Práctica 1 – Configuración de Red II

1.1 Introducción

Un cortafuego en una red computadores consiste en una pasarela/barrera que separa dos redes o subredes. Normalmente una red interna (*intranet*) de una externa (*extranet*) a la organización. Dichos elementos, nos permiten tener un control de los servicios a los que se accede y comunicaciones que se efectúan entre ambas redes. En la Figura 1, se observa un ejemplo típico de localización de cortafuegos dentro de una organización. En dicha figura se observa un *router* de acceso que hace barrera entre la *intranet* de la empresa y el exterior, así como varios departamentos también protegidos por sus correspondientes cortafuegos. Además, se observa una DMZ (Demilitarized Zone) en donde se concentran aquellos servicios que son accesibles desde el exterior a través del *router* de acceso.

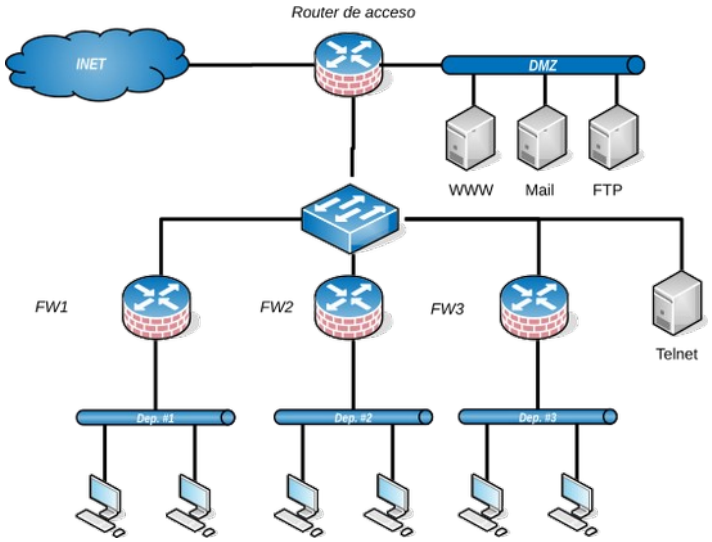

Figura 1: Ubicación típica de cortafuegos dentro de una ogranización.

Existen dos tipos principales de cortafuegos: de filtrado (IP) o de aplicación (*proxy*). Con respecto a los primeros, principalmente, ofrecen de una serie de filtros (reglas) que permiten controlar el acceso a determinados servicios, *hosts,* etc. Dichos filtros se pueden establecer en base a parámetros diversos tales como IP origen o destino, puerto origen o destino, protocolo (TCP/UDP), interfaz, etc.

Con respecto a los segundos, se trabaja a alto nivel (aplicación) y, a diferencia de los cortafuegos de filtrado, el *proxy* actúa de intermediario entre la petición del cliente (interno) y el servidor (externo). Esto es, de cara al exterior todas las peticiones provienen del *proxy* de manera que los clientes se ocultan al exterior.

1.1.1 Cadenas

Las cadenas básicas de filtrado definidas en un router Mikrotik, tal como muestra la Figura 2, son:

- **INPUT**: se aplica a los paquetes que tienen como dirección de destino alguna perteneciente al *router*, es decir, va dirigido al *router*.
- **OUTPUT**: se aplica a los paquetes que tienen como dirección de origen alguna IP perteneciente al *router*, es decir, la genera el propio dispositivo.
- **FORWARD**: se aplica a los paquetes que debe reenviar el *router* según sus tablas de encaminamiento, es decir, que ni ha sido generado ni va dirigido al propio dispositivo.

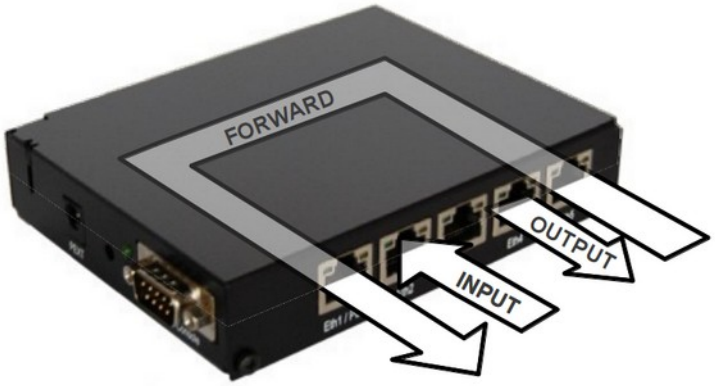

Figura 2: Cadenas de reglas de filtrado básicas.

1.1.2 Reglas

Las reglas de filtrado, como su propio nombre indica, establecen la política de acceso y control sobre un determinado paquete IP. Se deben entender como los criterios para seleccionar o no un paquete IP. Dichas reglas siempre se asocian a una determinada cadena.

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: impedir (*drop*) el paso de los paquetes que cumplan con el criterio de selección.

Los criterios básicos de selección de paquetes suelen basarse en campos de los paquetes tales como: la dirección IP de destino u origen, el puerto destino u 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 sobre dicho datagrama. Existen varias acciones predefinidas, aunque las básicas son:

- **accept**: acepta los paquetes que cumplen el criterio de selección, y sigue procesándolo normalmente.
- **drop**: descarta el paquete seleccionado.
- **reject**: además de descartar el paquete seleccionado, el *router* envía al origen un mensaje ICMP del tipo que se especifique.

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 Acceso al puesto de usuario y elección de sistema operativo

Para la realización de esta práctica, es necesario formar parejas. Después arrancar su puesto de usuario con la opción "Redes"→"Ubuntu 20.04".

Una vez que se haya identificado como "**administrador**"/"**finisterre**", puede pasar a modo *superusuario* mediante el siguiente comando, y utilizando la contraseña "**finisterre**"

```
# sudo su
```

1.2.2 Escenario de trabajo y dispositivos implicados

En la Figura 3 se observa el escenario de trabajo y los dispositivos implicados para la realización de la sesión de prácticas. El direccionamiento IP de los elementos que aparecen en la figura, se corresponde con aquellas direcciones que se encontrarían en la isla 1. Como cada pareja configurará el router al que tiene acceso directo desde su subred, será necesario dialogar con las demás parejas de la isla para realizar y probar las tareas que se exponen al final del presente guión.

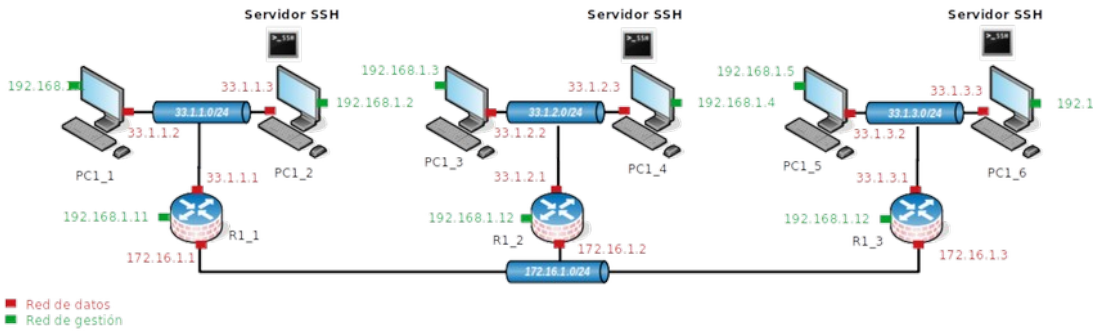

Figura 3: Escenario de trabajo y dispositivos implicados. Ejemplo para los dispositivos de la isla 1.

1.2.3 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.

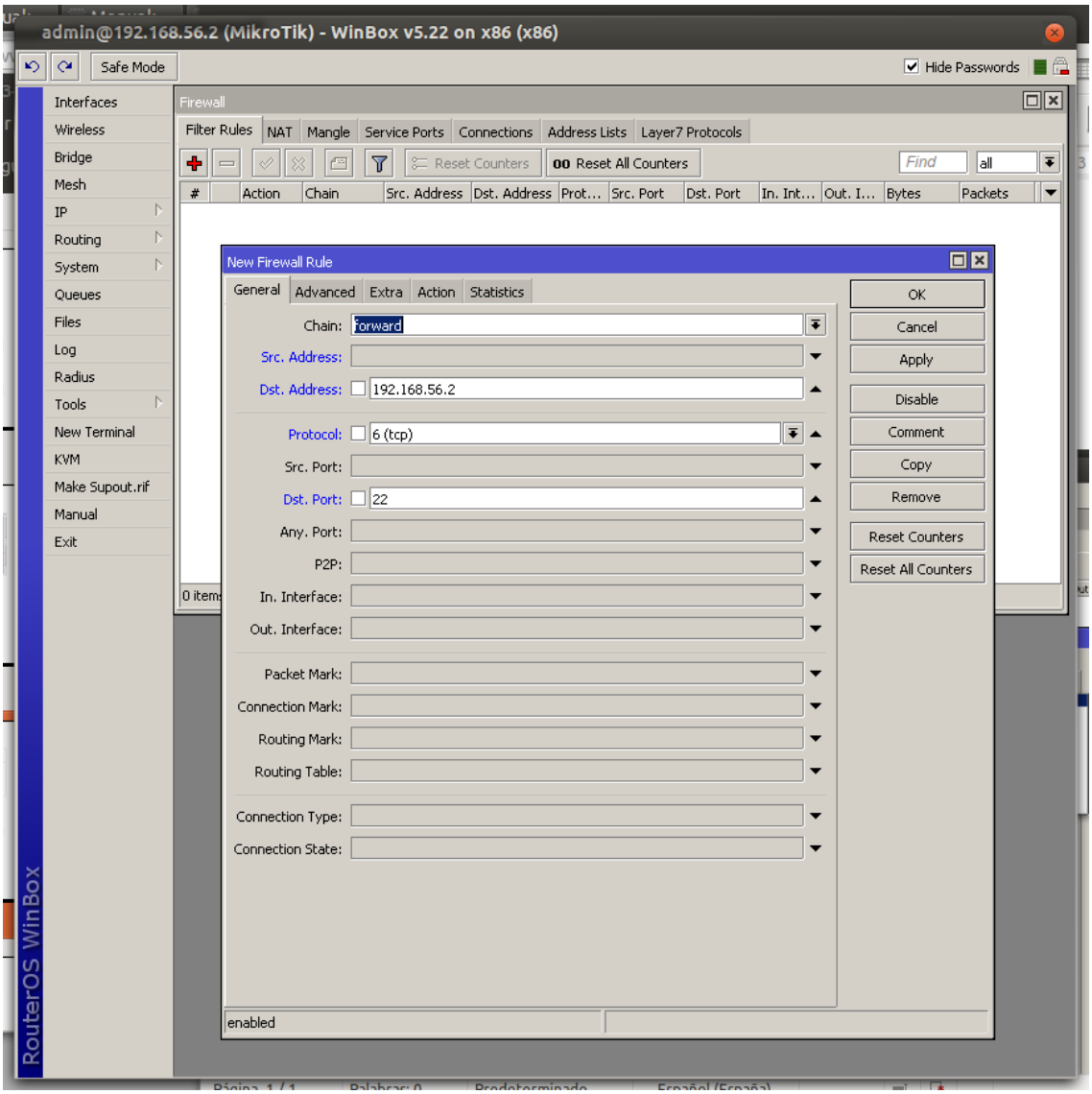

Figura 4: Configuración de una regla de filtrado desde WinBox.

Para configurar una nueva regla, seleccionar los campos y los valores que deben cumplir los paquetes en la pestaña "General" (ver Figura 4). La acción a realizar con esos paquetes se puede configurar en la pestaña "Action" (ver Figura 5).

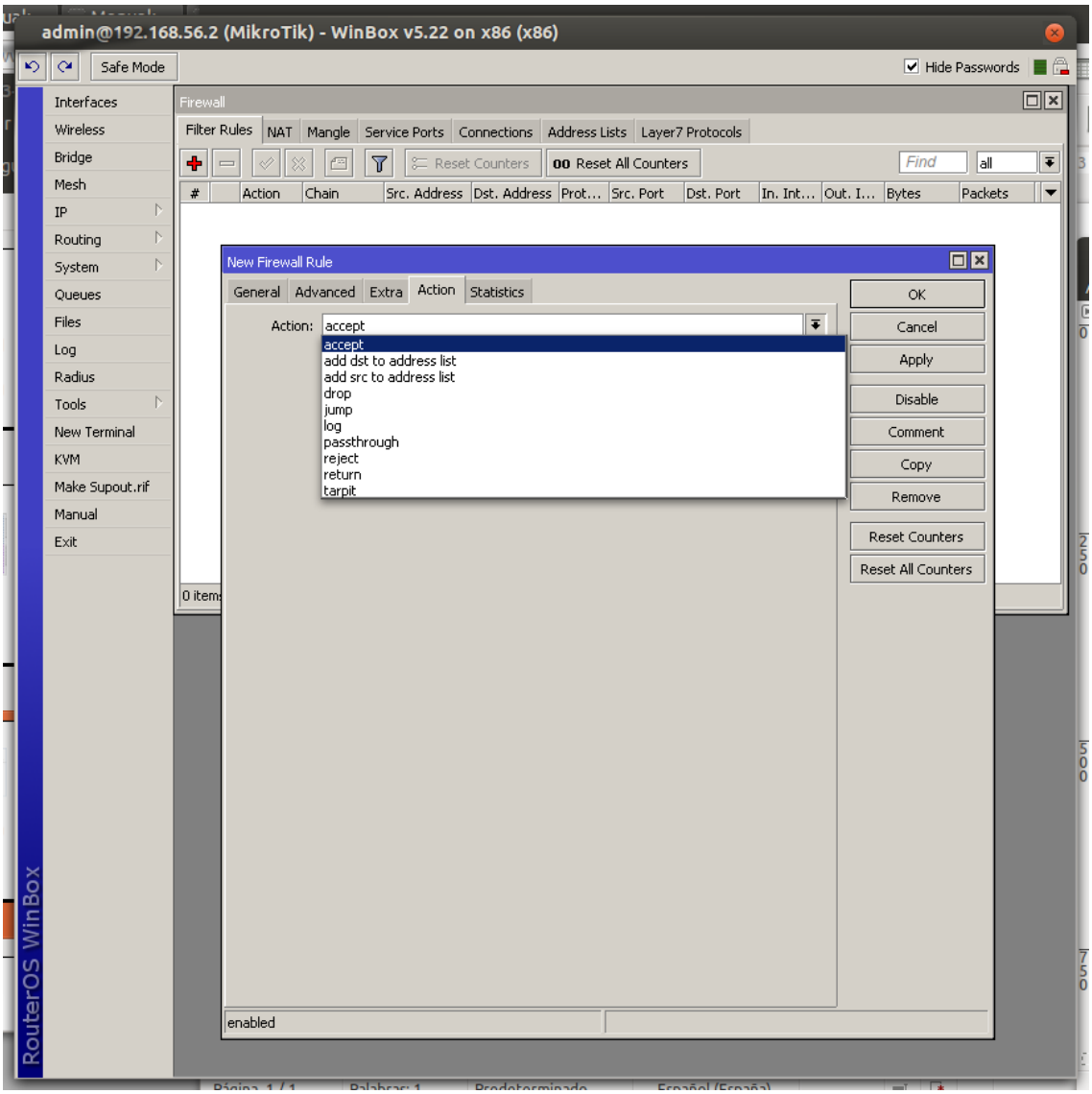

Figura 5: Configuración de la acción de una regla de filtrado.

1.3 Realización práctica

Es necesario configurar las tablas de encaminamiento tanto en los *routers* como en los dispositivos finales para estos últimos tengan conectividad entre ellos.

1) Configure su router, el que está directamente conectado a su subred, 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. Compruebe que ahora no es posible establecer conexiones entre los PC de diferentes subredes.

2) A continuación, configure el cortafuegos de su router para que permita a otros ordenadores conectarse únicamente al servidor de SSH instalado en uno de los PCs de su red (ver Figura 3).

Tenga en cuenta que el protocolo SSH transporta sus mensajes sobre TCP y utiliza el puerto 22.

Para conectarse remotamente a un PC remoto con SSH, utilizar el siguiente comando, donde `<usuario_PC_remoto>` es el usuario de la máquina remota con IP `<IP_PC_remoto>`

```
# ssh <usuario_PC_remoto>@<IP_PC_remoto>
```

3) (Opcional) Configure el mismo *router* para que permita hacer ping de un ordenador a otro, pero no en sentido contrario (ver Figura 3).

Tenga en cuenta que la herramienta `ping` envía mensajes ICMP de tipo `echo request` y recibe mensajes ICMP de tipo `echo reply`.

1.4 Bibliografía

[1] Manual de MikroTik. http://wiki.mikrotik.com/wiki/Manual:TOC
[2] Filtrado con MikroTik. https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter