



Firewall

Manual del usuario

CENTRO DE SEGURIDAD VERSIÓN 1.0



COPYRIGHT

© 2003 Networks Associates Technology, Inc. Reservados todos los derechos. Queda prohibida la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a ningún idioma de este documento o parte de él en ningún formato o por ningún medio sin el consentimiento previo por escrito de Networks Associates Technology, Inc., sus proveedores o empresas filiales. Para obtener este permiso, escriba a la atención del departamento jurídico de Network Associates a la dirección: Network Associates International BV, PO Box 58326, 1040 HH Amsterdam, Países Bajos.

ATRIBUCIONES DE MARCAS COMERCIALES

Active Firewall, Active Security, Active Security (en Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware y diseño, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert y diseño, Covert, Design (N estilizada), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (en Katakana), Dr Solomon's, la etiqueta de Dr Solomon's, Enterprise SecureCast, Enterprise SecureCast (en Katakana), Event Orchestrator (en Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (en Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (en Katakana), M y diseño, Magic Solutions, Magic Solutions (en Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (en Katakana), McAfee y diseño, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (en Katakana), NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, Recoverkey, Recoverkey - International, Registry Wizard, Remote Desktop, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (en Hangul), Stalker, SupportMagic, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (en Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (en Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Los productos de la marca Sniffer[®] están realizados exclusivamente por Network Associates, Inc. Todas las demás marcas, registradas y sin registrar, mencionadas en este documento son propiedad exclusiva de sus respectivos titulares.

Este producto incluye, o podría incluir, software desarrollado por OpenSSL Project para su utilización en OpenSSL Toolkit (<http://www.openssl.org/>).

Este producto incluye, o podría incluir, software criptográfico elaborado por Eric Young (ey@cryptsoft.com).

Este producto incluye, o podría incluir, algunos programas de software que se conceden bajo licencia (o sublicencia) al usuario mediante una licencia pública general GNU (GPL) u otras licencias similares de software gratuito que, entre otros derechos, permiten al usuario copiar, modificar y redistribuir ciertos programas, o determinadas partes de ellos, así como acceder al código fuente. Esta licencia pública general requiere que cualquier software proporcionado con este tipo de licencia se distribuya en formato binario ejecutable y que el código fuente se ponga a disposición de estos usuarios. El código fuente del software con licencia pública general se incluye también en el CD. Si cualquier licencia de software gratuito requiere que Network Associates proporcione derechos de utilización, copia o modificación de un programa de software que sean más amplios que los aquí expuestos, tales derechos prevalecerán sobre los derechos y restricciones aquí expresados.

ACUERDO DE LICENCIA

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL ACUERDO LEGAL APROPIADO CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTABLECE LOS TÉRMINOS Y CONDICIONES GENERALES DE USO DEL SOFTWARE PARA EL QUE SE CONCEDE LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA U OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDE, PODRÁ DEVOLVER EL PRODUCTO A NETWORK ASSOCIATES O AL ESTABLECIMIENTO EN QUE LO HAYA ADQUIRIDO PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.



contenido

1	Introducción	5
	Funciones nuevas	5
	Documentación	7
	Requisitos del sistema	7
	Desinstalación de otros cortafuegos	7
	Instalación de McAfee® Personal Firewall Plus™	8
	Comprobación de McAfee® Personal Firewall Plus™	12
	Utilización de McAfee® SecurityCenter™	13
2	Uso de McAfee® Personal Firewall Plus™	15
	Información acerca del Resumen	15
	Información acerca de aplicaciones de Internet	20
	Cambio de permisos	21
	Cambio de aplicaciones	21
	Información acerca de los eventos entrantes	22
	Explicación del concepto de evento	23
	Información acerca de las direcciones IP	23
	Eventos desde 0.0.0.0	23
	Eventos de 127.0.0.1	24
	Eventos procedentes de equipos de la LAN	25
	Eventos procedentes de direcciones IP privadas	25
	Visualización de eventos en el registro de eventos entrantes	26
	Visualización de los eventos del día en curso	26
	Mostrar eventos de la semana en curso	26
	Visualización del registro completo de eventos entrantes	26



Visualización sólo de los eventos de un día concreto	27
Visualización sólo de los eventos de una dirección de Internet concreta	27
Visualización sólo de eventos con la misma información de eventos	27
Respuesta a eventos entrantes	28
Rastreo del evento seleccionado	28
Obtención de consejos de HackerWatch.org	28
Informes sobre un evento	28
Registro en HackerWatch.org	29
Confianza en una dirección	29
Prohibición de una dirección	30
Gestión del registro de eventos entrantes	30
Compresión del registro de eventos entrantes	30
Visualización del registro de eventos entrantes comprimido	31
Borrado del registro de eventos entrantes	31
Exportación de eventos mostrados	32
Copiado de un evento en el portapapeles	32
Eliminación del evento seleccionado	32
Información acerca de las alertas	33
Alertas rojas	33
Alertas verdes	33
Alertas azules	34
Intento de conexión bloqueado	34
Aplicación de Internet bloqueada	35
La aplicación desea tener acceso a Internet	36
Se ha modificado la aplicación	37
La aplicación desea tener acceso al servidor	38
El programa tiene permitido el acceso a Internet	39
Índice alfabético	41

Bienvenido a McAfee Personal Firewall Plus

El software McAfee Personal Firewall Plus ofrece protección avanzada para su ordenador y sus datos personales. Personal Firewall Plus establece una barrera entre su equipo e Internet y controla en segundo plano si se realizan operaciones de tráfico de Internet que son sospechosas.

Gracias a este cortafuegos, obtendrá las siguientes funciones:

- Protección contra ataques e intentos de ataque de los piratas informáticos.
- Complemento de defensas antivirus.
- Vigilancia de la actividad de Internet y de la red.
- Alerta contra eventos potencialmente hostiles.
- Información detallada sobre tráfico de Internet sospechoso.
- Integración con la funcionalidad Hackerwatch.org, que incluye la elaboración de informes de eventos, herramientas de autocomprobación y la posibilidad de enviar a las autoridades en línea los informes recibidos.
- Proporciona funciones de rastreo y búsqueda de eventos.

Funciones nuevas

Integración mejorada con HackerWatch.org

Resulta más fácil que nunca informar acerca de potenciales piratas informáticos. McAfee Personal Firewall Plus mejora la funcionalidad de HackerWatch.org, que incluye el envío de eventos potencialmente malintencionados a la base de datos.

Mejoras en la gestión inteligente de las aplicaciones

Cuando una aplicación pretende acceder a Internet, Personal Firewall Plus comprueba en primer lugar si la reconoce como fiable o malintencionada. Si Personal Firewall Plus reconoce la aplicación como fiable, permitirá automáticamente su acceso a Internet sin necesidad de la intervención del usuario. Esta base de datos ha sido mejorada para proporcionar a los usuarios más detalles sobre las aplicaciones y su conexión a Internet.

- **Detección avanzada de troyanos**

McAfee Personal Firewall Plus combina la administración de la conexión entre las aplicaciones con una base de datos mejorada para detectar y bloquear el acceso a Internet y la posible transmisión de sus datos personales a las aplicaciones potencialmente más peligrosas, como los troyanos.

- **Mejoras en el rastreo visual**

McAfee Personal Firewall Plus incluye una herramienta actualizada para rastrear intrusiones conocida como Visual Trace. Visual Trace incluye mapas gráficos muy fáciles de leer que muestran la fuente que origina los ataques hostiles y el tráfico mundial, además de información detallada sobre contactos y titulares de las direcciones IP de origen y de todos los pasos subsiguientes hasta llegar a su equipo. McAfee Personal Firewall Plus ha añadido información geográfica a la función de Visual Trace, con lo que mejora los detalles sobre la ubicación de los intrusos y permite una localización señalizada más visual de dichos intrusos. Visual Trace permite a los usuarios rastrear visualmente la ubicación en que se originan las intrusiones; con esta información los usuarios pueden ver una mejor representación gráfica de sus búsquedas.

- **Mayor facilidad de uso**

McAfee Personal Firewall Plus incluye un Asistente para la configuración y un tutorial para guiar a los usuarios durante la configuración y utilización del cortafuegos. A pesar de que el producto se ha diseñado para funcionar sin intervención alguna del usuario, McAfee proporciona a los usuarios una gran variedad de recursos para que puedan entender y apreciar la gran utilidad del cortafuegos.

- **Mejoras en la prevención de intrusiones**

McAfee Personal Firewall Plus protege su privacidad más que nunca al proporcionar la prevención de intrusiones procedentes de posibles amenazas de Internet. Gracias a una funcionalidad heurística, McAfee ofrece protección de tercer nivel mediante el bloqueo de los elementos que presenten síntomas de ataques o características de los intentos de ataques de piratas informáticos.

- **Mejoras en el análisis del tráfico**

McAfee Personal Firewall Plus permite que los usuarios vean tanto los datos que entran como los que salen de su equipo, y, además, muestra las conexiones de las aplicaciones, incluidas las que están "a la escucha" de conexiones abiertas. Esto permite a los usuarios vigilar y actuar con las aplicaciones que pueden estar expuestas a la intrusión.

Documentación



La documentación de Personal Firewall Plus comprende el presente manual del usuario y el archivo de ayuda en línea. Este manual es un subconjunto de la ayuda en línea. Para obtener una información e instrucciones más completas acerca de la utilización de Personal Firewall Plus, consulte la ayuda en línea. Una vez que haya instalado Personal Firewall Plus, podrá acceder a la ayuda en línea tras ejecutar el programa y hacer clic en el icono **Ayuda** ubicado en el panel superior, o bien hacer clic en el botón **Ayuda** que aparece en algunos cuadros de diálogo.

Requisitos del sistema

- Microsoft® Windows 98, ME, 2000 o XP
- PC con procesador a 133 MHz o superior (se recomienda Pentium)
- 16 MB de RAM como mínimo; se recomiendan 32 MB
- 8 MB de espacio libre en el disco duro (para la instalación)
- Microsoft® Internet Explorer 5.5 o posterior

NOTA

Para obtener la última versión de Internet Explorer, visite el sitio Web de Microsoft en la dirección <http://www.microsoft.com/worldwide/>.

Desinstalación de otros cortafuegos

Antes de instalar McAfee Personal Firewall Plus, es necesario desinstalar cualquier otro programa *firewall* cortafuegos que se encuentre instalado en el equipo. Para ello, siga las instrucciones de desinstalación del programa *firewall* cortafuegos que tenga instalado.

NOTA

Si utiliza Windows XP, no es necesario que desactive la función de cortafuegos incorporada antes de instalar el software McAfee Personal Firewall Plus. No obstante, recomendamos que desactive la función de cortafuegos incorporada. De no hacerlo, no recibirá eventos en el registro de eventos entrantes de McAfee Personal Firewall Plus.

Instalación de McAfee® Personal Firewall Plus™

Antes de descargar e instalar Personal Firewall Plus, debe contratar el servicio. Para ello, puede acceder al Centro de Seguridad Terra. Siga los pasos que se le indican para poder contratar el servicio *firewall* a través de Terra.

- 1 Escriba <http://www.seguridad.terra.es/descarga.asp> y haga clic en el botón **Continuar**.



Figura 1-1. Pantalla de contratación de Terra

- 2 A continuación podrá ver la pantalla **Identifíquese en McAfee Security**, donde se le solicitarán los siguientes datos (correspondientes a la información que Terra le ha facilitado en el correo de bienvenida al servicio):
 - ◆ Dirección de correo electrónico.
 - ◆ Número de licencia.



Figura 1-2. Pantalla de identificación en McAfee Security

- 3 Una vez completados los campos, haga clic en el botón **Enviar**.
- 4 Visualizará una pantalla donde aparecerán detallados los productos que ha adquirido. Localice **McAfee Personal Firewall Plus** en la lista **Los servicios Web** y, a continuación, haga clic en el icono **Actualizar/Descargar** que aparece junto al producto. El proceso de descarga comenzará de forma automática.

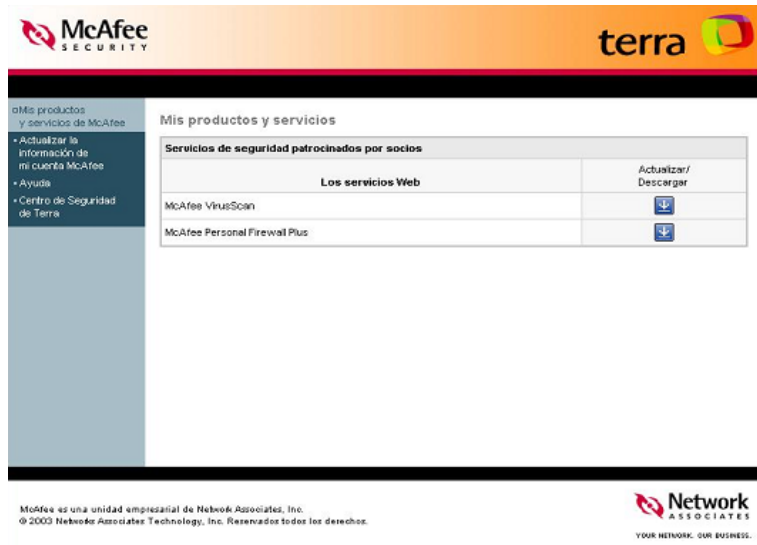


Figura 1-3. Pantalla de productos y servicios

Para instalar Personal Firewall Plus:

- 1 Si ha descargado Personal Firewall Plus del sitio Web de McAfee, aparecerá el Asistente para la configuración.
- 2 Siga las instrucciones que le indica el asistente para completar la instalación.

Al completarse la instalación, aparece el Asistente para la configuración de Personal Firewall Plus. (Figura 1-4).



Figura 1-4. Asistente para la configuración

Uso del Asistente para la configuración

No es preciso que utilice el Asistente para la configuración dado que Personal Firewall ya está configurado para proteger el equipo desde el principio. El Asistente para la configuración le ayuda a explorar el equipo en busca de virus y a configurar lo siguiente:

- Tipos de alerta que desea recibir
- Tipo de conexión de red
- Opciones de recomendaciones de aplicaciones

Puede hacer clic en **Cancelar** en cuanto lo desee para aceptar las opciones predeterminadas. También puede modificar cuando lo desee las opciones de configuración de Personal Firewall Plus.

NOTA

Si está efectuando la actualización a una versión nueva de Personal Firewall Plus y quiere mantener los mismos ajustes de configuración del cortafuegos, haga clic en **Cancelar**.

Después de usar el Asistente para la configuración, debe reiniciar el equipo para completar la instalación.


Para utilizar el Asistente para la configuración:

- 1 Haga clic en **Siguiente**.
- 2 Siga las instrucciones de los cuadros de diálogo que aparezcan.
- 3 Haga clic en **Finalizar** cuando termine de utilizar el Asistente para la configuración.

Se le pedirá que reinicie el equipo. Haga clic en **Aceptar** para reiniciar el equipo ahora o en **Cancelar** para reiniciarlo más tarde. Deberá reiniciar el equipo para poder usar Personal Firewall Plus.

Comprobación de McAfee® Personal Firewall Plus™

Para comprobar Personal Firewall Plus:

- 1 Haga clic con el botón derecho en el icono de McAfee , seleccione **Personal Firewall Plus** y, a continuación, haga clic en **Comprobar cortafuegos**.
- 2 Personal Firewall Plus abre Internet Explorer y se dirige a <http://www.hackerwatch.org/>, un sitio Web que mantiene McAfee. Siga las instrucciones de la página Hackerwatch.org para comprobar Personal Firewall Plus.

NOTA

Si se conecta a Internet mediante un servidor proxy o un servidor NAT (del inglés Network Address Translation, conversión de direcciones de red), como ocurre con la mayoría de redes de las oficinas (LAN), la lectura que obtendrá no será la correcta.

La herramienta de comprobación de cortafuegos de Hackerwatch.org buscará el equipo que solicitó la comprobación y efectuará una prueba de dicho equipo. Si se conecta a través de un proxy o un servidor NAT, simplemente transmite la solicitud de comprobación, por lo que Hackerwatch.org comprobará un equipo distinto del que realiza la solicitud. Los resultados obtenidos serían los del servidor proxy, no los del equipo del usuario.


Utilización de McAfee® SecurityCenter™

McAfee SecurityCenter es una herramienta de seguridad integrada, a la que puede tener acceso con el icono situado en la bandeja del sistema de Windows o directamente desde el escritorio de Windows. Gracias a éste, puede realizar estas útiles tareas:

- Obtener un análisis de seguridad del equipo.
- Ver alertas de virus actualizados continuamente y la información más reciente sobre productos.
- Acceder a las preguntas más frecuentes e información detallada de su cuenta de usuario en el Centro de Seguridad Terra.

NOTA

Si desea obtener más información sobre sus funciones, Seleccione la opción **Ayuda** en el cuadro de diálogo de McAfee SecurityCenter.


Cuando McAfee SecurityCenter se encuentra en ejecución y todas las funciones de McAfee están activadas en el equipo, se mostrará un icono rojo con una M  en la bandeja del sistema de Windows. Esta área se encuentra normalmente en la esquina inferior derecha del escritorio de Windows e incluye el reloj.

Si cualquiera de las aplicaciones de McAfee instaladas se encuentra desactivada, el icono de McAfee aparecerá en color negro .

Para abrir McAfee SecurityCenter:

- 1 Haga clic con el botón derecho en el icono de McAfee .
- 2 Haga clic en **Abrir SecurityCenter**.

Para acceder a una función de McAfee Personal Firewall Plus:

- 1 Haga clic con el botón derecho en el icono de McAfee .
- 2 Seleccione **Personal Firewall Plus** y, a continuación, haga clic en la función que desee utilizar.

Uso de McAfee® Personal Firewall Plus™

2

Para abrir Personal Firewall Plus:

Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Ver resumen**, **Aplicaciones de Internet**, **Eventos entrantes** o **Utilidades**.

Información acerca del Resumen

El Resumen de Personal Firewall Plus incluye cuatro secciones:

- a** Resumen principal.
- b** Resumen de aplicaciones.
- c** Resumen de eventos.
- d** Resumen de HackerWatch.




Cada una de estas secciones contiene una serie de informes sobre los eventos entrantes recientes, el estado de las aplicaciones y la actividad de intrusión mundial recogida por HackerWatch.org. También encontrará vínculos sobre tareas comunes realizadas en Personal Firewall Plus.

Para abrir las páginas de resumen de Personal Firewall Plus, haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Resumen**. Aparecerá la página Resumen principal (Figura 2-1).



Figura 2-1. Página Resumen principal

Haga clic en los siguientes vínculos para desplazarse por las secciones del resumen:

Elemento	Descripción
Cambiar vista	Haga clic en Cambiar vista para abrir una lista de páginas de resumen. Seleccione en la lista la página de resumen que desea ver.
 Flecha derecha	Haga clic en el icono de flecha derecha para ver la siguiente página de resumen.
 Flecha izquierda	Haga clic en el icono de flecha izquierda para ver la página de resumen anterior.
 Inicio	Haga clic en el icono de inicio para volver a la página Resumen principal .

La página Resumen principal incluye los datos siguientes:

Elemento	Descripción
Configuración de seguridad	La configuración de seguridad muestra el nivel de seguridad definido para el cortafuegos. Haga clic en el vínculo para cambiar el nivel de seguridad.
Eventos bloqueados	Eventos bloqueados muestra el número de eventos bloqueados en el día actual. Haga clic en el vínculo para ver detalles de eventos procedentes de la página Eventos entrantes.
Cambios de reglas de aplicación	Muestra el número de reglas de aplicación que han cambiado recientemente. Haga clic en el vínculo para ver la lista de aplicaciones permitidas y bloqueadas o para modificar los permisos de las aplicaciones.
Novedades	Novedades muestra la última aplicación a la que se concedió acceso pleno a Internet.
Último evento	Último evento muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de dicha dirección llegue hasta su equipo.
Informe diario	Informe diario muestra el número de eventos entrantes bloqueados por Personal Firewall Plus en el día semana y mes en curso. Haga clic en el vínculo para ver detalles de eventos procedentes de la página Eventos entrantes.
Aplicaciones activas	Aplicaciones activas permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo en cada momento. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de Tareas comunes para ir a las páginas de Personal Firewall Plus, donde podrá consultar la actividad del cortafuegos y llevar a cabo algunas tareas.

Para ver la página Resumen de aplicaciones, haga clic en **Cambiar vista** y seleccione **Resumen de aplicaciones**. La página Resumen de aplicaciones incluye los datos siguientes:

Elemento	Descripción
Control del tráfico	Control del tráfico muestra el volumen de tráfico entrante y saliente en la conexión de Internet durante los últimos diez minutos. Haga clic en el gráfico para ver los detalles de control del tráfico.
Aplicaciones activas	Aplicaciones activas muestra el uso de ancho de banda que han hecho las aplicaciones con mayor actividad del equipo durante las últimas 24 horas. Aplicación: aplicación que accede a Internet. %: porcentaje de ancho de banda utilizado por la aplicación. Permiso: tipo de acceso a Internet que se permite a la aplicación. Regla creada: fecha de creación en que se creó la regla de aplicación.
Novedades	Novedades muestra la última aplicación a la que se concedió acceso pleno a Internet.
Aplicaciones activas	Aplicaciones activas permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo en cada momento. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de Tareas comunes para ir a las páginas de Personal Firewall Plus, donde podrá consultar el estado de la aplicación y llevar a cabo algunas tareas.

Para ver la página Resumen de eventos, haga clic en **Cambiar vista** y seleccione **Resumen de eventos**. La página Resumen de eventos incluye los datos siguientes:

Elemento	Descripción
Comparación de puertos	Comparación de puertos muestra un gráfico de sectores de los puertos del equipo que se han intentado abrir con mayor frecuencia durante los últimos 30 días. Haga clic en el nombre de un puerto para ver detalles de la página Eventos entrantes. También puede situar el cursor sobre el número de puerto para ver una descripción de dicho puerto.
Principales sospechosos	Principales sospechosos indica las direcciones IP bloqueadas con mayor frecuencia, cuándo se produjo el último evento entrante de cada dirección y el número total de eventos entrantes registrados de cada dirección en los últimos 30 días. Haga clic en un evento para ver detalles de la página Eventos entrantes.

Elemento	Descripción
Informe diario	Informe diario muestra el número de eventos entrantes bloqueados por Personal Firewall Plus en el día, semana y mes en curso. Haga clic en un número para ver detalles de eventos procedentes del registro de eventos entrantes.
Último evento	Último evento muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de dicha dirección llegue hasta su equipo.
Tareas comunes	Haga clic en un vínculo de Tareas comunes para ir a las páginas de Personal Firewall Plus, donde podrá consultar los detalles de los eventos y llevar a cabo algunas tareas.

Para ver la página Resumen de HackerWatch, haga clic en **Cambiar vista** y seleccione **Resumen de HackerWatch**. La página Resumen de HackerWatch incluye los datos siguientes:

Elemento	Descripción
Actividad mundial	Actividad mundial muestra un mapa del mundo que identifica la actividad bloqueada recientemente y controlada por HackerWatch.org. Haga clic en el mapa para abrir el mapa de análisis de amenazas mundiales en HackerWatch.org.
Volumen de eventos	Volumen de eventos muestra el número de eventos entrantes enviados a HackerWatch.org.
Actividad mundial de puertos	Actividad mundial de puertos muestra los puertos que han recibido un mayor número de amenazas en los últimos cinco días. Haga clic en un puerto para ver su número y descripción.
Tareas comunes	Haga clic en un vínculo de Tareas comunes para ir a las páginas de HackerWatch.org, donde podrá obtener información adicional sobre las actividades de piratería a escala mundial.

Información acerca de aplicaciones de Internet

La página Aplicaciones de Internet permite consultar una lista de las aplicaciones permitidas y bloqueadas.

Haga clic con el botón derecho en **Personal Firewall Plus** y, después, en **Aplicaciones de Internet**. Aparecerá la página Aplicaciones de Internet (Figura 2-2).

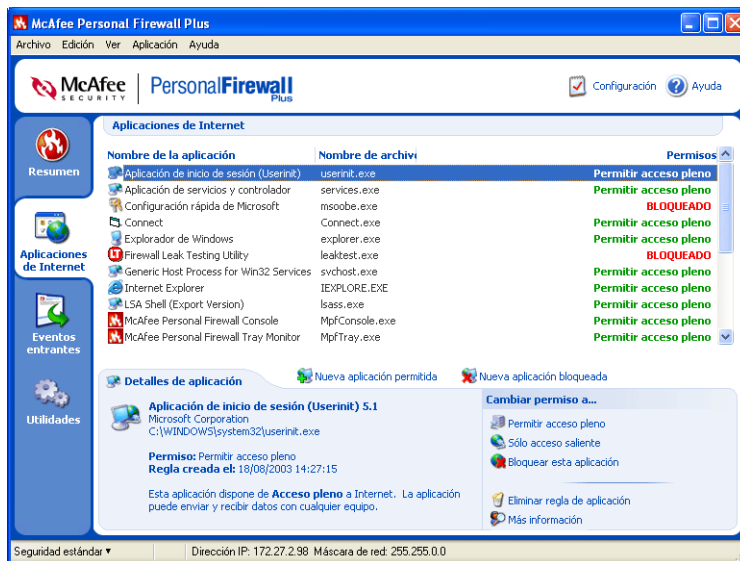


Figura 2-2. Página Aplicaciones de Internet

La página Aplicaciones de Internet incluye los datos siguientes:

- Nombres de aplicaciones.
- Nombres de archivos.
- Niveles de permisos actuales.
- Detalles de aplicaciones: rutas, fechas y horas de los permisos y explicaciones de los tipos de permisos

Cambio de permisos

Personal Firewall Plus permite establecer el nivel de permiso para cada una de las aplicaciones que solicite acceder a Internet.

Para cambiar un nivel de permiso:

- 1 Haga clic con el botón derecho en **Personal Firewall Plus** y, después, en **Aplicaciones de Internet**.
- 2 En la lista **Permisos**, haga clic con el botón derecho en el nivel de permiso de una aplicación y, a continuación, seleccione un nivel diferente:
 - ◆ Seleccione **Permitir acceso pleno** para permitir que la aplicación envíe y reciba datos.
 - ◆ Haga clic en **Sólo acceso saliente** para evitar que la aplicación reciba datos.
 - ◆ Haga clic en **Bloquear esta aplicación** para evitar que la aplicación envíe y reciba datos.

Para eliminar un nivel de permiso:

- 1 Haga clic con el botón derecho en **Personal Firewall Plus** y, después, en **Aplicaciones de Internet**.
- 2 En la lista **Permisos**, haga clic con el botón derecho en el nivel de permiso para la aplicación y, a continuación, seleccione **Eliminar regla de aplicación**.

La próxima vez que la aplicación solicite acceder a Internet, será posible establecer su nivel de permiso para que se vuelva a agregar a la lista.

Cambio de aplicaciones

Para modificar la lista de aplicaciones a las que se permite y bloquea el acceso a Internet:

- 1 Haga clic con el botón derecho en **Personal Firewall Plus** y, después, en **Aplicaciones de Internet**.
- 2 Agregue o elimine aplicaciones de la lista **Nombre de la aplicación**:
 - ◆ Para agregar una aplicación a la que se permite el acceso, haga clic en **Nueva aplicación permitida**, seleccione la aplicación y, a continuación, haga clic en **Abrir**.
 - ◆ Para agregar una nueva aplicación bloqueada, haga clic en **Nueva aplicación bloqueada**, seleccione la aplicación y, a continuación, haga clic en **Abrir**.
 - ◆ Para eliminar una aplicación de la vista, pulse en **Eliminar regla de aplicación**.

Información acerca de los eventos entrantes

La página Eventos entrantes permite consultar el registro de eventos entrantes generado cuando Personal Firewall Plus bloquea el tráfico de Internet no solicitado.

Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**. Aparecerá la página Eventos entrantes (Figura 2-3).

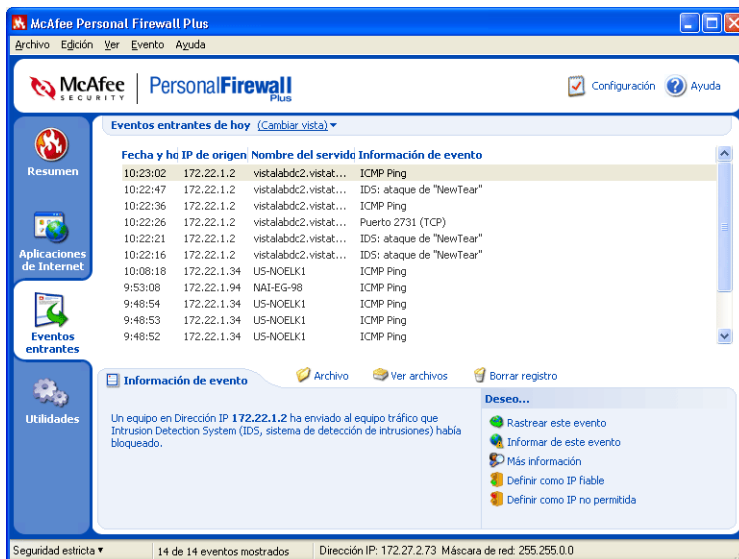


Figura 2-3. Página Eventos entrantes

La página Eventos entrantes incluye los datos siguientes:

- Fechas y horas de los eventos.
- IP de origen.
- Nombres de servidores.
- Nombres de servicio o de aplicaciones.
- Detalles del evento: tipos de conexión, los puertos en los que éstas se han realizado y explicaciones sobre los eventos producidos en los puertos.

Explicación del concepto de evento

Información acerca de las direcciones IP

Las direcciones IP están compuestas por números: para ser más exactos, cuatro números comprendidos entre 0 y 255. Estos números permiten identificar un lugar concreto al que dirigir el tráfico a través de Internet.

Direcciones IP especiales

Existen diversas IP que no se utilizan con demasiada frecuencia por diversas razones:

Direcciones IP no encaminables: también se conocen como "espacio de IP privadas". Estas direcciones IP no se pueden utilizar en Internet. Los bloques de 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 retorno es 127.x.x.x.

Dirección IP nula: se trata de una dirección no válida. Cuando se ve, indica que el tráfico presenta una 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 sería una dirección IP nula.

Eventos desde 0.0.0.0

Si observa eventos procedentes de la dirección IP 0.0.0.0, existen dos causas probables. La primera, y más común, es que por algún motivo el equipo ha recibido un paquete defectuoso. Internet no es siempre fiable al 100%, por lo que puede que reciba paquetes dañados. Dado que Personal Firewall Plus 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 está trucada o simulada. Los paquetes trucados pueden ser un indicio de que alguien realiza una exploración en busca de troyanos y, por casualidad, ha llegado a su equipo. Personal Firewall Plus ya ha bloqueado esta dirección, por lo que su equipo estará seguro.

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 de retorno.

En términos generales, 127.0.0.1 siempre se refiere al usuario, independientemente del equipo en que se encuentre. Esta dirección también suele llamarse "localhost" (servidor local), pues el nombre de equipo "localhost" siempre se remitirá a la dirección IP 127.0.0.1.

¿Significa eso que el equipo intenta un ataque a sí mismo? ¿Hay algún troyano o software espía intentando manipular el equipo? Probablemente no. Muchos programas habituales utilizan la dirección de bucle de retorno para la comunicación entre sus componentes. Por ejemplo, muchos servidores Web o servidores personales de correo permiten configurarlos a través de una interfaz Web a la que se accede normalmente a través de una dirección similar a `http://localhost/`.

Sin embargo, Personal Firewall Plus permite el tráfico procedente de dichos programas, de modo que si ve eventos procedentes de 127.0.0.1, lo más probable es que la dirección IP sea simulada o trucada. Los paquetes trucados suelen presentar signos de que alguien está buscando troyanos. Personal Firewall Plus ya ha bloqueado esta dirección, por lo que su equipo estará seguro. Obviamente, presentar un informe sobre eventos procedentes de 127.0.0.1 no tiene ninguna utilidad, por lo que no se hará.

Una vez dicho esto, hay algunos programas, entre ellos Netscape 6.2 y versiones posteriores, que requieren que agregue la dirección 127.0.0.1 a la lista de IP fiables. Los componentes de estos programas se comunican entre sí de tal forma, que Personal Firewall Plus no puede determinar si el tráfico es local o no.

En el ejemplo de Netscape 6.2, si no confía en la dirección 127.0.0.1, no podrá utilizar su lista de contactos. Por lo tanto, si ve tráfico procedente de 127.0.0.1 y todas las aplicaciones instaladas en su equipo funcionan con normalidad, resulta completamente seguro bloquear este tráfico. Pero si un programa (como Netscape) experimenta algún problema, coloque la dirección 127.0.0.1 en la lista de IP fiables de Personal Firewall Plus y compruebe si se ha solucionado el problema.

Si de esta forma se soluciona el problema, debe sopesar las opciones siguientes: si confía en la dirección 127.0.0.1, el programa funcionará, pero estará más expuesta a sufrir ataques desde IP simuladas. Si no confía en esta dirección, el programa no funcionará, pero permanecerá protegido frente al tráfico malintencionado.

Eventos procedentes de equipos de la LAN

Los eventos pueden originarse en equipos situados en la red de área local (LAN). Para indicar que estos eventos proceden de un lugar cercano, Personal Firewall Plus los muestra en verde.

En la mayoría de las configuraciones de redes de área local (LAN) empresariales, normalmente se activa la opción "Confiar en todos los equipos de la LAN" en las opciones de IP fiables.

No obstante, debe recordar que, en algunas situaciones, la red local puede resultar tan peligrosa, o incluso más, que la red externa. Esto es especialmente probable en redes públicas de gran ancho de banda, como DSL o módems por cable. En este tipo de casos, se recomienda no activar la opción "Confiar en todos los equipos de la LAN".

Si se encuentra en una red de banda ancha, agregue manualmente las direcciones IP de los equipos locales a la lista de IP fiables. Recuerde que puede utilizar direcciones del tipo .255 para confiar los bloques enteros. Por ejemplo, puede confiar en toda una red ICS (compartición de conexión a Internet, del inglés Internet Connection Sharing) definiendo como fiable la dirección IP 192.168.255.255.

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 llamarse direcciones IP no encaminables o privadas. 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 una red ICS, y ve eventos con este bloque, es posible que desee agregar la dirección IP 192.168.255.255 a la lista de IP fiables. De esta forma confiará en 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 trucada o simulada. Los paquetes trucados normalmente presentan signos de que alguien está buscando troyanos. Personal Firewall Plus ya ha bloqueado esta dirección, por lo que su equipo estará seguro.

Dado que las direcciones IP privadas se refieren a diferentes equipos en función de la red en que se encuentren, informar acerca de estos eventos no tiene ninguna utilidad, por lo que no se hará.

Visualización de eventos en el registro de eventos entrantes

El registro de eventos entrantes permite consultar cómodamente los eventos de varias formas. La vista predeterminada se limita a los eventos del día actual. También se pueden ver los eventos que se han producido durante la semana anterior, o incluso consultar el registro completo.

Personal Firewall Plus también permite consultar los eventos entrantes producidos en un día concreto, los procedentes de determinadas direcciones IP o los que presentan la misma información.

Para obtener información acerca de un evento, haga clic en él; la información se mostrará en el área **Información de evento** situada en la parte inferior de la página Eventos entrantes.

Visualización de los eventos del día en curso

Para mostrar sólo los eventos que se han producido en el día en curso:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar eventos de hoy**.

El registro de eventos entrantes muestra sólo los eventos que se han producido en el día actual.

Mostrar eventos de la semana en curso

Para mostrar los eventos que se han producido durante la semana en curso:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar eventos de esta semana**.

El registro de eventos entrantes muestra sólo los eventos que se han producido en la semana actual.

Visualización del registro completo de eventos entrantes

Para mostrar todos los eventos del registro de eventos entrantes:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar registro completo**.

El registro de eventos entrantes mostrará todos los eventos del registro, sin incluir los archivos comprimidos.

Visualización sólo de los eventos de un día concreto

Esta función resulta de gran utilidad cuando desea consultar los eventos que se produjeron un día concreto. Se ocultarán todos los eventos que no se hayan producido el día seleccionado.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar sólo eventos de un día concreto**.

Los eventos que se hayan producido en el día actual se mostrarán en el registro de eventos entrantes.

Visualización sólo de los eventos de una dirección de Internet concreta

Esta opción resulta de gran utilidad para consultar los eventos procedentes de una dirección de Internet concreta. El resto de los eventos no se muestra.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar sólo eventos de una dirección de Internet concreta**.

Los eventos originados en la dirección de Internet seleccionada se mostrarán en el registro de eventos entrantes.

Visualización sólo de eventos con la misma información de eventos

Esta opción resulta de gran utilidad cuando se necesita comprobar si existen otros eventos en el registro que presentan la misma información en la columna **Información de evento** que el evento seleccionado. Podrá consultar cuántas veces ha ocurrido y si tienen el mismo origen. La columna Información de evento ofrece una descripción del evento y, si se conoce, el programa o servicio que suele utilizar dicho puerto.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Ver**, haga clic en **Mostrar sólo eventos con la misma información de eventos**.

Los eventos cuya información coincida se mostrarán en el registro de eventos entrantes.

Respuesta a eventos entrantes

Además de obtener detalles sobre los eventos del registro de eventos entrantes, puede intentar efectuar un rastreo visual de las direcciones IP de un evento concreto, o incluso obtener detalles en el sitio Web antihackers HackerWatch.org.

Rastreo del evento seleccionado

Puede intentar un rastreo visual de las direcciones IP correspondientes a un evento del registro de eventos entrantes.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Pulse con el botón derecho en el evento que desea rastrear y seleccione **Rastrear evento seleccionado**.

También puede hacer doble clic en el evento para iniciar el rastreo.

De forma predeterminada, Personal Firewall Plus inicia un rastreo visual mediante el programa Visual Trace integrado.

Obtención de consejos de HackerWatch.org

Puede obtener más información sobre un evento en la comunidad en línea contra la piratería informática HackerWatch.org siguiendo estos pasos:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Busque el evento sobre el que desea obtener más información y haga clic en él.
- 3 En el menú **Evento**, haga clic en **Más información sobre el evento**.

Se abrirá el navegador Web y se dirigirá al sitio Web de HackerWatch.org en <http://www.hackerwatch.org/> para obtener detalles sobre el tipo de eventos y consejos sobre si debe informar al respecto.

Informes sobre un evento

Para informar sobre un evento que considere un ataque sobre su equipo, siga estos pasos:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Haga clic en el evento sobre el que desea informar y seleccione **Informar de este evento** en el panel inferior derecho.

Personal Firewall Plus informa sobre el evento al sitio Web HackerWatch.org mediante su identificación exclusiva.

Registro en HackerWatch.org

Al abrir la página Resumen, Personal Firewall Plus se pondrá en contacto con HackerWatch.org para generar la identificación exclusiva del usuario. Si ya es usuario, su registro se validará de inmediato. Si es un usuario nuevo, introduzca un nombre de usuario y una dirección de correo electrónico y, a continuación, haga clic en el vínculo de validación del mensaje de correo electrónico de confirmación remitido por HackerWatch.org para poder utilizar las funciones de filtro y correo electrónico de su sitio Web.

Puede informar sobre eventos a HackerWatch sin validar su identificación de usuario. Sin embargo, para filtrar eventos y mandarlos por correo electrónico a un amigo, debe registrarse en el servicio.

Si se registra en este servicio, sus envíos serán rastreados y nos permitirá notificarle si HackerWatch.org necesita más información u otra cosa de usted. También necesitamos que se registre porque debemos confirmar toda la información recibida para que resulte de utilidad.

HackerWatch.org se compromete a mantener la confidencialidad de todas las direcciones de correo electrónico que se le proporcionen. Si un proveedor de servicios de Internet realiza una solicitud para obtener información adicional, dicha petición se encaminará a través de HackerWatch.org, por lo que su dirección de correo electrónico nunca se verá expuesta.

Confianza en una dirección

Si ve un evento en el registro de eventos que contenga una dirección IP que necesite autorizar, puede configurar Personal Firewall Plus para que permita todas las conexiones procedentes de ella en todo momento:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Haga clic con el botón derecho del ratón en el evento en cuya dirección IP desee confiar y, después, en **Confiar en dirección IP de origen**.
- 3 Verifique que la dirección IP que muestra el mensaje de confirmación de confianza en esta dirección es correcta y haga clic en **Aceptar**.

La dirección IP se agregará a la lista de IP fiables.

Para verificar que la dirección IP se ha agregado:

- 1 Haga clic en la ficha **Utilidades**.
- 2 Haga clic en el icono **IP fiables y no permitidas**, y después en la ficha **Direcciones IP fiables**.

La dirección IP aparecerá en la lista **IP fiables**.

Prohibición de una dirección

Si aparece una dirección IP en el registro de eventos entrantes, el tráfico procedente de dicha dirección se habrá bloqueado. Por lo tanto, la prohibición de una dirección no incrementa la protección del sistema a menos que su equipo tenga abiertos, intencionadamente, determinados puertos a través de la función de servicios del sistema o que incluya una aplicación con permiso para recibir tráfico.

Agregue una dirección IP a la lista de direcciones prohibidas sólo si su equipo tiene uno o más puertos abiertos intencionadamente y no tiene razones para creer que resulte necesario bloquear el acceso a los puertos abiertos por parte de dicha dirección.

Si ve un evento del registro de eventos entrantes que contenga una dirección IP que desee prohibir, puede configurar Personal Firewall Plus para que rechace todas las conexiones procedentes de ella:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Haga clic con el botón derecho en el evento cuya dirección IP desee prohibir y haga clic en **Definir IP de origen como no permitida**.
- 3 Verifique que la dirección IP que muestra el mensaje de confirmación de prohibición de esta dirección es correcta y haga clic en **Aceptar**.

La dirección se agregará a la lista de IP no permitidas.

Para verificar que la dirección IP se ha agregado:

- 1 Haga clic en la ficha **Utilidades**.
- 2 Haga clic en el icono **IP fiables y no permitidas** y, a continuación, en la ficha **Direcciones IP no permitidas**.

La dirección IP aparecerá en la lista de IP no permitidas.

Gestión del registro de eventos entrantes

Puede utilizar la página Eventos entrantes para gestionar los eventos del registro de eventos entrantes que genera Personal Firewall Plus al bloquear tráfico no solicitado de Internet.

Compresión del registro de eventos entrantes

Puede archivar el registro de eventos entrantes actual en un archivo comprimido dentro del disco duro. Es aconsejable comprimir el registro de eventos de manera regular porque puede alcanzar un tamaño considerable.

Para comprimir el registro de eventos entrantes:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Archivo**, seleccione **Archivar registro**.
- 3 Haga clic en **Sí** en el mensaje de confirmación.
- 4 Haga clic en **Guardar** para guardar el archivo comprimido en la ubicación predeterminada, o bien diríjase a la ubicación en la que desea guardarlo.

Visualización del registro de eventos entrantes comprimido

Puede ver todos los registros de eventos entrantes que haya archivado con anterioridad en un archivo comprimido.

ADVERTENCIA

Para consultar los archivos comprimidos, deberá comprimir el registro actual de eventos entrantes. De lo contrario, el registro de eventos entrantes se borrará al ver un archivo comprimido.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Archivo**, haga clic en **Ver registros archivados**.
- 3 Haga clic en el nombre del archivo comprimido (puede que necesite buscarlo primero) y, después, en **Abrir**.

Los datos del archivo comprimido se mostrarán en el registro de eventos entrantes.

Borrado del registro de eventos entrantes

Puede borrar toda la información del registro de eventos entrantes.

ADVERTENCIA

Una vez borrado, el registro de eventos entrantes no podrá recuperarse. Si cree que va a necesitar el registro de eventos en el futuro, es mejor que lo guarde en un archivo comprimido.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú **Archivo**, seleccione **Borrar registro**.
- 3 Haga clic en **Sí** en el cuadro de confirmación para borrar el registro.

El registro de eventos quedará vacío.

Exportación de eventos mostrados

Puede exportar el registro de eventos a un archivo de texto en caso de que necesite compartirlo con su proveedor de servicios de Internet (ISP), con el servicio de asistencia técnica o con las autoridades públicas pertinentes.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 En el menú Archivo, haga clic en **Exportar eventos mostrados**.
- 3 Busque la ubicación en la que desea guardar los eventos.
- 4 Cambie el nombre del archivo, si lo cree necesario, y haga clic en **Guardar**.

Los eventos se guardarán en un archivo .txt en la ubicación escogida.

Copiado de un evento en el portapapeles

Puede copiar un evento en el portapapeles para pegarlo en un archivo de texto con el Bloc de notas.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Haga clic en el evento del registro de eventos entrantes que debe exportar.
- 3 En el menú **Edición**, haga clic en **Copiar evento seleccionado en el portapapeles**.
- 4 Abra el Bloc de notas:

Haga clic en el botón Inicio de Windows, seleccione Programas, Accesorios y Bloc de notas.

- 5 En el menú **Edición**, haga clic en **Pegar**. El evento se mostrará en el Bloc de notas. Repita este paso hasta que tenga todos los eventos necesarios.
- 6 Guarde el archivo del Bloc de notas en un lugar seguro.

Eliminación del evento seleccionado

Puede eliminar eventos del registro de eventos entrantes.

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall Plus** y haga clic en **Eventos entrantes**.
- 2 Haga clic en el evento del registro de eventos entrantes que desea eliminar.
- 3 En el menú **Edición**, haga clic en **Eliminar el evento seleccionado**.

El evento quedará eliminado del registro de eventos entrantes.

Información acerca de las alertas

Es muy recomendable familiarizarse con los distintos tipos de alertas que aparecerán al utilizar Personal Firewall Plus. Revise los siguientes tipos de alerta que aparecen y las posibles respuestas para poder responder con seguridad a una alerta.

NOTA

Las recomendaciones de las alertas ayudan a decidir cómo reaccionar en cada situación. Para que las alertas incluyan recomendaciones, haga clic en la ficha **Utilidades**, en el icono **Configuración de alertas** y seleccione **Utilizar recomendaciones inteligentes** (valor predeterminado) o **Mostrar sólo recomendaciones inteligentes** en la lista **Recomendaciones inteligentes**.

Alertas rojas

Las alertas rojas contienen información importante que requiere atención inmediata. Las alertas rojas tienen el siguiente aspecto:

- **Aplicación de Internet bloqueada:** esta alerta aparece cuando Personal Firewall Plus bloquea el acceso de una aplicación a Internet. Por ejemplo, si aparece una alerta sobre un programa troyano, McAfee denegará automáticamente el acceso del programa a Internet y recomendará que se explore el equipo en busca de virus.
- **La aplicación desea tener acceso a Internet:** esta alerta aparece cuando Personal Firewall Plus detecta tráfico procedente de una red o de Internet para aplicaciones nuevas. (Seguridad Estándar o Estricta)
- **Se ha modificado la aplicación:** esta alerta aparece cuando Personal Firewall Plus detecta que se ha modificado una aplicación con acceso a Internet autorizado. Si ha actualizado recientemente la aplicación en cuestión, debería tener cuidado a la hora de concederle permiso de acceso a Internet. (Seguridad Fiable, Estándar o Estricta)
- **La aplicación desea tener acceso al servidor:** esta alerta aparece cuando Personal Firewall Plus detecta que una aplicación con permiso para acceder a Internet solicita acceder a Internet como servidor. (Seguridad Estricta)

Alertas verdes

Las alertas verdes informan de cambios que se han realizado en Personal Firewall Plus. Por ejemplo, pueden informar de las aplicaciones a las que Personal Firewall Plus ha concedido acceso automático a Internet, o informar de nuevas reglas de aplicación.

El programa tiene permitido el acceso a Internet: esta alerta aparece cuando Personal Firewall concede acceso a Internet automáticamente a todas las aplicaciones nuevas o modificadas y lo notifica con posterioridad (Seguridad Estándar). Un ejemplo de aplicación modificada sería la que tuviera reglas modificadas que permitieran acceder automáticamente a Internet.

Alertas azules

Las alertas azules contienen información, pero no requieren ninguna acción por parte del usuario.

- **Intento de conexión bloqueado:** esta alerta aparece cuando Personal Firewall Plus bloquea tráfico no deseado procedente de una red o de Internet. (Seguridad Fiable, Estándar o Estricta)

Intento de conexión bloqueado

Si ha seleccionado la seguridad **Fiable, Estándar** o **Estricta**, Personal Firewall Plus muestra una alerta (Figura 2-4) al bloquear el tráfico de red o de Internet no deseado.

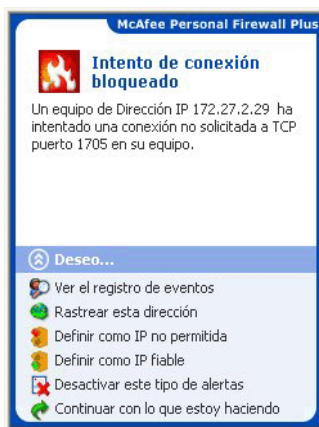


Figura 2-4. Alerta "Intento de conexión bloqueado"

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de eventos** para obtener detalles sobre el evento del registro de eventos entrantes de Personal Firewall Plus (consulte [Información acerca de los eventos entrantes en la página 22](#) para obtener información detallada al respecto).
- Haga clic en **Rastrear esta dirección** para realizar un rastreo visual de las direcciones IP correspondientes al evento.

- Haga clic en **Definir como IP no permitida** para evitar que se acceda al equipo desde esta dirección. La dirección se agregará a la lista de IP no permitidas.
- Haga clic en **Definir como IP fiable** para permitir que se acceda al equipo desde esta dirección.
- Haga clic en **Continuar con lo que estoy haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall Plus.

Aplicación de Internet bloqueada

Si aparece una alerta sobre un programa troyano (Figura 2-5), Personal Firewall Plus denegará automáticamente el acceso del programa a Internet y recomendará que se explore el equipo en busca de virus.



Figura 2-5. Alerta "Aplicación de Internet bloqueada"

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Más información** para obtener detalles sobre el evento del registro de eventos entrantes (consulte [Información acerca de los eventos entrantes en la página 22](#) para obtener información detallada al respecto).
- Pulse en **Iniciar McAfee VirusScan Online** para analizar el equipo en busca de virus.
- Haga clic en **Continuar con lo que estoy haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall Plus.

La aplicación desea tener acceso a Internet

Si selecciona el nivel **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall Plus muestra una alerta (Figura 2-6) cuando detecta tráfico de red o de acceso a Internet proveniente de aplicaciones nuevas o modificadas.



Figura 2-6. Alerta "La aplicación desea tener acceso a Internet"

Si aparece una alerta que recomienda precaución a la hora de permitir el acceso a Internet a la aplicación, haga clic en **Haga clic aquí para obtener más información** para ver información adicional de la aplicación. Esta opción aparece en la alerta sólo cuando Personal Firewall Plus está configurado para utilizar recomendaciones inteligentes.

McAfee podría no reconocer la aplicación que intenta obtener acceso a Internet (Figura 2-7)



Figura 2-7. McAfee no ha reconocido esta alerta de aplicación

Por lo tanto, McAfee no podría aconsejarle acerca de cómo gestionar la aplicación. Puede informar a McAfee acerca de la aplicación si hace clic en **Notifique a McAfee la existencia de este programa**. Aparece una página Web en donde se le solicita información sobre la aplicación. Introduzca toda la información de que disponga

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación envíe y reciba datos no solicitados desde un puerto que no sea del sistema.
- Pulse en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

IMPORTANTE

Debe conceder acceso a las aplicaciones que necesiten acceder a Internet para obtener actualizaciones en línea del programa (como ocurre con los servicios de McAfee Security) para mantenerlos al día.

Se ha modificado la aplicación

Si selecciona **Fiable**, **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall Plus muestra una alerta (Figura 2-8) cuando detecta que se ha modificado una aplicación a la que se había concedido permiso de acceso a Internet. Si ha actualizado recientemente la aplicación en cuestión, debe tener cuidado a la hora de concederle permiso de acceso a Internet.

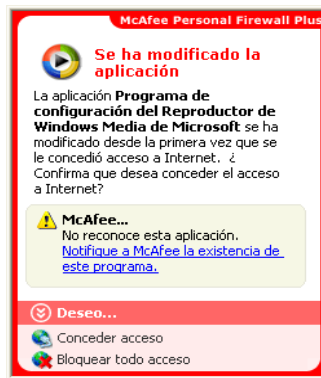


Figura 2-8. Alerta "Se ha modificado la aplicación"

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación envíe y reciba datos no solicitados desde un puerto que no sea del sistema.
- Haga clic en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

La aplicación desea tener acceso al servidor

Si selecciona el nivel de seguridad **Estricta** en las opciones de Configuración de seguridad, Personal Firewall Plus mostrará una alerta ([Figura 2-9](#)) al detectar que un aplicación con permiso de acceso a Internet solicita acceso a Internet como servidor.

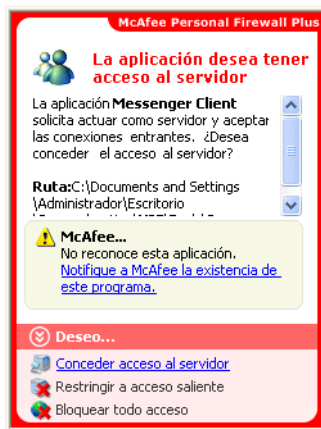


Figura 2-9. Alerta "La aplicación desea tener acceso al servidor"

Por ejemplo, aparecerá una alerta cuando MSN Messenger solicite acceso de servidor para enviar un archivo durante una sesión de chat.

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso al servidor** para permitir que la aplicación envíe y reciba datos.
- Haga clic en **Restringir a acceso saliente** para impedir que la aplicación reciba datos.
- Haga clic en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

El programa tiene permitido el acceso a Internet

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall Plus concederá acceso a Internet de forma automática a todas las aplicaciones nuevas o modificadas, y se lo notificará mediante una alerta (Figura 2-10).



Figura 2-10. El programa tiene permitido el acceso a Internet

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento del registro de aplicaciones de Internet (consulte *Información acerca de aplicaciones de Internet en la página 20* para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para evitar la activación de alertas de este tipo.
- Haga clic en **Continuar con lo que estoy haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall Plus.

Índice alfabético

A

- alertas, 33
 - Intento de conexión bloqueado, 34
 - La aplicación desea tener acceso a Internet, 33
 - La aplicación desea tener acceso al servidor, 33
 - Nueva aplicación permitida, 34
 - Se ha modificado la aplicación, 33
- aplicaciones de Internet
 - cambiar aplicaciones, 21
 - cambiar permisos, 21
 - información acerca de, 20

C

- comprobar Personal Firewall Plus, 12

D

- descargar Personal Firewall Plus, 8
- desinstalar
 - otros cortafuegos, 7
- direcciones IP
 - información acerca de, 23

E

- eventos
 - borrado el registro de eventos, 31
 - bucle de retorno, 24
 - comprimir registro de eventos, 30
 - consultar a HackerWatch.org, 28
 - copiar, 32
 - de 127.0.0.1, 24
 - de direcciones IP privadas, 25
 - desde 0.0.0.0, 23
 - desde equipos de la LAN, 25
 - eliminar, 32
 - exportar, 32
 - información acerca de, 22
 - información adicional, 28

informar, 28

mostrar

- con la misma información de eventos, 27
- del día actual, 26
- día concreto, 27
- dirección concreta, 27
- semana actual, 26
- todos, 26

rastrear

- entender, 22
 - ver registro de eventos comprimidos, 31
- responder a, 28

F

- funciones nuevas, 5

H

- HackerWatch.org
 - consejos, 28
 - informar sobre un evento a, 28
 - registrarse, 29

I

- informar sobre un evento, 28
- instalar Personal Firewall Plus, 8
- introducción, 5

M

- mostrar eventos en el registro de eventos, 26

P

- Página Resumen, 15
- Personal Firewall Plus
 - abrir, 15
 - comprobar, 12
 - instalar, 8
 - usar, 15

R

rastrear un evento, [28](#)

registro de eventos

 gestionar, [30](#)

 información acerca de, [22](#)

 ver, [31](#)

requisitos del sistema, [7](#)