¿Qué es un Cortafuegos (Firewall) para Internet?

Juan Carlos Yustas Romo

¡INTERNET, HOY!

En la actualidad, en nuestro país, hay cerca de 2 millones de usuarios conectados a Internet para obtener información, y que utilizan este medio para comunicarse. El sistema de comunicación es sencillo, un usuario conectado a Internet tiene asociada una dirección IP y puede conectarse a cualquier máquina conociendo su dirección o simplemente su nombre, pues unas máquinas (DNS) se encargan de traducir el nombre a su dirección IP; y los enrutadores encaminan los mensajes y las líneas de Internet se encargan de enviarlos. El proceso es equivalente a una "llamada telefónica" por Internet. Hoy en día, muchas empresas en el mundo han instalado servicios de información para sus clientes; que se suelen denominar Web, oficinas de soporte a los clientes, compra y venta de sus servicios, etc. Así pues, la red Internet se ha convertido actualmente en un mecanismo universal y muy fácil para transmitir información.

¿INTERNET ES SEGURA?

La contestación es sencilla: **¡No!** La red Internet es totalmente pública, pero a su vez opaca para quien la utiliza; nunca se sabe por dónde va a pasar su información, ni quién puede estar observándola. La gran ventaja de Internet es el protocolo de comunicaciones TCP/IP, que nos permite comunicar fácilmente nuestra red y otras redes, pero su desventaja es que nos deja expuestos a riesgos y accesos no autorizados que no existían anteriormente, y que pueden ser, tanto malintencionados, como simples errores humanos. Así pues, la inseguridad inherente y el deliberado espionaje de la red han traído una nueva preocupación a las empresas en este país y otros países. Algunas empresas, empiezan a preocuparse, pues ya han sufrido algún trastorno en sus aplicaciones en Internet, o algún ataque a través de ordenadores conectados a Internet, aunque ¡no lo confiesan! Algunos ejemplos típicos son:

- **Pasivos:** El buen "oyente" puede leer las cabeceras de los paquetes TCP/IP pudiendo: obtener la dirección origen y destinatario de la comunicación, obtener información acerca de actividad, saber las horas habituales de intercambio de información, etc. La detección de los ataques pasivos es muy difícil, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su gran éxito mediante el cifrado de la información.
- **Activos:** Algún "despistado internauta" puede cambiar los datos de una transacción, algún buen

"actor" puede suplantar al comprador o al vendedor, un hábil "intruso" puede bloquear el servicio de ventas que tenemos trabajando en el servidor de Internet. Un ejemplo típico, es que multitud de llamadas a un servicio, que controla un protocolo, puede provocar que el servidor deje de responder por exceso de carga. La única defensa posible es una configuración correcta y eliminar todos aquellos servicios de protocolos, que no sean estrictamente imprescindibles

4 **Agujeros**: Por deficiencias en la propia programación, por debilidades de las herramientas de programación en Internet Explorer, Netscape, Internet Information Server, Netscape Communicator, etc.

Los ataques en Internet son cada vez más frecuentes y su objetivo, en la mayoría de los casos, es demostrar que quien logra realizarlos es muy listo, es capaz de provocar defectos en su explotación o de robar información.

¡Pero no hay que extrañarse! Los protocolos para Internet, como HTTP, se crearon para un sistema abierto, amigable y confiado; que facilitara de una forma sencilla el intercambio de información. De este modo, no tiene que sorprendernos, que protocolos como TCP/IP, UDP, FTP, etc., son actualmente inseguros; pues, sin ninguna duda, la seguridad no era un elemento imprescindible para intercambiar información entre universidades, centros de investigación, etc.

La explosión de Internet en la intercomunicación humana, el uso de servicios informativos utilizando el protocolo HTTP, han provocado que muchos de los protocolos de Internet: como IPSec, sistema de cifrado, Telnet (servicio acceso remoto), FTP (transferencia de información) se estén volviendo a revisar para darles una mayor seguridad, integridad y fiabilidad. Aun así, estamos muy lejos de que la comunicación sea segura, de evitar que nuestras conversaciones se escuchen, que algún travieso (*hackers*) no modifique esta información, o algún malintencionado no realice operaciones deshonestas. Para evitar esto, necesitamos establecer una política de seguridad.

¿POLÍTICA DE SEGURIDAD?

El responsable de una red interna corporativa (Intranet), que deseamos mantener conectada a la red pública mundial (Internet) debe realizarse las siguientes preguntas:

- Si mi organización tiene acceso al exterior, ¿**el exterior tiene acceso a mi organización**?
- Si la red Internet no es una empresa, ¿***a quién reclamo***?

Una empresa necesita establecer una política de seguridad para evitar que pueda ser vulnerada por habilidosos o malintencionados internautas. Así pues, es imprescindible un control estrecho del punto de unión entre nuestra red (Intranet), teóricamente segura, y la red Internet, que es prácticamente insegura. Un punto obligado, es evitar que la información confidencial de nuestra red, se escape a la red Internet de dominio público; es decir, evitar que nadie acceda a determinada información sin la debida autorización.

Las medidas de seguridad para proteger nuestra Intranet, tienen que ser proporcionales al valor de los recursos que se pretenden proteger; teniendo siempre en cuenta, no sólo el valor de la información, sino también, el impacto en la imagen de la organización que puede suponer la difusión de una noticia sobre la falta de seguridad de unas instalaciones informáticas. Para poder realizar estas medidas de seguridad se debe tener en cuenta:

a) **Una política de seguridad en los elementos que se desean proteger**, denominada "defensa en profundidad". Consiste en aplicar la política de seguridad deseada en el mismo dispositivo que se pretende proteger, pero suele ser propia de los servicios y del sistema operativo utilizados en cada empresa.

b) **Una política que distinga entre redes consideradas seguras e inseguras**, para aislar determinados servicios y tráfico entre ambas redes. Esto provoca el concepto de red externa (no confiable) y de red interna (confiable), y la existencia de una "defensa perimetral" de nuestra red. Este tipo de seguridad consiste en la utilización de sistemas "cortafuegos", para aislar la red que deseamos proteger del resto de redes consideradas como inseguras y tiene la ventaja de aislar nuestros puntos de control (política de seguridad) exclusivamente en estos elementos. Normalmente, el elemento de conexión entre redes suele ser único, pero no olvide tener algún sistema de redundancia, por si existiera algún fallo en este punto de conexión.

En este artículo trataremos a nivel general los "cortafuegos", por ser un elemento muy crucial de la "defensa

perimetral" de una red, que a su vez, es un elemento fundamental de la política de seguridad. El cortafuegos es un sistema de control que se sitúa entre una red corporativa e Internet, véase la figura 1. La función principal del cortafuegos es constituir un punto de paso para el intercambio de información entre ambas redes; por lo que en este dispositivo determinará cuáles son los protocolos, es decir los servicios, que pueden atravesarlo y bajo qué condiciones.

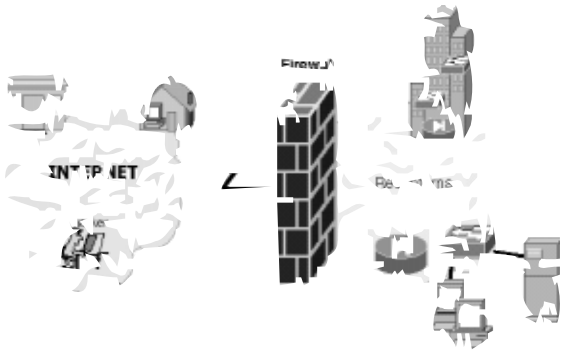

Figura 1. *Situación del cortafuegos*

¿QUIÉN NECESITA UN CORTAFUEGOS PARA INTERNET?

Una empresa que necesite permitir o denegar los flujos de información entre su red y otras redes. Por ejemplo, si desea establecer que determinados clientes sólo se conecten a determinadas zonas de nuestra red (subredes) en las que residen los servicios que necesitan. Otros ejemplos son: evitar que se conozcan las direcciones TCP/IP de nuestra red interna, para que no pueda tener acceso a ellas personal no deseado, prohibir protocolos no deseables, como Telnet, etc.

¿TIPOS DE CORTAFUEGOS?

Los cortafuegos se suelen clasificar según el tipo de información que analizan:

1. **Filtrado de paquetes:** Trabajan examinando a nivel de paquetes IP independientes y decidiendo si dicho paquete puede atravesar el cortafuegos en base a sus parámetros básicos (direcciones IP, protocolos, opciones, etc.). Se comportan como un enrutador (router) filtrando direcciones IP origen y destino, protocolo, y puertos origen y destino. Realmente, no crean un perímetro de defensa de por sí; por ejemplo, si se abre el puerto IP número 25, y en la red interna existe un dispositivo con un Telnet mal configurado, éste quedará expuesto. Véase la figura 2.

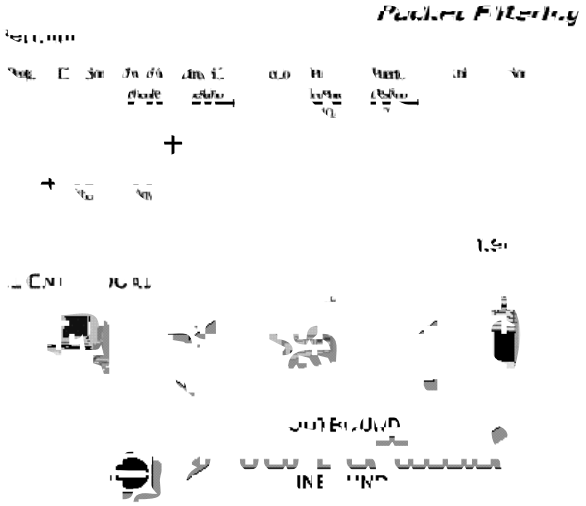

Figura 2. *Filtrado con un cortafuegos de paquetes*

La ventaja de un cortafuegos de filtrado de paquetes es su rapidez, pues opera a nivel de red de OSI, pero requiere conocer y saber filtrar bien todos los protocolos. Las reglas de filtrado son a veces muy complejas de especificar para casos excepcionales. Otro fallo, es que algunos cortafuegos con más de un enlace de red no permiten realizar filtrados diferentes dependiendo del enlace de la red origen. El principal inconveniente, es que la mayoría excepto que se ejecuten en el mismo sistema operativo, no permiten reglas intermedias, como permitir a unos usuarios utilizar un protocolo y prohibirlo a otros usuarios, esto es debido a que no puede actuar a nivel de aplicación.

2. **Nivel de circuito:** Trabajan creando un sistema cliente-servidor de pasarelas (*gateway o proxies*) que actúan filtrando paquetes por protocolos; además permiten funciones avanzadas de autentificación a través del cortafuegos para algunos protocolos. Establecen un control sobre el tráfico de cada protocolo, pero requieren un software especial para cada protocolo. El cliente de nuestra red, situado en un lado del cortafuegos, habla con un protocolo (servicio) situado en el propio cortafue-

gos. Este servicio le identifica, registra sus peticiones y, si lo considera oportuno, encamina éstas hacia el verdadero servidor situado al otro lado del cortafuegos. La contestación regresa por el mismo camino quedando igualmente registrada. El cortafuegos actúa como una pasarela (proxie), actúa como si fuera el cliente que pide el servicio al servidor de Internet, y finalmente envía la información al cliente original, véase la figura 3. La mayoría de los cortafuegos de pasarela (proxie) pueden actuar de traductor de direcciones, pudiendo ocultar las direcciones de los clientes de nuestra red; esto permite que la única dirección definida como válida en la red Internet sea la dirección del cortafuegos. El único problema es que una vez establecida la conexión, se permite a cualquier aplicación ejecutarse sobre el protocolo utilizado. Las reglas de filtrado son menos complejas. Si bien, una desventaja es que para las aplicaciones cliente-servidor, tales como Telnet, se requiere conectarse primero al cortafuegos, y después, desde el cortafuegos al servidor destino. Tenga precaución, pues estos cortafuegos requieren un cuidado especial en las palabras de acceso de sus usuarios de gestión. Por ejemplo, si un *hacker* adquiere el control de una palabra de acceso de un usuario del cortafuegos, que tiene suficientes privilegios, puede dañar el tráfico de toda la red.

Figura 3. *Filtrado con un cortafuegos de pasarela*

3. **Aplicación:** Los cortafuegos que son aplicaciones cliente-servidor y que trabajan a nivel de aplicación, pueden actuar hasta el nivel 7 de OSI, simulando los procesos de aplicación, contraseñas y verificación. El sistema actúa como una "red virtual" que chequea los procesos de entrada y salida. El principal inconveniente, es que suelen tener un coste muy elevado. Estos cortafuegos no tratan paquetes entre las interfaces a nivel de red, nivel 3 de OSI, por el contrario disponen de programas específicos para cada protocolo, a nivel de aplicación, que se encargan de analizar todos los paquetes que tratan de pasar de una red a otra. Véase la figura 4. Aunque por su nivel de complejidad suelen ser menos eficientes, son mucho más seguros que cualquiera de los dos tipos anteriores. La mayoría de los cortafuegos de tipo aplicación, suelen utilizar sus reglas para establecer un fijado estático de filtrado de paquetes, y los más hábiles suelen crear mecanismos abreviados de filtrado para las conversaciones que consideran seguras.

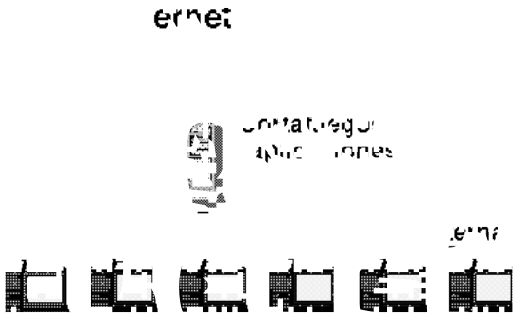

Figura 4. *Filtrado con cortafuegos de aplicación*

¿QUÉ HACE EL CORTAFUEGOS?

Hemos visto, que el cortafuegos es un agente de tráfico que filtra la información que se transmite entre nuestra red y otras redes. Para esto, puede utilizar uno, o varios elementos adicionales, que permiten implementar un mayor o menor nivel de defensa perimetral de nuestra red, que siempre tiene que ser conforme, a una política de seguridad definida. Las funciones que puede realizar un cortafuegos son:

- **Política:** Fijar "lo permitido" en el tráfico entre nuestra red y otras redes, "lo que se deniega" de dicho tráfico. Para esto, aplica unas reglas para restringir el tráfico de paquetes, fijando en un axioma básico de seguridad: **Prohibir la entrada a todos los "paquetes" menos a los que están expresamente autorizados**. Esta característica proporciona al administrador de la red flexibilidad ilimitada y un control completo sobre el sistema de acceso a la red.
- **Control de redes:** Permite fijar los elementos, subredes, que pueden establecer este tráfico. Por ejemplo, los clientes de la red 35.0.0.0 del área comercial pueden salir a Internet, y desde Internet

se pueden conectar a los servidores de esta red; otro ejemplo es que los clientes de tesorería, subred 28.0.0.0 pueden salir a la red Internet, pero está prohibido que desde Internet puedan consultar sus servidores.

- **Control de servicios**: Proporciona seguridad total a aplicaciones comunes TCP/IP, Gopher, http (www), FTP, Telnet, etc. La mayoría de los cortafuegos pueden actuar a nivel de control de red, y a nivel de subredes, que pueden utilizar estos protocolos.

- **Procesos de conexión**: Los cortafuegos de tipo aplicación permiten una funcionalidad exhaustiva en tiempo real sobre la conexión (log-in), auditoría, monitorización e informes. Algunos cortafuegos permiten un sofisticado control de procedimientos de identificación de usuario, por ejemplo, S/Key y SecurID.

- **Ocultación:** Permite ocultar a la red insegura cualquier información sobre la red interna. Esto requiere emplear un cortafuegos que actúe de proxy, no facilitando las direcciones IP internas, lo que evita que usuarios no autorizados se identifiquen como entidades legales de la red (acción denominada *spoofing*). También puede permitir ocultar los servidores de DNS, que establecen la relación entre los nombres de nuestros servidores y su dirección IP.

- **Traducción de direcciones**: Permite el soporte de direcciones ilegales en Internet, y proporciona la ventaja de trabajar sobre la red Internet, sin necesidad de declarar las direcciones en el registro de direcciones NIC de Internet.

- **Seguridad:** Avisa al vigilante de la red de las anomalías en el tráfico, registra el tráfico efectuado para su tratamiento estadístico. Permite en algunos casos detectar ataques fallidos, y ponernos en guardia respecto a lo que pasa entre nuestra Intranet y la red Internet.

La conexión de la red de la empresa siempre se realiza a través del cortafuegos, y se consigue a través de una serie de componentes como son routers, pasarelas (proxies), etc.; que nos permiten establecer una política de control de acceso entre ambas redes (la nuestra, que deseamos proteger, y cualquier otra, por lo general Internet). El cortafuegos se instala en un bastión que permite separar la política interna frente a política externa de interconexión. Pero tenga muy claro, que en ningún caso, es una garantía absoluta de seguridad que nos permite respirar tranquilamente, aunque permite saber de dónde vienen los tiros antes de que nos alcancen.

¿DE QUÉ NO PROTEGE UN CORTAFUEGOS?

La mayoría de los cortafuegos no protegen de determinados riesgos y, si lo hacen, suelen retrasar enormemente su labor. Los elementos más destacados son:

- **Virus:** Programas ejecutables que se ejecutan sin el consentimiento del equipo en que residen, y fuera del control consciente de sus usuarios. Su fin, es dañino por ocupar indebidamente nuestros equipos y recursos; y en el peor de los casos, nos causarán daños en los datos, destruyéndolos o haciéndolos accesibles a quien no debiera. Si un virus pretende entrar a través del cortafuegos y éste es capaz de detectarlo, puede desactivarlo e inmediatamente avisar del pretendido ataque, marcando al remitente. Pero, si no queremos ralentizar el servicio del cortafuegos hasta extremos inaceptables, lo ideal es que los sistemas de detección de virus se instalen detrás del cortafuegos. Por ejemplo, para detectarlos antes de servicios como el correo electrónico, en servidores especializados.

- **Applets:** Las aplicaciones **Java** o **ActiveX**, diseñadas por Microsoft y Sun Microsystems, que son componentes empaquetados, que habitualmente son descargados desde un servidor y que se ejecutan en los clientes, pero cuyo contenido no es visible hasta que se ejecutan.

LAS REGLAS ESENCIALES DEL CORTAFUEGOS

Un elemento importante para efectividad de un cortafuegos es gestionar un mapa actualizado de nuestra red fijando las zonas confiables. Sí, esas zonas por las que los datos puedan distribuirse sin miedo de que lleguen a manos indebidas, y en las que los usuarios pueden ir de un sitio a otro sin la pesadez de tener que identificarse a cada momento. A la hora de diseñar un cortafuegos hay que tomar en consideración varios elementos esenciales:

- **Simplicidad**: En zonas no conflictivas de la red utilice como cortafuegos un enrutador, también denominado encaminador; es una decisión inteligente, pues la operación será igual de válida, pero más eficiente. Por hacer, un símil, es como si en un cruce pone un guardia urbano que sólo decide qué coches pueden pasar y cuáles no, dependiendo de su origen y destino. La velocidad a la que se encamina cada paquete hacia su destino solicitado es más rápida, que si el guardia se dedica a la vez a apuntar las matrículas. Y más hábilmente, puede fijar, que en otro cruce posteriormente, se pueden establecer otros controles más severos para filtrar paquetes no deseados.

- **Segmentación de direcciones IP:** Establecer una división lógica de las direcciones IP de la red extensa (WAN) de la empresa, usar subdireccionamiento IP para reducir las tablas de los enrutadores (router), y ocultar más fácilmente las direcciones de nuestras subredes IP.

- **Canales seguros:** Para enlazar dos cortafuegos a través de una red no segura, por ejemplo, una línea de una compañía telefónica extranjera, utilice una red privada virtual (VPN) entre ambos extremos; y verifique que las VPN son compatibles con el protocolo IPSec, para evitar problemas. Por ejemplo, para enlazar un cortafuegos situado en una oficina de Australia con la oficina central. La ventaja es que utiliza un túnel cifrado, que permite que los datos sean cifrados al salir de un extremo y descifrados al llegar al otro, evitando posibles escuchas no deseadas. Tenga la seguridad, de que los túneles cifrados realizan una fase previa de autentificación mutua, de forma que un cortafuegos esté seguro de que está hablando con quien quiere. Una vez autentificadas ambas partes, se decide una clave de sesión (quedando establecido el túnel cifrado) que, por seguridad, no tiene que reutilizarse en otra sesión, e incluso suele modificarse periódicamente (cada tantos minutos) para mayor seguridad. El objetivo es no dar mucho material cifrado a posibles enemigos exteriores que estén intentando obtener información de nuestra red.

- **Prudencia:** La utilización de cortafuegos y túneles privados no debe hacernos olvidar algunos puntos importantes de seguridad global: **a)** sólo protegen de extremo a extremo del enlace y no hacen nada frente a personas mal intencionadas que estén dentro de la empresa; **b)** la seguridad de dos redes conectadas a una VPN es siempre la de la red más insegura de ambas, es un canal seguro, pero que puede ser utilizado de modo inseguro; y **c)** los enemigos pueden aún extraer conclusiones a partir del análisis estadístico del volumen y frecuencia del tráfico intercambiado, sin conocer su contenido.

¿DÓNDE SITUAR UN CORTAFUEGOS?

El esquema más simple es disponer de un elemento cortafuegos con dos puertos IP, uno que consideramos inseguro, y otro que consideramos seguro. El problema de este esquema tan simple se debe a un defecto importante: sólo hay un nivel de seguridad. Por tanto, si se equivoca en las reglas de tránsito o el sistema operativo del bastión resulta violado, tenemos al enemigo dentro de casa. Y no olvide, que un enemigo instalado en el bastión, tiene acceso directo a la red y puede monitorizarla mediante cualquier programa, por ejemplo, obtenido de un shareware. De este modo, puede visualizar tráfico interno, comprometiendo la seguridad de los datos confidenciales, acceder a otros equipos que se fían del origen de la conexión, etc. Para evitar esta debilidad estructural se suelen utilizar técnicas de "defensa en profundidad", estableciendo uno o más niveles intermedios. La figura 5, muestra un esquema de conexión de un cortafuegos con 2 niveles de defensa, separados por una zona de defensa perimetral (usualmente denominada **DMZ** (*demilitarized zone*). Además puede apreciar cómo combinar elementos distintos de un cortafuegos: uno a nivel de encaminador externo (nivel 3 de red de OSI) que sólo autorizan los flujos marcados, otro a nivel de aplicación (**proxies** de servicios específicos), y final-

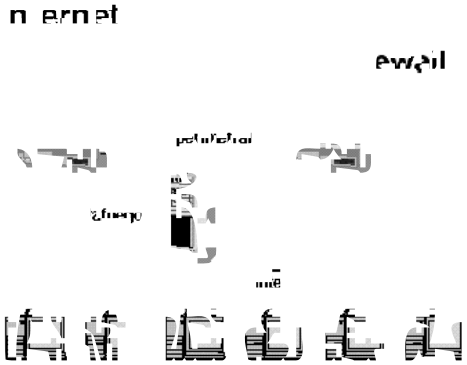

Figura 5. *Filtrado con cortafuegos utilizando DMZ*

mente, un encaminador interno que tiene todas las restricciones de tráfico.

Estos elementos se pueden combinar de múltiples formas y maneras. La figura 6 muestra otro esquema típico en nuestro país, donde la existencia de InfoVía, la intranet de Telefónica, se incorpora al cortafuegos. El bastión funciona como un embudo que encamina peticiones de ambos sitios hacia el servidor interno común.

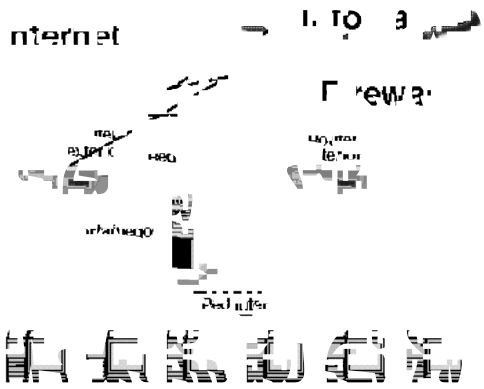

Figura 6. *Filtrado múltiple con cortafuegos utilizando DMZ*

¿CUÁNTOS CORTAFUEGOS?

Es necesario instalar tantos cortafuegos como interfaces entre redes o segmentos de red con políticas diferentes de seguridad. Pero la regla principal es disminuir al máximo el número de estos elementos, pues se reducen el mantenimiento y los puntos de control. Por ejemplo, no hace falta un cortafuegos entre dos tramos de red separados para atender a zonas alejadas físicamente unidas por un puente (*bridges*). Sin embargo, puede tener sentido un cortafuegos para controlar el tráfico entre dos redes con medidas de seguridad distintas, que incluso pudieran compartir el mismo medio físico, o si existen puestos en la red que tienen conectado un módem (portátiles) para obtener información externa por medio tramos no seguros, por ejemplo, un sistema FTP de Internet.

¿DÓNDE FIJAR LOS SERVICIOS?

Si todos los clientes están en la misma red, el cortafuegos se sitúa siempre lo más próximo a los clientes y se prohiben los servicios que no deseamos que salgan de la red. Pero cuando los clientes de un servicio no están en la misma red, surge la necesidad de cruzar el cortafuegos; esto nos llevará a clasificar los servicios por el tipo de acceso: **a)** datos de información confidencial, **b)** datos con acceso a los servicios con identificación del usuario, **c)** datos con acceso para modificarlos, **d)** datos con acceso de sólo lectura, etc. Veamos algunos puntos importantes en un ejemplo:

- Un servidor WWW de la empresa tiene acceso público en la red Internet, acceso más completo por autentificado para el personal propio de la empresa, y un equipo de mantenimiento que se encarga de mantener actualizadas las bases de datos corporativas. Un punto indispensable, es garantizar la confidencialidad e integridad de la base de datos. La integridad se puede garantizar replicando la base de datos de operación (interna) en una base de datos de sólo lectura (expuesta), asegurándose que este proceso no sea visible desde el exterior; pero esto suele ser una operación bastante complicada.

- El cortafuegos realiza un servicio de **proxy**. Los servicios de entrada son el multiprotocolo: **http** de cara al público, y un servicio **ODBC** para la base de datos que utiliza TCP/IP por el puerto 1433. Un consejo, cuando utilice **ODBC**, es preferible que utilice palabras de acceso cifradas, pues si no, se pueden escuchar en texto claro en Internet.

- Los servicios salientes del cliente interno en Intranet al servidor externo en Internet, suelen ser más simples de diseñar; pues el cliente interno se identifica por su dirección de origen y puede autorizar su salida al exterior, con los registros de actividad y traducción de direcciones IP pertinentes.

- La traducción de los nombres de nuestras máquinas a sus direcciones IP y viceversa, denominada DNS (*Domain Name System*), no tiene que salir de nuestra red, pero sí el nombre del cortafuegos. Para esto, es habitual el establecimiento de una jerarquía de dos niveles: un servidor de DNS externo, que sólo envía al exterior la información del cortafuegos y oculta las restantes direcciones; y un servidor interno que traduce las direcciones IP privadas de nuestra red, separadas de Internet; los clientes locales recurren al servidor interno, cuando se solicita información de redes externas, y el servidor interno consulta al servidor DNS externo para obtener las direcciones de Internet.

- Los servicios de mensajería o de noticias que utilizan un almacenamiento intermedio (*store and forward*) se reciben en el cortafuegos. En él se pueden aplicar algunos chequeos, tales como evitar mensajes en tránsito no autorizados que puedan utilizar nuestra red como vehículo de transporte para terceros. Los mensajes aceptables se encaminan a un segundo servidor interno, que funciona como estafeta de correos del sistema de mensajería, evitando que los mensajes internos salgan a la red externa innecesariamente. Habitualmente, este servidor puede verificar su contenido para evitar la entrada de virus en nuestra red, tarea que no se puede encargar al cortafuegos, pues reduciría su rendimiento.

¿CÓMO PLANIFICAR UN CORTAFUEGOS?

Lamentablemente, planificar un cortafuegos no es una tarea sencilla aunque sea muy fácil adquirirlo, instalar sus dos conexiones a la red y enredar en su configuración. No es una tarea imposible; simplemente es una tarea laboriosa, que requiere una planificación previa de la estructura de la red, un seguimiento disciplinado y un esfuerzo permanente de mantenimiento. Y no piense que añadir conexiones de red a un cortafuegos es el sistema más fácil de conectar múltiples equipos, pues puede encontrarse que las soluciones en estrella compliquen mucho las reglas del cortafuegos, o incluso que provoquen grandes agujeros en la red.

CONSIDERACIONES PARA LA COMPRA

Un factor muy importante es el soporte que tiene el producto en nuestro país. El segundo punto es que tiene que ser un sistema que se proteja a sí mismo, pues no sólo debe proporcionar una función de barrera, sino que tiene que carecer de agujeros. El tercer punto es el sistema operativo, este punto es fundamental, y para no entrar en discusiones interminables: el mejor consejo es que el sistema operativo sea conocido en su empresa. Pero si quiere saber mi opinión, para una gran empresa prefiero UNIX, pues el rendimiento es mejor y la experiencia de los fabricantes es mayor en este sistema. Si bien, el punto final, es que es **imprescindible** saber bloquear sistemáticamente todos los problemas de seguridad del sistema operativo en el que se ejecuta este producto, reflexione sobre ello.

¡EL MANTENIMIENTO!

Un cortafuegos no es una máquina que se instala y nos permite dormir tranquilos. **¡No!** Hay que mantenerla y vigilarla permanentemente. Algunos puntos importantes para controlar un cortafuegos son:

- Comprender las reglas que permiten el tránsito de información conviene, añadir unos mensajes de alarma en caso de detección de intrusos, ataques fallidos y comportamientos irregulares de los usuarios en general.

- Utilizar las herramientas del cortafuegos para realizar controles, y gestionar el tráfico de la red desde un solo punto que incluya la configuración de redes remotas. Todo esto lo tiene que realizar con un protocolo que no sea en "texto plano", para que no se pueda escuchar fácilmente en la red. Y si tiene un **monitor de actividades sospechosas**, téngalo siempre activo, pues los intrusos no duermen.

- Utilice herramientas para espiar su propia red, como Satan, Cops, ISS, etc. La red puede cambiar por algún despiste de un administrador de un servidor.

Para terminar, dos consejos: las reglas del cortafuegos hay que cambiarlas con calma, las prisas provocan siempre algún fallo, y algunos internautas son muy listos para detectarlos; por último, considere que ellos son más hábiles que nosotros, y suelen tener más experiencia, así que aplique la prudencia.