

Guía para el principiante de Outpost Network Security

Introducción

Esta guía está enfocada a usuarios principiantes y trata sobre asuntos básicos de Internet, así como también una introducción al cortafuegos Outpost Network Security Client.

☑ Consulte el [Glosario en línea](#) para mayor información.

Comenzando por lo básico

Información elemental sobre redes

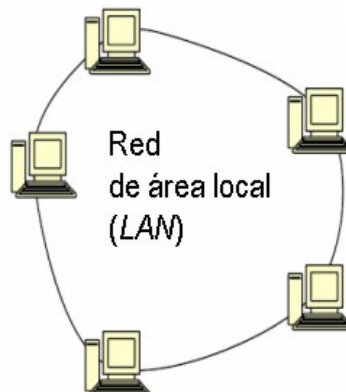
Una red está compuesta por dos o más ordenadores conectados entre sí, para que de esta manera, los ficheros puedan ser compartidos y/o accedidos desde uno u otro ordenador.

La red más simple es la de tipo **LAN** (*Local Area Network*, Red de área local).

Los ordenadores pertenecientes a una red de área local están ubicados en la misma oficina o edificio.

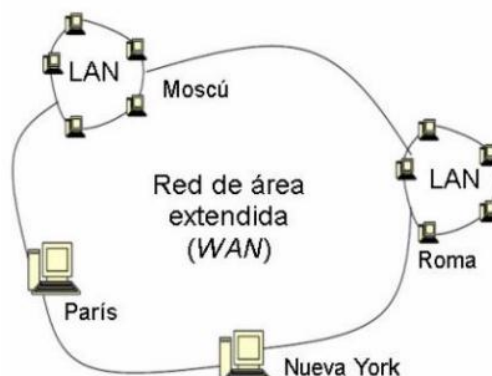
Una red de área local puede tener virtualmente cualquier cantidad de ordenadores.

Cuando conecta dos ordenadores en su oficina o en su casa, usted está haciendo una red LAN.



Cuando los ordenadores están conectados entre sí, pero se encuentran en distintas ubicaciones físicas, la red es denominada **WAN** (*Wide Area Network*, Red de área extendida).

Las redes **WAN** pueden estar compuestas por diferentes ordenadores independientes y/o distintas redes LAN.



Como funciona Internet

Internet es una red de redes.

Existen dos tipos fundamentales de ordenadores en Internet: **servidores** y **clientes**.

Un **ordenador servidor** (denominado **Host** en inglés) es un ordenador configurado especialmente para compartir sus archivos permitiendo que los mismos estén disponibles para ser abiertos o descargados por ordenadores clientes.

Un **ordenador cliente** es cualquier dispositivo apropiado que se utiliza para acceder a Internet: ordenadores de escritorio, ordenadores portátiles, dispositivos móviles, etc.

Los archivos que están almacenados en el ordenador servidor y que son accedidos desde el ordenador cliente, pueden ser tanto páginas Web, videos, como sonidos e imágenes entre otros.

Para que su ordenador, tanto en su hogar como en su oficina, pueda recibir cualquier tipo de dato desde un servidor, deberá solicitarle a este ordenador servidor dicha información.

Y esto sucede cada vez que usted ingresa una **URL** (*Uniform Resource Locator*, dirección de una página Web) en su navegador, o cuando recibe o envía un correo electrónico, entre otras muchas posibilidades.

Cualquier ordenador puede ser configurado como un cliente o un servidor y, de hecho, cuando usted "solicita" información también está "enviando" cierto tipo de datos.

Sin las precauciones necesarias, cualquiera puede acceder a sus ficheros cuando su ordenador está conectado a Internet.

Este es el principal motivo por el cual se debe usar un cortafuegos.

Un cortafuegos es una simple forma de proteger su ordenador evitando que se exponga su información a cualquiera en Internet y sin su consentimiento.

Existen muchos tipos de cortafuegos y todos poseen características particulares.

Como sucede con la mayoría de los programas, los más poderosos cortafuegos por *software* (como una aplicación más instalada en su ordenador) son los más difíciles de utilizar, con la única excepción de Outpost Firewall, que ha sido diseñado para ser el más poderoso y a su vez, más simple de usar.

Los peligros de Internet

Todos hemos escuchado de los peligros de Internet y el ciberespacio y aunque mucho de lo escuchado, es exagerado, no es menos cierto que un ordenador conectado a una red tan grande y diversa como es Internet, es realmente susceptible de ser atacada con diversos fines.

Desafortunadamente, existen criminales y gente perversa (muchas veces, ambas características en una sola persona) que disfrutan haciéndole la vida difícil a los demás.

Muchos de estos criminales poseen los conocimientos necesarios para acceder, de forma remota, a los ficheros de un ordenador desprotegido.

A estas personas se les denomina *hackers* o *crackers*.

Para mantener nuestros ordenadores protegidos, necesitamos poseer un cortafuegos sólido.

Estas son las amenazas más difundidas:

- **Aplicaciones no autorizadas** que pueden ser ejecutadas desde su ordenador sin su consentimiento explícito, como por ejemplo: objetos ActiveX o aplicaciones Java embebidas en sitios Web a los cuales usted está accediendo.
Esos programas, construidos maliciosamente, pueden llevar a cabo cualquier acción en su ordenador, desde transferir archivos personales hasta eliminar ficheros de sus discos rígidos.
- **Si su sistema no está configurado correctamente**, otros ordenadores podrían acceder a su ordenador de forma directa llegando a ejecutar cualquier aplicación del mismo.
- Alguna información personal o privada, bajo la forma de **cookies*** o **referencias***, puede ser almacenada en su ordenador, y de ese modo, gente maliciosa puede obtener datos de las páginas visitadas o incluso sus intereses.

📄 **Cookies:** Es un archivo con una pequeña porción de información que es transferida desde un servidor hacia el navegador del visitante, siendo guardado en el disco duro del ordenador cliente durante un tiempo variable, que puede oscilar entre una sesión abierta y un plazo extendido.

En ciertas circunstancias, dicha información, puede ser enviada al servidor de origen. Habitualmente, es usada para individualizar las preferencias de navegación del usuario.

📄 **Referencia (*Referrer*, también llamado Remitente)** es parte de una petición HTTP que contiene la URL de la última página visitada antes del envío de dicha petición.

- Los **troyanos*** pueden ser instalados en su ordenador sin que usted lo sepa.

Los troyanos son programas usados por *hackers** y *crackers** para abrir puertas en su ordenador hacia información privada, como contraseñas, datos bancarios o números de tarjetas de crédito.

La diferencia fundamental entre un troyano y un virus es que los virus se ejecutan de forma autónoma, mientras que los troyanos son construidos para ser utilizados de forma directa por intrusos.

📄 **Troyano:** Es un programa instalado subrepticamente en un ordenador, desde el cual se establece una conexión no autorizada hacia un atacante remoto.

El troyano ejecuta acciones según las instrucciones que arriban desde el ordenador atacante, así como puede transmitir automáticamente información hacia otros equipos, siendo habitual el envío de contraseñas y otros datos confidenciales guardados en el ordenados atacado.

📄 **Hacker, Cracker.** Con ligeras variantes es la denominación que se le da al individuo que logra obtener acceso no autorizado a un ordenador

- Los **gusanos de Internet** pueden llegar a su ordenador por medio de ficheros adjuntos en mensajes de correo electrónico.

Algunos clientes de correo electrónico ejecutan los archivos adjuntos automáticamente y sin su consentimiento. Así como también, algunos usuarios no concientes de los peligros de Internet, ejecutan todos los ficheros adjuntos de forma manual y, una vez instalado, el gusano infecta su sistema rápidamente.

- Las **imágenes publicitarias (*Banners*)** y otros anuncios de propaganda, utilizan su ancho de banda.

A pesar que las imágenes publicitarias no representan ningún riesgo para su información, éstas pueden provocar que su conexión funcione más lenta, sobre todo si es efectuada a través de módem telefónico.

- Los **programas espía (*Spyware*)** son similares en varios aspectos a los troyanos.

Estos programas obtienen información suya y sobre sus intereses (hábitos de navegación, programas instalados, etc.) sin su consentimiento.

Los programas espía son utilizados por compañías con fines netamente comerciales.

Introducción a Outpost Firewall

Requerimientos de sistema

Requisitos mínimos que debe cumplir su sistema para poder utilizar **Outpost Network Security Client** :

- Windows 98 / 98SE / ME / 2000 /XP / 2003 Server
- Intel Pentium o compatible. 450 MHz o superior
- 50 MB espacio libre en disco duro
- 64 MB RAM para Windows 98 / Me
128 MB RAM para Windows 2000 / XP / 2003 Server

⚠ **Importante:** No es necesario ningún tipo especial de adaptador o conexión de red para el normal funcionamiento de esta aplicación.

Características de Outpost Firewall

Outpost Network Security Client es una avanzada aplicación cortafuegos que le brinda una protección sólida con una interfaz sencilla de usar.

Para utilizar Outpost de manera efectiva, no es necesario poseer ningún conocimiento especial, ya que, nuestros ingenieros configuraron, de forma predeterminada, las opciones que usted seguramente necesitará.

Y si bien estos valores satisfacen a la gran mayoría de los usuarios, usted podrá cambiar cualquiera de esas opciones cuando lo estime conveniente.

📄 Para mayor información sobre como configurar Outpost Firewall, por favor, consulte el Manual del usuario de Outpost.

Una de las características más potentes y que distinguen a Outpost Firewall, es su organización modular, organizada en elementos denominados **complementos o Plug-Ins**, que permiten mejorar las prestaciones de forma individual e incluso, que los usuarios desarrollen sus propios complementos para adecuarlos a sus particulares requerimientos. Cada módulo (con extensión .OFP) es independiente y puede ser agregado muy sencillamente.

Principales beneficios que le brinda la instalación de Outpost Firewall

- Outpost Firewall lo protege de una gran cantidad de amenazas a la seguridad, su privacidad y contra vulnerabilidades.
- Comienza a utilizarse inmediatamente después de su instalación y sin requerir ninguna intervención por parte del usuario.
- La utilización del asistente de configuración le otorgará la mejor protección en pocos minutos y de forma automática, o podrá crear manualmente políticas de seguridad para sus particulares requerimientos de seguridad y sin interrumpir su trabajo.
- La interfaz del usuario permite modificar complicados aspectos de la configuración con sólo unas pocas pulsaciones del ratón.
- Outpost Firewall tiene soporte para 7 idiomas.

Algunas de las principales fortalezas de Outpost Firewall

- Posee diversas opciones para restringir el acceso a la red hacia su ordenador o desde sus aplicaciones. Los usuarios avanzados pueden ajustar las reglas para diversos protocolos de servicio y crear especiales condiciones de seguridad cuando sea necesario.
- El módulo integrado anti-espía provee una protección superior de su privacidad salvaguardando su ordenador contra la instalación de programas espía e impidiendo la activación de los mismos o la transmisión de información, así como una posible reinstalación. Asimismo, permite establecer una lista de datos sensibles asignándoles un bloqueo total y permanente evitando la fuga de los mismos.
- El modo Invisible hace que su ordenador permanezca oculto a los *hackers* mientras navega por Internet.
- La estructura modular del cortafuegos le permitirá agregar nuevos esquemas de protección bajo la forma de complementos (*Plug-Ins*).
- Outpost Firewall es compatible con todas las versiones de Windows 98 / 98SE/ ME / 2000 / XP y 2003 Server.
- Mínima utilización de recursos del sistema.
- Es posible restringir la lista de aplicaciones que pueden acceder a Internet y especificar los protocolos y puertos que serán permitidos, como también, establecer la dirección del tráfico para cada aplicación (entrante o saliente).
- Bloqueo de información no solicitada enviada a su ordenador, en particular:
 - Imágenes publicitarias (*Banners*).
 - Publicidad en sitios de Internet.
 - Contenidos cuestionables de páginas específicas de Internet.
- Restricción y/o denegación de acciones maliciosas por contenidos de Internet como aplicaciones Java, guiones ActiveX y JavaScript.
- Restricción y/o denegación de *cookies*.

- Es posible especificar una lista de direcciones IP seguras o sitios de confianza, como por ejemplo, su propia red de área local.
Las direcciones IP que estén en esta lista, no serán controladas o restringidas por Outpost Firewall.
- Posibilidad de cambiar la extensión de los archivos adjuntos en mensajes de correo y, de esa forma, establecer una virtual cuarentena que impida su ejecución, protegiéndolo de gusanos provenientes de Internet.
- Emisión de alertas al detectarse cualquier indicio de violación de la seguridad o intento de intrusión en su sistema, efectuando además, el bloqueo instantáneo del atacante.
- Bloqueo de todas las pruebas conocidas de fuga de información (*Leak Test*).

Soporte Técnico

Para cualquier consulta adicional sobre Outpost Network Security visite la [página principal de soporte](#), donde encontrará una variedad de recursos y formas de contacto, a su disposición.