CORTAFUEGOS (*FIREWALLS*): QUÉ SON Y PARA QUÉ SIRVEN

Los *firewalls* o cortafuegos son una de las herramientas básicas de la seguridad informática. Permiten controlar las conexiones de red que acepta o emite un dispositivo, ya sean conexiones a través de Internet o de otro sistema.

Existen infinidad de variantes de cortafuegos (dedicados, de tipo *appliance*, gestionados, etc.). Este artículo se centrará exclusivamente en los cortafuegos personales (también conocidos como firewalls) y cómo sacarles el mayor provecho.

Los cortafuegos personales son habitualmente programas que, o bien están integrados en el sistema operativo, o bien son aplicaciones de terceros que pueden ser instaladas en ellos.

I Datos preliminares

Todos los sistemas conectados en una red (y estos entre sí, en Internet) tienen una dirección que los identifica, ya sean ordenadores o servidores. Esto es lo que se conoce como la dirección IP. En la versión actual del protocolo está formada por cuatro grupos de números menores de 256 separados por puntos (por ejemplo: 123.123.123.123). Esta dirección es única para cada uno de los dispositivos conectados directamente a Internet, y permite que sea encontrado a través de los diferentes routers y que pueda comunicarse con cualquier dispositivo también conectado.

A su vez, cada sistema operativo posee unos puertos lógicos. Esto quiere decir que, al contrario que los puertos físicos (USB, HDMI, etc.) solo existen virtualmente para el ordenador. Los sistemas operativos tienen más de 65.000 puertos virtuales disponibles para abrir conexiones y se las ceden a los programas para que vuelquen sus datos en la red. Los programas los solicitan y el sistema operativo los gestiona para poder utilizarlos y establecer una conexión lógica. Esto permite que puedan comunicarse con otro ordenador "punto a punto". Al final, toda comunicación entre dos dispositivos en Internet se traduce en un flujo de datos entre dos puertos virtuales abiertos por algún programa.

Si unimos todo, nos queda que una comunicación en Internet, se establece entre un cliente y un servidor, por ejemplo, de manera similar a la prevista en la tabla siguiente.

Tabla 1: Ejemplo de conexión entre dos sistemas con IPv4[1]

CLIENTE			SERVIDOR		
IP	Programa	Puerto	IP	Programa	Puerto
111.111.111.111	Navegador	5698	222.222.222.222	Servidor Web	80

Fuente: INTECO

En este ejemplo, la comunicación se realiza entre el puerto 5698 del ordenador con IP 111.111.111.111 y el puerto 80 de la máquina 222.222.222.222 y viceversa. Estos puertos dentro del ordenador son reservados temporal o permanentemente por programas como el navegador, el cliente de correo, etc. Cuando se termina la comunicación (por ejemplo cuando se deja de visitar una web o se cierra una aplicación) los puertos del sistema que ha iniciado la comunicación quedan disponibles para ser usados por otro programa que se lo solicite al sistema operativo. Aunque en el ejemplo se utilicen el navegador y el servidor web, este tipo de conexiones se establecen entre todos los programas que utilicen conexión a Internet: cliente de correo hacia su servidor, sistema operativo hacia su servidor de actualizaciones, etc.

Clientes y servidores

Los programas que comienzan la comunicación en un puerto se llaman "clientes" y los programas que están siempre usando un puerto esperando que los clientes se conecten a él, se llaman "servidores".

Por ejemplo, una página web, está siempre esperando que un cliente (el navegador) se conecte para mostrarle su contenido. El servidor web suele utilizar permanente el puerto 80 para esperar conexiones entrantes y los navegadores suelen usar (solo mientras lo necesitan) un puerto cualquiera de los 65.000 para establecer el flujo de comunicación. El hecho de que se utilice el puerto 80 para ofrecer páginas web es una convención histórica, pero en realidad podría utilizarse cualquier otro. Para enviar y recibir correo, por ejemplo, se utiliza el 25.

Supongamos que tenemos un caso en el que el servidor web está "escuchando" en el puerto 80, en la IP 222.222.222.222, esperando que los clientes se conecten a él para mostrarle una página web.

En un momento dado, el cliente (un usuario en su casa), con dirección IP 111.111.111.111, utiliza el puerto 5698 para acudir al servidor web en 222.222.222.222 y ver la web. Se establecería un flujo de datos de esta manera:

[1]IPv4 es la versión del protocolo IP más usada. Actualmente está en marcha un proceso de migración a IPv6, que permite un número mayor de dispositivos conectados a Internet, cada uno con su propia dirección IP.

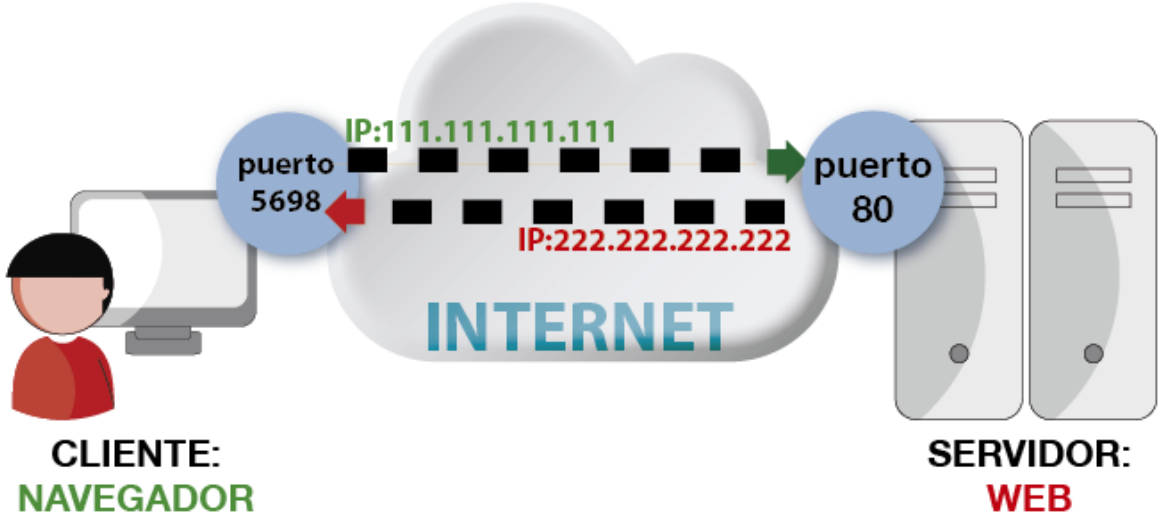
Tabla 2: Ejemplo de conexión a una página web

CLIENTE			SERVIDOR		
IP	Programa	Puerto	IP	Programa	Puerto
111.111.111.111	Navegador	5698	222.222.222.222	Servidor Web	80

Fuente: INTECO

Este intercambio de información fluye por Internet según un protocolo que puede variar en función del programa que se esté usando. Para la navegación web se utiliza HTTP. Esta tabla de información (dos direcciones IP y dos puertos) es única en todo Internet. Habrá otros usuarios, (quizás con la 123.123.123.123) desde otro puerto (puede que 6781) accediendo también a 222.222.222.222:80 y viendo la página web. Incluso el mismo usuario en 111.111.111.111 podría usar otro puerto diferente para conectarse al servidor. Pero la combinación "IP Cliente:puerto + IP Servidor:puerto" será siempre única en el mundo.

Ilustración 1: Ejemplo de conexión entre cliente y servidor



Fuente: INTECO

Un ordenador puede ser cliente y servidor al mismo tiempo, puesto que puede estar a la vez conectándose a un sistema y atendiendo a otro que quiere conectarse a él.

II Qué hace un cortafuegos

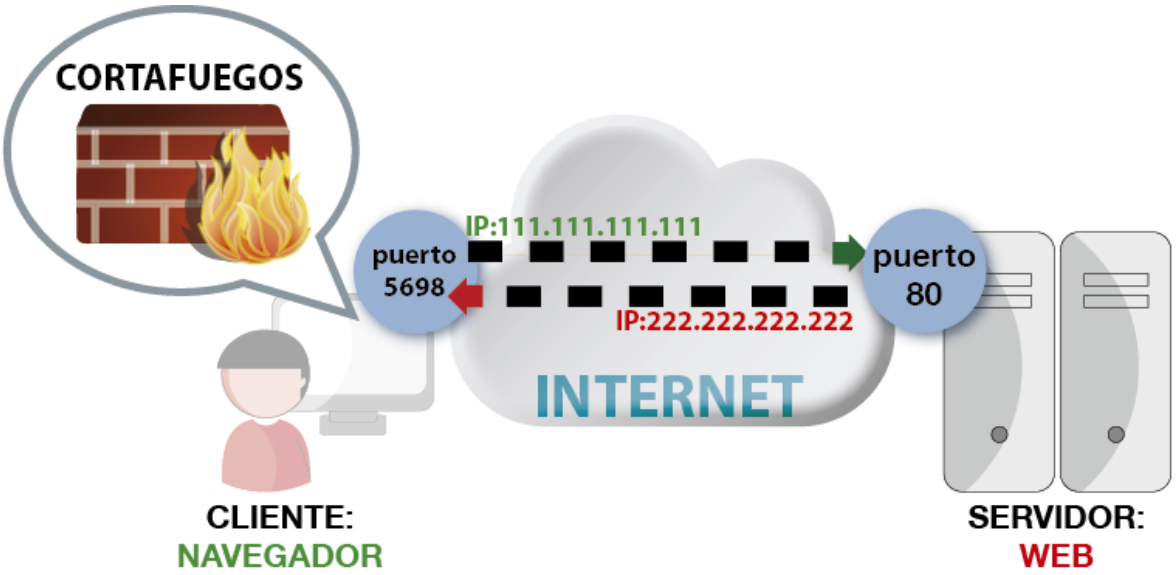
El cortafuegos se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores. Es como un semáforo que, en función de la dirección IP y el puerto (entre otras opciones), dejará establecer la conexión o no siguiendo unas reglas establecidas.

De este modo, el firewall controla qué combinaciones "IP Cliente:puerto + IP Servidor:puerto" son válidas o no. Por ejemplo, si el administrador del servidor 222.222.222.222 decide que no quiere que el cliente con dirección IP 111.111.111.111 vea su página web desde casa, podría indicarle a su cortafuegos en el servidor que bloquee esa dirección IP y no le permita acceder a su puerto 80.

Básicamente, el cortafuegos personal es un programa que se interpone entre el sistema operativo y las aplicaciones en la red, y comprueba una serie de parámetros antes de permitir que se establezca una conexión. Cuando se instala un *firewall*, el sistema operativo le cede el control de la gestión de esos puertos virtuales y de las conexiones de red en general, y hará lo que tenga definido como reglas. Las comprobaciones del cortafuegos están asociadas a unas reglas (que le indican qué debe hacer con esas conexiones). Estas reglas son normalmente "bloquear", "permitir" o "ignorar". Básicamente, cuando un programa quiere establecer una conexión o reservar un puerto para volcar datos en la red, el *firewall* pregunta:

- ¿De qué IP proviene este intento de conexión?
- ¿Desde qué puerto proviene?
- ¿A qué IP va destinada este intento de conexión?
- ¿A qué puerto?
- ¿Qué debo hacer con ella? (Bloquear, permitir o ignorar)

Ilustración 2: Ejemplo de conexión entre cliente y servidor con cortafuegos



Fuente: INTECO

Desde el punto de vista de un servidor

Un servidor suele tener programas "oyendo" en los puertos, y permanentemente ocupados con esos programas, esperando que los clientes se conecten. Así, por ejemplo, los servidores web normalmente tienen el puerto 80 ocupado con el servidor web esperando que clientes se conecten. Pero también puede que ofrezcan otros servicios además de una página. Por ejemplo también pueden ser servidores de correo. En este caso tendrán el puerto 25 ocupado con un servidor de correo (Postfix, Exchange, etc.) esperando que los clientes se conecten para enviar o recibir un correo.

Si alguien desde la IP 111.111.111.111 quiere ver la web, se establecerá esta conexión:

Tabla 3: Ejemplo de conexión a un servidor web

CLIENTE			SERVIDOR		
IP	Programa	Puerto	IP	Programa	Puerto
111.111.111.111	Navegador	31201	222.222.222.222	Servidor Web	80

Fuente: INTECO

Y ese mismo usuario quiere enviar un correo:

Tabla 4: Ejemplo de conexión a un servidor de correo

CLIENTE			SERVIDOR		
IP	Programa	Puerto	IP	Programa	Puerto
111.111.111.111	Cliente de correo	54681	222.222.222.222	Postfix	25

Fuente: INTECO

En las dos tablas anteriores, los puertos de origen son meros ejemplos. El cortafuegos del servidor puede decidir que no quiere que se conecte el usuario 111.111.111.111 a su sistema de correo e impedir que llegue al puerto 25. O puede que quiera bloquear la web para esa dirección IP y añada una regla a su cortafuegos que indique que no debe permitir conexiones que provengan de la IP 111.111.111.111 hacia el puerto 80.

Esto se llamaría "lista negra" en el servidor. O sea, una lista de direcciones IP que no queremos que se conecten a nuestro servidor.

Imaginemos que el servidor tiene un programa de gestión remota, que permite controlarlo. Este programa oye permanentemente en el puerto 5900. Así, el administrador del servidor, desde su casa con dirección IP 44.44.44.44 se conecta habitualmente a 222.222.222.222:5900 para gestionar el servidor. Si el administrador es cuidadoso,

configurará su cortafuegos para que solo y exclusivamente deje pasar conexiones que vengan desde esa IP hacia su servidor y hacia ese puerto.

Tabla 5: Ejemplo de reglas de un cortafuegos desde el punto de vista del servidor

CLIENTE (origen)			SERVIDOR (destino)			
IP	Programa	Puerto Origen	IP	Programa	Puerto Destino	Cortafuegos
44.44.44.44	Cliente VNC	Cualquiera	222.222.222.222	Servidor VNC	5900	Dejar pasar
Resto	Cualquiera	Cualquiera	222.222.222.222	Servidor VNC	5900	Bloquear

Fuente: INTECO

Y descartará el resto. Esto sería una "lista blanca". O sea, una lista de direcciones IP que queremos que puedan conectarse a nuestro servidor, descartando el resto.

III Tipos de cortafuegos

Aunque existen sistemas o máquinas específicamente diseñadas para hacer de cortafuegos, nos centramos en este caso en los cortafuegos personales, habitualmente integrados en los sistemas operativos.

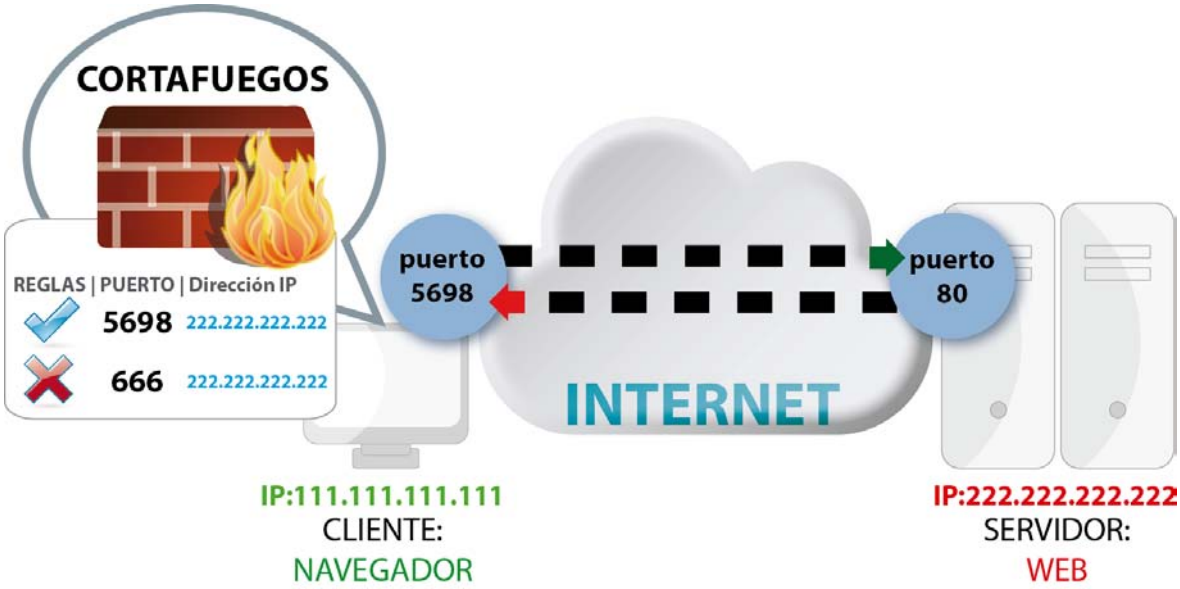
Entrante

El cortafuegos de tipo entrante es el que controla las conexiones que "entran" en el sistema. Esto quiere decir que está pensado en mayor medida para servidores, para comprobar desde qué direcciones IP se quieren establecer conexiones a sus servicios. Por ejemplo, desde el punto de vista de un servidor que muestra páginas web, un cliente que desee visualizar esa página, será una conexión entrante que deberá verificar en su tabla de reglas.

Este tipo de cortafuegos es muy usado tanto en servidores como en sistemas que habitualmente actúan como clientes. Por ejemplo, Windows XP lo activa por defecto desde su Service Pack 2, publicado en 2004. Desde entonces, todos los sistemas Windows cuentan con un cortafuegos entrante activado por defecto.

También, la inmensa mayoría de los routers usados para establecer una conexión ADSL tienen un firewall entrante activado por defecto, que protege al ordenador interno.

Ilustración 3: Ejemplo de conexión entre cliente y servidor, pasando por un cortafuegos del lado del cliente



Fuente: INTECO

Saliente

El cortafuegos de tipo saliente controla las conexiones que "salen" del sistema, esto es, las que acuden a un servidor. Está pensado en mayor medida para clientes, para comprobar hacia qué direcciones IP o qué puertos se conecta nuestro ordenador.

Este tipo de cortafuegos es mucho menos usado que el entrante, aunque es más seguro, puesto que nos permite tener control total de hacia dónde intentan conectarse los programas y, por tanto, nuestros datos. Con un cortafuegos saliente se podría, por ejemplo, establecer reglas como estas:

Tabla 6: Ejemplo de reglas de un cortafuegos desde el punto de vista del cliente, para el tráfico saliente

CLIENTE (origen)				SERVIDOR (destino)		
IP	Programa	Puerto Origen	Cortafuegos	IP	Programa	Puerto Destino
Nuestra	Internet Explorer	Cualquiera	Bloquear	Cualquiera	Servidor Web	81
Nuestra	Internet Explorer	Cualquiera	Dejar pasar	Cualquiera	Servidor Web	80

Fuente: INTECO

Con esta regla, se estaría indicando al cortafuegos saliente que, siempre que Internet Explorer se intente conectar desde nuestra dirección IP, desde cualquier puerto y

pretenda a ir a cualquier dirección IP de destino, al puerto 81, lo bloquee. Sin embargo, si pretende ir al puerto 80 del servidor, permitirá la conexión normalmente.

IV Otros tipos de cortafuegos

Hasta ahora se han visto las funciones básicas de los firewalls y el concepto original para el que fueron creados. Sin embargo, los cortafuegos personales y de servidores han evolucionado para ofrecer funcionalidades avanzadas que han ayudado a proteger aún más los servidores. Veamos algunos ejemplos:

Controlar el tipo de conexión

Las conexiones y flujos de datos entre puertos y direcciones IP pueden establecerse de forma errónea o malintencionada. Existen programas destinados a manipular este tipo de conexiones e intentar confundir al servidor para violar su seguridad o hacer que deje de responder. Así, pueden intentar establecer conexiones incompletas, confusas, sin sentido, etc. Dependiendo del programa destino, el sistema actuará de una manera u otra.

La mayoría de los cortafuegos ya están preparados para manejar este tipo de conexiones extrañas y no dejarlas pasar para que no causen problemas. Muchos están cargados por defecto con reglas de ataques conocidos que impiden que cualquier establecimiento de conexión que no sea conforme a los estándares, sea descartado.

Controlar la denegación de servicio

La denegación de servicio es un efecto bloqueo que ocurre cuando muchos sistemas intentan acceder a un mismo puerto de un servidor, saturándolo. El programa que escucha en el puerto puede manejar un número limitado de conexiones al mismo tiempo, y si ese número se supera, no permitirá que nuevas conexiones se establezcan. Así, si alguien consigue saturar al servidor e impedir que otras conexiones se establezcan, a través de conexiones que genere él mismo u otros sistemas, estaremos ante una denegación de servicio. Sería como organizar a un grupo de personas para que compren en una misma tienda al mismo tiempo, pero que retrasen el pedido distrayendo al comerciante. Clientes legítimos que quieran comprar algo no podrán realmente acceder a la tienda y por tanto, ésta tendrá un perjuicio.

Los cortafuegos permiten controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto (o que estas se establecen con demasiada velocidad) pueden añadir reglas automáticamente para bloquearlas y mantener el servicio a salvo.

Controlar las aplicaciones que acceden a Internet

Otros cortafuegos permiten controlar, además de qué direcciones IP se conectan a qué puertos, cuáles son las aplicaciones que lo están haciendo. Así, es posible indicar que un programa deje de conectarse a un puerto o una IP en concreto.

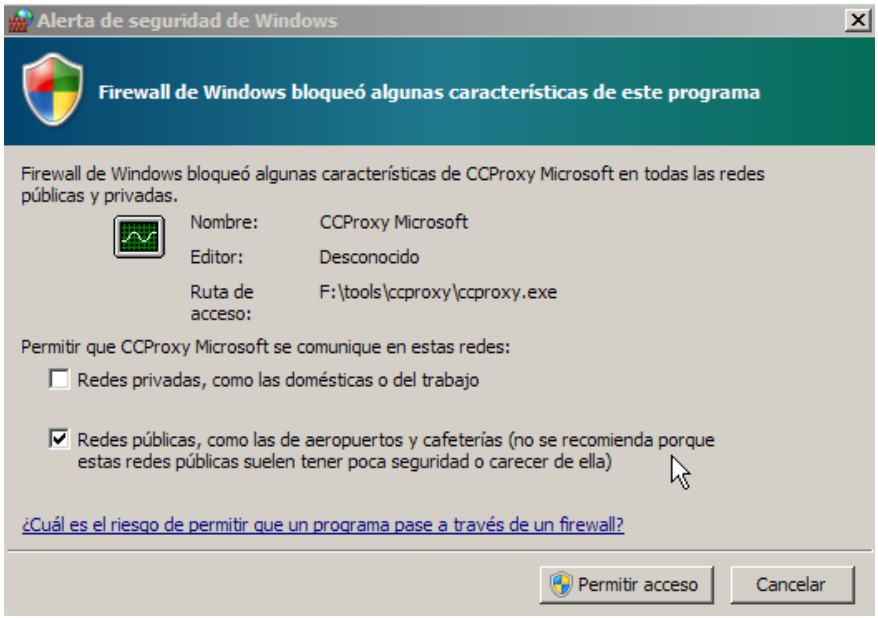
Si se realiza una lista blanca de programas que pueden conectarse a ciertos puertos, basados en el uso habitual del sistema, es posible conseguir un nivel de seguridad muy alto. Con esta técnica, se impedirá que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior.

Controlar las aplicaciones que acceden a un puerto

Un cortafuegos en el sistema puede también detectar cuándo una aplicación desea hacer uso de un puerto no para establecer una conexión, sino para ponerse a oír en él y esperar conexiones. Este es un comportamiento habitual de los troyanos de hace algunos años. Se conectaban a un puerto (o sea, convertían a la víctima en un servidor) y el atacante, como cliente, se conectaba a ese puerto. Por tanto, los cortafuegos también advierten al usuario cuando una aplicación quiere utilizar un puerto para esperar conexiones entrantes, puesto que puede suponer un riesgo de seguridad.

El firewall de Windows advierte de esta manera de que, en este ejemplo el programa Ccproxy, quiere ponerse a oír en un puerto. Da la oportunidad al usuario de permitir la conexión o no.

Ilustración 4: Cortafuegos de Windows alertando de que un programa quiere utilizar un puerto del sistema para enlazar un programa

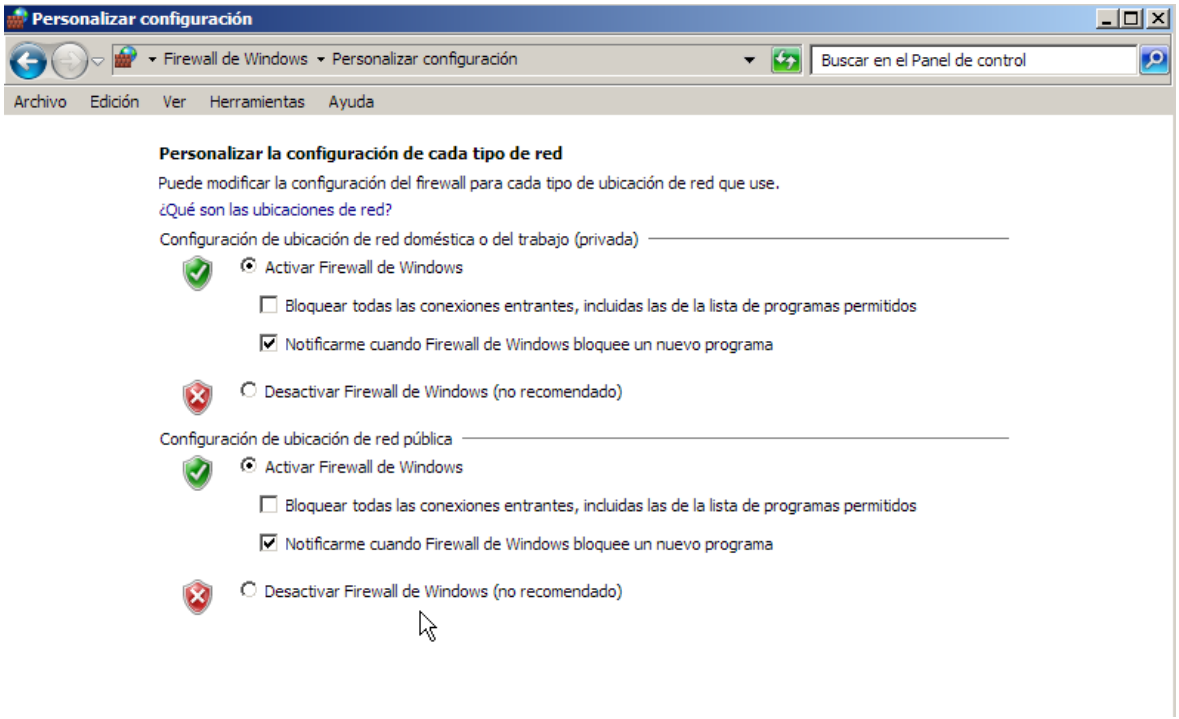


Fuente: INTECO

V Ejemplos de cortafuegos

Windows cuenta con un cortafuegos integrado, tanto entrante como saliente. Su interfaz básica es muy sencilla.

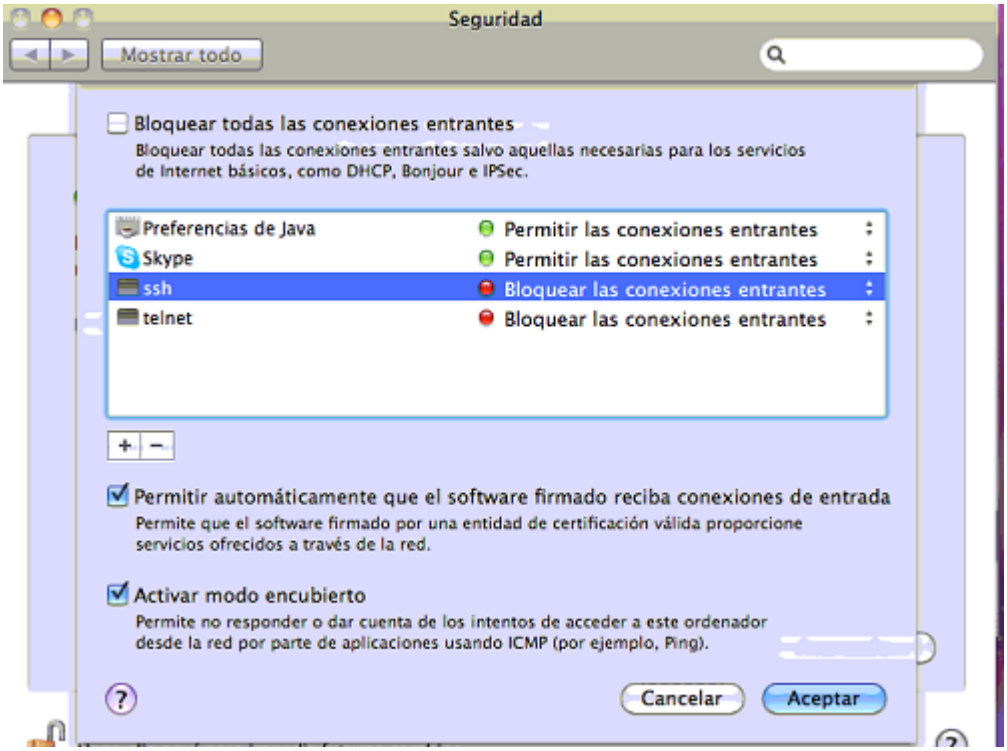
Ilustración 5: Configuración básica del cortafuegos de Windows en Vista y 7



Fuente: INTECO

Mac OS X cuenta con un cortafuegos integrado, sólo para conexiones entrantes.

Ilustración 6: Cortafuegos con configuración típica en Mac OS



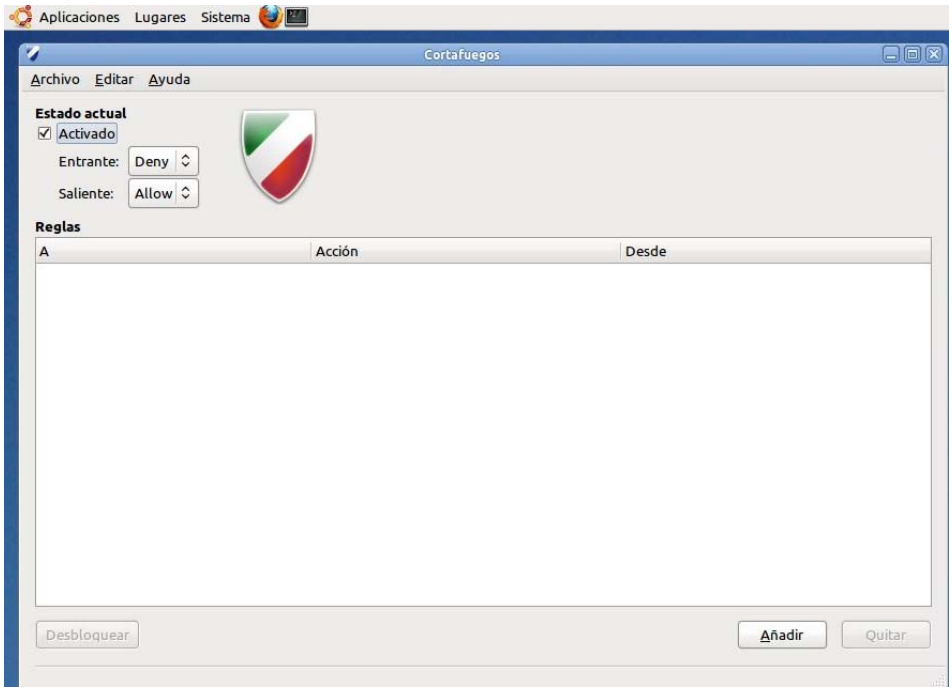
Fuente: INTECO

Para sistemas Linux, es necesario utilizar la línea de comando. Se utilizan reglas llamadas *iptables*, que están implementadas en todos los kernel[2] de todos los Linux. Son configurables a través de líneas de comando, y permiten total control de puertos y direcciones (tanto entrantes como salientes).

[2] El kernel es el núcleo del sistema operativo en Linux. Gestiona la comunicación básica con los componentes físicos del ordenador.

Sin embargo, existen diferentes "interfaces" gráficas que pueden ser instaladas para manejar de forma más cómoda el cortafuegos y sus reglas *iptables.*

Ilustración 7: Ejemplo de interfaz gráfica para cortafuegos en Ubuntu



Fuente: INTECO

Desde la página web de INTECO se pueden descargar diferentes programas de seguridad gratuitos tanto para usuarios como para entidades (http://cert.inteco.es/software/Proteccion/utiles_gratuitos/). Entre ellos se encuentra una serie de cortafuegos disponibles para diferentes plataformas.