Puede buscar por el nombre completo del archivo, por parte de él o por su ruta y puede restringir su búsqueda especificando el tamaño de archivo aproximado y la fecha en la que se archivó por última vez.

Cuando ubique un archivo, puede abrirlo directamente en el navegador del archivo local. Data Backup abre el archivo en su programa nativo, permitiéndole realizar cambios sin salir del navegador del archivo local. El archivo se guarda en la ubicación de observación original del equipo y se archiva automáticamente en función de la programación de archivado definida.

Cómo ordenar archivos archivados

Puede ordenar los archivos y las carpetas archivadas por los siguientes criterios: nombre, tipo de archivo, tamaño, estado (es decir, archivado, no archivado o archivo en progreso), la fecha en la que se archivaron los archivos por última vez o la ubicación de los archivos en su equipo (ruta).

Para ordenar archivos archivados:

1. Haga clic en **Archivo local**.
2. En el panel de la derecha, haga clic en el nombre de una columna.

Cómo buscar un archivo archivado

Si tiene un amplio repositorio de archivos archivados, puede encontrar un archivo rápidamente al buscarlo. Puede buscar por el nombre completo del archivo, por parte de él o por su ruta y puede restringir su búsqueda especificando el tamaño de archivo aproximado y la fecha en la que se archivó por última vez.

Para buscar un archivo archivado:

1. Escriba el nombre completo o parte de él en el cuadro de diálogo **Buscar** situado en la parte superior de la pantalla y pulse INTRO.
2. Escriba la ruta completa o parte de ella en el cuadro de diálogo **Todo o parte de la ruta**.
3. Especifique el tamaño aproximado del archivo que está buscando realizando uno de los siguientes pasos:
   - Haga clic en **<100 KB**, **<1 MB** o **>1 MB**.
   - Haga clic en **Tamaño en KB** y especifique los valores de tamaño apropiados en los cuadros de diálogo.
4. Especifique la fecha aproximada en la que se realizó la última copia en línea del archivo realizando uno de los siguientes pasos:
   - Haga clic en **Esta semana**, **Este mes** o **Este año**.
   - Haga clic en **Especificar fechas**, haga clic en **Archivados** en la lista y haga clic en los valores de fecha adecuados en las listas de fecha.
5. Haga clic en **Buscar**.

Nota: Si desconoce el tamaño o la fecha del último archivo aproximados, haga clic en **Desconocidos**.

Cómo abrir un archivo archivado

Puede examinar el contenido de un archivo archivado abriéndolo directamente en el navegador del archivo local.

Para abrir un archivo archivado:

1. Haga clic en **Archivo local**.
2. En el panel de la derecha, haga clic en un nombre de archivo y clic en **Abrir**.

Sugerencia: También puede abrir un archivo archivado haciendo doble clic en el nombre del archivo.

Recuperación de archivos archivados

Si un archivo observado se daña, falta o se elimina por error, puede recuperar una copia reciente del mismo desde un archivo local. Por este motivo, es importante asegurarse de que archiva sus archivos de forma regular. También puede recuperar versiones de archivos anteriores desde un archivo local. Por ejemplo, si archiva un archivo de manera regular, pero desea restablecer una versión anterior de un archivo, puede hacerlo localizando el archivo en la ubicación del archivado. Si la ubicación del archivo es un disco local o de red, puede buscar el archivo. Si la ubicación del archivo es un disco duro externo o USB, debe conectar el disco al equipo y a continuación buscar el archivo. Si la ubicación del archivo es un CD o DVD, debe introducirlo en el equipo y a continuación buscar el archivo.

También puede recuperar archivos que haya archivado en equipo desde otro equipo diferente. Por ejemplo, si archiva un conjunto de archivos en un disco duro externo en el equipo A, puede recuperarlos en el equipo B. Para ello, debe instalar McAfee Data Backup en el equipo B y conectar el disco duro externo. A continuación, en Data Backup, busque los archivos que se añaden a la lista **Archivos que faltan** para su recuperación.

Si desea obtener más información sobre el archivado de archivos, consulte Cómo archivar archivos. Si elimina un archivo observado de su equipo de manera intencionada, también puede eliminar la entrada de la lista **Archivos que faltan**.

Recuperación de archivos que faltan desde un archivo local

El archivo local de Data Backup le permite recuperar datos que faltan desde una ubicación de observación de su equipo local. Por ejemplo, si un archivo se saca de una carpeta de observación o si se elimina, y ya se ha archivado, puede recuperarlo desde el archivo local.

Para recuperar un archivo que falta desde un archivo local:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, seleccione la casilla situada junto al nombre del archivo que desea recuperar.
3. Haga clic en **Restaurar**.

Sugerencia: Puede recuperar todos los archivos de la lista **Archivos que faltan** haciendo clic en **Restaurar todo**.

Recuperación de una versión anterior de un archivo desde el archivo local

Si desea recuperar una versión anterior de un archivo archivado, puede localizarlo y agregarlo a la lista **Archivos que faltan**. A continuación, puede recuperar el archivo, del mismo modo que cualquier otro archivo en la lista **Archivos que faltan**.

Para recuperar una versión anterior de un archivo desde el archivo local:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, haga clic en **Examinar** y vaya a la ubicación en la que se almacena el archivo.

   Los nombres de las carpetas archivadas tienen el siguiente formato: `cre ddmmaa_hh-mm-ss_***`, donde `ddmmaa` es la fecha en la que se archivaron los archivos, `hh-mm-ss` es la hora en la que se archivaron los archivos y `***` es `Completo`o `Inc`, en función de si se ha realizado un archivo completo o rápido.
3. Seleccione la ubicación y haga clic en **Aceptar**.

   Los archivos contenidos en la ubicación seleccionada aparecen en la lista **Archivos que faltan**, listos para ser recuperados. Para obtener más información, consulte Recuperación de archivos que faltan desde un archivo local.

Eliminación de archivos de la lista de archivos que faltan

Cuando un archivo archivado se saca de una carpeta observada o se elimina, aparece automáticamente en la lista **Archivos que faltan**. Esto le advierte del hecho de que existe una incoherencia entre los archivos archivados y los archivos dentro de las carpetas observadas. Si el archivo se ha sacado de la carpeta observada o si se ha eliminado intencionadamente, puede eliminarlo de la lista **Archivos que faltan**.

Para eliminar un archivo de la lista Archivos que faltan:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, seleccione la casilla situada junto al nombre del archivo que desea eliminar.
3. Pulse en **Eliminar**.

Sugerencia: Puede eliminar todos los archivos de la lista **Archivos que faltan** haciendo clic en **Suprimir todo**.

Gestión de archivos

Puede ver un resumen de la información sobre sus archivos completos y rápidos en cualquier momento. Por ejemplo, puede ver la información sobre la cantidad de datos observados actualmente, la cantidad de datos archivados y la cantidad de datos actualmente observada pero que aún no han sido archivados. También puede ver información sobre la programación de archivo, como la fecha del último y el siguiente archivo.

Cómo ver un resumen de su actividad de archivado

Puede ver la información sobre su actividad de archivado en cualquier momento. Por ejemplo, puede ver el porcentaje de archivos archivados, el tamaño de los datos observados, el tamaño de los datos archivados y el tamaño de los datos observados pero que aún no han sido archivados. También puede ver las fechas del último y el siguiente archivo.

Para ver un resumen de su actividad de copias de seguridad:

1. Haga clic en **Archivo local**.
2. En la parte superior de la pantalla, haga clic en **Resumen de la cuenta**.

CAPÍTULO 28

McAfee EasyNetwork

McAfee® EasyNetwork permite compartir archivos de forma segura, simplifica la transferencia de archivos y automatiza el uso compartido de impresoras entre los equipos de su red doméstica.

Antes de comenzar a usar EasyNetwork, puede familiarizarse con algunas de las funciones más conocidas. Encontrará información mas detallada sobre la configuración y uso de estas funciones en la ayuda de EasyNetwork.

En este capítulo

Funciones

EasyNetwork ofrece las funciones siguientes.

Uso compartido de archivos

EasyNetwork hace que compartir archivos de su equipo con otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a otros equipos a estos archivos. Sólo los equipos que sean miembros de la red gestionada (es decir, con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros miembros.

Transferencia de archivos

Puede enviar archivos a otros equipos que sean miembros de la red gestionada. Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que otros equipos de la red le envíen.

Uso compartido de la impresora automatizado

Después de conectarse a una red gestionada, EasyNetwork comparte automáticamente cualquier impresora local que esté conectada con su equipo, utilizando el nombre actual de la impresora como nombre de impresora compartida. También detecta impresoras compartidas por otros equipos de la red y le permite configurar y utilizar estas impresoras.

CAPÍTULO 29

Configuración de EasyNetwork

Antes de poder utilizar las funciones de EasyNetwork, deberá iniciar el programa e incorporarse a la red gestionada. Tras la incorporación, puede decidir salir de la red en cualquier momento.

En este capítulo

Inicio de EasyNetwork

De forma predeterminada, se le pedirá que inicie EasyNetwork inmediatamente después de la instalación; sin embargo, también puede iniciar EasyNetwork más tarde.

Iniciar EasyNetwork

De forma predeterminada, se le pedirá que inicie EasyNetwork inmediatamente después de la instalación; sin embargo, también puede iniciar EasyNetwork más tarde.

Para iniciar EasyNetwork:

- En el menú **Inicio**, seleccione **Programas**, **McAfee** y, a continuación, haga clic en **McAfee EasyNetwork**.

Sugerencia: si ha decidido crear iconos de escritorio e inicio rápido durante la instalación, también puede iniciar EasyNetwork haciendo doble clic en el icono de McAfee EasyNetwork del escritorio o haciendo clic en el icono de McAfee EasyNetwork del área de notificación a la derecha de la barra de tareas.

Incorporarse a una red gestionada

Tras instalar SecurityCenter, un agente de red se agrega a la impresora y funciona en segundo plano. En EasyNetwork, el agente de red es responsable de detectar una conexión válida a la red, detectar impresoras locales para compartir y controlar el estado de la red.

Si no se encuentra ningún otro equipo que ejecute el agente de red en la red a la que está conectado actualmente, se convierte automáticamente en miembro de la red y se le pedirá que identifique si la red es de confianza. Cuando el primer equipo se une a la red, el nombre de su equipo está incluido en el nombre de la red; sin embargo, puede cambiar el nombre de la red en cualquier momento.

Cuando un equipo se conecta a la red, se envía una solicitud de incorporación a todos los equipos que están actualmente en la red. Cualquier equipo con permisos administrativos en la red puede conceder la solicitud. El equipo que la admita puede determinar también el nivel de permiso para el equipo que se está uniendo a la red en esos momentos; por ejemplo, como invitado (solamente posibilidad de transferencia de archivos) o completo/administrador (posibilidad de transferir y compartir archivos). En EasyNetwork, los equipos con acceso de administrador pueden conceder el acceso a otros equipos y administrar permisos (esto es, promover o degradar equipos); los equipos con un acceso completo realizan estas tareas administrativas. Antes de permitir que el equipo se una, deberá realizarse una comprobación de seguridad.

Nota: tras incorporarse, si tiene instalados otros programas de McAfee de conexión a redes (por ejemplo, McAfee Wireless Network Security o Network Manager), el equipo también queda reconocido como equipo gestionado en estos programas. El nivel de permisos que se asigna a un equipo se aplica a todos los programas de conexión a redes de McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporación a la red

Cuando un equipo se conecta a una red de confianza por primera vez tras instalar EasyNetwork, aparece un mensaje preguntándole si desea incorporarse a la red gestionada. Cuando un equipo está de acuerdo con la incorporación, se envía una solicitud a todos los demás equipos de la red que tengan derechos de administrador. Esta solicitud debe admitirse antes de que el equipo pueda compartir impresoras o archivos, o enviar y copiar archivos en la red. Si el equipo es el primero en la red, se conceden permisos de administración en la red automáticamente.

Para incorporarse a la red:

1. En la ventana Archivos compartidos, haga clic en **Sí, deseo incorporarme ahora**.
   Cuando un equipo de administrador de la red admite su solicitud, aparece un mensaje preguntándole si desea permitir que este equipo y otros equipos de la red gestionen la configuración de seguridad de los demás.
2. Para permitir que este y otros equipos de la red gestionen la configuración de seguridad de los demás, haga clic en **Sí**; de lo contrario, haga clic en **No**.
3. Compruebe que el equipo que concede el permiso muestre las tarjetas que se visualizan en esos momentos en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Confirmar**.

Nota: si el equipo que concede el permiso no muestra las mismas tarjetas que se visualizan en el cuadro de diálogo de confirmación de la seguridad, se ha producido una brecha de seguridad en la red gestionada. En ese caso, la incorporación a la red pondría en peligro a su equipo; por consiguiente, haga clic en **Rechazar** en el cuadro de diálogo de confirmación.

Concesión de acceso a la red

Cuando un equipo solicita incorporarse a una red gestionada, se envía un mensaje a todos los demás equipos de la red que tengan derechos de administrador. El primer equipo en responder al mensaje se convierte en el equipo que realiza la concesión. Como tal, usted es responsable de decidir qué tipo de acceso desea conceder al equipo: invitado, completo o administrador.

Para conceder acceso a la red:

1. En la alerta, marque una de las siguientes casillas de verificación:
   - **Conceder acceso de invitado**: permite al usuario enviar archivos a otros equipos, pero no compartir archivos.

- **Conceder acceso completo a todas las aplicaciones de red gestionadas**: permite al usuario enviar y compartir archivos.
- **Conceder acceso administrativo a todas las aplicaciones de red gestionadas**: permite al usuario enviar y compartir archivos, conceder acceso a otros usuarios y ajustar niveles de permiso de otros equipos.

2 Haga clic en **Conceder acceso**.

3 Compruebe que el equipo muestre las tarjetas que se visualizan en esos momentos en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Confirmar**.

Nota: si el equipo no muestra las mismas tarjetas que se visualizan en el cuadro de diálogo de confirmación de la seguridad, se ha producido una brecha de seguridad en la red gestionada. La concesión de acceso a este equipo podría poner su equipo en peligro; por lo tanto, haga clic en **Rechazar** en el cuadro de diálogo de confirmación de la seguridad.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el nombre del primer equipo que se incorporó a ella; sin embargo, puede cambiar el nombre de la red en cualquier momento. Cuando cambie el nombre de la red, cambie la descripción de la red mostrada en EasyNetwork.

Para cambiar el nombre de la red:

1. En el menú **Opciones** , haga clic en **Configurar**.
2. En el cuadro de diálogo Configurar, escriba el nombre de la red en el cuadro **Nombre de red**.
3. Haga clic en **Aceptar**.

Abandonar una red gestionada

Si se incorpora a una red gestionada y después decide que no quiere seguir siendo miembro de ella, puede abandonarla. Tras renunciar a formar parte de ella, puede volver a incorporarse en cualquier momento; no obstante, debe obtener permiso para incorporarse y volver a realizar la comprobación de seguridad. Para obtener más información, consulte Incorporación a una red gestionada (página 205).

Abandonar una red gestionada

Puede abandonar una red gestionada a la que se haya incorporado previamente.

Para abandonar una red gestionada:

1. En el menú **Herramientas**, haga clic en **Abandonar red**.
2. En el cuadro de diálogo Abandonar red, seleccione el nombre de la red que desea abandonar.
3. Haga clic en **Abandonar red**.

CAPÍTULO 30

Compartir y enviar archivos

EasyNetwork hace que compartir y enviar archivos de su equipo entre los otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a otros equipos a estos archivos. Sólo los equipos que sean miembros de la red gestionada (es decir, con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros.

En este capítulo

Compartir archivos

EasyNetwork hace que compartir archivos de su equipo con otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a otros equipos a estos archivos. Sólo los equipos que sean miembros de la red gestionada (es decir, con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros. Si comparte una carpeta, se comparten todos los archivos incluidos en esa carpeta y sus subcarpetas; sin embargo, los archivos que se agreguen posteriormente a la carpeta no se compartirán automáticamente. Si se elimina un archivo o carpeta, se elimina automáticamente de la ventana Archivos compartidos. Puede dejar de compartir un archivo en cualquier momento.

Puede acceder a un archivo compartido de dos formas: abriendo el archivo directamente desde EasyNetwork o copiando el archivo en una ubicación del equipo, y reabriéndolo. Si la lista de archivos compartidos es demasiado larga, puede buscar el archivo o archivos compartidos a los que desea acceder.

Nota: no se puede acceder a los archivos compartidos con EasyNetwork desde otros equipos con el Explorador de Windows. Los archivos EasyNetwork se comparten a través de conexiones seguras.

Compartir un archivo

Cuando se comparte un archivo, todos los demás miembros pueden acceder a él automáticamente con acceso completo o derechos de administrador a la red gestionada.

Para compartir un archivo:

1. En el Explorador de Windows, localice el archivo que desea compartir.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta la ventana Archivos compartidos de EasyNetwork.

Sugerencia: también puede compartir un archivo haciendo clic en **Compartir archivos** del menú **Herramientas** . En el cuadro de diálogo Compartir, acceda a la carpeta donde esté almacenado el archivo que desee compartir, seleccione el archivo y, a continuación, haga clic en **Compartir**.

Detener el uso compartido de un archivo

Si comparte un archivo en la red gestionada, puede detener el uso compartido en cualquier momento. Cuando deja de compartir un archivo, otros miembros de la red gestionada ya no podrán acceder a él.

Para detener el uso compartido de un archivo:

1. En el menú **Herramientas**, haga clic en **Detener el uso compartido de archivos**.
2. En el cuadro de diálogo Detener el uso compartido de archivos, seleccione el archivo que ya no desea compartir.
3. Haga clic en **No compartir**.

Copiar un archivo compartido

Puede copiar archivos compartidos a su equipo desde cualquier equipo de la red gestionada. Así, si el equipo detiene el uso compartido del archivo, usted tendrá una copia.

Para copiar un archivo:

- Arrastre un archivo desde la ventana Archivos compartidos en EasyNetwork hasta una ubicación del Explorador de Windows o al Escritorio de Windows.

Sugerencia: también puede copiar un archivo compartido seleccionando el archivo en EasyNetwork y haciendo clic en **Copiar a** del menú **Herramientas**. En el cuadro de diálogo Copiar a carpeta, acceda a la carpeta en la que quiera copiar el archivo, selecciónela y haga clic en **Guardar**.

Buscar un archivo compartido

Puede buscar un archivo que no lo haya compartido usted ni ningún otro miembro de la red. Mientras escribe sus criterios de búsqueda, EasyNetwork muestra automáticamente los resultados correspondientes en la ventana Archivos compartidos.

Para buscar un archivo compartido:

1. En la ventana Archivos compartidos, haga clic en **Buscar**.
2. Haga clic en una de las opciones siguientes de la lista **Contiene**:
   - **Contiene todas las palabras**: Busca nombres de archivos o rutas que contienen todas las palabras que especifique en la lista **Nombre de archivo o ruta**, en cualquier orden.
   - **Contiene alguna de las palabras**: Busca nombres de archivos o rutas que contienen alguna de las palabras que especifique en la lista **Nombre de archivo o ruta**.

- **Contiene la cadena de texto exacta**: Busca nombres de archivos o rutas que contienen la frase exacta que especifique en la lista **Nombre de archivo o ruta**.

3 Escriba parte o todo el nombre del archivo en la lista **Nombre de archivo o ruta**.

4 Haga clic en uno de los tipos de archivo siguientes en la lista **Tipo**:

- **Cualquiera**: busca todos los tipos de archivos compartidos.
- **Documento**: busca todos los documentos compartidos.
- **Imagen**: busca todos los archivos de imagen compartidos.
- **Vídeo**: busca todos los archivos de vídeo compartidos.
- **Audio**: busca todos los archivos de audio compartidos.

5 En las listas **De** y **A**, haga clic en las fechas que representan el intervalo de fechas en las que se haya creado el archivo.

Envío de archivos a otros equipos

Puede enviar archivos a otros equipos que sean miembros de la red gestionada. Antes de enviar un archivo, EasyNetwork comprueba que el equipo que recibe el archivo tiene suficiente espacio disponible en el disco.

Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que otros equipos de la red le envíen. Si tiene abierto EasyNetwork al recibir un archivo, este archivo aparece al instante en su buzón de entrada; de lo contrario, aparece un mensaje en el área de notificación a la derecha de la barra de herramientas de Windows. Si no quiere recibir mensajes de notificación, puede desactivar esta opción. Si ya existe un archivo con el mismo nombre en el buzón de entrada, el nuevo archivo cambia de nombre por un sufijo numérico. Los archivos se mantienen en el buzón de entrada hasta que los acepte (es decir, deberá copiarlos en una ubicación de su equipo).

Enviar un archivo a otro equipo

Puede enviar un archivo directamente a otro equipo de la red gestionada sin compartirlo. Antes de que el usuario del equipo receptor pueda ver el archivo, deberá guardarlo en una ubicación local. Para obtener más información, consulte Aceptar un archivo de otro equipo (página 216).

Para enviar un archivo a otro equipo:

1. En el Explorador de Windows, localice el archivo que desea enviar.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta el icono de un equipo activo de EasyNetwork.

Sugerencia: Puede enviar múltiples archivos a un equipo presionando CTRL al seleccionar los archivos. También puede enviar archivos haciendo clic en **Enviar** del menú **Herramientas**, seleccionando los archivos y después haciendo clic en **Enviar**.

Aceptar un archivo de otro equipo

Si otro equipo de la red gestionada le envía un archivo, deberá aceptarlo (guardándolo en una carpeta de su equipo). Si no tiene abierto EasyNetwork ni está en primer plano cuando se envía un archivo a su equipo, recibirá un mensaje de notificación en el área de notificación a la derecha de la barra de tareas. Haga clic en el mensaje de notificación para abrir EasyNetwork y acceder al archivo.

Para recibir un archivo de otro equipo:

- Haga clic en **Recibido** y arrastre el archivo desde el buzón de entrada de EasyNetwork a una carpeta del Explorador de Windows.

Sugerencia: también puede recibir un archivo desde otro equipo seleccionando el archivo en su buzón de entrada de EasyNetwork y, a continuación, haciendo clic en **Aceptar** del menú **Herramientas** . En el cuadro de diálogo Aceptar en la carpeta, acceda a la carpeta en la que quiera guardar los archivos que esté recibiendo, selecciónela y, a continuación, haga clic en **Guardar**.

Recibir una notificación cuando se envíe el archivo

Puede recibir una notificación cuando otro equipo de la red gestionada le envíe un archivo. Si EasyNetwork no está actualmente abierto o no está en primer plano de su escritorio, aparecerá un mensaje de notificación en el área de notificación a la derecha de la barra de tareas de Windows.

Para recibir una notificación cuando se envíe un archivo:

1. En el menú **Opciones** , haga clic en **Configurar**.
2. En el cuadro de diálogo Configurar, marque la casilla de verificación **Notificarme cuando otro equipo me envíe archivos**.
3. Haga clic en **Aceptar**.

CAPÍTULO 31

Compartir impresoras

Después de incorporarse a una red gestionada, EasyNetwork comparte automáticamente cualquier impresora local conectada a su equipo. También detecta impresoras compartidas por otros equipos de la red y le permite configurar y utilizar estas impresoras.

En este capítulo

Trabajar con impresoras compartidas

Después de conectarse a una red gestionada, EasyNetwork comparte automáticamente cualquier impresora local que esté conectada con su equipo, utilizando el nombre actual de la impresora como nombre de impresora compartida. También detecta impresoras compartidas por otros equipos de la red y le permite configurar y utilizar estas impresoras. Si ha configurado un controlador de impresora para imprimir a través de un servidor de impresión en red (por ejemplo, un servidor de impresión USB inalámbrico), EasyNetwork considera que la impresora es una impresora local y la comparte automáticamente en la red. También puede dejar de compartir una impresora en cualquier momento.

EasyNetwork también detecta impresoras compartidas por todos los demás equipos de la red. Si detecta una impresora remota que no esté todavía conectada a su equipo, el vínculo **Impresoras de red disponibles** de la ventana Archivos compartidos aparece al abrir EasyNetwork por primera vez. Esto le permite instalar impresoras disponibles o desinstalar impresoras que ya estén conectadas a su equipo. Asimismo, puede actualizar la lista de impresoras detectadas en la red.

Si aún no se ha incorporado a una red gestionada pero está conectada a ella, puede acceder a las impresoras compartidas desde el panel de control de impresoras estándar de Windows.

Detener el uso compartido de una impresora

Puede dejar de compartir una impresora en cualquier momento. Los miembros que tengan instalada la impresora ya no podrán imprimir en ella.

Para detener el uso compartido de una impresora:

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Gestionar impresoras de red, haga clic en el nombre de la impresora que ya no desea compartir.
3. Haga clic en **No compartir**.

Instalar una impresora de red disponible

Como miembro de una red gestionada, puede acceder a las impresoras que estén compartidas en la red. Para ello, deberá instalar el controlador de la impresora utilizado por dicha impresora. Si el propietario de la impresora detiene el uso compartido después de que usted la haya instalado, ya no podrá utilizar esa impresora.

Para instalar una impresora de red disponible:

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Impresoras de red disponibles, haga clic en un nombre de impresora.
3. Haga clic en **Instalar**.

CAPÍTULO 32

Referencia

El glosario de términos lista y define la terminología de seguridad más comúnmente utilizada en los productos de McAfee.

Acerca de McAfee le proporciona información legal acerca de McAfee Corporation.

Glosario

8

802.11

Conjunto de estándares IEEE para tecnología LAN inalámbrica. 802.11 especifica una interfaz a través de ondas entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos. Las distintas especificaciones de 802.11 incluyen: 802.11a, estándar que admite hasta 54 Mbps en la banda de 5 Ghz; 802.11b, estándar que admite hasta 11 Mbps en la banda de 2,4 Ghz; 802.11g, estándar que admite hasta 54 Mbps en la banda de 2,4 Ghz y 802.11i, un conjunto de estándares de seguridad para todas las redes Ethernet inalámbricas.

802.11a

Extensión de 802.11 que se aplica a redes LAN inalámbricas y envía datos a una velocidad de hasta 54 Mbps en la banda de 5 GHz. Aunque la velocidad de transmisión es mayor que en el caso de 802.11b, la distancia de cobertura es mucho menor.

802.11b

Extensión de 802.11 que se aplica a redes LAN inalámbricas y que proporciona una velocidad de transmisión de 11 Mbps en la banda de 2,4 GHz. 802.11b se considera actualmente el estándar para redes inalámbricas.

802.11g

Extensión de 802.11 que se aplica a redes LAN inalámbricas y que proporciona una velocidad de transmisión de hasta 54 Mbps en la banda de 2,4 GHz.

802.1x

No admitido por Wireless Home Network Security. Estándar IEEE para la autenticación de redes con cable e inalámbricas, aunque se utiliza principalmente con redes inalámbricas 802.11. Este estándar proporciona sólida autenticación mutua entre un cliente y un servidor de autenticación. Además, 802.1x puede proporcionar claves WEP dinámicas por usuario y por sesión, lo que elimina el trabajo de administración y los riesgos de seguridad de las claves WEP estáticas.

A

adaptador inalámbrico

Contiene el sistema de circuitos que permiten a un equipo u otro dispositivo comunicarse con un enrutador inalámbrico (conectado a una red inalámbrica). Los adaptadores inalámbricos pueden venir integrados en el sistema de circuitos principal de un dispositivo de hardware o bien como un complemento independiente que puede insertarse en un dispositivo a través del puerto adecuado.

análisis de imagen

Impide que se muestren imágenes que podrían ser inapropiadas. Las imágenes se bloquean para todos los usuarios excepto para los miembros del grupo de adultos.

análisis en tiempo real

Los archivos se analizan en busca de virus y otras actividades sospechosas cuando el usuario o el equipo accede a ellos.

ancho de banda

Cantidad de datos que pueden transmitirse en un período de tiempo fijo. En el caso de dispositivos digitales, el ancho de banda se expresa normalmente en bits por segundo (bps) o bytes por segundo. En el caso de dispositivos analógicos, se expresa en ciclos por segundo o hercios (Hz).

archivado completo

Archivado de un conjunto de datos completo basado en los tipos y ubicaciones de los ficheros observados que haya configurado.

archivado rápido

Sirve para archivar únicamente aquellos archivos observados que se han modificado desde la última operación de archivado rápido o completo.

archivar

Crear una copia de los archivos observados localmente en un CD, un DVD, una unidad USB, un disco duro externo o una unidad de red.

archivar

Crear una copia de los archivos observados localmente en un CD, un DVD, una unidad USB, un disco duro externo o una unidad de red.

ataque de diccionario

Estos ataques consisten en probar gran cantidad de palabras de una lista para intentar averiguar la contraseña de un usuario. Los agresores no prueban todas las combinaciones de forma manual, sino que disponen de herramientas que intentan identificar automáticamente la contraseña de la víctima.

ataque de fuerza bruta

Se trata de un método de ensayo y eliminación de error utilizado por aplicaciones cuyo objetivo es descodificar datos cifrados, como contraseñas, realizando un esfuerzo contundente (mediante la fuerza bruta) en lugar de emplear estrategias intelectuales. Al igual que un delincuente que intentara abrir una caja fuerte probando con muchas combinaciones posibles, una aplicación de descifrado por fuerza bruta intenta todas las combinaciones posibles de caracteres legales por orden. La fuerza bruta se considera un método infalible, aunque lleva mucho tiempo.

ataque de intermediario

El agresor intercepta mensajes en un intercambio de clave pública y los retransmite, sustituyendo su propia clave pública por la solicitada, de manera que las dos partes originales continúan comunicándose entre sí directamente. El agresor utiliza un programa que simula ser el servidor para el cliente y el cliente para el servidor. El ataque puede utilizarse sencillamente para obtener acceso a los mensajes o para permitir al agresor modificarlos antes de transmitirlos de nuevo. El término en inglés (Man-in-the-Middle Attack) procede de un juego de pelota en el que un número de personas intentan lanzarse la pelota directamente entre ellas mientras que otra persona en el centro intenta interceptarla.

autenticación

Proceso de identificación de un individuo, que habitualmente consiste en un nombre de usuario y una contraseña. La autenticación garantiza que el individuo es quien dice ser, aunque no influye en sus derechos de acceso.

B

biblioteca

Área de almacenamiento en línea para los archivos publicados por los usuarios de Data Backup. La biblioteca es un sitio Web de Internet al que puede acceder cualquier persona con acceso a Internet.

browser

Programa cliente que utiliza el Protocolo de transferencia de hipertexto (HTTP) para enviar solicitudes a servidores Web a través de Internet. Los navegadores Web muestran al usuario los contenidos de forma gráfica.

C

Caja fuerte de contraseñas

Área de almacenamiento segura de las contraseñas personales. Permite almacenar las contraseñas con la seguridad de que ningún otro usuario (ni siquiera un administrador de McAfee o un administrador del sistema) puede acceder a ella.

cifrado

Proceso mediante el que los datos se transforman de texto en código, de forma que la información queda oculta y resulta ilegible para aquellas personas que no saben cómo descifrarla.

clave

Serie de letras y/o números utilizados por dos dispositivos con objeto de autenticar sus comunicaciones. Ambos dispositivos deben disponer de la clave. Véase también WEP, WPA, WPA2, WPA-PSK y WPA2- PSK.

cliente

Aplicación que se ejecuta en un equipo personal o estación de trabajo y que depende de un servidor para realizar algunas operaciones. Por ejemplo, un cliente de correo electrónico es una aplicación que permite enviar y recibir mensajes de correo electrónico.

cliente de correo electrónico

Cuenta de correo electrónico. Por ejemplo, Microsoft Outlook o Eudora.

compartir

Operación que permite a los destinatarios de mensajes de correo electrónico acceder a los archivos copiados seleccionados durante un período de tiempo limitado. Cuando se comparte un archivo, el usuario manda una copia del archivo a los destinatarios de correo electrónico especificados. Los destinatarios reciben un mensaje de correo electrónico procedente de Data Backup en el que se indica que se han compartido archivos con ellos. Este mensaje contiene también un vínculo a los archivos compartidos.

compresión

Proceso mediante el que los datos (archivos) se comprimen en un formato que minimiza el espacio necesario para su almacenamiento y transmisión.

contraseña

Código (por lo general alfanumérico) que se utiliza para acceder a un equipo, a un programa determinado o a un sitio Web.

controles paternos

Parámetros que permiten configurar clasificaciones de contenido con el fin de restringir los sitios Web y el contenido que un usuario puede ver, así como los límites de tiempo en Internet, con lo que se especifica el período y la duración del tiempo que un usuario puede estar en Internet. Los controles paternos también permiten restringir el acceso universal a determinados sitios Web y conceder o bloquear el acceso basándose en grupos de edades y palabras claves asociadas.

cookie

En el entorno de World Wide Web, bloque de datos que un servidor Web almacena en un sistema cliente. Cuando un usuario vuelve a visitar la misma página Web, el navegador envía una copia de la cookie de vuelta al servidor. Las cookies se utilizan para identificar a los usuarios, solicitar al servidor que envíe una versión personalizada de la página Web, enviar información de la cuenta del usuario y otras finalidades administrativas.

Las cookies permiten que el sitio Web recuerde la identidad de los usuarios y haga un seguimiento de las personas que visitan el sitio, cuándo lo hacen y a qué páginas acceden. Las cookies también ayudan a una compañía a personalizar su sitio Web para los usuarios. Muchos sitios Web solicitan un nombre de usuario y una contraseña para acceder a determinadas páginas, y envían una cookie al equipo para que no sea necesario iniciar sesión cada vez que se visita el sitio. Sin embargo, las cookies pueden utilizarse con malas intenciones. Las compañías de publicidad en línea utilizan cookies para determinar qué páginas visita el usuario habitualmente para enviarle anuncios de sus sitios Web favoritos. Antes de permitir cookies de un sitio, asegúrese de que éste es de confianza.

Aunque las cookies son una fuente de información para las compañías que las utilizan de forma legítima, también pueden convertirse en una fuente de datos para los piratas informáticos. Muchos sitios Web con tiendas en línea almacenan la información de las tarjetas de crédito y otros datos personales en cookies para simplificar las compras de los clientes. Lamentablemente, existen bugs de seguridad que permiten a los piratas informáticos acceder a la información de las cookies almacenadas en los equipos de los clientes.

correo electrónico

Mensajes enviados por Internet o dentro de la LAN o WAN de una empresa. Los archivos que se adjuntan en los mensajes de correo electrónico en forma de archivos EXE (ejecutables) o VBS (secuencias de comandos o guiones de Visual Basic) se han convertido en una forma cada vez más habitual de transmitir virus y troyanos.

cortafuegos

Sistema diseñado para impedir el acceso no autorizado de entrada o salida de una red privada. Los cortafuegos pueden estar basados en hardware y en software, o en una combinación de ambos. Se utilizan con frecuencia para impedir que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet y, en particular, a una intranet. Todos los mensajes que entran o salen de la intranet atraviesan el cortafuegos. Éste examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados. Un cortafuegos se considera la primera línea de defensa para la protección de la información confidencial. Para conseguir un mayor nivel de seguridad, los datos pueden cifrarse.

crear copia de seguridad

Crear una copia de los archivos observados en un servidor en línea seguro.

cuarentena

Cuando se detectan archivos sospechosos, se ponen en cuarentena. Posteriormente, podrá efectuarse la operación apropiada.

cuenta de correo electrónico estándar

La mayoría de los usuarios domésticos tienen este tipo de cuenta. Véase también cuenta POP3.

cuenta de MSN

Siglas inglesas de Microsoft Network. Es un servicio en línea y un portal de Internet. Se trata de una cuenta de correo basada en Web

cuenta MAPI

Siglas en inglés de Messaging Application Programming Interface (interfaz de programación de aplicaciones de mensajería). Especificación de la interfaz de Microsoft que permite que diferentes aplicaciones de mensajería y grupos de trabajo (incluido el correo electrónico, el correo de voz y el fax) funcionen a través de un único cliente, como el cliente de Exchange. Por este motivo, MAPI se suele usar en entornos corporativos cuando en la organización se utiliza Microsoft® Exchange Server. Sin embargo, muchas personas utilizan Microsoft Outlook para su correo electrónico personal de Internet.

cuenta POP3

Siglas inglesas de Post Office Protocol 3 (protocolo de oficina postal 3). La mayoría de los usuarios domésticos tienen este tipo de cuenta. Es la versión actual del estándar Post Office Protocol que se utiliza habitualmente en las redes TCP/IP. También se conoce como cuenta de correo electrónico estándar.

D

denegación de servicio

En Internet, un ataque de denegación de servicio (DoS) es un incidente en el que a un usuario u organización se le priva de los servicios de un recurso del que dispondría en condiciones normales. Por lo general, la pérdida de servicio es la imposibilidad de utilizar un servicio de red concreto, como el correo electrónico, o la pérdida temporal de todos los servicios y conectividad de red. Un ejemplo de un caso grave sería el de un sitio Web al que acceden millones de personas y que podría verse forzado a cesar sus operaciones de forma temporal. Un ataque de denegación de servicio también puede destruir programas y archivos en un equipo informático. Aunque habitualmente se trata de ataques intencionados y agresivos, también pueden producirse en ocasiones de manera accidental. Es un tipo de ataque a la protección de un sistema informático que no termina, por lo general, en el robo de información ni conlleva ninguna otra pérdida de seguridad. Sin embargo, estos ataques pueden ocasionar a la persona o a la compañía que los sufren una pérdida importante de tiempo y dinero.

desbordamiento del búfer

Los desbordamientos del búfer pueden tener lugar si un programa o proceso sospechoso intenta guardar datos en el búfer (área de almacenamiento temporal de datos del equipo) por encima del límite, con lo que los datos de los búfers adyacentes se sobrescriben o se dañan.

dirección IP

La dirección del protocolo de Internet o dirección IP es un número único compuesto de cuatro partes separadas por puntos (por ejemplo, 63.227.89.66). Todos los equipos de Internet, desde los grandes servidores hasta los portátiles que se comunican a través de un teléfono móvil, tienen asignado un número IP exclusivo. No todos los equipos cuentan con un nombre de dominio, pero sí con una dirección IP.

A continuación se muestran algunos tipos de direcciones IP poco usuales:

- Direcciones IP que no se pueden enrutar: también se conocen como "Espacio de IP privadas". Son direcciones IP que no se pueden utilizar en Internet. Los bloques de direcciones IP privadas son 10.x.x.x, 172.16.x.x - 172.31.x.x y 192.168.x.x.
- Direcciones IP de bucle de retorno**:** estas direcciones se utilizan para efectuar comprobaciones. El tráfico enviado a este grupo de direcciones IP se devuelve directamente al dispositivo que haya generado el paquete. Nunca abandona el dispositivo y se utiliza principalmente para realizar comprobaciones de hardware y software. El bloque de IP de bucle de invertido es 127.x.x.x.

Direcciones IP nulas: se trata de direcciones IP no válidas. Cuando aparecen, indican que el tráfico presenta una dirección IP vacía. Obviamente, esto no es normal e indica, con frecuencia, que el emisor oculta deliberadamente el origen del tráfico. El emisor no podrá recibir ninguna respuesta de tráfico a no ser que el paquete lo reciba una aplicación que comprenda su contenido, que a su vez incluya instrucciones específicas para dicha aplicación. Las direcciones que empiezan por 0 (0.x.x.x) son direcciones nulas. Por ejemplo, 0.0.0.0 es una dirección IP nula.

dirección MAC (Media Access Control Address)

Una dirección de nivel bajo asignada al dispositivo físico que accede a la red.

disco duro externo

Disco duro que se encuentra fuera de la carcasa del equipo.

DNS

Siglas inglesas de Domain Name System (sistema de nombres de dominio). Sistema jerárquico por el que los hosts de Internet tienen tanto direcciones de nombres de dominio (por ejemplo, bluestem.prairienet.org) como direcciones IP (por ejemplo, 192.17.3.4). Los usuarios utilizan las direcciones de nombres de dominio. Estas direcciones se traducen automáticamente en una dirección IP numérica para que la utilice el software de enrutamiento de paquetes. Los nombres DNS se componen de un dominio de nivel superior (como .com, .org o .net), un dominio de nivel secundario (el nombre del sitio de una empresa, una organización o un individuo) y, muy probablemente, uno o varios subdominios (servidores comprendidos dentro del dominio de nivel secundario). Véase también servidor DNS y dirección IP.

dominio

Dirección de una conexión de red que identifica al propietario de dicha dirección en un formato jerárquico: servidor.organización.tipo. Por ejemplo, www.whitehouse.gov identifica el servidor Web de la Casa Blanca, que forma parte del Gobierno de Estados Unidos.

E

encabezado

Un encabezado es información que se agrega al mensaje durante su ciclo de vida. El encabezado indica al software de Internet cómo debe entregar el mensaje, dónde se deben enviar las respuestas, un identificador único de ese correo electrónico en cuestión y otra información administrativa. Algunos ejemplos de los campos del encabezado son: Para, De, CC, Fecha, Asunto, Id de mensaje y Recibido.

enrutador o router

Dispositivo de red que reenvía paquetes de una red a otra. Los enrutadores están basados en las tablas de enrutamiento internas, leen todos los paquetes entrantes y deciden cómo reenviarlos. La interfaz del enrutador a la que se envían los paquetes salientes viene determinada por cualquier combinación de direcciones de origen y destino, así como por las condiciones del tráfico actual, como la carga, los costes de la línea y las líneas defectuosas. También se le conoce como punto de acceso.

ESS (Extended Service Set)

Conjunto de servicios ampliados. Grupo de dos o más redes que forman una subred única.

evento

Eventos de 0.0.0.0

Si visualiza eventos procedentes de una IP con la dirección 0.0.0.0, hay dos causas probables. La primera y más común suele ser que, por alguna razón, el equipo haya recibido un paquete que contiene errores. Internet no es fiable al 100% y, en ocasiones, se producen este tipo de paquetes. Dado que el cortafuegos ve los paquetes antes de que se validen mediante TCP/IP, es posible que informe acerca de estos paquetes como un evento.

La otra situación se produce cuando la IP de origen se simula o se truca. Este tipo de paquetes pueden indicar que alguien está realizando una exploración en busca de troyanos y, por casualidad, pone a prueba su equipo. Es importante recordar que el cortafuegos bloquea estos intentos.

Eventos de 127.0.0.1

En ocasiones, los eventos mostrarán 127.0.0.1 como IP de origen. Es importante recordar que esta IP es especial y suele llamarse IP de bucle invertido.

No importa el equipo que se esté utilizando, 127.0.0.1 siempre hace referencia al equipo local. Esta dirección también suele llamarse "localhost" (servidor local), pues el nombre de equipo "localhost" siempre se resuelve con la dirección IP 127.0.0.1. ¿Significa eso que el equipo intenta atacarse a sí mismo? ¿Hay algún troyano o software espía intentando manipular el equipo? No es probable. Muchos programas legítimos utilizan la dirección de bucle invertido para establecer la comunicación entre sus componentes. Por ejemplo, muchos servidores Web o servidores personales de correo permiten su configuración a través de una interfaz de Web a la que se accede normalmente mediante una dirección similar a http://localhost/.

Sin embargo, el cortafuegos permite el tráfico procedente de esos programas, de modo que cuando vea eventos procedentes de 127.0.0.1, lo más probable es que la dirección IP de origen sea simulada o trucada. Los paquetes trucados suelen indicar normalmente que alguien está buscando troyanos. Es importante recordar que el cortafuegos bloquea estos intentos. Obviamente, presentar un informe sobre los eventos de 127.0.0.1 no resulta muy útil, así que no es necesario hacerlo.

Dicho esto, algunos programas, el más destacado de los cuales es Netscape 6.2 y versiones posteriores, requieren que se agregue 127.0.0.1 a la lista de **direcciones IP fiables**. Los componentes de estos programas se comunican entre sí de tal forma que el cortafuegos no puede determinar si el tráfico es local o no.

En el ejemplo de Netscape 6.2, si no define la dirección 127.0.0.1 como fiable, no podrá utilizar la lista de contactos. Por lo tanto, si detecta tráfico procedente de 127.0.0.1 y todos los programas instalados en su equipo funcionan con normalidad, resulta seguro bloquear este tráfico. No obstante, si algún programa (como Netscape) experimenta problemas, agregue la dirección 127.0.0.1 a la lista de **direcciones IP fiables** del cortafuegos y compruebe si se soluciona el problema.

Si agregando la dirección 127.0.0.1 a la lista de **direcciones IP fiables** se soluciona el problema, debe sopesar las opciones siguientes: si confía en la dirección 127.0.0.1, el programa funcionará, pero estará más expuesto a sufrir ataques desde IP falsificadas. Si no confía en esta dirección, el programa no funcionará, pero permanecerá protegido frente al tráfico malintencionado.

Eventos procedentes de equipos de la LAN

En la mayor parte de las configuraciones de las LAN corporativas, es necesario confiar en todos los equipos de la LAN.

Eventos procedentes de direcciones IP privadas

Las direcciones IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx y 172.16.0.0 - 172.31.255.255 suelen denominarse direcciones IP privadas o que no se pueden enrutar. Estas direcciones IP nunca deben abandonar la red, por lo que casi siempre resultan fiables.

El bloque 192.168 se utiliza con Microsoft Internet Connection Sharing (ICS). Si utiliza ICS y ve eventos que proceden de este bloque, es posible que le convenga agregar la dirección IP 192.168.255.255 a la lista de **direcciones IP fiables**. De esta forma, se definirá como fiable todo el bloque 192.168.xxx.xxx.

Si no se encuentra en una red privada y ve eventos con direcciones similares, es posible que la dirección IP de origen haya sido falsificada o simulada. Los paquetes falsificados normalmente indican que alguien realiza una exploración en busca de troyanos. Es importante recordar que el cortafuegos bloquea estos intentos.

Dado que las direcciones IP privadas son independientes de las direcciones IP de Internet, no sirve de nada informar de este tipo de eventos.

falsificación de IP

Como su propio nombre indica, se trata de la falsificación de la dirección IP de un paquete IP. Se utiliza en muchos tipos de ataques, incluidos los secuestros de sesiones. También se utiliza con frecuencia en la falsificación de encabezados de mensajes SPAM, para complicar su seguimiento.

grupos de clasificación de contenido

Grupos de edad a los que pertenecen los usuarios. El contenido se clasifica (es decir, está disponible o bloqueado) en función del grupo de clasificación de contenido al que pertenece el usuario. Los grupos de clasificación de contenido incluyen: niños de corta edad, niños, adolescentes, jóvenes y adultos.

guardián del sistema

Los guardianes del sistema detectan cambios no autorizados en el equipo y le alertarán cuando tengan lugar.

gusano

Un gusano es un virus capaz de replicarse que reside en la memoria activa y puede enviar copias de sí mismo a través de mensajes de correo electrónico. Los gusanos replican y consumen los recursos del sistema, reduciendo su rendimiento o interrumpiendo tareas.

hotspot o zona de cobertura inalámbrica

Ubicación geográfica específica en la que un punto de acceso proporciona servicios públicos de red inalámbrica de banda ancha a visitantes móviles a través de una red inalámbrica. Los hotspots o zonas de cobertura inalámbrica se encuentran con frecuencia en lugares con gran afluencia de público, como aeropuertos, estaciones de tren, bibliotecas, puertos deportivos, palacios de congresos y hoteles. Generalmente, su alcance de acceso es corto.

Internet

Internet se compone de un número ingente de redes interconectadas que utilizan los protocolos TCP/IP para localizar y transferir datos. Internet evolucionó a partir de un proyecto de conexión de equipos de universidades y facultades (a finales de los años 60 y principios de los 70) financiado por el Departamento de Defensa de EE.UU., que se denominó ARPANET. Hoy en día Internet es una red mundial integrada por unas 100.000 redes independientes.

intranet

Red privada, perteneciente normalmente a una organización, que funciona de forma similar a Internet. Se ha convertido en una práctica habitual permitir el acceso a las intranets desde equipos individuales que utilizan estudiantes que no se encuentran en la universidad o trabajadores desplazados de su centro de trabajo. Los cortafuegos, los procedimientos de inicio de sesión y las contraseñas están diseñados para proporcionar seguridad.

itinerancia

También conocido como roaming, es la capacidad para moverse de una zona de cobertura de un punto de acceso a otra sin que se produzca una interrupción del servicio ni una pérdida de conectividad.

lista blanca

Lista de sitios Web a los que se permite el acceso dado que no se consideran fraudulentos.

lista negra

Una lista de sitios Web que se consideran malintencionados. Un sitio Web puede incluirse en una lista negra por una operación fraudulenta o por aprovechar la vulnerabilidad del navegador para enviar programas no deseados al usuario.

MAC (Media Access Control o Message Authenticator Code)

Para la primera acepción, véase dirección MAC. La segunda se refiere a un código que se utiliza para identificar un mensaje determinado (p.ej., un mensaje RADIUS). Se emplea un código hash criptográficamente fuerte del contenido del mensaje que incluye un valor exclusivo para protegerse contra transmisiones.

mapa de la red

En Network Manager, una representación gráfica de los equipos y componentes que forman una red doméstica.

nodo

Un solo equipo conectado a una red.

palabra clave

Palabra que se puede asignar a un archivo de copia de seguridad para establecer una relación o conexión entre este archivo y otros archivos que tengan las misma palabra clave asignada. Al asignar palabras clave, resulta más fácil buscar los archivos que están publicados en Internet.

phishing

Se pronuncia "fishing" y es un fraude electrónico para robar información valiosa, como los números de la tarjeta de crédito y de la Seguridad Social, los identificadores de usuario y las contraseñas. Las víctimas potenciales reciben un mensaje de correo electrónico con aspecto "oficial" que se supone procede de su proveedor de servicios de Internet, su banco o un comercio. Los mensajes de correo se pueden enviar a personas de listas seleccionadas o de cualquier lista, ya que se prevé que un determinado porcentaje de destinatarios tiene una cuenta con la organización real.

PPPoE

Acrónimo del inglés Point-to-Point Protocol Over Ethernet, Protocolo punto a punto en Ethernet. Utilizado por muchos proveedores de DSL, PPPoE admite las capas de protocolos y la autenticación que más se utilizan en PPP y permite que se establezca una conexión punto a punto en la arquitectura multipunto de Ethernet.

programa potencialmente no deseado

Los programas potencialmente no deseados incluyen el software espía, el software publicitario y otros programas que reúnen y transmiten los datos del usuario sin su permiso.

protocolo

Formato acordado para la transmisión de datos entre dos dispositivos. Desde la perspectiva de un usuario, el único aspecto interesante sobre los protocolos está en el hecho de que su equipo o dispositivo debe admitir los protocolos adecuados si quiere comunicarse con otros equipos. El protocolo se puede basar en hardware o en software.

proxy

Un equipo (o el software que lo ejecuta) que actúa como barrera entre una red e Internet presentando únicamente una sola dirección de red a los sitios externos. Al actuar como intermediario en representación de todos los equipos internos, el proxy protege las identidades de la red a la vez que proporciona acceso a Internet. Véase también servidor proxy.

publicar

Hacer pública la copia de seguridad de un archivo en Internet.

puerta de enlace integrada

Dispositivo que combina las funciones de un punto de acceso, un enrutador y un cortafuegos. Algunos dispositivos también pueden incluir funciones de mejora de la seguridad y enlace inalámbrico.

puerto

Lugar por el que entra y sale la información de un equipo. Un módem analógico convencional, por ejemplo, se conecta a un puerto serie. Los números de puerto de las comunicaciones TCP/IP son valores virtuales que se utilizan para dividir el tráfico en secuencias específicas de cada aplicación. Los puertos se asignan a protocolos estándar como SMTP o HTTP para que los programas sepan a qué puerto deben intentar conectarse. El puerto de destino de los paquetes TCP indica la aplicación o el servidor que se está buscando.

Punto de acceso (PA)

Dispositivo de red que permite a clientes 802.11 conectarse a una red de área local (LAN). Los puntos de acceso amplían el alcance de servicio físico de un usuario inalámbrico. También se conoce como enrutador inalámbrico.

puntos de acceso no autorizados

Punto de acceso para el que una empresa no ha concedido autorización. El problema radica en que un punto de acceso no autorizado no cumple las directivas de seguridad de redes LAN (WLAN) inalámbricas. Un punto de acceso no autorizado permite la conexión abierta e insegura a una red corporativa desde el exterior del centro físico controlado.

En una red WLAN convenientemente protegida, los puntos de acceso no autorizados son más dañinos que los usuarios malintencionados. Los usuarios no autorizados que intentan acceder a una red WLAN tienen pocas posibilidades de llegar a recursos valiosos de la empresa si hay implantados mecanismos de autenticación eficaces. Sin embargo, los principales problemas aparecen cuando un empleado o pirata informático conecta un punto de acceso no autorizado. Estos puntos permiten el acceso a la red corporativa a cualquiera que disponga de un dispositivo equipado con 802.11. Esto les sitúa muy cerca de los recursos de vital importancia.

RADIUS (Remote Access Dial-In User Service)

Protocolo que proporciona autenticación para usuarios, normalmente en el contexto del acceso remoto. Originalmente definido para el uso con servidores de acceso telefónico remoto, este protocolo se utiliza en la actualidad en varios entornos de autenticación, entre ellos, en la autenticación 802.1x de un secreto compartido de usuario WLAN.

red

Cuando se establece una conexión entre dos o más equipos, se crea una red.

red de área local (LAN)

Red de equipos informáticos que cubre un área relativamente pequeña. La mayoría de las redes LAN están limitadas a un edificio o un grupo de edificios. Sin embargo, una red LAN puede estar conectada a otras redes LAN sin límite de distancia a través del teléfono u ondas de radio. A los sistemas de redes LAN conectadas de esta forma se les llama redes de área extensa (WAN). La mayoría de las redes LAN conectan estaciones de trabajo y equipos personales, habitualmente a través de concentradores o conmutadores sencillos. Cada nodo (equipo individual) de una red LAN dispone de su propia CPU con la que ejecuta los programas, pero también puede acceder a los datos y dispositivos (p. ej., impresoras) de cualquier parte de la red. Esto significa que muchos usuarios pueden compartir dispositivos costosos, como impresoras láser, además de datos. Los usuarios también pueden utilizar la red LAN para comunicarse entre sí; por ejemplo, a través del correo electrónico o mediante sesiones de chat.

red de área local inalámbrica (WLAN)

Véase también LAN. Red de área local que utiliza un medio inalámbrico para la conexión. Una WLAN utiliza ondas de radio de alta frecuencia en lugar de cables para la comunicación entre nodos.

red gestionada

Una red doméstica con dos tipos de miembros: miembros gestionados y miembros no gestionados. Los miembros gestionados permiten que otros equipos de la red supervisen su estado de protección de McAfee; los miembros no gestionados no lo permiten.

red privada virtual (VPN)

Red que se configura utilizando una red pública para unir nodos. Por ejemplo, hay sistemas que permiten crear redes utilizando Internet como medio de transporte de datos. Estos sistemas utilizan el cifrado y otros mecanismos de seguridad para garantizar que sólo los usuarios autorizados puedan acceder a la red y para impedir que se intercepten los datos.

repositorio de la copia de seguridad en línea

Ubicación del servidor en línea en que se almacenan los archivos observados después de hacer la copia de seguridad.

restaurar

Recuperar una copia de un fichero desde un repositorio de copias de seguridad en línea o un archivo.

secreto compartido

Véase también RADIUS. Protege partes importantes de los mensajes RADIUS. Este secreto compartido es una contraseña que se comparte entre el autenticador y el servidor de autenticación de manera segura.

secuencia de comandos

Las secuencias de comandos pueden crear, copiar o eliminar archivos. También pueden abrir el registro de Windows.

servidor

Equipo o software que proporciona servicios específicos para el software que se ejecuta en otros equipos. El servidor de correo del ISP es un programa de software que gestiona todo el correo de entrada y salida de todos los usuarios. Un servidor de una LAN es hardware que constituye el nodo principal de la red. También puede incluir software que proporcione servicios específicos, datos y otras funciones a todos los equipos cliente que se conecten a él.

servidor DNS

Abreviatura de servidor de Domain Name System (sistema de nombres de dominio). Un equipo puede responder a las consultas de Domain Name System (DNS). El servidor DNS alberga una base de datos de los equipos del host y sus correspondientes direcciones IP. Por ejemplo, si introdujéramos el nombre apex.com, el servidor DNS podría devolvernos la dirección IP de la compañía ficticia Apex. También se denomina: servidor de nombres. Véase también DNS y dirección IP.

servidor proxy

Cortafuegos que gestiona el tráfico de Internet de entrada y salida de una red de área local (LAN). Un servidor proxy puede mejorar el rendimiento suministrando datos que se solicitan con frecuencia, como una página Web muy visitada, y puede filtrar y desechar solicitudes que el titular no considere convenientes, como el acceso no autorizado a archivos de propiedad.

servidor SMTP

Siglas en inglés de Simple Mail Transfer Protocol (protocolo simple de transferencia de correo). Protocolo TCP/IP para el envío de mensajes de un equipo a otro en una red. Este protocolo se utiliza en Internet para enrutar los correos electrónicos.

sincronizar

Resolver inconsistencias entre los acrhivos copiados y los archivos almacenados en el equipo local. Los archivos se sincronizan cuando la versión del archivo que se encuentra en el repositorio de la copia de seguridad en línea es más reciente que la versión de otros equipos. Al sincronizar, se actualiza la copia del archivo que está en los equipos con la versión del repositorio de la copia de seguridad en línea.

SSID (Service Set Identifier)

Nombre de red de los dispositivos de un subsistema LAN inalámbrico. Se trata de una cadena de 32 caracteres de texto sin formato que se añade al encabezado de todos los paquetes WLAN. Los SSID diferencian una WLAN de otra, de manera que todos los usuarios de una red deben facilitar el mismo SSID para acceder a un determinado punto de acceso. Un SSID impide el acceso a cualquier dispositivo cliente que no disponga del SSID. Sin embargo, de manera predeterminada, un punto de acceso difunde su SSID en su señal. Incluso si se desactiva la difusión del SSID, un pirata informático puede detectarlo a través de interceptación (sniffing).

SSL (Secure Sockets Layer)

Protocolo desarrollado por Netscape para transmitir documentos privados a través de Internet. SSL utiliza una clave pública para cifrar datos que se transfieren a través de la conexión SSL. Tanto Netscape Navigator como Internet Explorer utilizan y admiten SSL; asimismo, muchos sitios Web utilizan este protocolo para obtener información confidencial del usuario, como números de tarjetas de crédito. Como norma general, las direcciones URL que requieren una conexión SSL empiezan por https: en lugar de por http:

tarjeta adaptadora inalámbrica PCI

Conecta un equipo de sobremesa con una red. La tarjeta se inserta en una ranura de expansión PCI dentro del equipo.

tarjeta adaptadora inalámbrica USB

Proporciona una interfaz serie Plug and Play ampliable. Esta interfaz proporciona una conexión inalámbrica estándar de bajo coste para dispositivos periféricos como teclados, ratones, joysticks, impresoras, escáneres, dispositivos de almacenamiento y cámaras de videoconferencia.

tarjeta de interfaz de red (NIC)

Acrónimo del inglés Network Interface Card. Tarjeta que se inserta en un portátil u otro dispositivo y que conecta el dispositivo a la red LAN.

texto cifrado

Datos que se han cifrado. El texto cifrado es ilegible hasta que se convierte en texto normal (se descifra) mediante una clave.

texto normal

Cualquier mensaje que no esté cifrado.

tipos de archivos observados

Tipos de archivos (por ejemplo, .doc, .xls, etc.) que Data Backup copia o archiva en las ubicaciones de observación.

TKIP (Temporal Key Integrity Protocol)

Método rápido de superar el punto débil inherente a la seguridad WEP, en concreto la reutilización de claves de cifrado. TKIP cambia las claves temporales cada 10.000 paquetes, proporcionando un método de distribución dinámico que mejora de manera significativa la seguridad en la red. El proceso de seguridad TKIP comienza con una clave temporal de 128 bits compartida entre clientes y puntos de acceso. TKIP combina la clave temporal con la dirección MAC (del equipo cliente) y agrega entonces un vector de inicialización de 16 octetos relativamente grande para generar la clave que cifra los datos. Este procedimiento garantiza que cada estación utilice secuencias de claves distintas para cifrar los datos. TKIP utiliza RC4 para realizar el cifrado. WEP también utiliza RC4.

Troyano

Los troyanos son programas que parecen aplicaciones inofensivas. Los troyanos no son virus porque no se replican, pero pueden ser igual de destructivos.

ubicación de observación en profundidad

Carpeta del equipo, así como todas sus subcarpetas, en la que se supervisan los cambios que se realizan mediante Data Backup. Si se establece una ubicación de observación en profundidad, Data Back crea una copia de los tipos de archivos observados en dicha carpeta y sus subcarpetas.

ubicaciones de observación

Carpetas del equipo supervisadas por Data Backup.

ubicaciones de observación superficial

Carpeta del equipo en la que se supervisan los cambios que se realizan mediante Data Backup. Si establece una ubicación de observación superficial, Data Backup hace una copia de los tipos de archivos observados en dicha carpeta, pero no incluye sus subcarpetas.

unidad de red

Disco o unidad magnética que se conecta a un servidor de una red que comparten varios usuarios. Las unidades de red se denominan a veces unidades remotas.

URL

Siglas en inglés de Uniform Resource Locator (localizador universal de recursos). Es el formato estándar de las direcciones de Internet.

ventanas emergentes

Pequeñas ventanas que aparecen en la parte superior de otras ventanas en la pantalla del equipo. Las ventanas emergentes se utilizan con frecuencia en los navegadores Web para mostrar anuncios. McAfee bloquea las ventanas emergentes que se abren automáticamente cuando se carga una página Web en el navegador. McAfee no bloquea las ventanas emergentes que se cargan al hacer clic en un vínculo.

wardriver

Intrusos armados con equipos portátiles, software especial y hardware improvisado, que deambulan por ciudades, barrios periféricos y parques empresariales con el objetivo de interceptar tráfico de redes LAN inalámbricas.

Web bugs

Pequeños archivos de gráficos que pueden incorporarse a las páginas HTML y permitir que un origen no autorizado introduzca cookies en el equipo. Estas cookies pueden después enviar información al origen no autorizado. Los Web bugs también se denominan microespías, señales o balizas Web, pixel tags o GIF invisibles.

WEP (Wired Equivalent Privacy)

Protocolo de cifrado y autenticación definido como parte del estándar 802.11. Las versiones iniciales se basan en algoritmos de cifrado RC4 y presentan fallos importantes. WEP tiene como objetivo proporcionar seguridad mediante el cifrado de los datos a través de ondas de radio para protegerlos cuando se transmiten de un punto a otro. Sin embargo, se ha demostrado que el protocolo WEP no es tan seguro como se pensaba al principio.

Wi-Fi (Wireless Fidelity)

Utilizado genéricamente para referirse a cualquier tipo de red 802.11, ya sea 802.11b, 802.11a, banda dual, etc. Es el término utilizado por la Wi-Fi Alliance.

Wi-Fi Alliance

Organización formada por los principales proveedores de software y equipos inalámbricos con objeto de (1) certificar la interoperabilidad de todos los productos basados en 802.11 y (2) promocionar el término Wi-Fi como marca global entre mercados para todos los productos LAN inalámbricos basados en 802.11. La organización actúa como consorcio, laboratorio de pruebas y centro de intercambio de información para proveedores que desean promocionar la interoperabilidad y el crecimiento de la industria.

Mientras que todos los productos 802.11a/b/g se conocen como Wi-Fi, sólo los productos que superan las pruebas de la Wi-Fi Alliance pueden denominarse Wi-Fi Certified (marca registrada). Los productos que superan dichas pruebas deben identificarse mediante un sello en el paquete con la leyenda Wi-Fi Certified y la banda de frecuencia de radio que utilizan. El grupo se denominaba anteriormente Wireless Ethernet Compatibility Alliance (WECA), pero cambió de nombre en octubre de 2002 para reflejar de una forma más precisa la marca Wi-Fi que desea crear.

Wi-Fi Certified

Cualquier producto probado y aprobado como Wi-Fi Certified (marca registrada) por la Wi-Fi Alliance tiene el certificado de interoperabilidad con otro producto, incluso si pertenecen a fabricantes distintos. Un usuario que disponga de un producto Wi-Fi Certified puede utilizar cualquier marca de punto de acceso con otra marca de hardware cliente que también esté certificada. No obstante, cualquier producto Wi-Fi que utilice la misma frecuencia de radio (por ejemplo, 2,4 GHz para 802.11b o 11g, 5 GHz para 802.11a) funciona, en general, con cualquier otro, aunque no sea Wi-Fi Certified.

WPA (Wi-Fi Protected Access)

Especificación estándar que aumenta de manera significativa el nivel de protección de los datos y el control de acceso de los sistemas LAN inalámbricos actuales y futuros. Diseñada para ejecutarse en hardware existente como ampliación de software, WPA procede del estándar IEEE 802.11i y es compatible con él. Cuando se instala adecuadamente, ofrece a los usuarios de una LAN inalámbrica amplias garantías de que sus datos permanecen protegidos y de que sólo los usuarios autorizados pueden acceder a la red.

WPA-PSK

Modo WPA especial para usuarios domésticos que no necesitan seguridad de tipo empresarial y que no tienen acceso a servidores de autenticación. En este modo, el usuario introduce la contraseña inicial para activar el modo Wi-Fi Protected Access con clave precompartida y debe cambiar regularmente la contraseña larga en cada equipo inalámbrico y punto de acceso. Véase también WPA2-PSK y TKIP.

WPA2

Véase también WPA. WPA2 es una actualización del estándar de seguridad WPA y se basa en el estándar IEEE 802.11i.

WPA2-PSK

Véase también WPA-PSK y WPA2. WPA2-PSK es similar a WPA-PSK y se basa en el estándar WPA2. Una característica común de WPA2-PSK es que los dispositivos normalmente admiten varios modos de cifrado (p. ej. AES, TKIP) simultáneamente, mientras que otros dispositivos sólo admiten por lo general un único modo de cifrado a la vez (p. ej., todos los clientes tendrían que utilizar el mismo modo de cifrado).

Acerca de McAfee

McAfee, Inc., con sede central en Santa Clara, California, y líder mundial en prevención de intrusiones y gestión de riesgos de seguridad, proporciona servicios y soluciones proactivas y probadas que protegen sistemas y redes en todo el mundo. Su experiencia y su compromiso inigualable con la innovación permiten a McAfee dotar a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de bloquear ataques, evitar problemas y controlar y mejorar de manera continua su seguridad.

Copyright

Índice

C

D

E

F

G

H

I

L

M

S

T

U

V

W