Mecanismos de prevención

Joaquín García Alfaro

Índice

Introducción

Cuando un equipo se conecta a una red informática, se pueden identificar cualquiera de las tres áreas de riesgo siguientes:

Primero, se incrementa el número de puntos que se pueden utilizar como origen para realizar un ataque contra cualquier componente de la red. En un sistema aislado (sin conexión), un requisito necesario para que sea atacado es forzosamente la existencia de un acceso físico hacia el equipo. Pero en el caso de un sistema en red, cada uno de los equipos que pueda enviar información hacia la víctima podrá ser utilizado por un posible atacante.

Algunos servicios (como, por ejemplo Web y DNS) necesitan permanecer públicamente abiertos, de forma que cualquier equipo conectado a internet podría ser el origen de una actividad maliciosa contra los servidores de estos servicios. Esto hace que sea muy probable la existencia de ataques regulares contra dichos sistemas.

La segunda área de riesgo abarca la expansión del perímetro físico del sistema informático al que el equipo acaba de ser conectado. Cuando la máquina está aislada, cualquier actividad se puede considerar como interna en el equipo (y por lo tanto, de confianza). El procesador trabaja con los datos que encuentra en la memoria, que al mismo tiempo han sido cargados desde un medio de almacenamiento secundario. Estos datos están realmente bien protegidos contra actos de modificación, eliminación, observación maliciosa, ... al ser transferidos entre diferentes componentes de confianza.

Pero esta premisa no es cierta cuando los datos se transfieren a través de una red. La información transmitida por el medio de comunicación es retransmitida por dispositivos que están totalmente fuera de control del receptor. La información podria ser leída, almacenada, modificada y, posteriormente, retransmitida al receptor legítimo. En grandes redes, y en especial internet, no es trivial la autenticación del origen que se presenta como el de emisor de un mensaje.

Por último, la tercera área de riesgo se debe al aumento en el número de servicios de autenticación (generalmente, un servicio de *login-password*) que un sistema conectado a una red deberá ofrecer, respecto a un sistema aislado. Estos servicios no dejan de ser simples aplicaciones (con posibles deficiencias de programación o de diseño) que protegen el acceso a los recursos de los equipos del sistema. Una vulnerabilidad en algunos de estos servicios podría comportar el compromiso del sistema al completo.

La prevención de ataques supondrá la suma de todos aquellos mecanismos de seguridad que proporcionen un primer nivel de defensa y tratarán de evitar el éxito de los ataques dirigidos contra la red que está bajo su protección.

Objetivos

Los objetivos que se deben alcanzar con el estudio de este módulo son:

1) Entender el funcionamiento de las tecnologías cortafuegos.

2) Ver los distintos métodos existentes para el filtrado de tráfico TCP/IP.

3) Comprender las distintas posibilidades de configuración de los sistemas cortafuegos.

2.1. Sistemas cortafuegos

Los sistemas cortafuegos* son un mecanismo de control de acceso sobre la capa de red. La idea básica es separar nuestra red (donde los equipos que intervienen son de confianza) de los equipos del exterior (potencialmente hostiles).

* En inglés, *firewalls.*

Un sistema cortafuegos actúa como una barrera central, para reforzar el control de acceso a los servicios que se ejecutan tanto en el interior como en el exterior de la red. El cortafuegos intentará prevenir los ataques del exterior contra las máquinas internas de nuestra red denegando intentos de conexión desde partes no autorizadas.

Un cortafuegos puede ser cualquier dispositivo utilizado como mecanismo de control de acceso a nivel de red para proteger a una red en concreto o a un conjunto de redes. En la mayoría de los casos, los sistemas cortafuegos se utilizan para prevenir accesos ilícitos en el interior de la red.

Un cortafuegos es aquel sistema de red expresamente encargado de separar redes informáticas, efectuando un control del tráfico existente entre ellas. Este control consiste, en última instancia, en permitir o denegar el paso de la comunicación de una red a otra mediante el control de los protocolos TCP/IP.

A la hora de instalar y configurar un sistema cortafuegos en nuestra red, debemos tener presente lo siguiente:

1) Todo el tráfico que sale del interior hacia el exterior de la red que se quiere proteger, y viceversa, debe pasar por el cortafuegos. Esto se puede conseguir bloqueando físicamente todo el acceso al interior de la red a través del sistema.

2) Solo el tráfico autorizado, definido en las políticas de seguridad locales del sistema, podrá traspasar el bloqueo.

3) El propio cortafuegos debe estar protegido contra posibles intrusiones. Esto implica el uso de un sistema operativo de confianza con suficientes garantías de seguridad.

2.2. Construcción de sistemas cortafuegos

En el sentido más general, un sistema cortafuegos consta de *software* y *hardware*. El *software* puede ser propietario, *shareware* o *freeware*. Por otro lado, el *hardware* podrá ser cualquiera que pueda soportar este *software*.

Actualmente, tres de las tecnologías más utilizadas a la hora de construir sistemas cortafuegos son las siguientes:

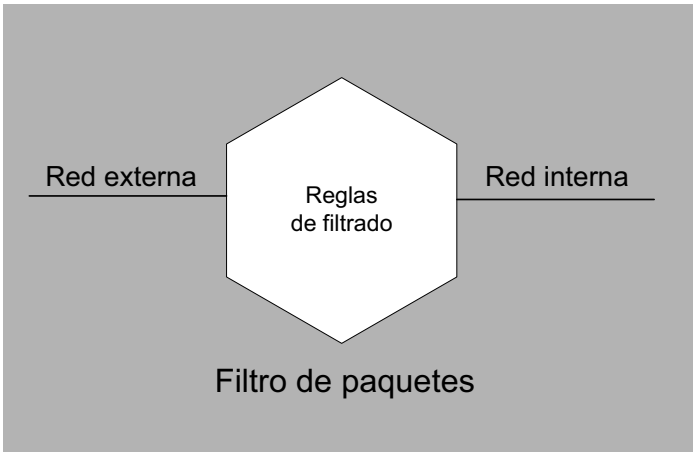
- Encaminadores con filtrado de paquetes.
- Pasarelas a nivel de aplicación.
- Pasarelas a nivel de circuito.

A continuación estudiaremos con más detalle cada una de estas categorías.

2.2.1. Encaminadores con filtrado de paquetes

Se trata de un dispositivo que encamina el tráfico TCP/IP (encaminador* de TCP/IP) sobre la base de una serie de reglas de filtrado que deciden qué paquetes se encaminan a través suyo y cuales se descartan.

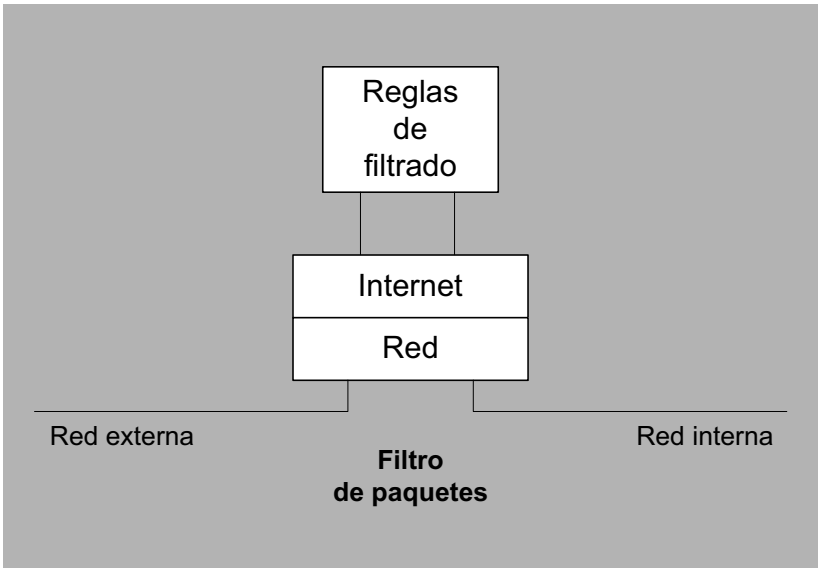
* En inglés, *router.*



Las reglas de filtrado se encargan de determinar si a un paquete le está permitido pasar de la parte interna de la red a la parte externa, y viceversa, verificando el tráfico de paquetes legítimo entre ambas partes.

Los encaminadores con filtrado de paquetes, al trabajar a nivel de red, pueden aceptar o denegar paquetes fijándose en las cabeceras del protocolo (IP, UDP, TCP, ...), como pueden ser:

- Direcciones de origen y de destino.
- Tipos de protocolo e indicadores (*flags*) especiales.
- Puertos de origen y de destino o tipos de mensaje (según el protocolo).
- Contenido de los paquetes.
- Tamaño del paquete.



Estas reglas estarán organizadas en conjuntos de listas con una determinada política por defecto (denegarlo todo, aceptarlo todo, ...).

Cada paquete que llegue al dispositivo será comparado con las reglas, comenzando por el principio de la lista hasta que se encuentre la primera coincidencia. Si existe alguna coincidencia, la acción indicada en la regla se activará (denegar, aceptar, redirigir, ...).

Por contra, si no es posible ninguna coincidencia, será consultada la política por defecto para saber qué acción hay que tomar (dejar pasar el paquete, descartarlo, redireccionarlo, etc). Si se trata, por ejemplo, de una política de denegación por defecto, en el caso de no existir ninguna coincidencia con el paquete, éste será descartado.

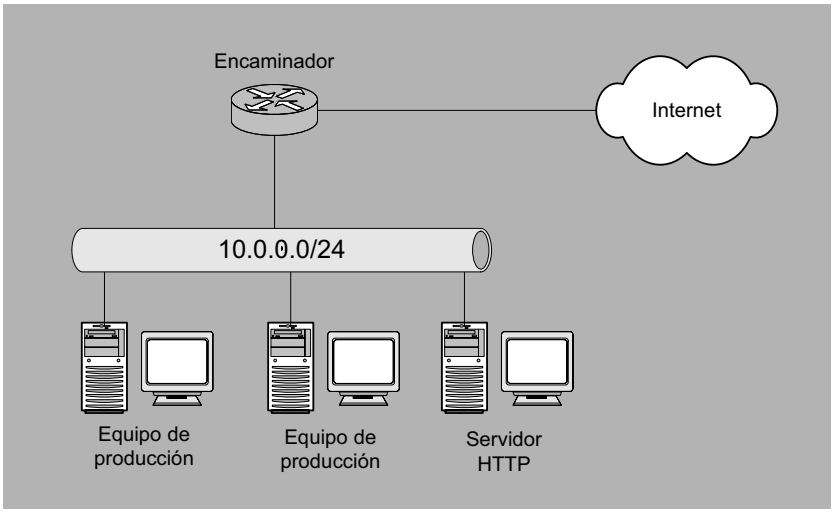
Una política de denegación por defecto suele ser más costosa de mantener, ya que será necesario que el administrador indique explícitamente todos los servicios que tienen que permanecer abiertos (los demás, por defecto, serán denegados en su totalidad).

En cambio, una política de aceptación por defecto es más sencilla de administrar, pero incrementa el riesgo de permitir ataques contra nuestra red, ya que requiere que el administrador indique explícitamente qué paquetes es necesario descartar (los demás, por defecto, serán aceptados en su totalidad).

Ejemplos de configuración

En la figura siguiente se presenta una posible red en la que se ha implantado la siguiente política de seguridad mediante la configuración de un conjunto de reglas de filtrado de paquetes aplicadas en el mismo encaminador:

- Todos los sistemas de la red interna 10.0.0.0 pueden acceder a cualquier servicio TCP de internet.
- El tráfico ICMP sólo está permitido de salida, no de entrada (para evitar la extracción de información mediante este protocolo).
- Los sistemas externos no se pueden conectar a ningún sistema interno, excepto al servidor de HTTP (10.0.0.1).

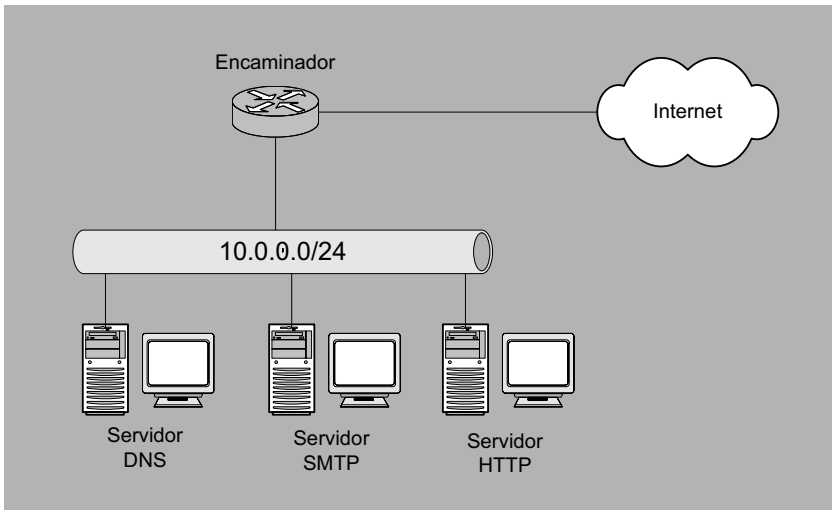


Las reglas de filtrado configuradas en el encaminador corresponden a la siguiente tabla:

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Permite	10.0.0.0	*	*	*	ICMP	Permite tráfico ICMP de salida
2	Permite	10.0.0.0	*	*	*	TCP	Permite conexiones TCP de salida
3	Permite	*	*	10.0.0.1	80	TCP	Permite conexiones HTTP de entrada
4	Rechaza	*	*	10.0.0.0	*	*	Rechaza cualquier otra conexión a la red interna

Como segundo ejemplo, podemos pensar en la misma red, pero con la siguiente política de seguridad:

- Todos los sistemas de la red interna 10.0.0.0 pueden acceder a cualquier servicio TCP de la red internet, exceptuando HTTP.
- Se deben de autorizar accesos al servidor de DNS (10.0.0.3).
- Los sistemas externos no se pueden conectar a ningún sistema interno, excepto al servidor de HTTP (10.0.0.1) y de SMTP (10.0.0.2).



Las reglas de filtrado de este segundo ejemplo podrían corresponder a las expresadas en la siguiente tabla:

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Rechaza	10.0.0.0	*	*	80	TCP	Rechaza cualquier conexión a servidores HTTP
2	Permite	10.0.0.0	*	*	*	TCP	Permite conexiones TCP de salida
3	Permite	*	*	10.0.0.1	80	TCP	Permite conexiones HTTP entrantes
4	Permite	*	*	10.0.0.2	25	TCP	Permite conexiones SMTP entrantes
5	Permite	*	*	10.0.0.3	53	UDP	Permite conexiones DNS entrantes
6	Rechaza	*	*	10.0.0.0	*	*	Rechaza cualquier otra conexión a la red interna

Ventajas y desventajas de los encaminadores con filtrado de paquetes

La construcción de un sistema cortafuegos mediante un encaminador con filtrado de paquetes es realmente económica, ya que generalmente suelen ser construidos con *hardware* ya disponible. Además, ofrece un alto rendimiento para redes con una carga de tráfico elevada. Adicionalmente, esta tecnología permite la implantación de la mayor parte de las políticas de seguridad necesarias.

Un ejemplo de encaminador con filtrado de paquetes podría ser la utilización de un sistema GNU/Linux actuando como encaminador de tráfico IP, junto con sus herramientas de administración asociadas para la construcción de las reglas de filtrado.

Las **políticas de seguridad** son el resultado de documentar las expectativas de seguridad, intentando plasmar en el mundo real los conceptos abstractos de seguridad.

Se pueden definir de forma procesal (plasmando de forma práctica las ideas o filosofías de la empresa en cuanto a seguridad) o de manera formal (utilizando un modelo matemático que intente abarcar todos los posibles estados y operaciones).

Aun con estas ventajas, los encaminadores de red con filtrado de paquetes pueden presentar algunas deficiencias como, por ejemplo:

* En inglés, *logging*.

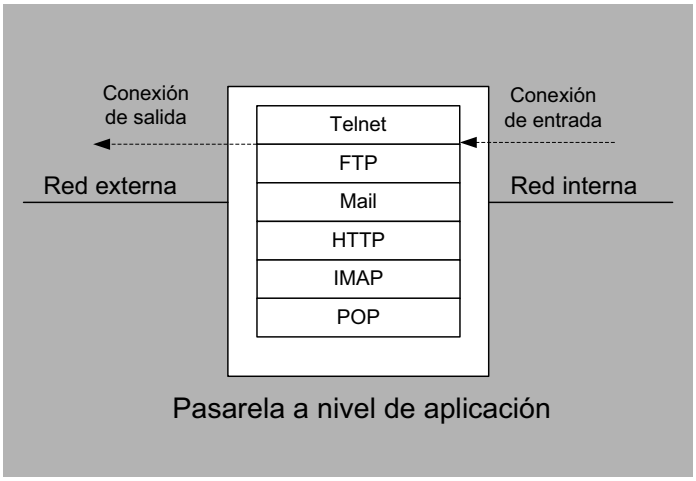
- Muchos de los encaminadores utilizados pueden ser vulnerables a ataques existentes (aunque la mayoría de los distribuidores tendrán los correspondientes parches para solucionarlo). Aparte, no siempre activan sus capacidades de registro*. Esto provoca que para el administrador sea difícil conocer si su encaminador está siendo atacado.

- Su capacidad de actuación puede llegar a deteriorarse a causa de la utilización de un filtro excesivamente estricto, dificultando también el proceso de gestión del dispositivo si este número de reglas llegara a ser muy elevado.

- Las reglas de filtrado pueden ser muy complejas, y en ocasiones sucede que posibles distracciones en su configuración sean aprovechadas por un atacante para realizar una violación de la política de seguridad.

2.2.2. Pasarelas a nivel de aplicación

Una pasarela a nivel de aplicación, conocida también como servidor intermediario (o en inglés *proxy*), no encamina paquetes a nivel de red sino que actúa como retransmisor a nivel de aplicación. Los usuarios de la red contactarán con el servidor intermediario, que a su vez estará ofreciendo un servicio *proxy* asociado a una o más aplicaciones determinadas.

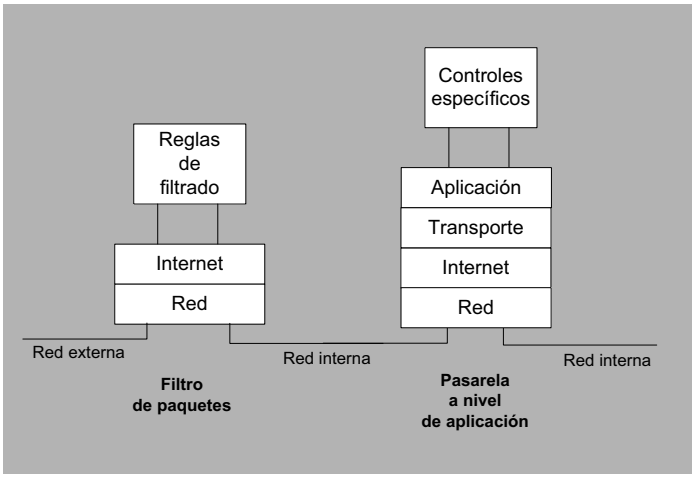


El servicio *proxy* se encargará de realizar las conexiones solicitadas con el exterior y, cuando reciba una respuesta, se encargará de retransmitirla al equipo que había iniciado la conexión. Así, el servicio *proxy* ejecutado en la pasarela aplicará las normas para decidir si se acepta o se rechaza una petición de conexión.

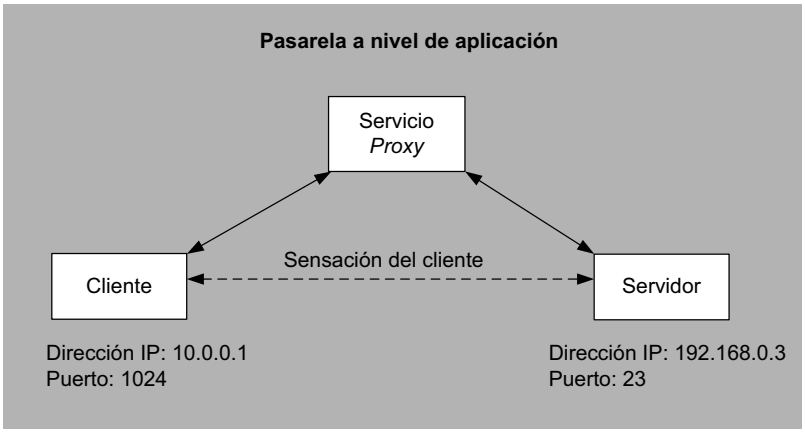
Una pasarela separa completamente el interior del exterior de la red en la capa de enlace, ofreciendo únicamente un conjunto de servicios a nivel de aplicación. Esto permite la autenticación de los usuarios que realizan peticiones de conexión y el análisis de conexiones a nivel de aplicación.

Estas dos características provocan que las pasarelas ofrezcan una mayor seguridad respecto a los filtros de paquetes, presentando un rango de posibilidades muy elevado. Por el contrario, la penalización introducida por estos dispositivos es mucho mayor. En el caso de una gran carga de tráfico en la red, el rendimiento puede llegar a reducirse drásticamente.

En la práctica, las pasarelas y los dispositivos de red con filtrado de paquetes son complementarios. Así, estos dos sistemas se pueden combinar, proporcionando más seguridad y flexibilidad que si se utilizara solamente uno, como se muestra en la siguiente figura:



Cuando la pasarela verifica al cliente, abre una conexión al servidor *proxy*, siendo éste el responsable de transmitir los datos que reciba el cliente del servidor intermediario.



Este funcionamiento particular provoca que las pasarelas a nivel de aplicación presenten un rendimiento inferior que los filtros de paquetes (debido al elevado número de conexiones adicionales que hay que realizar). Para evitarlo, los servidores intermediarios se pueden configurar para realizar una copia de los datos recibidos de un sistema y entregarlos de nuevo más tarde si otro equipo de la red los solicita*.

* Sistemas conocidos como *proxy cache*.

El uso de las pasarelas proporciona varios beneficios. De entrada, una pasarela podría permitir el acceso únicamente a aquellos servicios para los que hay un servidor *proxy* habilitado. Así, si una pasarela contiene servicios intermediarios tan solo para los servicios HTTP y DNS, entonces sólo HTTP y DNS estarán permitidos en la red interna. El resto de servicios serían completamente rechazados.

Otro beneficio del uso de pasarelas es que el protocolo también se puede filtrar, prohibiendo así el uso de distintos subservicios dentro de un mismo servicio permitido. Por ejemplo, mediante una pasarela que filtrara conexiones FTP, sería posible prohibir únicamente el uso del comando PUT de FTP, dejando habilitado el resto de comandos. Esta característica no sería posible haciendo uso únicamente de filtros de paquetes.

Adicionalmente, los servidores intermediarios también pueden implantar el filtro de conexiones por dirección IP de la misma forma que los filtros de paquetes, ya que la dirección IP está disponible en el ámbito de aplicación en el cual se realizará el filtrado.

Aun obteniendo más control global sobre los servicios vigilados, las pasarelas también presentan algunas problemáticas. Uno de los primeros incovenientes que hay que destacar es la necesidad de tener que configurar un servidor *proxy* para cada servicio de la red que se debe vigilar (HTTP, DNS, Telnet, FTP, ...). Además, en el caso de protocolos cliente-servidor como, por ejemplo, FTP, pueden llegar a ser necesarios algunos pasos adicionales para conectar el punto final de la comunicación.

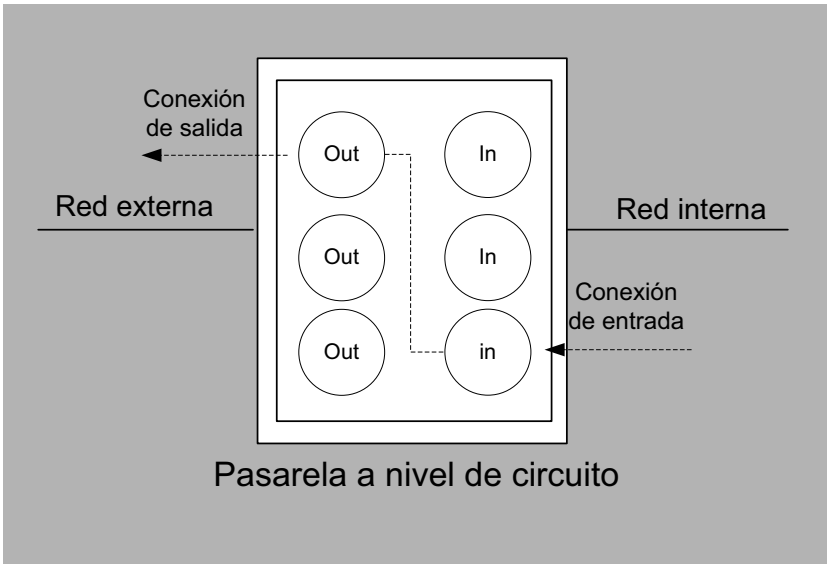
2.2.3. Pasarelas a nivel de circuito

Las pasarelas a nivel de circuito son un híbrido entre los esquemas de filtrado de paquetes y el uso de servidores intermediarios.

Una **pasarela a nivel de circuito** es un dispositivo similar al de pasarela a nivel de aplicación, donde el usuario establece primero una conexión con el sistema cortafuegos y éste establece la conexión con el equipo de destino.

Pero, en contraste con una pasarela tradicional, una pasarela a nivel de circuito opera de manera similar a un filtro de paquetes a nivel de red una vez que la conexión ha sido inicializada.

Así, una vez establecida la conexión, el dispositivo se encargará de retransmitir todo el tráfico entre ambas partes sin inspeccionar el contenido de los paquetes a nivel de aplicación, tal y como muestra la siguiente figura:



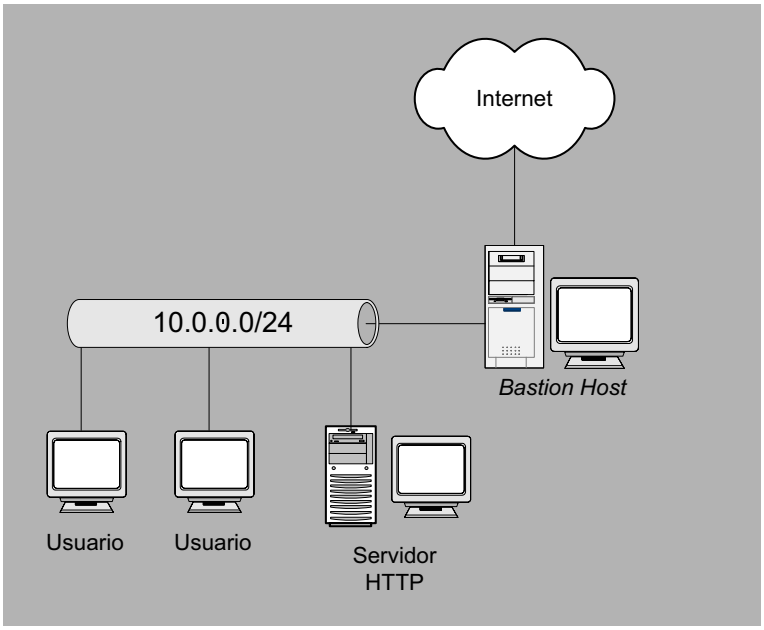
La función de seguridad que ofrece este tipo de dispositivo consiste en determinar qué conexiones están permitidas, antes de bloquear conexiones hacia el exterior.

Esta forma de trabajar es mucho más rápida que un sistema tradicional, ya que las conexiones pueden ser restringidas a nivel de usuario sin necesidad de analizar todo el contenido de los paquetes transmitidos.

2.3. Zonas desmilitarizadas

En ciertas instalaciones, no es suficiente un único dispositivo cortafuegos. Aquellas redes formadas por múltiples servidores, accesibles públicamente desde el exterior, juntamente con estaciones de trabajo que deberían estar completamente aisladas de conexiones con el exterior, se beneficiarán de la separación entre dos grupos de sistemas cortafuegos.

Supongamos, por ejemplo, la siguiente red:



En la figura anterior vemos un único sistema cortafuegos como punto de protección, implantado mediante la utilización de un equipo bastión con una arquitectura *dual-homed*.

Equipo bastión

El nombre de *equipo bastión* (*bastion host*) proviene de las murallas fuertemente protegidas que separaban los castillos medievales del exterior.

Un **equipo bastión** (en inglés *bastion host*) es un sistema informático que ha sido fuertemente protegido para soportar los supuestos ataques desde un lugar hostil (en este caso, internet) y que actúa como punto de contacto entre el interior y el exterior de una red.

Una **arquitectura de cortafuegos *dual-homed*** se construye mediante el uso de un equipo *dual-homed* con la capacidad de encaminamiento desactivada. De esta forma, los paquetes IP de un extremo de la red (la parte hostil) no serán encaminados hacia la parte protegida, y viceversa, a no ser que se indique lo contrario.

Equipo *dual-homed*

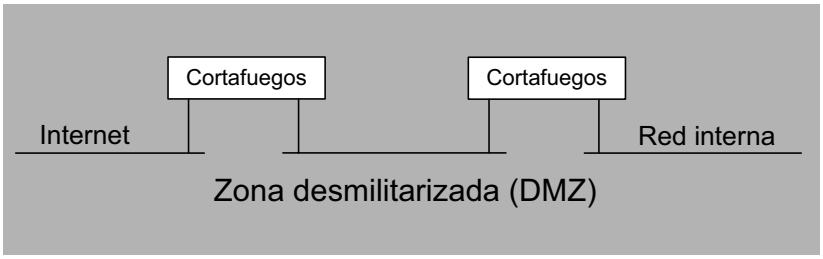
Se trata de un equipo informático de propósito general que tiene, al menos, dos interfícies de red (en inglés, *network interfaces* o *homes*).

Mediante esta arquitectura, los equipos de la red interna se pueden comunicar con el equipo *dual-homed*, los equipos de la red externa pueden comunicarse con el equipo *dual-homed*, pero los equipos de la red interna y externa no se pueden poner en comunicación directamente, sino que un servidor intermediario se encarga de realizar las conexiones en nombre de estas dos partes.

Esto hace que este cortafuegos con arquitectura *dual-homed* sea un punto crítico en la seguridad de la red. Si un atacante consigue comprometer cualquiera de los servidores que se encuentre detrás de este punto único, las otras máquinas podrán ser atacadas sin ninguna restricción desde el equipo que acaba de ser comprometido.

Para prevenir estas situaciones, es posible la utilización de dos dispositivos cortafuegos, introduciendo el concepto de zona desmilitarizada o DMZ*.

* En inglés, *DeMilitarized Zone.*

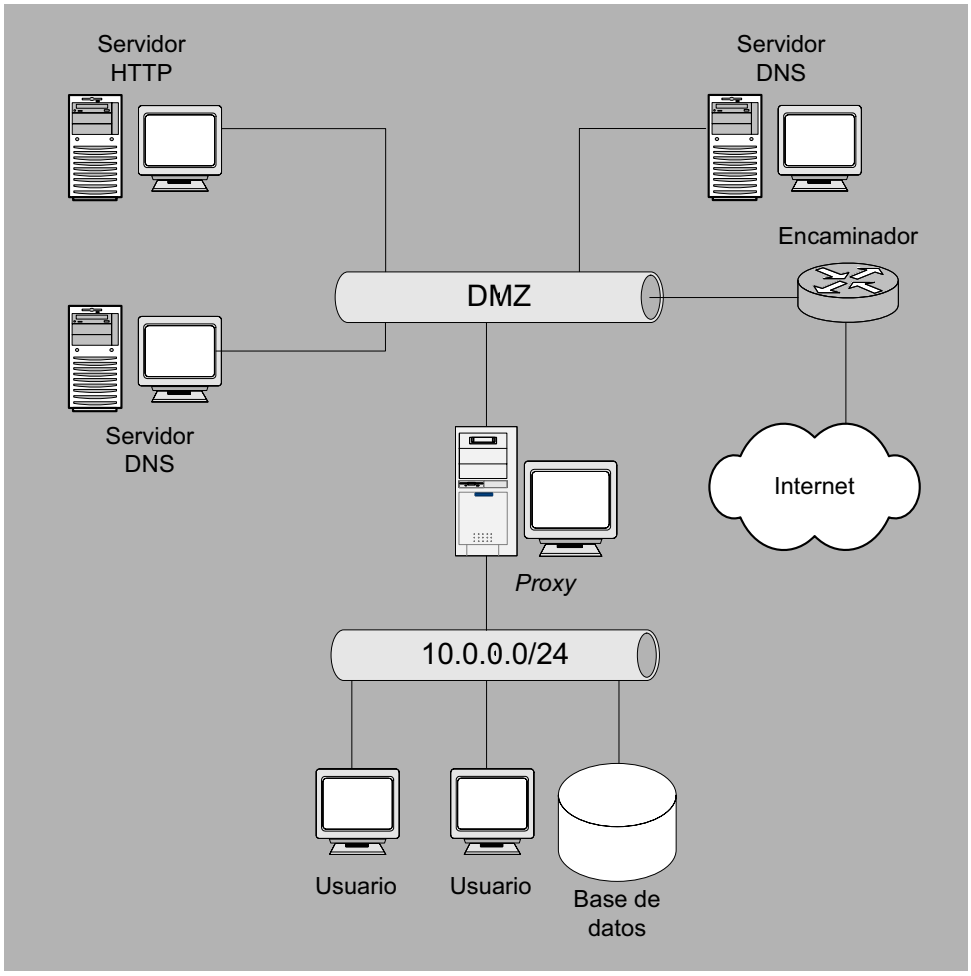


En la instalación que se muestra en la figura anterior, un cortafuegos separa el exterior de la red del segmento desmilitarizado (la DMZ) y los servidores que tienen que ser públicos desde el exterior de la red. El segundo cortafuegos, que hace de punto de contacto entre la red interna y la zona desmilitarizada, se configurará para que rechace todos los intentos de conexión que vayan llegando desde el exterior.

Así, si un atacante consigue introducirse en uno de los servidores de la zona desmilitarizada, será incapaz de atacar inmediatamente una estación de trabajo. Es decir, aunque un atacante se apodere del segmento de los servidores, el resto de la red continuará estando protegida mediante el segundo de los cortafuegos.

Combinación de tecnologías para la construcción de una DMZ

En la figura siguiente podemos ver el uso de un encaminador con filtrado de paquetes, juntamente con la utilización de un servidor intermediario para el establecimiento de una zona desmilitarizada.



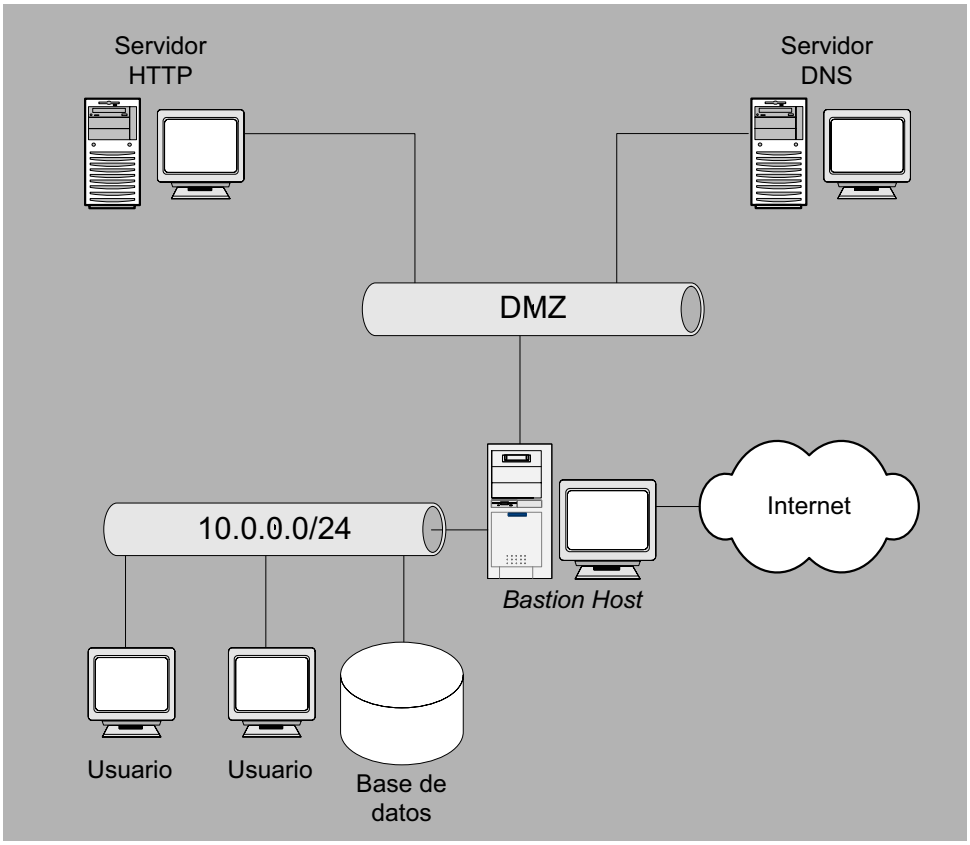
Otra forma de solucionar los mismos problemas planteados consiste en la utilización de un sistema que implemente una inspección de estados en el filtro de paquetes.

La **inspección de estados***, diseñada por la empresa de productos de seguridad *Chekpoint* e implementada inicialmente en el producto *Firewall-1*, combina (al igual que las pasarelas a nivel de circuito) el rendimiento de los filtros de paquetes con la seguridad adicional que presenta la utilización de servidores intermediarios.

* En inglés, *stateful multi layer inspection.*

De esta forma se puede simplificar el esquema planteado anteriormente y mantener a la vez un nivel de rendimiento sin renunciar a las capacidades de monitorización que ofrece la utilización de un punto de protección único.

En la figura siguiente se ilustra la implantación de un equipo bastión con arquitectura de cortafuegos *dual-homed* y con implantación de inspección de estados.



2.4. Características adicionales de los sistemas cortafuegos

Como hemos visto, la utilización de un sistema cortafuegos supone una barrera de control que mantendrá la red protegida de todos aquellos accesos no autorizados, actuando como un punto central de control y realizando las tareas de administración más simples.

No obstante, este control y protección de la red es únicamente una de las posibilidades que pueden ofrecer los sistemas cortafuegos más modernos.

Por el hecho de situarse en un punto de choque, los sistemas cortafuegos pueden ofrecer otras funciones interesantes. Algunas de estas características adicionales incluyen:

- **Filtrado de contenidos.** Muchas organizaciones desean evitar que sus usuarios utilicen los recursos corporativos para navegar por determinados sitios web no deseados. El filtrado de contenidos ofrecido por algunos sistemas cortafuegos puede bloquear el acceso a estos sitios web, a la vez que protege la red contra cualquier código malicioso insertado en sus páginas, como por ejemplo *ActiveX* y código *Java* hostil.

- **Red privada virtual*.** Este tipo de funcionalidad ofrecida por la mayoría de los sistemas cortafuegos actuales, permite la construcción de un túnel seguro entre dos puntos de la red, normalmente para proteger las comunicaciones de una red corporativa al atravesar una red hostil (como es el caso de internet).

- **Traducción de direcciones de red**.** Aunque no se trata estrictamente de una funcionalidad relacionada con la seguridad, la mayoría de los sistemas cortafuegos ofrecen la posibilidad de realizar NAT y poder así asociar direcciones IP reservadas (indicadas en el RFC 1918) a direcciones válidas. Un ejemplo podría ser la traducción de direcciones IP del rango 10.0.0.0/24 de una red privada para que salgan hacia internet com la dirección IP pública 212.46.31.224.

- **Balanceo de la carga.** El balanceo de la carga ofrecida por muchos sistemas cortafuegos es la tarea de segmentar el tráfico de una red de forma distribuida. Algunos sistemas cortafuegos ofrecen actualmente funcionalidades que pueden ayudar, por ejemplo, a distribuir tráfico FTP o HTTP de forma totalmente distribuida.

- **Tolerancia a fallos.** Algunos sistemas cortafuegos ofrecen actualmente soporte para determinar tipos de fallos. Para ello, se suele utilizar funcionalidades de alta disponibilidad ***. En estas situaciones, la mayor parte de las estrategias incluyen la utilización de distintos sistemas cortafuegos sincronizados, de manera que uno de los sistemas estará a la espera de que se produzca un fallo en el equipo original para ponerse en funcionamiento y sustituirlo.

-* En inglés, *Virtual Private Networking, (VPN).*
-** En inglés, *Network Address Translation, (NAT).*
-*** En inglés, *High-Availability, (HA).*

- **Detección de ataques e intrusiones.** Muchos de los fabricantes de sistemas cortafuegos incorporan a sus productos la capacidad de detectar exploraciones y ataques conocidos. Aunque este tipo de funcionalidad no comporta un problema en sí mismo, deberíamos tener presente que puede llegar a suponer una carga de trabajo adicional y que puede entorpecer la actividad principal del sistema cortafuegos.

- **Autentificación de usuarios.** Dado que el sistema cortafuegos es un punto de entrada a la red, puede llevar a cabo una autentificación adicional a la que efectúan los servicios ofrecidos por la misma. Así, la autentificación de usuarios en un sistema cortafuegos tendrá la finalidad de permitir o rechazar la conexión al usuario que solicita una conexión con un servicio interno (normalmente, mediante un mecanismo más fuerte que el implantado por el servicio al que se conecta).

Finalmente, cabe comentar que la construcción de servicios adicionales en un sistema cortafuegos incrementa el número de vulnerabilidades sobre éste y, por lo tanto, el riesgo. La práctica de implantar distintos servicios sobre un cortafuegos no es recomendable. Desde el punto de vista de la seguridad es mejor buscar una arquitectura distribuida.

Resumen

Cuando un sistema se conecta a una red informática, se expone a un conjunto de amenazas que siempre estarán presentes. Como ya hemos visto en el módulo anterior, es muy probable que estos sistemas presenten deficiencias de seguridad, aumentando la probabilidad de que se produzcan estas amenazas.

Los sistemas cortafuegos focalizan las decisiones de seguridad en un único punto de choque, tratando de rechazar cualquier conexión que no esté expresamente permitida.

Mediante un escenario de configuración de filtrado de paquetes en sistemas cortafuegos simples, se podrán aplicar tecnológicamente las decisiones de una política de seguridad definida por la organización.

También es posible la construcción de sistemas cortafuegos mediante tecnologías de servidores intermediarios o pasarelas, de manera que todo el tráfico recibido se pueda interpretar a niveles superiores del de red.

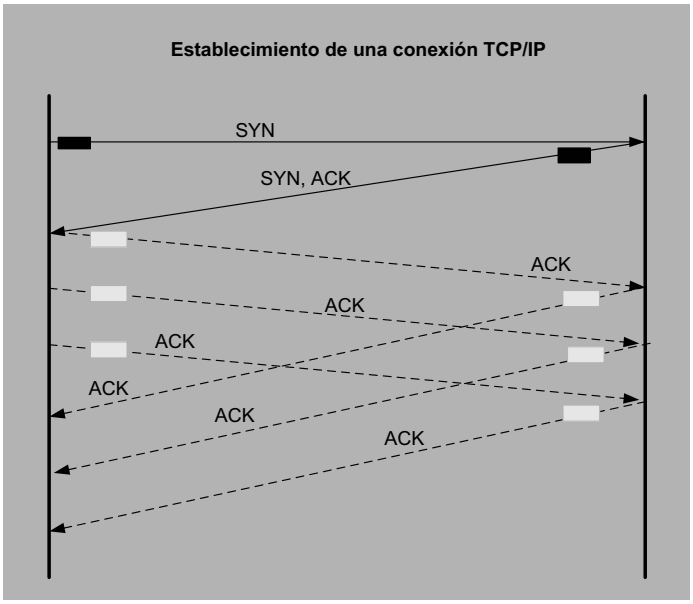
Así pues, la utilización de un sistema cortafuegos supone una barrera de control que mantendrá la red protegida de todos aquellos accesos no autorizados, actuando como un punto central de control y facilitando las tareas de administración.

Por otro lado, por el hecho de situarse en un punto intermedio, los sistemas cortafuegos ofrecen otras funciones de seguridad interesantes como podrían ser la monitorización de las conexiones de red, el análisis de contenidos, la realización de controles de autenticación adicionales, la construcción de redes privadas virtuales, etc. También pueden realizar funciones no relacionadas directamente con la seguridad de la red, como la traducción de direcciones IP (NAT), la gestión de servicios de red, el control del ancho de banda, ...

Finalmente, debemos tener presente que los sistemas cortafuegos son únicamente mecanismos de prevención y que no son una solución única para solventar todos los problemas de seguridad de una red conectada a internet. Estos sistemas no podrán proteger nunca a la red de aquellos ataques que se produzcan en su interior y es posible que un atacante externo pueda ser ayudado por un usuario interno para colaborar en un posible ataque. Tampoco podrán evitar ataques contra servicios con acceso global, ni podrán proteger a la red contra la transferencia de aplicaciones maliciosos (virus, gusanos, ...). Sería impracticable la utilización de un dispositivo que se dedicara a analizar todo el tráfico que circula a través suyo. Por este motivo, serán necesarios mecanismos de protección adicionales, como los que se presentarán en los módulos siguientes.

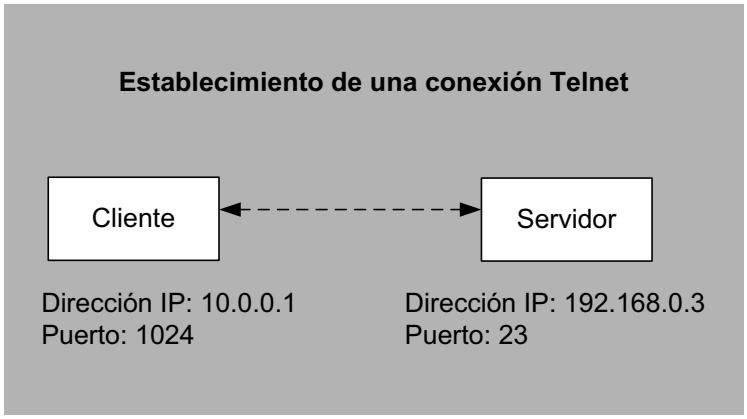
Ejercicios de autoevaluación

1) Según el siguiente esquema (donde se ilustra cómo ocurre una conexión TCP):



¿Qué tipo de paquetes podría inspeccionar un encaminador con filtrado de paquetes para poder controlar los intentos de conexión? ¿Y para identificar las respuestas?

2) A partir de la siguiente figura, donde se observa una conexión Telnet realizada desde el cliente hacia el servidor:

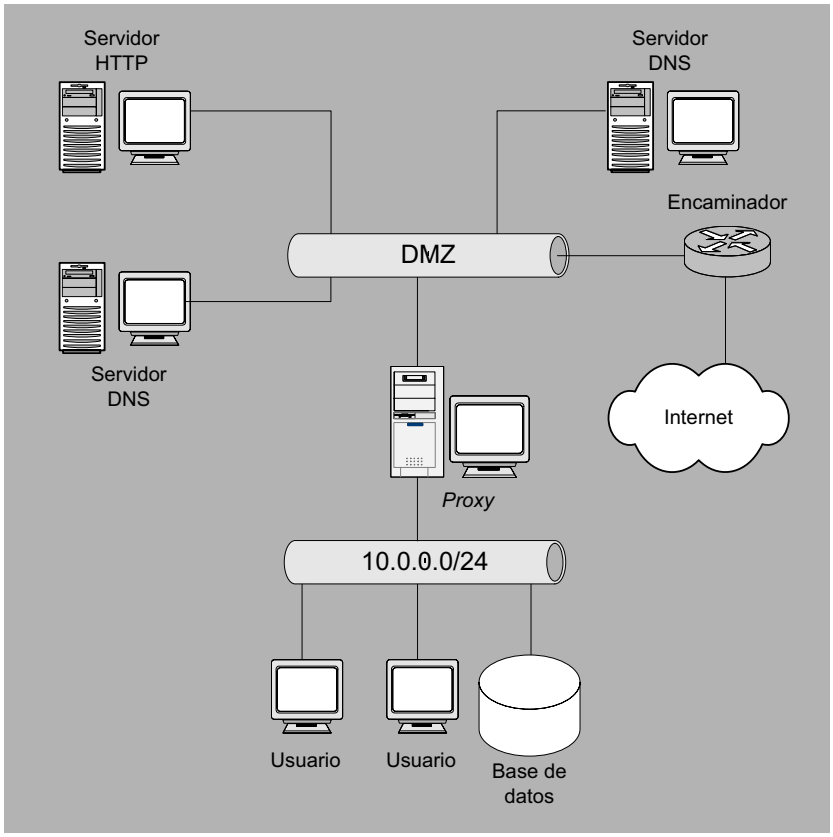


Si suponemos que el servidor 192.168.0.3 es el servidor Telnet de la red interna, ¿cómo se pueden bloquear las conexiones destinadas a éste, exceptuando las procedentes del sistema 10.0.0.1?

3) Según la siguiente política de seguridad, ¿cómo impediríais que se hicieran conexiones a servidores HTTP externos que funcionan sobre un puerto distinto del 80?

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Rechaza	10.0.0.0	*	*	80	TCP	Rechaza cualquier conexión a servidores HTTP
2	Permite	10.0.0.0	*	*	*	TCP	Permite conexiones TCP de salida
3	Permite	*	*	10.0.0.1	80	TCP	Permite conexiones HTTP entrantes
4	Permite	*	*	10.0.0.2	25	TCP	Permite conexiones SMTP entrantes
5	Permite	*	*	10.0.0.3	53	UDP	Permite conexiones DNS entrantes
6	Rechaza	*	*	10.0.0.0	*	*	Rechaza cualquier otra conexión a la red interna

4) ¿Por qué no encontramos la base de datos de la siguiente figura dentro de la zona desmilitarizada?



Soluciones

1) El filtro de paquetes inspeccionará únicamente el paquete de sincronismo o petición de inicio de conexión (con el indicador SYN activado); si se autoriza el paso a este paquete, se permite el establecimiento de la conexión.

Para identificar respuestas se recurre a la inspección del paquete que tienen los indicadores ACK y SYN activados. El resto de paquetes no son relevantes.

2) Para bloquear las conexiones destinadas al servidor 192.168.0.3, exceptuando las procedentes del sistema 10.0.0.1, podemos actuar de la siguiente manera:

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Permite	10.0.0.1	> 1023	192.168.0.3	23	TCP	Permite conexiones del sistema de teletrabajo
2	Rechaza	*	*	*	*	*	Rechaza cualquier otra conexión

3) A nivel de red no se puede distinguir si los paquetes dirigidos a un puerto arbitrario corresponden al protocolo HTTP o no. Por lo tanto, con un filtro de paquetes la única solución sería rechazar todos los paquetes con origen en la red interna, excepto los que puedan ser respuestas a peticiones de los servicios permitidos (puertos TCP de origen 25 y 80).

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Permite	10.0.0.0	80	*	*	TCP	Permite respuestas a peticiones HTTP
2	Permite	10.0.0.0	25	*	*	TCP	Permite respuestas a peticiones SMTP
3	Rechaza	10.0.0.0	*	*	*	TCP	Rechaza cualquier otro paquete de salida
4	Permite	*	*	10.0.0.1	80	TCP	Permite conexiones HTTP entrantes
5	Permite	*	*	10.0.0.2	25	TCP	Permite conexiones SMTP entrantes
6	Permite	*	*	10.0.0.3	53	UDP	Permite conexiones DNS entrantes
7	Rechaza	*	*	10.0.0.0	*	*	Rechaza cualquier otra conexión a la red interna

4) En la configuración del ejemplo se supone que el acceso a la base de datos únicamente se puede realizar desde la red interna. Por lo tanto, es mejor aislarla del exterior con dos sistemas cortafuegos (el encaminador y la pasarela) en lugar de dejarla en la zona desmilitarizada, donde sólo la separaría de la red externa el encaminador.

Otro criterio es el de poner el servicio lo más cerca posible de los sistemas; evidentemente, la base de datos es un servicio para la red interna (con clientes en la zona desmilitarizada). Nunca se accede a ésta directamente a través de internet. Si esto fuera realmente necesario, se podría recurrir a la utilización de una réplica de la base de datos accesible desde el exterior, habilitando únicamente las opciones de lectura.

Glosario

Arquitectura *dual-homed*: equipo informático de propósito general que tiene, al menos, dos interfaces de red.

Encaminador con filtrado de paquetes: dispositivo de red que encamina tráfico TCP/IP sobre la base de una serie de reglas de filtrado que deciden qué paquetes se encaminan a través suyo y cuáles son descartados.

Equipo bastión: sistema informático que ha sido fuertemente protegido para soportar los supuestos ataques desde un lugar hostil y que actúa como punto de contacto entre el interior y el exterior de una red.

Pasarela a nivel de aplicación: dispositivo de red que actúa com retransmisor a nivel de aplicación.

Pasarela a nivel de circuito: similar a una pasarela a nivel de aplicación en cuanto a la conexión, pero operando de manera similar a un filtro de paquetes a nivel de red (una vez que la conexión ha sido inicializada).

Política de seguridad: resultado de documentar las expectativas de seguridad de una red, tratando de plasmar en el mundo real los conceptos abstractos de seguridad.

Seguridad perimetral: seguridad basada únicamente en la integración en la red de sistemas cortafuegos y otros mecanismos de control de acceso.

Servidor intermediario: servidor *software* que se encarga de realizar las conexiones solicitadas con el exterior y retransmitirlas hacia el equipo que inició la conexión. En inglés, *proxy*.

Cortafuegos: elemento de prevención que realizará un control de acceso con el objetivo de separar nuestra red de los equipos del exterior (potencialment hostiles). En inglés, *firewall*.

Zona desmilitarizada: dentro de una red protegida por un cortafuegos, zona separada de los servidores públicos por un segundo cortafuegos.

Bibliografía

[1] Buch i Tarrats, J. (2000). *Sistemes de comunicacions - Arquitectures segures de xarxes (Sistemes tallafocs).* FUOC.

[2] Cheswick, W. R.; Bellovin, S. M.; Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker, 2nd ed.* Addison-Wesley Professional Computing.

[3] Hare, C.; Siyan, K. (1996). *Internet Firewalls and Network Security, 2nd ed.* New Riders.

[4] Zwicky, E. D.; Cooper, S.; Chapman, D. B. (2000). *Building internet Firewalls, 2nd ed.* O'Reilly & Associates.

Mecanismos de protección

Xavier Perramon