

¿Por qué necesito un cortafuegos?



Outpost Firewall

¿Por qué necesito un cortafuegos?

¿Qué sucede con su ordenador mientras está en línea?_ 3

Distintas amenazas _____ 4

Es hora de prevenir _____ 6

¿Por qué necesito un cortafuegos?

¿Qué sucede con su ordenador mientras está en línea?

Haga lo que haga en Internet, todo es comunicación.

No se sorprenda: incluso si usted no está conversando con sus amigos o utilizando mensajeros instantáneos, su ordenador igual se está comunicando activamente.

Usualmente usted no ve esto y probablemente le costará entender la forma en que los ordenadores "hablan" en su mundo, ya que estos tienen su propio lenguaje, pero se puede intentar una comparación muy simple que le permitirá aproximarse al "mundo" de los ordenadores:

La gente utiliza palabras para intercambiar información, en cambio, los ordenadores utilizan datos en forma de ceros y unos agrupados en entidades denominadas bytes.

Lo que es una oración para nosotros, es un paquete de bytes de datos para su ordenador.

La gente habla diferentes idiomas, mientras que los ordenadores "hablan" paquetes especiales de bytes bajo la forma de sistemas de datos codificados según normas específicas y a los que se denomina protocolos.

Para que su ordenador pueda estar en línea, debe intercambiar múltiples paquetes de datos bajo diferentes protocolos al mismo tiempo.

La gente tiene boca para hablar y oídos para escuchar, mientras que los ordenadores poseen los denominados "puertos", que son "puertas" virtuales a través de las cuales la información es enviada y recibida y, de esa particular forma, pueden "oir" y "hablar".

Distintas amenazas

Sin embargo, la gente puede decidir que decir o escuchar y estar en silencio o prestar atención en situaciones particulares, en cambio, los ordenadores no pueden.

Windows y las aplicaciones abren ciertos puertos para poder enviar y recibir información por la red.

El problema, es que esto, permite que el ordenador pueda ser atacado o que la información pueda ser accedida por personas no autorizadas.

Un ordenador desprotegido en el mundo de Internet es incluso más vulnerable que un turista perdido en un país en el cual jamás antes había estado y en el cual no maneja el idioma principal.

El ordenador no puede defenderse de los intrusos e irse después.

Con excepción de los paquetes de datos inofensivos (protocolos legítimos y paquetes de datos específicos) el mundo de Internet tiene sus propias amenazas, como cualquier frontera.

Un ordenador desprotegido podría ser un blanco atractivo para:

- **Virus**

Programas o trozos de código que "infectan" uno o más programas insertando en ellos sus propias instrucciones.

Básicamente, los programas "se enferman" y empiezan a actuar de una manera extraña y en algunos casos, pueden provocar la caída del sistema.

- **Gusanos**

Programas maliciosos que se propagan por redes.

Los gusanos causan los mismos efectos que los virus, pero son más peligrosos, ya que son capaces de replicarse y diseminarse por ellos mismos.

- **Análisis de puertos**

Los *Hackers* (personas malintencionadas y con suficientes conocimientos, que intentan descubrir información sensible en sistemas vulnerables) buscan la existencia de puertos abiertos en su ordenador.

Si su ordenador responde a un puerto abierto, un *Hacker* puede enviar e instalar sin su consentimiento un virus o un gusano u otro tipo de código malicioso.

- **Cookies**

Pequeños archivos de datos que poseen información personal que usted haya introducido en algún formulario o página de Internet.

Por ejemplo, si usted ingresa el número de su tarjeta de crédito, una cookie almacena su número para que usted no tenga que volver a introducirlo.

Esto no es una mala idea, siempre que nadie quiera usar sus datos para fines distintos de los originalmente planteados.

- **Troyanos**

Programas que aparentando ser legítimos, sin embargo, realizan acciones no deseadas en el sistema.

Esta categoría de códigos maliciosos recibe este nombre por el caballo de madera que los griegos le dieron a los troyanos como un supuesto "regalo" inofensivo, y muchas veces, los usuarios creen que un programa puede tener características muy interesantes para justificar su descarga e instalación y reciben "de regalo" un troyano con fines no legítimos.

Una vez que el mismo es ejecutado por el usuario, e instalado (obviamente, sin su conocimiento real sobre las consecuencias) los troyanos, pueden abrir canales de acceso remoto a los *Hackers*, robar datos confidenciales como números de tarjetas de créditos o contraseñas, e incluso, destruir los archivos del disco duro.

Los troyanos pueden tener un comportamiento similar a los virus, pero no se diseminan por sí mismos.

- **Ataques de Denegación de Servicios (DoS)**

Este tipo de ataque ocurre cuando un atacante envía una gran cantidad de paquetes a un puerto abierto en su ordenador.

Como consecuencia, el puerto es incapaz de aceptar toda la información, los recursos del sistema se agotan y el sistema se cae, dando como resultado, la denegación del servicio.

- **Spyware o programas espía**

Estos programas obtienen información acerca suyo y de sus intereses, sin su consentimiento: hábitos de navegación, programas instalados, etc.

Los programas espía son utilizados con frecuencia por empresas, con propósitos netamente de mercadeo.

¡Es hora de prevenir!

Todos estos peligros, causan grandes problemas.

Por ejemplo, la epidemia del gusano Mydoom, ha provocado una pérdida cercana a los \$2,3 billones de euros con más de 400.000 ordenadores infectados en todo el mundo. El gusano Sasser, bloqueó el sistema de ordenadores del aeropuerto de Heathrow e invadió el sistema de correo de Alemania.

Cuando los sistemas informáticos se caen, la información personal puede ser perdida, incluso para siempre.

Sin embargo, muchos de estos problemas pueden evitarse si se considera el uso de una simple solución de protección:

- **¿Antivirus?**

Sí y no.

Sólo piense en proteger una casa en un barrio peligroso.

Usted no sólo pondría un guardia de seguridad para protegerse de los ladrones: usted también instalaría rejas alrededor de su casa.

En Internet, la cosa no es diferente.

Para propósitos defensivos, usted necesita un cortafuegos, que es un programa especial que evita que usuarios no autorizados tengan acceso a su ordenador para transferir información del mismo.

El trabajo que desempeña un cortafuegos es similar al de una pared que evita que el fuego siga extendiéndose de un lugar hacia otro.

Si un paquete entrante es detectado como peligroso por el cortafuegos, el paquete es inmediatamente bloqueado.

Por lo tanto, cualquier cortafuegos debería realizar las siguientes funciones:

- Proveer seguridad a sus comunicaciones haciendo que su ordenador sea invisible a cualquier atacante remoto.
Usted simplemente elige el modo de operación (invisible) y sus puertos no responderán a un análisis de puertos o ataques DoS, sin embargo aún así, los hackers podrán seguir obteniendo información confidencial.
- Evitar la fuga o robo de información protegiendo su privacidad al bloquear *Cookies* y referencias así como impedir los intentos de los programas espía de enviar información hacia el exterior de su ordenador.
- En cuanto a los troyanos, el cortafuegos debería cambiar el nombre de los archivos adjuntos provenientes del correo electrónico, evitando de esta forma que el usuario los ejecute ocasionalmente.
- El cortafuegos además, debe poseer control de aplicaciones y de la actividad de red.

Así, el cortafuegos garantizará que todas las aplicaciones estén ejecutando conexiones legítimas y bloqueará los puertos sensibles por donde pudiera enviarse información privada.

- Básicamente, esto hará que los *Hackers* "hablen" con un cortafuegos blindado.

Y esto es exactamente lo que usted necesita.

Outpost es el cortafuegos que le brinda una protección sólida. Outpost protege su ordenador contra robo de información, ataques de denegación de servicios, violación a su privacidad, troyanos, *Spyware* y más, mucho más.

Outpost además posee como características adicionales: bloqueo de contenido, bloqueo de contenido activo, bloqueo de publicidad, bloqueo de archivos adjuntos, caché DNS y visor de registros.

Outpost Firewall Pro no es un cortafuegos más, Outpost Firewall Pro es el cortafuegos que usted necesita.

Outpost Firewall Pro es el cortafuegos que usted siempre estuvo esperando.

¡Pruebe Outpost Firewall Pro y no lo abandonará jamás!



Traducción y adaptación al español:
Ontinet.com, S.L.