Seguridad Informática - 2º SMR
Tema 6: Seguridad de alto nivel en redes. Cortafuegos.

6.1 Seguridad de alto nivel

La seguridad de alto nivel pretende reducir al mínimo los elementos que pueden amenazar la seguridad de nuestro sistema. Para ello, se centra en actuar en el menor número posible de de elementos, pero en estos elementos se establece un control más estricto.

Los dos elementos fundamentales para este tipo de seguridad son los cortafuegos y los proxys. Que se tienen que combinar para optimizar la seguridad.

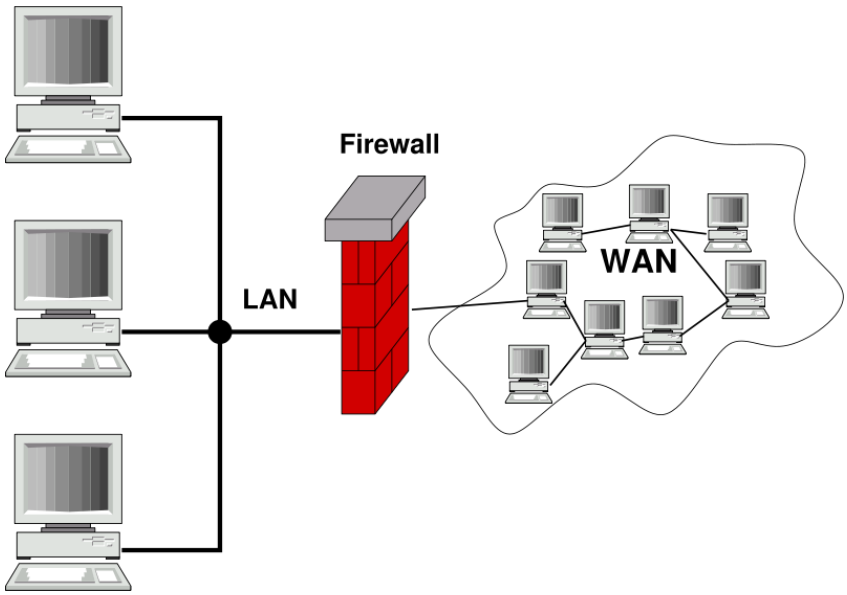
En los hogares normalmente el router hace de cortafuegos, pero en las empresas se han desarrollado una serie de arquitecturas y configuraciones más complicadas para alcanzar un seguridad óptima.

6.2 Cortafuegos

Los cortafuegos o *firewall* son uno de los principales mecanismos utilizados para mantener la seguridad de alto nivel. El nombre proviene de los cortafuegos utilizados para evitar que los incendios se propaguen. En nuestro caso el incendio es cualquier amenaza que intente entrar del exterior o trate de salir desde nuestra red.

Un cortafuegos es una parte de un sistema o una red que está diseñada para bloquear los accesos no autorizados y permitiendo al mismo tiempo aquellas comunicaciones autorizadas.

Un cortafuegos puede ser tanto un dispositivo hardware como software, podemos tener una máquina exclusivamente dedicada a esto o utilizar una aplicación en algunos de los equipos conectados a la red.



El cortafuegos se dedica a filtrar los paquetes a partir de unas reglas establecidas por el administrador de la red generalmente. Estas reglas tienen en cuenta la IP de origen, destino y el servicio de red con el que tienen relación para tomar la decisión de dejar pasar o no el paquete.

La función primaria de un cortafuegos es delimitar zonas con distintos niveles de seguridad. Es su configuración más sencilla existirán dos zonas, una zona segura que estará detrás del cortafuegos y una zona no segura que será Internet.

6.2.1 Ventajas de un cortafuegos

- **Protege de intrusiones**. El acceso a ciertos segmentos de la red sólo se permite desde ciertas máquinas autorizadas de otros segmentos de la red o de Internet.
- **Protección de información privada**. Permite definir distintos niveles de acceso a la información y a los servicios.
- **Optimización de acceso**. Identifica los elementos de la red interna optimizando la comunicación entre ellos.

> **Ejercicios propuestos**
>
> **6.2.1.** Realiza un esquema de la red de la clase y del instituto marcando las zonas en las que se divide el centro y donde están los cortafuegos. Indica a su vez qué funciones realizan cada uno de los cortafuegos.
>
> **6.2.2.** ¿Un cortafuegos protege contra la ingeniería social?¿Y contra espías corporativos? Razona tu respuesta.

6.2.2 Limitación de los cortafuegos

El cortafuegos filtra el tráfico de red, así que cualquier atacante que use tráfico aceptado por el cortafuegos o no use la red seguirá constituyendo una amenaza.

Además del filtrado de paquetes, los cortafuegos nos ofrecen una serie de servicios adicionales muy útiles para proteger nuestra red y nuestros servidores:

- **Bloqueo del trafico no autorizado**: Restringe servicios de Internet, bloquea páginas Web o rango de direcciones IP.
- **Ocultación de equipos en la LAN**: Oculta los equipos para evitar que sean atacados desde el exterior.
- **Registro del tráfico**: Como el cortafuegos se instala justo en la frontera entre la red interna y la externa, detecta todo el tráfico entre estas dos zonas, así que puede llevar un registro de este tráfico.
- **Redirección de tráfico entrante**: Redirige el tráfico entrante a la zona desmilitarizada de la organización evitando así que acceda a la red local.
- **Limitación de ancho de banda**: Permite limitar el ancho de banda utilizado por un protocolo en concreto o un tipo de tráfico.
- **Seguimiento de tráfico y monitorización de paquetes**: Genera estadísticas para detectar por ejemplo si un equipo se está descargando gran volumen de datos. Monitoriza también los ataques del exterior como el análisis y bloqueo de puertos para evitar los ataques más comunes.

6.3 Tipos de cortafuegos

6.3.1 En función de su ubicación

6.3.1.1 Cortafuegos personales

Este tipo de cortafuegos restringen la comunicación no autorizada con un equipo.

Se instala en el equipo del usuario y proporciona cinco funciones principales:

- Supervisa las conexiones con el exterior, tanto al resto de la red como Internet.
- Monitorizan los programas que tratan de acceder a Internet para que el usuario pueda decidir si lo permite o no.
- Permite bloquear los posibles intentos de intrusión al equipo u otro tipo de ataques como DoS que se puedan realizar desde Internet.
- Realiza un registro de todas las conexiones realizadas desde el equipo.
- Algunos incorporan filtros anti-spam, anti-virus u otros códigos malware.

Al principio estos programas se vendían con esta función exclusivamente, como era ZoneAlarm. Pero actualmente se incluyen en paquetes de seguridad como Panda o McAfee, o integrados en el sistema operativo como en Windows.

6.3.1.2 Cortafuegos de subredes

Aplican una política de seguridad a un grupo de sistemas desde un único punto. Para ello lo primero que se debe hacer es definir una serie de zonas de seguridad a las que se les aplicará una determinada política. Cada zona tendrá una serie de reglas diferentes del resto de las zonas.

Los cortafuegos se sitúan en los interfaces entre las distintas zonas, de forma que siempre tiene que haber un cortafuegos entre zona y zona.

Sus principales funciones son:

- Autorización de servicios tanto entrantes como salientes.
- Control de acceso a los servicios según la identidad del usuario o el equipo.
- Registro y monitorización de accesos a la red.

Este tipo de cortafuegos se basa en hacer una protección global sobre un único punto de forma que podemos relajar la protección de los equipos individuales. Esto facilita la administración de la política de seguridad y como los ataques se realizan sobre un único punto, facilitan su vigilancia.

6.3.2 Según su tecnología

- **Cortafuegos que actúan en el nivel de paquetes de datos**: De los paquetes de datos consulta la dirección destino, la dirección origen y el puerto y según estos parámetros deja pasar o no el paquete en función de las reglas que tenga establecidas. Trabaja en el **nivel de red** de la pila de protocolos OSI.
- **Cortafuegos que actúan en el nivel de circuitos**: De la pila OSI, este tipo de cortafuegos actúan en el **nivel de sesión**. Además de tener en cuenta las direcciones IP origen y destino y el puerto, también mira la información relativa a la sesión y los números de secuencia de los paquetes enviados. Por tanto, sabe cual es el paquete que se debe recibir en cada momento y se previenen ataques como el robo de sesión.
- **Cortafuegos que actúan como pasarelas de aplicación**: Actúa en el **nivel de aplicación** de la pila de protocolos. En vez de analizar los paquetes por separada, lo hace de todos los paquetes de un servicio en su conjunto por lo que son exclusivos de un servicio, necesitando por tanto, una pasarela de aplicación por cada servicio. Este tipo de cortafuegos consumen más recursos que los anteriores y necesitan un software específico en los equipos de los usuarios.
- **Cortafuegos transparentes**: Actúan en el **nivel de enlace**. Determinan que paquetes pasan y cuales no dependiendo de una serie de reglas. Son indetectables para los atacantes ya que no tienen una dirección IP.

6.4 Filtrado de paquetes

No todos los paquetes que intentan acceder a un equipo tienen por qué ser una amenaza. El filtrado de paquetes consiste en discriminar estos paquetes estableciendo cuales pueden pasar y cuales no en función de una serie de reglas.

Este método es uno de los más utilizados para la configuración de cortafuegos.

Los paquetes en su cabecera tienen información sobre su origen, destino así como el servicio y puerto utilizado en la comunicación, mediante una serie de reglas que tienen en cuenta esta información se puede realizar un filtrado de paquetes que proteja los equipos de posibles ataques.

6.4.1 Reglas de filtrado

Las reglas de filtrado nos permiten establecer políticas de seguridad para nuestra sistema. Se suelen expresar en una tabla de condiciones y acciones que se consulta en orden hasta que se encuentra con una regla que cumple y la ejecuta y no sigue leyenda el resto de reglas, de ahí la importancia en el orden de las reglas de filtrado.

Las reglas se pueden agrupar en tres tipos:

- Autoprotección del cortafuegos: no se permitirá la entrada de ningún paquete dirigido directamente al firewall.
- Reglas de salida: Pueden ser permisivas, donde se prohíben las excepciones y se permite el resto, o restrictivas, donde se prohíbe todo y se permiten las excepciones.
- Reglas de entrada: Está todo prohibido excepto aquello que se permite específicamente.

El ejemplo más claro de reglas de filtrado podemos verlo en el sistema Netfilter de linux que se gestiona con la utilidad llamada iptables.

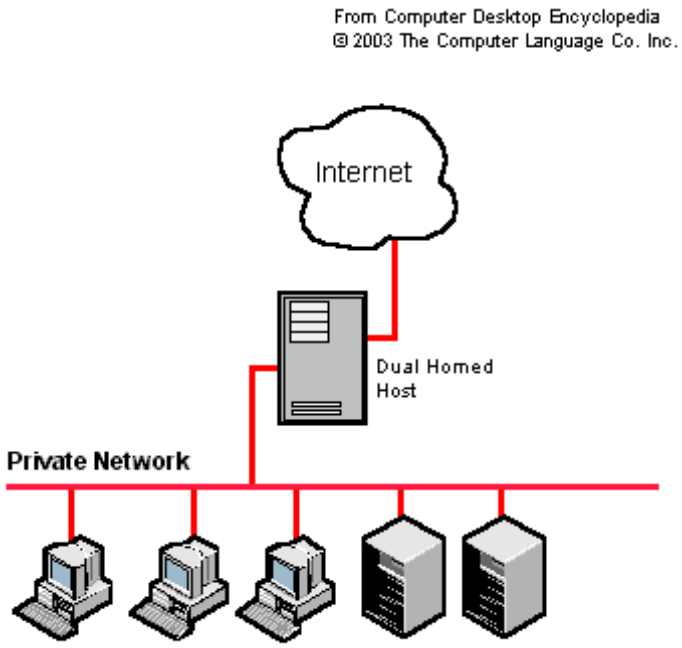
6.5 Elección del cortafuegos

Factores a tener en cuenta para elegir el cortafuegos:

- Política de seguridad del sistema: servicios o tráfico a bloquear.
- Nivel de monitorización: qué se permite y que se deniega.
- Económico, según el valor del sistema a proteger podremos hacer un desembolso mayor o menor.
- Localización: arquitectura a escoger
- Elementos físicos necesarios: bastión, routers...
- Sistema operativo del bastión o equipo donde se instala el cortafuegos.

6.6 Arquitecturas de red con cortafuegos

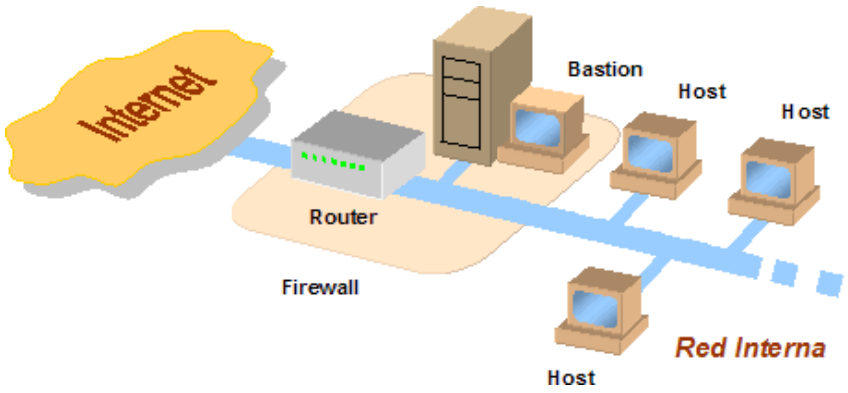
6.6.1 Dual-Homed Host



Esta estructura se base en la utilización de un equipo bastión con dos tarjetas de red. La red interna ve este equipo a través de una de las tarjetas de red y este equipo se conecta a la red externa mediante el otro interfaz de red, estando el tráfico entre estas dos redes aislados. Todo el tráfico de red interno pasará por el bastión donde estará instalado el cortafuegos y si queremos permitir algún servicio externo, como ver páginas web, habrá que instalar a su vez un proxy.

El inconveniente de este sistema consiste en que si un atacante se hace con el bastión, tendrá acceso a la red interna.

6.6.2 Screened Host



Esta arquitectura combina el uso de un bastión con un router, de esta forma el filtrado de paquetes se realiza primero por el router.

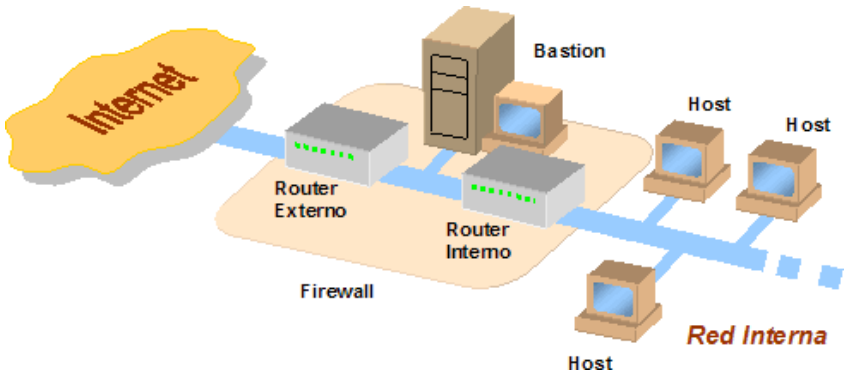
El bastión es el único sistema al que se puede acceder desde el exterior.

Cuando un equipo de la red interna quiera conectarse a Internet habrá dos opciones de configuración:

- Se pueden configurar las reglas del router para permitir algunos servicios directamente desde la red interna a Internet.
- Se puede configurar el router para prohibir cualquier tráfico de la red interna con Internet, de forma que el único equipo permitido para salir a la red externa sea el bastión.
- Se pueden combinar ambas opciones, de modo que haya servicios gestionados por el router y otros por el equipo bastión.

El inconveniente de esta arquitectura es que si un atacante se hace con el router o con el bastión, podrá tomar el control de la red interna.

6.6.3 Screened subnet



El bastión se aísla en una red perimétrica llamada **zona desmilitarizada** (DMZ). Está situada entre dos routers que conectan uno con la red interna y otro con la red externa. El router externo filtra las entradas desde la zona externa y las salidas a la misma. El router interno filtra a su vez el tráfico desde y hacia la red interna.

Esta arquitectura soluciona los problemas de las anteriores, ya que un atacante para llegar a la red interna necesitaría hacerse con el router externo, el bastión y el router interno.

6.7 Monitorización y logs

Lo registros de actividad o logs permiten detectar incidentes y comportamientos no habituales. Esta información puede resultar útil para:

- Localizar fallos o cambios en la configuración.
- Controlar el uso de recursos
- Proporcionar información sobre el rendimiento.

Los sistemas operativos incorporan logs para registrar información sobre procesos y usuarios. Además de estos registros de sucesos de los sistemas operativos, existen programas independientes que permiten gestionarlos.

Los cortafuegos proporcionan sus propios registros de actividad para analizar los bloqueos de accesos no autorizados y actividades anormales.

6.8 Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill
- http://www.alcancelibre.org/staticpages/index.php/como-shorewall-3-interfaces-red