El firewall de conexión a Internet

Un firewall de conexión a Internet es un dispositivo lógico o físico que comprueba los datos entrantes o salientes que van o vienen de redes externas como Internet. Así pues, un firewall le permite prevenir los ataques de hackers o programas malintencionados que intenten tomar el control del equipo de una manera u otra. Veamos cómo funciona el firewall de conexión a Internet integrado en Windows Vista. Pero antes, deberemos conocer qué es un puerto y un protocolo.

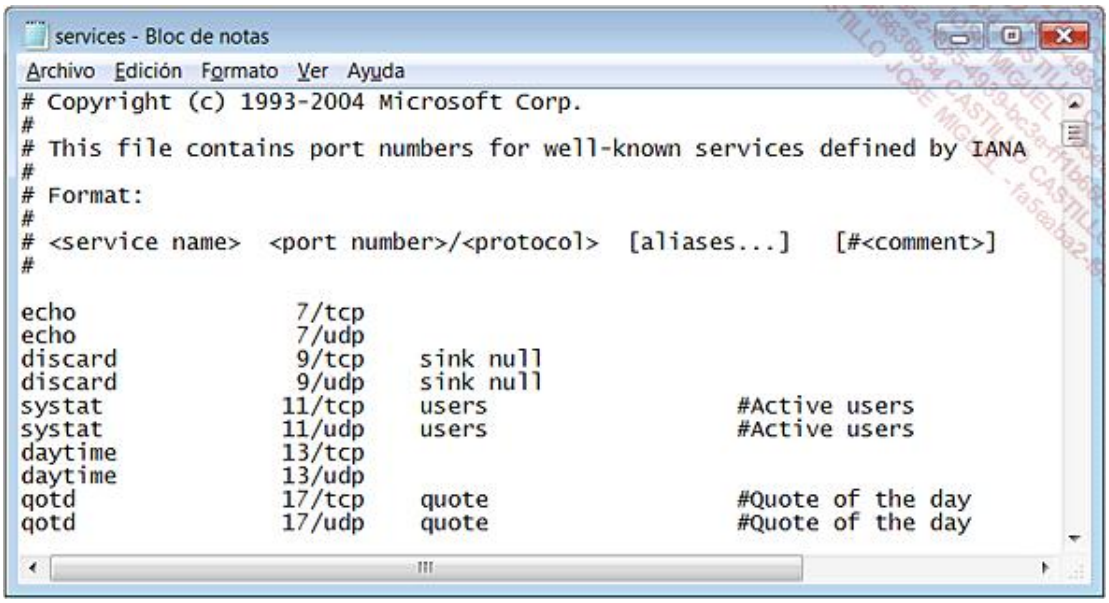
1. Puertos y protocolos de red

Un protocolo de red es un conjunto de reglas para un tipo de comunicación determinado. Los protocolos más conocidos son:

- FTP (*File Transfer Protocol*): se utiliza para el intercambio de archivos en Internet.
- HTTP (*Hypertext Transfer Protocol*): lo utilizan los navegadores Web para conectarse a Internet.
- SMTP (*Simple Mail Transfer Protocol*): sirve para transferir el correo electrónico a los servidores de correo.
- UDP (*User Datagram Protocol*): se trata de un protocolo que Internet utiliza y que forma parte de la capa de transporte de la pila de protocolo TCP/IP.
- TCP (*Transmission Control Protocol*): es un protocolo de control de transmisión de datos al igual que el de UDP.

Cuando una aplicación inicia una conexión entrante o saliente, ésta utiliza un protocolo al que se asocian uno o más puertos. Vamos a explicar este segundo concepto... En programación, un puerto es el nombre que se le atribuye a una conexión de tipo lógica y que un protocolo utiliza. Lo podríamos considerar como una puerta que se queda abierta o cerrada en el sistema operativo. En otras palabras, una aplicación como el navegador de Internet utilizará uno o varios protocolos y uno o varios puertos para comunicarse con el exterior. En orden inverso, una aplicación que se ejecute desde una máquina remota puede necesitar que uno o varios puertos estén abiertos en su equipo para conseguir realizar ciertas tareas como, por ejemplo, la instalación de una actualización.

Para obtener una lista de los puertos que están definidos en su equipo, sólo tendrá que ejecutar el siguiente comando: **%SystemRoot%\system32\drivers\etc\services**, después abra el archivo con un editor de texto como el Bloc de notas de Windows.

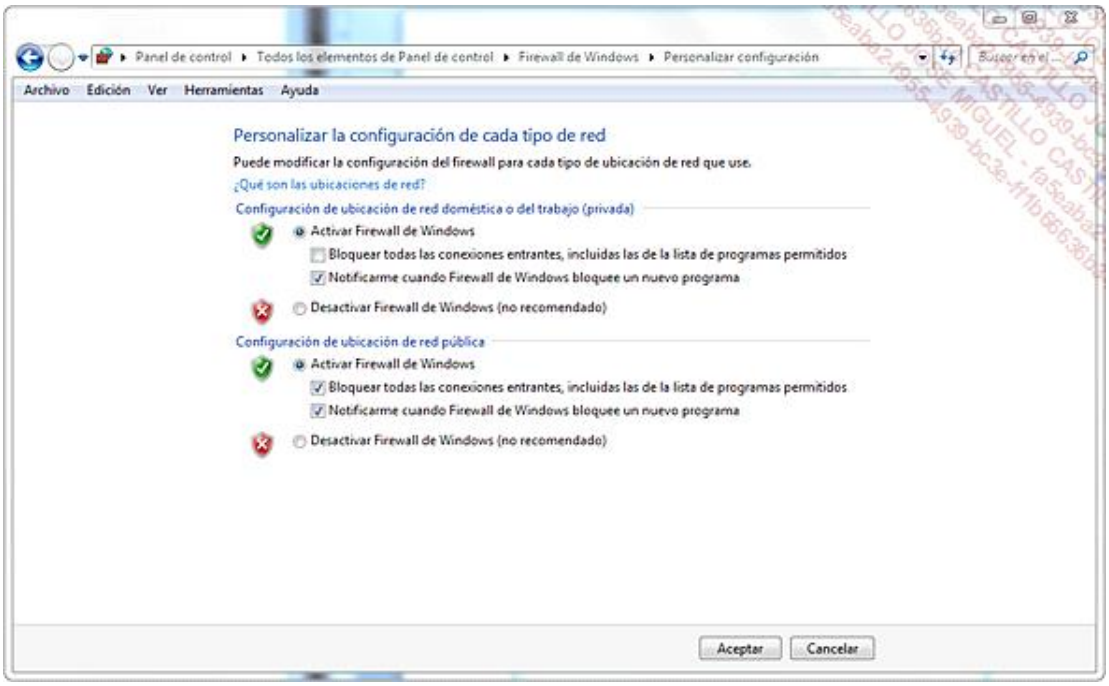


En conclusión, un firewall de conexión a Internet es un programa encargado de limitar las entradas que están abiertas en el sistema para ofrecerle la mayor seguridad posible. De manera predeterminada, un firewall impide cualquier conexión entrante o saliente a menos que se establezcan algunas excepciones. Esto consiste simplemente en crear una regla que, por ejemplo, autorice a una aplicación a abrir un puerto determinado y utilizar tal protocolo. Veamos un ejemplo: usted utiliza el programa Peer-To-Peer eMule y se da cuenta de que la tasa de transferencia es extremadamente lenta. Además, el icono del programa le indica que se le ha asignado una ID baja. Esto ocurre simplemente porque eMule utiliza el puerto 4662 por defecto y, por lo tanto, deberá abrirlo en el firewall de conexión a Internet mediante la creación de una regla para esta aplicación.

2. Configurar el Firewall de Windows

En Windows 7, el firewall está vinculado al tipo de ubicación de red. El firewall está activado por defecto, para las redes domésticas o de empresas y para las redes públicas.

A partir del **Panel de control** en la sección **Sistema y seguridad - Firewall de Windows**, haga clic en la opción **Activar o Desactivar el Firewall de Windows**.



En Windows 8, el panel de control está disponible desde el Escritorio Windows. Para cada tipo de ubicación de red, puede elegir entre tres opciones:

- **Activado**: esta configuración impide que una conexión exterior se conecte con el equipo, con la excepción de los programas que ha especificado en la pestaña **Excepciones**.
- **Bloquear todas las conexiones entrantes**: se ignorarán todas las excepciones que se hayan definido y ningún mensaje le avisará cuando el Firewall de Windows bloquee los programas.
- **Desactivado**: seleccione esta opción si ha instalado un firewall de otro fabricante o si dispone de un router o módem.

3. Administrar las excepciones

Por defecto, sólo se comprueban las conexiones entrantes. Si, por el contrario, uno de sus programas intenta comunicarse con el exterior puede hacerlo sin que se realice ninguna comprobación de los datos transferidos. La razón subyacente consiste en que si el sistema está protegido correctamente a nivel de conexiones entrantes, no

hay necesidad de comprobar las conexiones salientes.

Cuando instale un programa que necesita una conexión entrante, se le añadirá automáticamente a la lista de excepciones. Para autorizar o eliminar una de las excepciones que ya están configuradas, sólo tendrá que marcar o desmarcar la casilla correspondiente.

En Windows 7 y Windows 8, el concepto de excepción no es explícito. Se puede acceder a esta función a través del asistente **Permitir un programa o una característica a través de Firewall de Windows**.

Desde el **Panel de control**, en la sección **Sistema y seguridad - Firewall de Windows**, haga clic en la opción **Permitir un programa o una característica a través de Firewall de Windows**.

En Windows 8, desde la sección **Firewall de Windows** del panel de control, haga clic en **Permitir una aplicación o una característica a través de Firewall de Windows**.

4. Utilización avanzada del Firewall de conexión a Internet

Para acceder a la configuración avanzada de esta herramienta, siga las siguientes instrucciones:

- Haga clic en **Iniciar - Panel de control** y abra el módulo de **Herramientas administrativas**.
- Abra la rama **Firewall de Windows con seguridad avanzada**.

También puede ejecutar directamente este comando: **`wf.msc`**.

Este complemento le permite filtrar las conexiones entrantes y salientes, así como la configuración de IPsec que haya establecido. Debemos recordar que IPsec (*Internet Protocol Security*) es un conjunto de protocolos que le permite realizar intercambios de datos de manera segura en una red. Existen tres perfiles definidos:

- Un perfil de dominio, si el ordenador se conecta a un servidor de dominio de Windows.
- Un perfil privado si se conecta a una red privada.
- Un perfil público si, por ejemplo, se conecta a una red inalámbrica en un aeropuerto u hotel.

Existen tres posibles reglas:

- **Reglas de entrada**: estas reglas se encargan del tráfico entrante al equipo.
- **Reglas de salida**: estas reglas determinan cómo está configurado el tráfico saliente del equipo.
- **Reglas de seguridad de conexión**: se utilizan reglas de autenticación cuando dos equipos se comunican entre sí. Las tecnologías IPsec permiten configurar los intercambios de claves, métodos de autenticación y la comprobación y cifrado de datos.

5. Funcionamiento de las reglas de seguridad avanzadas

Las reglas permiten:

- Autorizar la conexión.
- Autorizar únicamente la conexión mediante la utilización de un protocolo de Internet seguro IPsec.
- Bloquear una conexión.

Puede configurarlas para que sólo afecten a un usuario, equipo, programa, servicio, puerto o protocolo concreto. También puede determinar a qué interfaz de red quiere que se aplique: red local (LAN), conexión inalámbrica, acceso telefónico, etc. Se aplicarán en este orden:

- Reglas de seguridad de conexión.
- Reglas llamadas "de bloqueo".
- Reglas "de permiso".

Un gran número de reglas ya están preestablecidas:

- un pequeño botón gris le señala que la regla no está activa;
- un pequeño botón verde indica que la regla está activa.

Las columnas colocadas en el panel central muestran:

- **Nombre**: el nombre de la regla.
- **Grupo**: el nombre del grupo al que pertenece la regla.
- **Habilitado**: indica si la regla está habilitada o no.
- **Acción**: indica si la regla es una regla de bloqueo o no.
- **Programa**: indica la ubicación y el nombre del archivo ejecutable correspondiente a la regla.
- **Dirección local**: indica la dirección IP en la que se aplica la regla.
- **Dirección remota**: indica la dirección IP o direcciones IP de los equipos remotos relacionadas con esta regla.
- **Protocolo**: indica el protocolo determinado por la regla (TCP o UDP).
- **Puerto local**: indica el número de puerto utilizado localmente por la aplicación de destino.
- **Puerto remoto**: indica los puertos utilizados por los equipos remotos cuando solicitan la aplicación que está establecida.
- **Usuarios y Equipos permitidos**: indica a qué usuarios o equipos les afecta la regla seleccionada.

En Windows 8, encontrará igualmente las siguientes columnas:

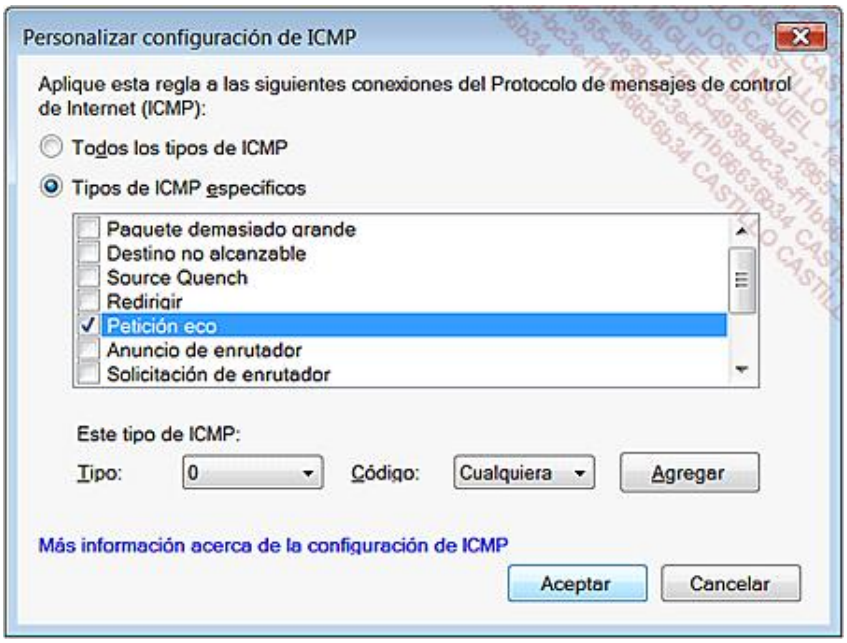
- **Entidades de seguridad locales permitidas**: indica si la regla se aplica a todos o a parte de las entidades de seguridad locales, como por ejemplo los usuarios locales.
- **Propietario de usuarios locales**: indica el propietario de la regla de seguridad. Se aplica en particular a las aplicaciones de Windows 8.
- **Paquete de aplicación**: indica la aplicación Windows 8 para la que se aplica la regla.

Haga doble clic en cada uno de los encabezados de columna si desea filtrar las diferentes listas en función de los valores presentes.

Vamos a observar un ejemplo sencillo: veamos cómo permitir las solicitudes de ping al equipo. Este comando le permitirá enviar una solicitud de eco a otro equipo. Si éste no responde, es posible que los dos equipos no puedan comunicarse entre sí.

→ Haga clic con el botón secundario del ratón en la rama **Reglas de entrada** y en el submenú **Nueva regla...**.

- Seleccione el botón de opción **Personalizada** y haga clic en **Siguiente**.
- Seleccione el botón de opción **Todos los programas** y haga clic en **Siguiente**.
- En la lista desplegable **Tipo de protocolo**, seleccione la opción **ICMPv4** y haga clic en el botón **Personalizar...**.
- Seleccione el botón de opción **Tipos de ICMP específicos** y seleccione la casilla **Petición eco**.



- Haga clic en los botones **Aceptar** y **Siguiente**.
- Si es necesario, determine cuáles son las direcciones IP locales y las direcciones IP de los equipos remotos.
- Haga clic dos veces en **Siguiente**.
- Indique en qué entorno se debe aplicar la regla y haga clic en **Siguiente**.
- Introduzca un nombre y una descripción para la regla y haga clic en **Finalizar**.