

La importancia, en los cortafuegos, de los filtros de tráfico saliente

En este artículo, aprenderemos la importancia que tiene en una protección cortafuegos, la existencia de un filtro sólido para las conexiones salientes.

En un interesante artículo publicado recientemente, los ejecutivos *Senior* de seguridad de Microsoft, compartieron sus puntos de vista acerca de la moderna seguridad de Windows. Con el nombre de **Develando mitos comunes de la seguridad**, el [documento](#) brinda una mirada, por momentos curiosa, sobre los puntos candentes de esta temática.

Entre los diversos puntos mencionados, el autor afirma que el usuario promedio conectado a Internet no necesita, en un cortafuegos, filtros para los datos salientes. Una perspectiva que muchas personas objetarían y que nos llevó a escribir nuestro propio artículo.

El reciente ingreso de Microsoft al mercado de la seguridad para el usuario final, con su servicio *OneCare*, además del futuro lanzamiento de Windows Vista, de próxima generación, previsto para el primer trimestre del próximo año, prometen una gran variedad de mejoras en la seguridad, sin embargo, [sin activar la protección de tráfico saliente](#).

Un momento. ¿No es esto lo mismo que sucedió con el [cortafuegos incorporado de Windows XP](#), que carece exactamente de la misma funcionalidad que se excluye esta vez? Probablemente, sí.

Analizando los argumentos

- **El filtro de tráfico saliente no es necesario.**
El objetivo del cortafuegos es protegerlo contra las amenazas del mundo, no proteger al resto del mundo de su actividad

Este argumento es básicamente erróneo: el objetivo de un cortafuegos es brindar una protección integral contra las amenazas, tanto entrantes como salientes.

Si solamente se utilizara protección de tráfico entrante (aún cuando usted esté protegido contra los ataques a través de Internet que sean efectuados directamente contra su ordenador) cualquier programa, incluyendo algunos nefastos (virus, programas espía y conexiones simplemente innecesarias) puede comunicar datos desde su ordenador sin restricciones, y hacia afuera.

Esta es una situación grave dado que su información personal, conocimiento del negocio u otra información crítica puede ser tomada de su ordenador, evitando los filtros del cortafuegos.

Los antivirus, aplicaciones contra programas espía u otras soluciones que dependen de una firma no pueden detener tales intentos. Esto se debe a que los proveedores todavía no han logrado el 100% de efectividad en la determinación de una huella dactilar adecuada para identificar la presencia de un virus o instancia de un programa espía.

A menudo, el proceso de desarrollo de la industria de la seguridad moderna está muy por detrás de los desarrolladores de código malicioso.

Un ejemplo reciente ocurre [aquí](#), con la vulnerabilidad, que todavía no ha sido corregida, en Microsoft Office, donde se utiliza Word para comprometer a los ordenadores en todo el mundo.

Los usuarios deben ampliar su perspectiva. ¿Cuál es realmente su miedo en Internet?

¿Es un ataque remoto nunca visible del exterior o la posibilidad que algo almacenado en su equipo de manera secreta llegue a manos de piratas?

Si bien no existe una respuesta universal, un buen cortafuegos debe brindar una respuesta simple. Debe proteger a su ordenador contra cualquier tipo de amenaza en Internet, sin importar la dirección. **¡Esta es la base del diseño de cualquier cortafuegos serio!**

- **El filtro de tráfico saliente en un cortafuegos, es demasiado técnico para que los usuarios comunes lo entiendan y apliquen.**

Con algunos cortafuegos, el argumento anterior puede ser cierto, especialmente cuando muchas aplicaciones habilitadas para Internet requieren un acceso saliente para enviar datos (su correo electrónico o programa de mensajería instantánea).

Para el usuario común, la decisión de permitir o rechazar un tipo de conexión en particular puede ser difícil.

Para aliviar esta situación, se han implementado algunas ayudas especiales para asistir al usuario a configurar correctamente su protección de tráfico saliente.

Outpost Firewall Pro, en su última versión, cuenta con el [sistema ImproveNet](#) que aprovecha al máximo la configuración automática del cortafuegos, evitándoles a los usuarios la necesidad de configurarlo por sí solos. Además, los conjuntos de reglas predefinidas para acceso a aplicaciones y la herramienta *Smart Advisor* ayudan a los usuarios en sus decisiones, brindando consejos y recomendaciones en tiempo real.

- **Los programas maliciosos utilizan técnicas sofisticadas para funcionar. Muy rara vez se arriesgan sin esconderse.**

Sí, este argumento puede ser cierto.

Los programas maliciosos no actúan como tales, sino que se esconden en programas legítimos y tratan de engañar al cortafuegos para que crea que un programa inofensivo desea acceso saliente.

En la práctica, un programa malicioso inyecta su código en una aplicación confiable, como por ejemplo el navegador *Internet Explorer*, y esto sería visto por un cortafuegos simple como que esta aplicación desea acceso. En realidad, el navegador ha sido secuestrado y es controlado por la aplicación intrusa.

Un cortafuegos integral debería detectar ese truco y evitar que una aplicación inofensiva, que contenga código malicioso, acceda a Internet y comprometa la integridad de la información.

Las pruebas de fuga, programas que simulan intentos de código malicioso para enviar información confidencial, sirven para demostrar que un cortafuegos que protege solamente el tráfico entrante no sirve para defenderlo de los intentos de robarle información.

- **Los cortafuegos ya son de por sí, molestos, y los cuadros emergentes relacionados con la protección de tráfico saliente harían que el trabajo se torne intolerable**

Este argumento contiene una falla.

Cuando un cortafuegos ha sido configurado y utilizado durante algunos días, la cantidad de mensajes se reducirá notablemente hasta que dejen de ser molestos.

En un ordenador conectado a Internet se desarrolla mucha actividad y, un cortafuegos, debería poder reconocer las acciones adecuadas, es por eso que realiza preguntas.

La clave aquí está en que el cortafuegos no confunda al usuario con sus preguntas. Si está informado y tiene conocimiento, el usuario puede responder casi cualquier pregunta del mismo.

Conclusión

Detallamos brevemente la importancia y los beneficios de la protección de tráfico saliente en un cortafuegos, sobre todo, que lo que se estará impidiendo, es nada más ni nada menos, que la fuga de su información privada y personal.