Práctica 3 – Configuración de Red II (1 sesión, 0,5 puntos)

1.1 Introducción

Los cortafuegos protegen una red de los accesos desde otras redes, permitiendo pasar algunos paquetes y bloqueando otros. Son un elemento fundamental de seguridad en redes. En esta práctica se configurará el tipo de cortafuegos más común, un cortafuegos de filtrado de paquetes. Normalmente, todo el tráfico entrante y saliente de una red se reenvía a través de un único *router*. Ese *router* suele implementar, adicionalmente, un cortafuegos con la funcionalidad de filtrado de paquetes. Este filtrado se especifica mediante *reglas*, y dichas reglas se agrupan en *cadenas*.

1.1.1 Cadenas

Las cadenas básicas definidas en un router Mikrotik, tal como muestra la Fig. 1, son:

- **INPUT:** se aplica a los paquetes que tienen como dirección de destino alguna perteneciente al *router*, es decir, los paquetes se dirigen al *router*.
- **OUTPUT:** se aplica a los paquetes que tienen como dirección de origen alguna IP perteneciente al *router*, es decir, los paquetes son generados por el propio router.
- **FORWARD:** se aplica a los paquetes que debe reenviar el *router* según sus tablas de encaminaniento, es decir, los paquetes ni han sido generados ni van dirigidos al *router*.

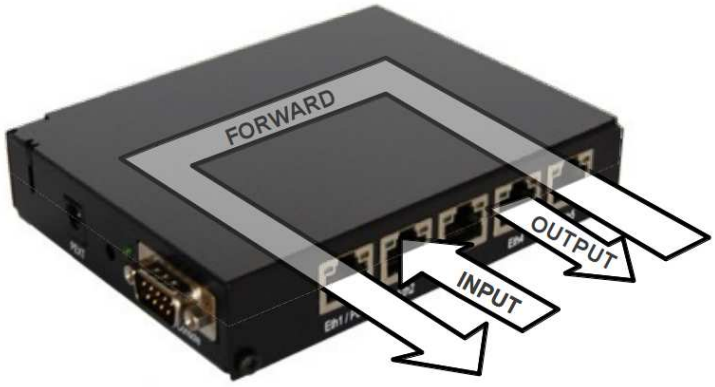

Figura 1: Cadenas de reglas de filtrado básicas.

1.1.2 Reglas

Las reglas de filtrado tienen dos partes:

1. El criterio de selección de los paquetes a los que aplicar la regla. Por ejemplo: el puerto de destino debe ser el 80.
2. La acción a llevar a cabo sobre los paquetes seleccionados previamente. Por ejemplo: bloquear el paso de los paquetes.

Los criterios básicos de selección de paquetes suelen basarse en campos de los paquetes tales como: la dirección IP de destino, el puerto origen, el tipo de protocolo de transporte (UDP o TCP...), etc. Existen otros atributos tales como el estado de las conexiones TCP, o el tipo de segmento TCP (Syn, Fin, Ack, etc.).

Tras definir el criterio de selección de un paquete, se ha de indicar la acción a realizar. Las acciones básicas son:

- *accept:* acepta los paquetes que cumplen el criterio de selección, y sigue procesándolos normalmente.
- *drop:* descarta los paquetes seleccionados.
- *reject:* además de descartar los paquetes seleccionados, el *router* envía al origen un mensaje ICMP del tipo que especificado (ver Fig. 3).

1.2 Información básica para la realización de la práctica

En esta sección se ofrece la información básica y las referencias necesarias para llevar a cabo las tareas que se proponen en la práctica.

1.2.1 Configuración de reglas de filtrado

Para configurar el cortafuegos, acceder al *menú IP->Firewall* del menú de WinBox. Para añadir una nueva regla, desde la pestaña de "Filter Rules", añadir las reglas requeridas.

 El orden en el que aparezcan las reglas de filtrado es importante, ya que es el orden en el que se aplicarán. Por ejemplo, si se añade al principio una regla para descartarlo todo, las siguientes reglas de la cadena no tendrán efecto.

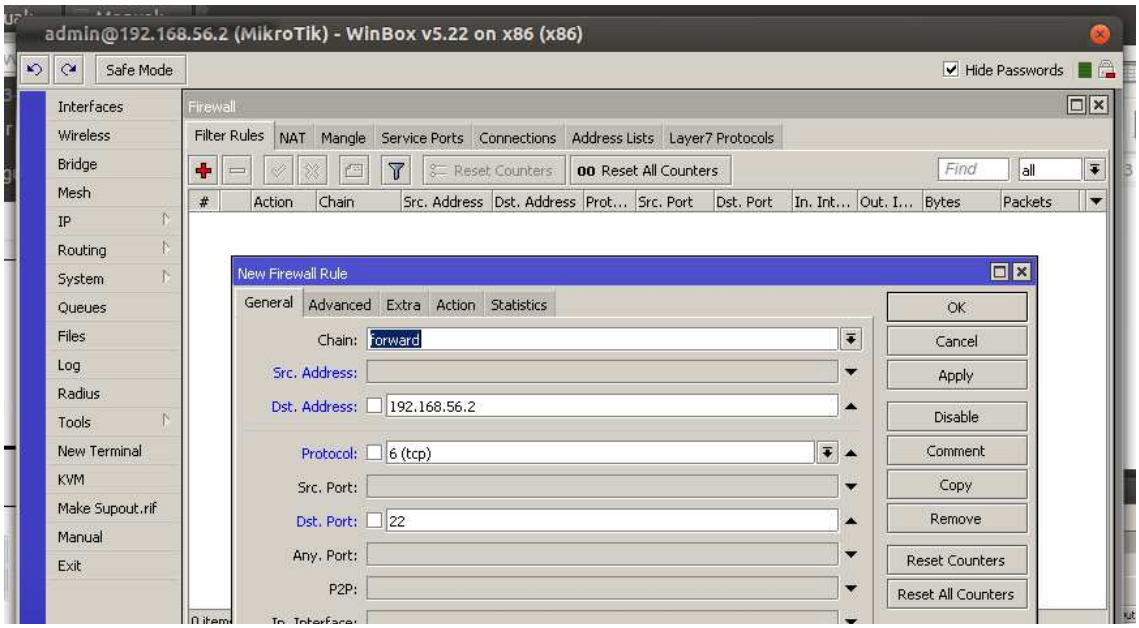

Figura 2: Configuración de una regla de filtrado desde WinBox.

Para configurar una nueva regla, seleccionar los campos y los valores que deben cumplir los paquetes en la pestaña "General" (ver Fig. 2). La acción a realizar con esos paquetes se puede configurar en la pestaña "Action" (ver Fig. 3).

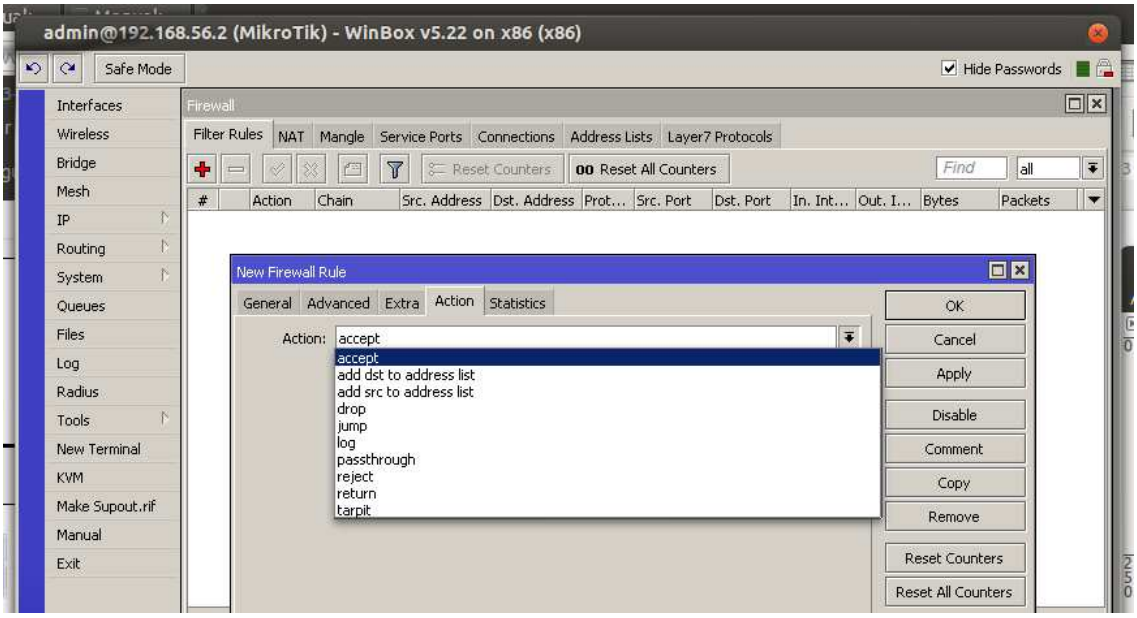

Figura 3: Configuración de la acción de una regla de filtrado.

1.3 Realización práctica

Es necesario configurar las tablas de encaminamiento de los ordenadores y del router al que se conectan de forma que todos los ordenadores de la isla sean alcanzables antes de continuar con los siguientes puntos.

1) Configure el *router* con el que está directamente conectado para que no reenvíe ningún tipo de tráfico (acción "drop"). Habitualmente, al configurar un cortafuegos, inicialmente se deniega cualquier acceso, y luego se añaden reglas para el tráfico que sí se desea dejar pasar.

2) A continuación configure el cortafuegos del *router* para que permita a otros ordenadores:
a) conectarse al servidor de SSH del ordenador que tenga la dirección 33.X.Y.2.
b) iniciar una conexión al servidor de SSH del ordenador que tenga la dirección 33.X.Y.3.

El servidor de SSH transporta sus mensajes sobre TCP, y por defecto escucha en el puerto 22. Esto significa que los paquetes dirigidos al servidor tendrán el número 22 como puerto de destino.

3) *(Opcional)* Configure el mismo router para que permita hacer ping de un ordenador a otro, pero no en sentido contrario. (Nota: la herramienta ping envía un mensaje ICMP de tipo "echo request", y recibe un mensaje ICMP del tipo "echo reply").

1.4 Bibliografía

Manual de MikroTik.
http://wiki.mikrotik.com/wiki/Manual:TOC