SGF. IES Haría
UT5. Actividad 2

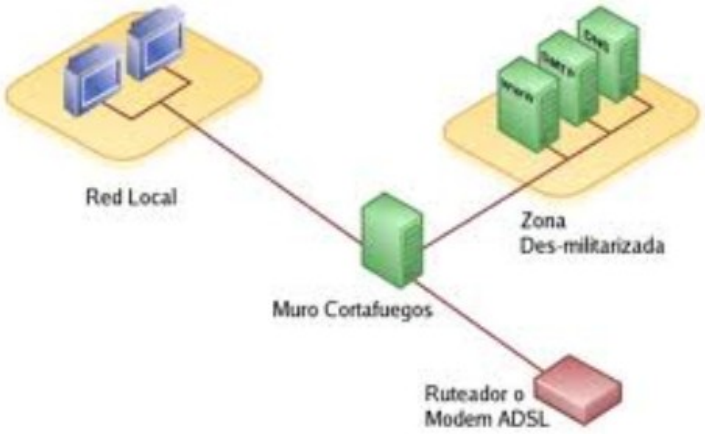
Cortafuegos

Objetivo

El objetivo de la actividad es conocer el funcionamiento de un sistema cortafuegos, conocer los niveles de red en los que trabaja, diferenciar los tipos de reglas y políticas que se pueden especificar y configurar un supuesto práctico de aplicación de un sistema de cortafuegos.

Teoría

Un firewall o cortafuegos es un dispostivo que está configurado para impedir el acceso no autorizado a una determinada zona de una red o dispositivo y que al mismo tiempo permite el paso a aquellas comunicaciones que están autorizadas.



Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan **acceso a redes privadas** conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos o pueden estar dirigidos al propio cortafuegos, que **examina** cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Los criterios de seguridad de los cortafuegos se aplican mediante **reglas** que especifican si se permite o no un determinado tráfico, filtrando el tráfico dirigido al cortafuegos o que lo atraviesa.

Aparte de aplicar reglas de filtrado también suele ser posible aplicar en los cortafuegos reglas reglas de NAT: estas se usan para hacer **redirecciones de puertos** o cambios (traducción) en las IPs de origen y destino.

También es frecuente conectar al cortafuegos a una tercera red, llamada «**zona desmilitarizada**» o **DMZ**, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

La implementación puede ser por software o por hardware y, ambas tienen dos posibles políticas de aplicación:

- **Política restrictiva**: impide todo el tráfico salvo el autorizado expresamente en la configuración.
- **Política permisiva**: permite el paso de toda comunicación salvo la expresamente prohibida.

A la hora de configurar un firewall hemos de tener en cuenta que este no nos protegerá de ataques internos ni de ataques a través de comunicaciones permitidas en la configuración del mismo.

Su **funcionamiento** es habitualmente muy simple:

- se analiza la **cabecera** de cada paquete, y en función de una serie de **reglas** establecidas de antemano la trama es bloqueada o se le permite seguir su camino
- estas reglas suelen contemplar campos como:
  - el **protocolo utilizado** (TCP, UDP, ICMP...),
  - las **direcciones fuente y destino** y
  - el **puerto destino**,

Por tanto, el *firewall* ha de ser capaz de trabajar en los **niveles de:**

- **red** (para discriminar en función de las direcciones origen y destino) y de
- **transporte** (para hacerlo en función de los puertos usados).

Además de la información de cabecera de las tramas, también se pueden especificar reglas basadas en la **interfaz** del *router* por donde se ha de reenviar el paquete, y también en la **interfaz** por donde ha llegado hasta nosotros.

Práctica

Como aplicación de cortafuegos utilizaremos la aplicación SHOREWALL. Se configurará una máquina virtual de Ubuntu Server con dos interfaces de red, una conectada a la red local (en modo puente) por la que accederemos a Internet a través del router del departamento y la otra en modo red interna, conectada a un equipo que hará de red local (192.168.10.0/24). El equipo hará también de encaminador de la red interna.

Realiza los siguientes pasos. Cuando termines avisa al profesor para que revise la práctica. En caso de que tengas alguna dificultad para realizar alguno de los pasos, no olvides realizar aportaciones a la base de datos describiendo el problema y la solución adoptada.

1) Averigua que son **netfilter** e **iptables** y para que los necesita **shorewall**.
2) Dibuja un esquema con las conexiones de la práctica especificando las direcciones IP de cada una de las zonas y de las interfaces de red involucradas. Nos podemos ayudar de la aplicación **Dia**.
3) Configurar las interfaces de red en el firewall comprobando que todo funciona correctamente en este punto.

4) Averigua en qué orden evalúa reglas y políticas el cortafuegos.
5) Configura Shorewall con la configuración por defecto para dos interfaces, inícialo y comprueba que el equipo de la red local puede acceder a Internet.
6) Añade una regla que permita acceder al firewall al cache de paquetes para instalar software. ¿En que IP y por qué puerto escucha el servidor de cache de paquetes de la red?.
7) Instalar ssh en el cortafuegos y configurar shorewall para poder acceder a dicho servicio desde tu equipo (red 172.16.0.0/16) y, posteriormente, desde la red 192.168.10.0/24.
8) Configurar en el equipo interno un servidor web y configura el cortafuegos de forma que podamos acceder a él desde cualquier equipo de la red 172.16.0.0/16.
9) Deshabilita el acceso por ssh al cortafuegos de un equipo en concreto de la red 172.16.0.0/16. Compruébalo.
10) Configurar el cortafuegos de forma que al *detenerlo* siga encaminando.

Opcional:

11) El paquete **dnsmasq** permite configurar un servidor de DNS en modo cache y un servidor DHCP. Instalarlo en el firewall y configurar ambas funcionalidades para que de servicio al equipo de la red interna. **Asegúrate que no interfiere en la red local del aula el servidor de DHCP (habilítalo sólo para la interfaz de red interna - eth1)**

Cuando termines avisa al profesor para que revise la práctica