

## Consultas frecuentes sobre Outpost Firewall Pro 3.5

### Introducción

Después del lanzamiento de Outpost Firewall Pro 3.5, recibimos muchas consultas de parte de los usuarios acerca del programa y su evolución en el futuro.

Nuestro arquitecto en jefe de aplicaciones, Alexey Belkin, accedió a responder las preguntas más comunes que han efectuado los usuarios.

### Consultas frecuentes

#### ¿Por qué debo actualizar a Outpost Firewall Pro 3.5?

La nueva versión, particularmente con la aplicación automática de reglas de acceso para programas conocidos, disminuye, de manera significativa, la cantidad de mensajes que el usuario recibirá.

Esto hace que el programa sea más práctico de utilizar.

Hay muchos menos pedidos de confirmaciones acerca de cómo tratar los pedidos de comunicaciones de aplicaciones.

Además, la capacidad para actualizar las reglas automáticamente permite a Outpost Firewall Pro 3.5 administrar mejor el manejo de las vulnerabilidades existentes de terceros, antes que el proveedor pueda generar actualizaciones de seguridad, lo que se denomina protección de hora cero.

Esta nueva versión también incluye más refuerzos de seguridad y brinda más seguridad que antes.

#### ¿Cuán seguro es Outpost Firewall Pro 3.5?

Esta nueva versión es más segura que la anterior.

Por ejemplo, si se detecta un error en las reglas existentes del cortafuegos, podemos arreglarla y distribuir una actualización casi inmediatamente a través de la infraestructura de ImproveNet.

Es común que ocurran errores en las reglas y, en versiones anteriores, solamente podíamos tratarlos generando una actualización y esperando que los usuarios la instalaran oportunamente.

Ahora, podemos hacer esa actualización de manera automática, simplemente distribuyendo nuevos grupos de reglas para la aplicación.

#### ¿Ha aprobado Outpost Firewall Pro 3.5 todas las pruebas de fuga?

Una prueba de fuga independiente (puede obtener información acerca de ella en <http://www.firewallleaktester.com/>) demostró que la seguridad del producto continúa en su alto nivel inicial.

En la próxima versión, nos concentraremos en incrementar aún más los niveles de seguridad, pero sin hacer que el producto sea difícil de usar.

#### ¿Cuán seguras son las reglas automáticas?

Gracias a la tecnología ImproveNet, nos enteramos no solamente de las reglas que faltan en las configuraciones de los usuarios, y las preguntas que realiza la instalación de Outpost Firewall Pro 3.5, sino también aprendemos acerca de los intentos para evitar la protección.

Basándose en informes posteriores al lanzamiento de la nueva versión 3.5, podemos ver que los grupos de reglas son, en general, mucho más seguros.

Si bien la configuración anterior estaba compuesta de una gran cantidad de grupos de reglas, de las cuales solamente unas pocas estaban siendo utilizadas, lo que podría causar algunos problemas de rendimiento, ahora las reglas se aplican solamente cuando son necesarias.

Las configuraciones de los usuarios están compuestas únicamente de las reglas realmente necesarias. Y si los usuarios instalan Outpost Firewall Pro 3.5, con una configuración bien definida y se activa la aplicación automática de reglas, se crean grupos de reglas específicamente para los requerimientos de su sistema. Por lo tanto, la aplicación automática puede interrumpirse después de uno o dos días, porque los grupos de reglas necesarios ya habrán sido creados.

Los usuarios pueden entonces modificar esas reglas utilizando las alertas del asistente para reglas si lo desean, pero no es realmente necesario.

Me gustaría mencionar una característica en la versión 3.5 que se pasa ampliamente por alto: la capacidad de los usuarios para realizar descargas en forma regular de nuevos grupos de reglas. Incluso si los usuarios desactivan la aplicación automática de reglas, le resultará útil actualizar los grupos de reglas con cierta frecuencia, para permitir, que las configuraciones actualizadas del asistente de reglas se encarguen de las actualizaciones en las aplicaciones instaladas. Ahora existe una serie de reglas deliberadamente más estrictas debido a la aplicación automática.

#### **¿Por qué quitaron la posibilidad de modificar los grupos de reglas en la versión 3.5?**

El nuevo formato de los grupos de reglas exige un conocimiento técnico significativamente mayor, de parte del usuario final, para poder llevar a cabo esas modificaciones, lo que también va en contra de nuestra misión de hacer que la seguridad en Internet sea fácil de utilizar.

Además, la tecnología ImproveNet considera la personalización de los grupos de reglas para sistemas individuales, como completamente innecesario.

Este aspecto se desarrollará aún más en la próxima versión.

Por supuesto, los usuarios aún pueden modificar las configuraciones por medio de la interfaz del programa, sin realizar cambios en los archivos internos, los que no están diseñados para tal fin.

#### **¿Es cierto que Outpost Firewall Pro 3.5 funciona más lento que antes y hace un uso más intensivo del procesador?**

Sí, esto es cierto si se compara la versión 3.0 y 3.5 con versiones anteriores.

El motivo fundamental es la introducción de la protección contra programas espía en tiempo real.

El control del tráfico en tiempo real utiliza más potencia de procesamiento, este es así para todos los programas.

Los usuarios que realmente están preocupados con esto pueden desactivar el control de programas espía en tiempo real; en la versión 3.5 incluso es posible hacerlo sin sacrificar la seguridad, porque el programa ofrece la capacidad de verificar aplicaciones para buscar programas espía cuando se solicita acceso a la red por primera vez, o si estas aplicaciones comienzan a comportarse como un programa espía.

Vale la pena mencionar, sin embargo, que también pueden generarse algunas situaciones de alto consumo de potencia de procesamiento al aplicar reglas incorrectas para ciertas configuraciones de acceso al sistema.

#### **¿Cuáles son los planes para mejorar aún más la seguridad en el futuro?**

Nuestro objetivo constante es cerrar todas los caminos, actualmente conocidos, para evitar la protección del cortafuegos en forma local, que son las llamadas pruebas de fuga.

Gracias a cambios significativos que se implementaron en la versión 3.5, así como también a la tecnología ImproveNet, esto puede lograrse con solo incrementar un poco la cantidad de mensajes al usuario durante la configuración inicial.

También es posible observar una reducción gradual en la cantidad de alertas a medida que la base de datos de ImproveNet se amplía.

Esto también se aplica a la base de aplicaciones legítimas que pueden utilizar tecnología riesgosa para integrar código.

También agregaremos funcionalidad que nos permitirá determinar la autenticidad de una aplicación en un 100%.

Esto también nos ayudará a crear grupos de reglas más estrictos.

#### **¿Cuál es el futuro de Outpost Firewall?**

Si bien Windows Vista no será presentando hasta el año que viene, continuamos probando el controlador para x64 de forma tal de estar listos cuando Microsoft realice el lanzamiento.

Una de las principales prioridades es la creación de protección proactiva, que resultará en un mejor rendimiento del sistema e incluso una mejor protección contra código malicioso más fuerte.

Nuestra intención en ese sentido es lanzar en forma simultánea la versión x64 y x86 de esa protección.

## Acerca de Alexey Belkin

Alexey es arquitecto en jefe de aplicaciones de Agnitum, y se ha desempeñado en este puesto durante más de dos años.

Las principales responsabilidades de su puesto son: diseño de arquitectura de aplicaciones de alto nivel, creación de interfaces de usuario, diseño de especificaciones funcionales para los productos de la empresa.

Alexey es especialista en interconexión de redes de Windows y cuenta con numerosas certificaciones como por ejemplo: *Oracle Certified Professional (OCP)*, *Microsoft Certified Solution Developer (MCSD)* y *Microsoft Certified Database Administrator (MSDBA)*.