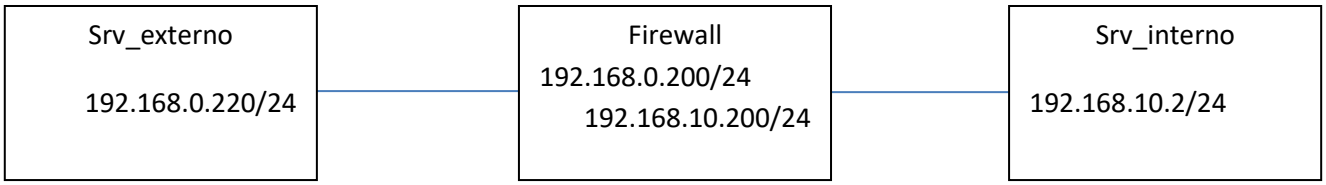
Práctica sobre protección de red mediante firewall

Disponemos de un entorno de 3 máquinas Linux, con la siguiente configuración de red:

Firewall: enp0s3– 192.168.0.200/24, enp0s8 – 192.168.10.200/24
Srv_externo: enp0s3– 192.168.0.220/24
Srv_interno: enp0s3 – 192.168.10.2/24



En esta práctica se trata de realizar las siguientes operaciones:

1- Asegurar que hay visibilidad entre los dos servidores y la máquina firewall.
2- Comprobar si la máquina firewall actúa como router y habilitar el enrutamiento en caso de no estar activado.
3- Determinar qué puertos están abiertos en el servidor interno, para tener en cuenta en la protección del mismo.
4- Comprobar las políticas por defecto del cortafuegos de la máquina firewall.
5- Arrancar un servidor web Apache en la máquina srv_interno.
6- Intentar acceder desde firewall a srv_interno a través de un navegador.
7- Configurar la máquina firewall mediante iptables para permitir:
    a. Conexión al servicio web de srv_interno desde la máquina firewall.
    b. Conexión al servicio web de firewall desde cualquier nodo.
    c. Conexiones locales (desde la red interna) para acceder a un servidor FTP en srv_interno.
    d. Conexiones a la máquina firewall desde cualquier servidor de la red interna.
    e. Conexión mediante ssh a srv_interno a través del puerto 9922, únicamente desde srv_externo.
    f. Conexión a servidores DNS externos desde srv_interno.
    g. Conexiones de salida a servidores web externos desde srv_interno (en una única regla).
    h. Peticiones ping desde el servidor externo al interno y viceversa.
    i. Peticiones ping a la máquina firewall, limitando la respuesta de esas peticiones a un ritmo máximo de una petición cada 2 segundos.
    j. Añadir una regla basada en la inspección de estados que permita la entrada de cualquier datagrama a la máquina firewall, siempre que no sea el primer datagrama de una comunicación.
8- Registrar el tráfico de control que provenga de la red interna, dirigido a cualquier ubicación.
9- Descartar el resto de tráfico

Como resultado de la práctica se entregará un script que contenga la configuración de la herramienta iptables para permitir el paso de paquetes de datos exigido en el enunciado.

Criterios de valoración de la tarea:

1. Funcionamiento correcto del filtrado
2. Claridad en las reglas
3. Documentación sobre el propio script