

Outpost Firewall Pro 2.5 comparado con Windows ICF

Debido a la creciente cantidad de amenazas y daños producidos a través de Internet que ocurren en la actualidad, Microsoft, con muy buen criterio, ha decidido integrar un cortafuegos con el Service Pack 2 de Windows XP y ha denominado al mismo como **ICF o Internet Connection Firewall** (Cortafuegos para la conexión a Internet).

Sin embargo, esto puede generar una falsa sensación de seguridad, ya que aunque esta nueva aplicación integrada ayuda a mejorar la seguridad de los ordenadores, quedan sin cubrir varios aspectos críticos que no bloquean la totalidad de las actuales amenazas y pueden permitir graves daños a la seguridad e integridad de su equipo, sus datos y su privacidad.

Fugas en su privacidad

Los programas espías (Spyware) recolectan información sobre usted y sus intereses, como por ejemplo, hábitos de navegación y programas instalados en su ordenador, entre otras posibilidades, sin su conocimiento ni su consentimiento.



Windows ICF (XP SP2)

El cortafuegos de Windows no filtra ni impide el tráfico saliente, por lo que sus datos personales pueden fugar hacia el exterior de su ordenador sin ningún tipo de control ni impedimento.



Outpost Firewall Pro 2.5

Outpost no tan sólo lo protege de la interceptación o robo de información sensible, sino que también sus datos privados permanecen alejados de una fuga hacia el exterior de su ordenador.

El complemento que bloquea el contenido activo permite esconder sus hábitos de navegación e impedir la instalación de *Cookies*.

El Control de componentes le impedirá la ejecución de programas legítimos que hubieran sido modificados maliciosamente, impidiendo el envío en línea y tiempo real de su información personal a servidores remotos.

Debido a que Outpost controla toda la actividad de su ordenador en una red (local y también en Internet) bloqueará toda conexión ilegal, impidiendo que programas maliciosos puedan fugar su información personal hacia servidores remotos, poniendo en riesgo su privacidad.

Troyanos y gusanos

Algunos troyanos pueden permitir y/o inyectar módulos dañinos como si fueran aplicaciones legítimas (como por ejemplo, su navegador) y de esa forma, obtener privilegios para proceder en línea sin su conocimiento ni consentimiento.

Los gusanos se propagan a través de las redes, reproduciéndose mientras se dispersan, provocando desde sobrecargas en el tráfico de red hasta múltiples efectos perniciosos.



Windows ICF (XP SP2)

El cortafuegos de Windows no filtra ni impide el tráfico saliente, no teniendo posibilidades de bloquear la actividad ilegal causada por troyanos.

Por la misma razón, no puede impedir la distribución de gusanos a través de su correo electrónico.



Outpost Firewall Pro 2.5

El **Control de componentes** de Outpost conserva un registro de toda la actividad de red efectuada por los elementos y módulos de cada aplicación, impidiendo toda conexión ilegal y, de esa forma, si hubiera troyanos instalados en su ordenador, estos no podrán cumplir su rutina dañina.

El **Control de procesos ocultos** añade un nuevo elemento de prevención al impedir que aplicaciones legítimas ejecuten programas desconocidos que pudieran poner en peligro su sistema.

Ataques por denegación de servicio (DoS)

Cuando un atacante logre respuesta de un puerto de su ordenador, enviará una enorme cantidad de datos a su equipo y, como el puerto atacado será incapaz de procesar tal cantidad de información, culminará agotando los recursos de su sistema provocando el colapso del mismo y que usted pierda el control, impidiendo de esa forma, su utilización, obligándolo a un reinicio forzado del sistema, con la consiguiente pérdida de tiempo y posible pérdida de datos y productividad.



Windows ICF (XP SP2)

El cortafuegos de Windows no está diseñado para efectuar un análisis exhaustivo y profundo del tráfico entrante de datos, así como tampoco tiene ninguna utilidad que detecte y alerte al ser víctima de un ataque por denegación de servicio (DoS) en su ordenador.

Como adicionalmente el cortafuegos de Windows no puede bloquear intrusos por dirección IP y cerrar el puerto atacado para evitar las consecuencias del accionar malicioso, su ordenador puede ser agredido y usted nunca tomará conocimiento de esto, más allá de sufrir las consecuencias.



Outpost Firewall Pro 2.5

Outpost detecta y bloquea rápidamente todo tipo conocido de ataques, incluyendo denegación de servicio (DoS). De forma predeterminada, Outpost pone a su sistema en Modo invisible.

El complemento (*Plug-In*) Detección de ataques protege el ingreso de datos a su ordenador impidiendo la introducción de paquetes peligrosos. Outpost le alertará y además bloqueará todo tipo de ataque generando un informe detallado de los mismos en el Visor de registros.

El filtrado de protocolos le permitirá establecer un exhaustivo control de todos los paquetes que pasan por los puertos de su ordenador, impidiendo el paso a códigos maliciosos.

De forma muy sencilla pero sofisticada, usted podrá establecer el nivel de seguridad con el que desea proteger su sistema y Outpost procederá según sus preferencias, alertándolo cada vez que un ataque sea bloqueado.

Contenido no deseado

Internet contiene una enorme cantidad de sitios cuyo contenido debería ser vedado para sus hijos o no debería estar disponible en su oficina.



Windows ICF (XP SP2)

El cortafuegos de Windows puede bloquear dominios de Internet, introduciendo manualmente su dirección en una lista de exclusión, pero no puede proveer filtrado de información basándose en palabras clave y consecuentemente, no está en condiciones de ofrecer un 100% de efectiva protección.



Outpost Firewall Pro 2.5

El complemento (*Plug-In*) Bloqueo de contenido puede impedir el acceso a dominios completos como, por ejemplo, sex.com o cualquier página que contenga en su dirección o dentro del texto, palabras determinadas por el usuario.

Una vez establecidos estos parámetros, es imposible acceder a los sitios y/o páginas bloqueadas sin conocer la contraseña definida por el administrador del ordenador, constituyéndose en una efectiva protección para padres y como control de su oficina o empresa.

Facilidad de uso

Un cortafuegos no tan sólo debe protegerlo sino que debe ser simple de usar sobre cualquier sistema y para cualquier nivel de conocimiento del usuario.



Windows ICF (XP SP2)

El cortafuegos de Windows no provee herramientas especiales para registrar y analizar la actividad de la red, siendo particularmente difícil de configurar para usuarios novatos.



Outpost Firewall Pro 2.5

Outpost Firewall Pro le provee una completa protección desde el momento mismo de su instalación.

El sistema de configuración automática, que comienza desde la instalación misma del cortafuegos, permite establecer los mejores parámetros de seguridad para cada programa instalado en su ordenador.

Posteriormente, durante su uso, el modo Asistente de reglas le ayudará a establecer las reglas de funcionamiento que mejor se adapten a cada nuevo programa o necesidad de comunicación, protegiendo permanentemente su ordenador.

El sistema de alertas visuales le informará cada vez que un ataque haya sido bloqueado o se haya cambiado el nombre a sospechosos mensajes de correo.

A modo de conclusión

El cortafuegos de Windows incluido en el Service Pack 2 de XP provee una protección mejorada pero muy básica, mientras que Outpost Firewall Pro le ofrece un verdadero arsenal de herramientas para proteger sus datos, su ordenador y su privacidad, siendo 100% seguro y muy fácil de usar.

Descargue la [versión de evaluación de Outpost Firewall Pro totalmente funcional y acceda](#) a la mejor protección para su ordenador y sus datos.

¡Pruebe Outpost Firewall y no lo abandonará jamás!