Práctica 1 – Configuración de Red II

1.1 Introducción

Un cortafuegos (*firewall*) en una red de computadores permite establecer una pasarela o barrera entre dos subredes tal que el administrador pueda filtrar y/o permitir el tráfico cursado de una forma controlada, además de otras funciones como por ejemplo la monitorización o la contabilidad (*accounting*) del tráfico. Los cortafuegos nos permiten tener por tanto un control de los servicios a los que se accede y de las comunicaciones que se llevan a cabo en una red.

En la Figura 1, se observa un ejemplo típico de la ubicación de varios cortafuegos dentro de una organización. En dicha figura se observa un *router* de acceso, que conecta varios departamentos (típicamente con direcciones privadas) protegidos por sus correspondientes cortafuegos, además, de una DMZ (Demilitarized Zone), usualmente con direcciones públicas, en donde se concentran aquellos servicios que son accesibles desde el exterior.

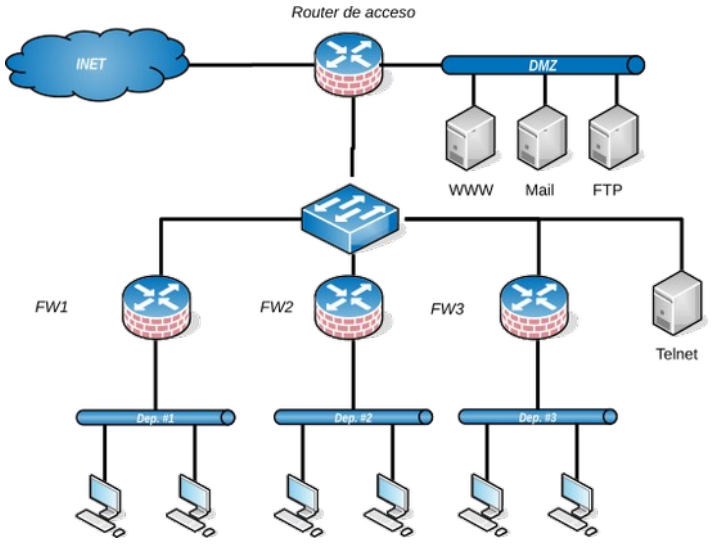
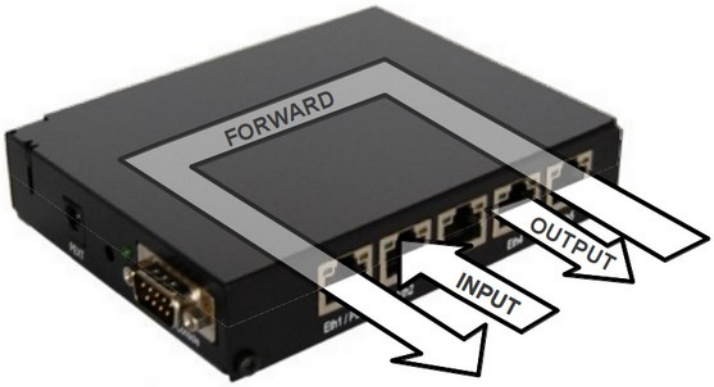


Figura 1: Ubicación típica de cortafuegos dentro de una ogranización.

Existen dos tipos principales de cortafuegos: de filtrado (*packet filters*) o de aplicación (*proxy*). Los primeros fundamentalmente ofrecen de una serie de filtros, definidos mediante un conjunto de reglas, que permiten controlar el acceso a determinados servicios, *hosts,* etc. Dichos filtros se pueden establecer teniendo en cuenta la IP origen o destino, o el campo protocolo del datagrama, el puerto origen o destino del segmento, la interfaz (dirección MAC), u otros campos de cualquiera de los protocolos implicados en capa de transporte e inferiores.

Los cortafuegos tipo *proxy* operan a nivel de aplicación y, a diferencia de los cortafuegos de filtrado, actúan de intermediarios entre los clientes (internos) y el servidor (externo). Esto es, de cara al exterior todas las peticiones provienen del *proxy* de manera que los clientes quedan ocultos.



1.1.1 Reglas

La definición del comportamiento de un firewall de filtrado se hace mediante reglas. Estas, como su propio nombre indica, definen la política de acceso y control sobre el tráfico cursado, mediante unos criterios para seleccionar o no los paquetes. Además cada regla define la acción a realizar sobre ese tráfico seleccionado. Las reglas de filtrado tienen, por tanto, 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 por el criterio de selección. Por ejemplo: descatar (*drop*) el reenvío de los paquetes que cumplan con el criterio de selección.

Los criterios básicos de selección de paquetes se suelen basar 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 se ha de indicar la acción a realizar. Existen varias acciones predefinidas, siendo las más habituales:

- **accept**: acepta los paquetes que cumplen el criterio de selección, y sigue procesándolos 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.

1.1.2 Cadenas

Las reglas se asocian según un criterio de selección previo que depende del tipo de paquetes a las que se aplican, formando lo que se conoce como cadenas (*chains*). Así en el *firewall* de los *routers* Mikrotik, tal y como muestra la Figura 2, las cadenas predefinidas son:

- **INPUT**: incluye las reglas que se aplican a paquetes que tienen como dirección destino alguna de las IPs del *router*, es decir aquellos paquetes que van dirigidos al *router*.

- **OUTPUT**: incluye las reglas que se aplican a paquetes generados por el propio router.
- **FORWARD**: incluye las reglas que se aplican a paquetes que reenvía el *router*, es decir los paquetes que ni se han generado ni van dirigidos al propio dispositivo.

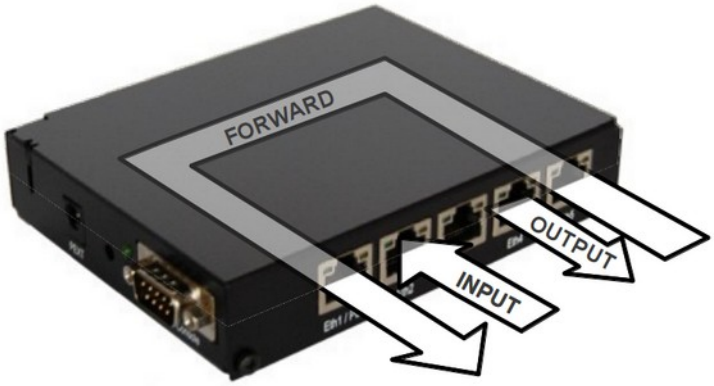


Figura 2: Cadenas de reglas de filtrado básicas.

1.2 Información básica para la realización de la práctica

En esta sección se ofrece 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 guion.

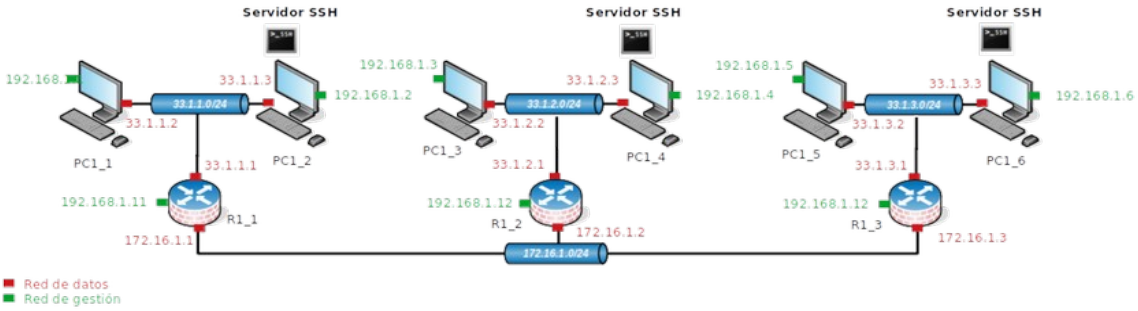


Figura 3: Escenario de trabajo y dispositivos implicados. Ejemplo para los dispositivos de la isla 1.

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 muy importante. Por ejemplo, si se añade al principio una regla genérica con acción *drop* para descartar todo el tráfico, las siguientes reglas de la cadena no tendrán efecto, por tanto esta debería ir en última posición.

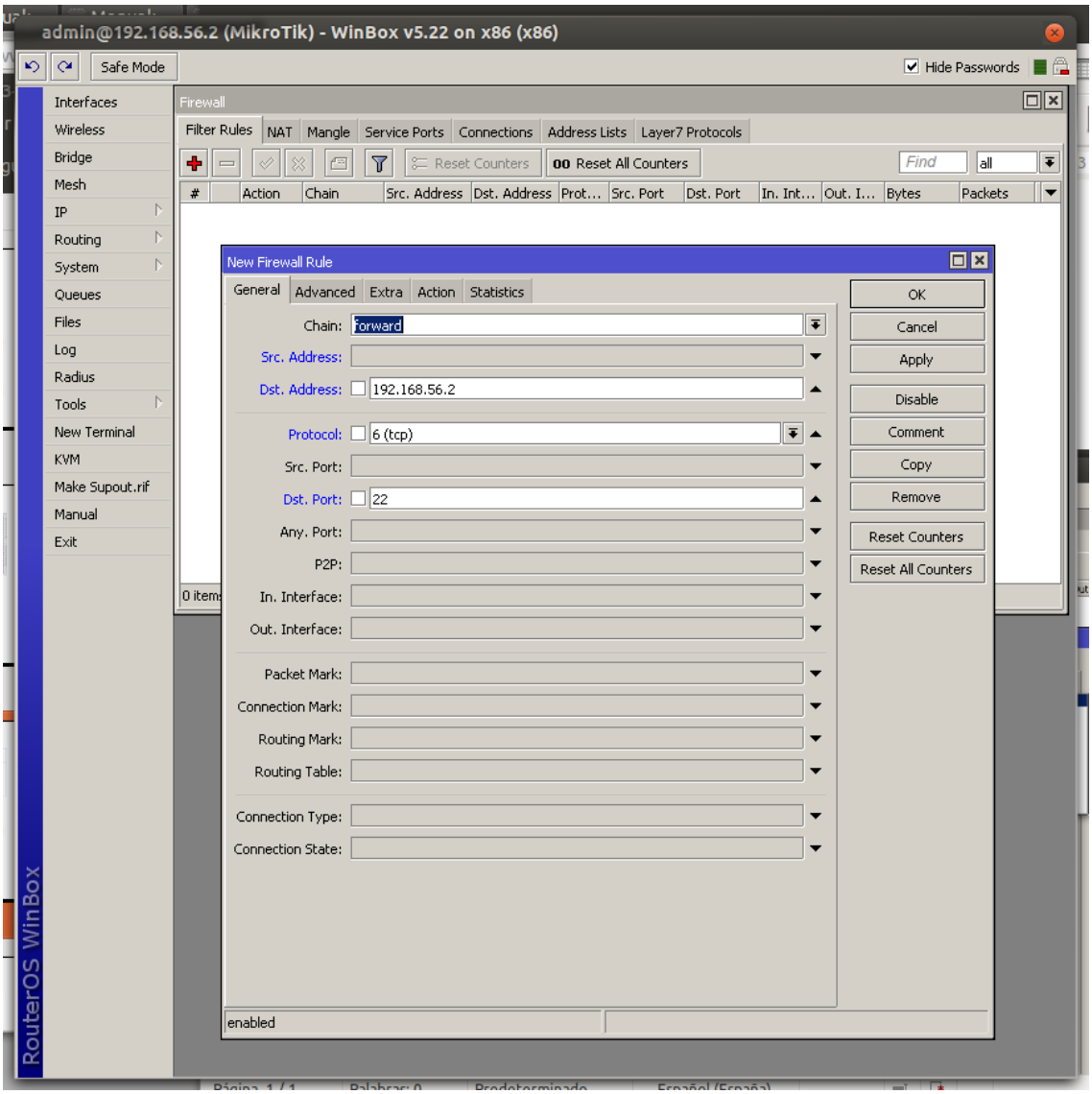


Figura 4: Configuración de una regla de filtrado desde WinBox.

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).

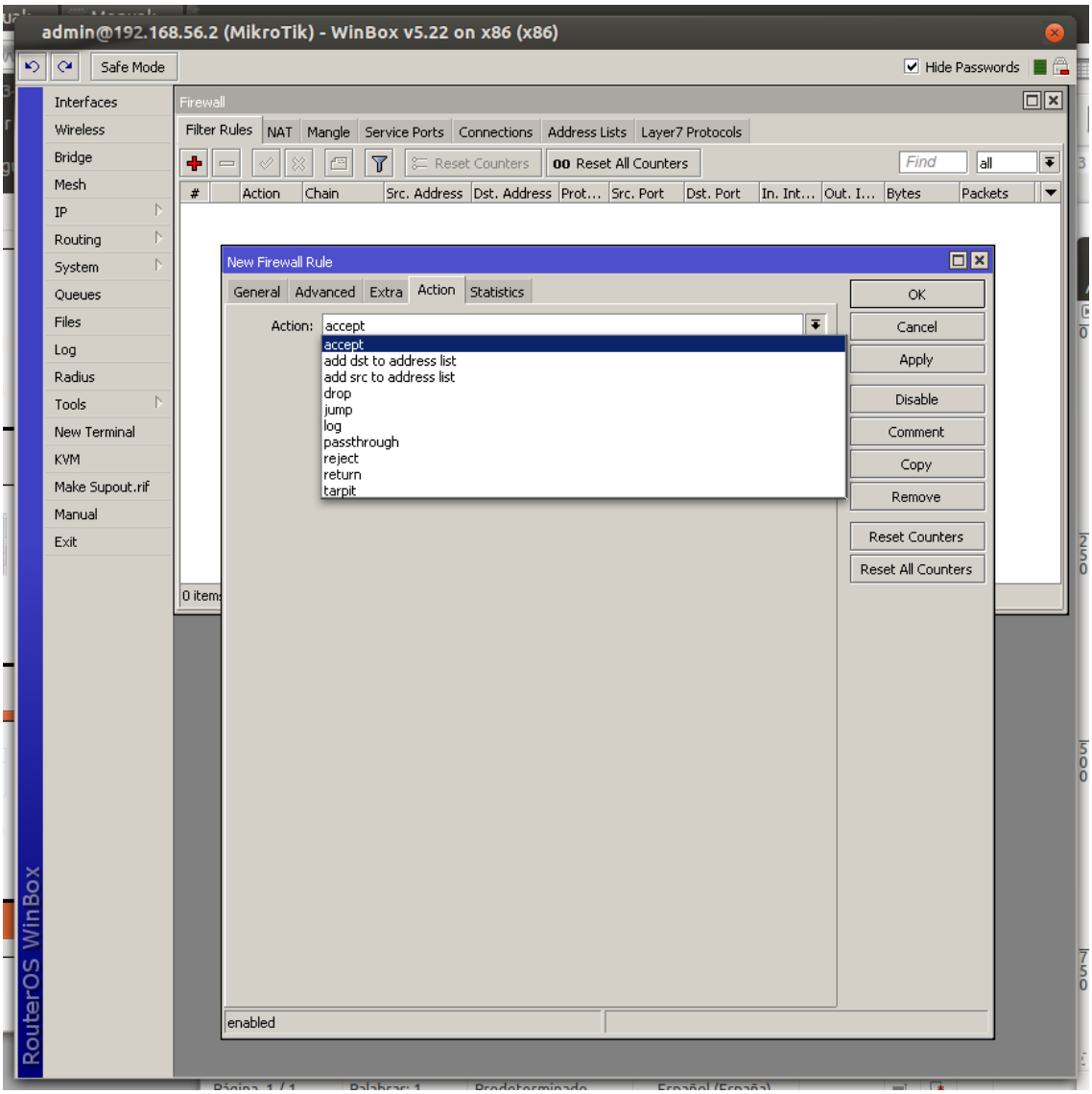


Figura 5: Configuración de la acción de una regla de filtrado.

1.3 Realización práctica

Es necesario configurar las tablas de encaminamiento tanto en los *routers* como en los PC para que 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 el reenvío de todo el tráfico, y luego se añaden reglas explícitas para el tráfico que sí se desea dejar pasar. Compruebe que ahora no es posible enviar o recibir tráfico entre los PC ubicados en 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.

Es necesario levantar el servicio SSH en el PC servidor. Para ello ejecute el siguiente comando.

```
# sudo systemctl start ssh.service
```

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