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, ofrece 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 Fig. 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, una DMZ (Demilitarized Zone) en dónde, usualmente, se exponen públicamente diferentes servicios de red.

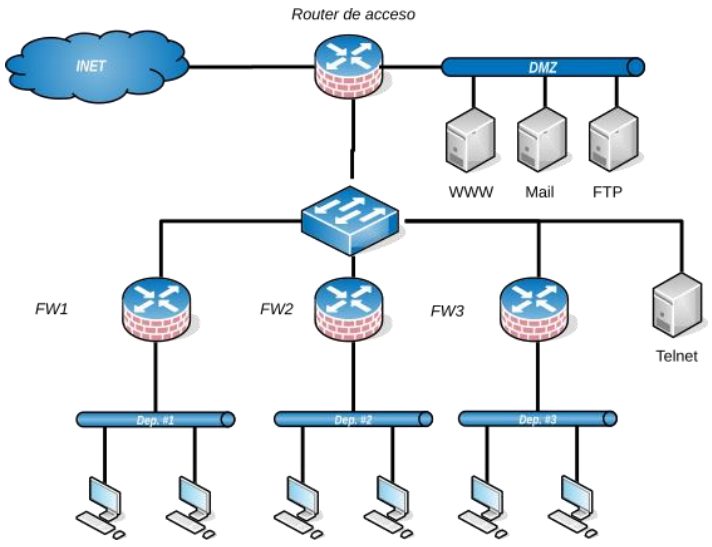

Figura 1: Ubicación típica de cortafuegos dentro de una ogranización.

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, 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 como 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.

En esta práctica configuraremos un cortafuegos de filtrado.

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: descartar (*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 Fig. 2, las cadenas predefinidas son:

- **INPUT**: incluye las reglas que se aplican a paquetes que tienen como dirección destino alguna de las IP del *router.* Es decir, aquellos paquetes que van dirigidos al propio *router*.
- **OUTPUT**: incluye las reglas que se aplican a paquetes generados por el propio *router.* Es decir, aquellos paquetes que tienen como IP origen alguna de las del *router* (de sus interfaces).
- **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. Por lo tanto, dichos paquetes no tienen ni IP origen ni destino que se correspondan con alguna de las del *router.* Sería tráfico que "lo atraviesa".

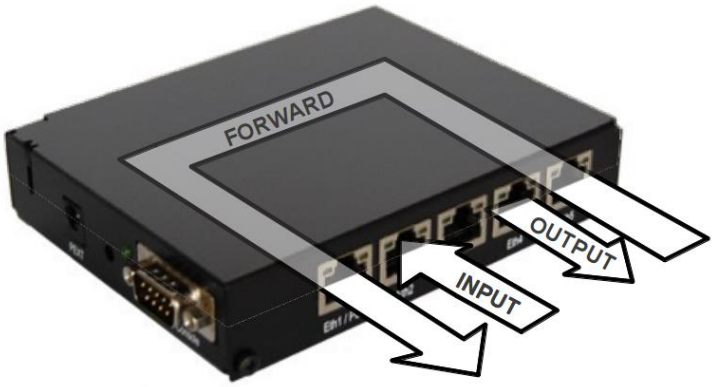

Figura 2: Cadenas de reglas de filtrado básicas.

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 Fig. 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.

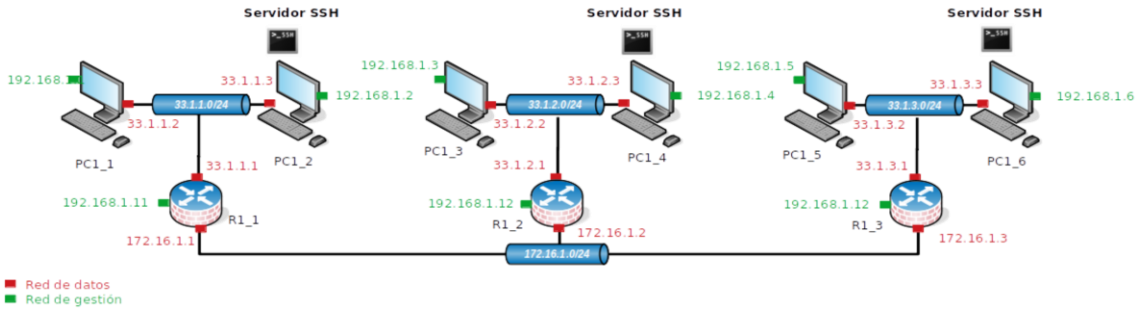

Figura 3: Escenario de trabajo y dispositivos implicados. Ejemplo para los dispositivos de la isla 1.

1.2.3 Configuración de reglas de filtrado

Para configurar el cortafuegos, acceder al menú *IP->Firewall* en 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.

ATENCIÓN: no definan reglas **drop** sobre las cadenas INPUT u OUTPUT. Esto puede hacer que el *router* quede inaccesible y no se pueda administrar.

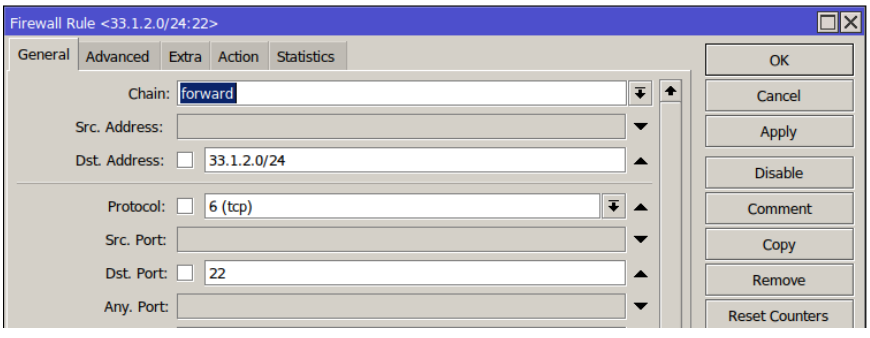

Figura 4: Configuración de una regla de filtrado desde WinBox.

Para configurar una nueva regla, seleccionar los campos y los valores que deben cumplir los paquetes en la pestaña "General". En la Fig. 4 se muestra un ejemplo de creación de una regla que permite el reenvío (*forward*) de toda aquella información con destino a la subred 33.1.2.0/24 y cuyas peticiones vayan dirigidas al puerto 22 de las máquinas destino.

La acción a realizar con esos paquetes se puede configurar en la pestaña "Action". En la Fig. 5 se selecciona la acción *accept* que significa que todos aquellos paquetes cumplan con el criterio de selección de la regla se dejarán pasar.

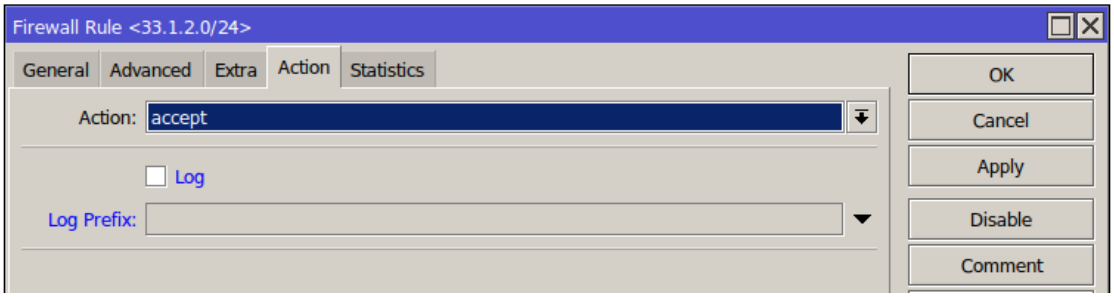

Figura 5: Configuración de la acción de una regla de filtrado.

Existen varias formas de ver si una regla se está evaluando, es decir, si la información de los paquetes que pasan por el *firewall* coincide con el criterio de selección de dicha regla. Esto nos ayudará a comprobar si la regla está bien construida. Para ello, en la ventana principal en dónde se exponen todas las reglas creadas, notar si los campos *Bytes* y *Packets* van cambiando. Esto será indicativo de que la regla se está evaluando (ver Fig. 6)

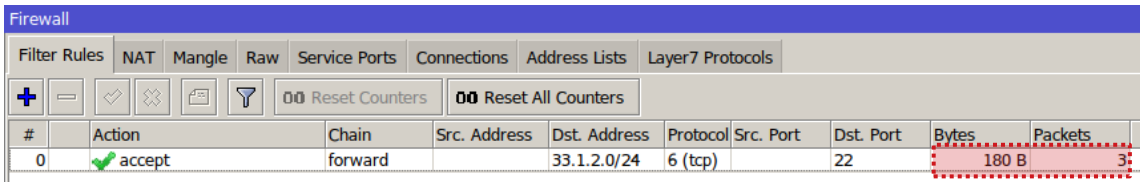

Figura 6: ¿Se está evaluando una regla? Los campos *Bytes* y *Packets* varían cuándo dicha regla se evalúa.

Otra opción muy útil y recomendable para ver cómo está funcionando el *firewall* y más específicamente si se están evaluando sus reglas es activar en el *router* desde la utilidad *System -> Logging* una nueva regla *Log Rule*. Para nuestro caso, aquella que hace *logging* de los eventos relacionados con el *firewall* y sus reglas. En la Fig. 7 se muestra un ejemplo de configuración de dicha regla de log y en la Fig. 8 se muestra cómo aparecen entradas en la ventana de *Log* (a esta ventana se acede directamente desde el menú del *router*) correspondientes, en este caso, a la evaluación de la regla de filtrado que se creó anteriormente y que se observa en la Fig. 6

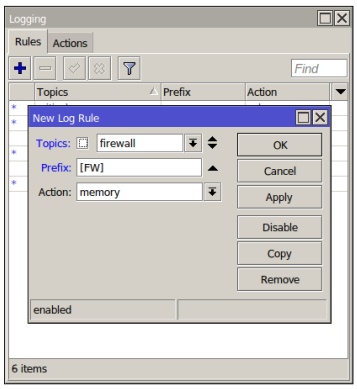

Figura 7: Configuración de la utilidad *Logging* para chequear si una regla se está evaluando.

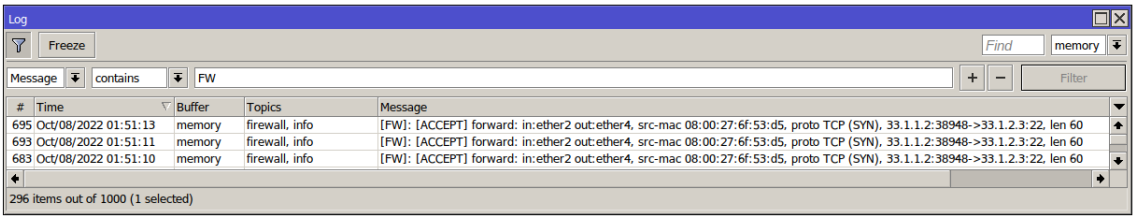

Figura 8: Entradas de *log* filtradas para el prefijo [FW] de la nueva regla de *log* creada anteriormente en la Fig. 7. Se observa como aparece una entrada por cada uno de los paquetes que se han evaluado correctamente por la regla del *firewall* creada en la Fig. 6

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. Se deberá comprobar que hay conectividad antes de configurar las reglas del *firewall*.

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 PC de su red (ver Fig. 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 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>
```

CHECKPOINT: Avise al profesor cuando termine esta tarea.

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

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

 CHECKPOINT: Avise al profesor cuando termine esta tarea.

1.4 Bibliografía

[1] Manual de MikroTik. http://wiki.mikrotik.com/wiki/Manual:TOC