# Tecnologies avançades d’Internet : Pràctica 1 : Iptables

## Configuracion de los workstations

Antes de comenzar a configurar Iptables, tenemos que configurar la tabla de ruteo de los Workstation para que tengan acceso a internet.

Por eso, añadimos un default Gateway qué redirige todos los paquetes al Gateway si no existe una ruta predefinida en la tabla de ruteo. Para eso ejecutamos este comando: ip route add default via 192.168.2.1.

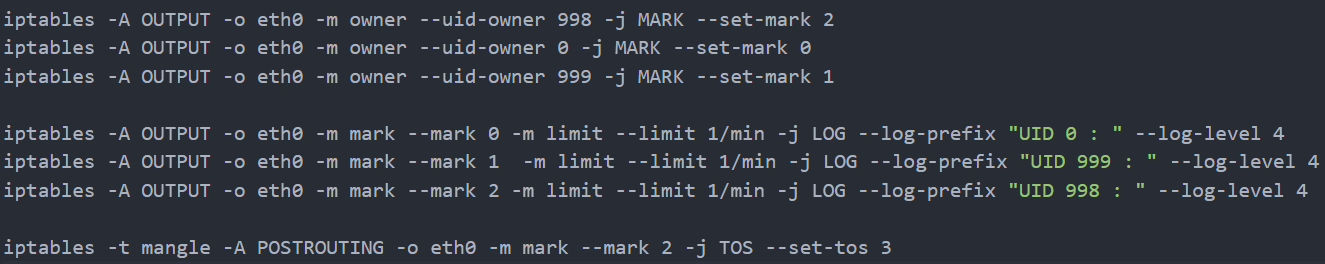
Después instalamos Rsyslog y lo hemos configurado para que los logs de iptables sea localizado en /var/log/iptables.log configurando el fichero /etc/syslog.conf.

Para que el servicio ssh funciona, lo activamos con el siguiente comando: service ssh start.

## Configuracion del Gateway

Para que el router funciona como un router, tenemos que activar el ip\_forward para que el Gateway transmite los paquetes a la realMachine. Por eso ejecutamos este comando: sysctl -w net.ipv4.ip\_forward=1.

## Configuracion del iptables de los workstations



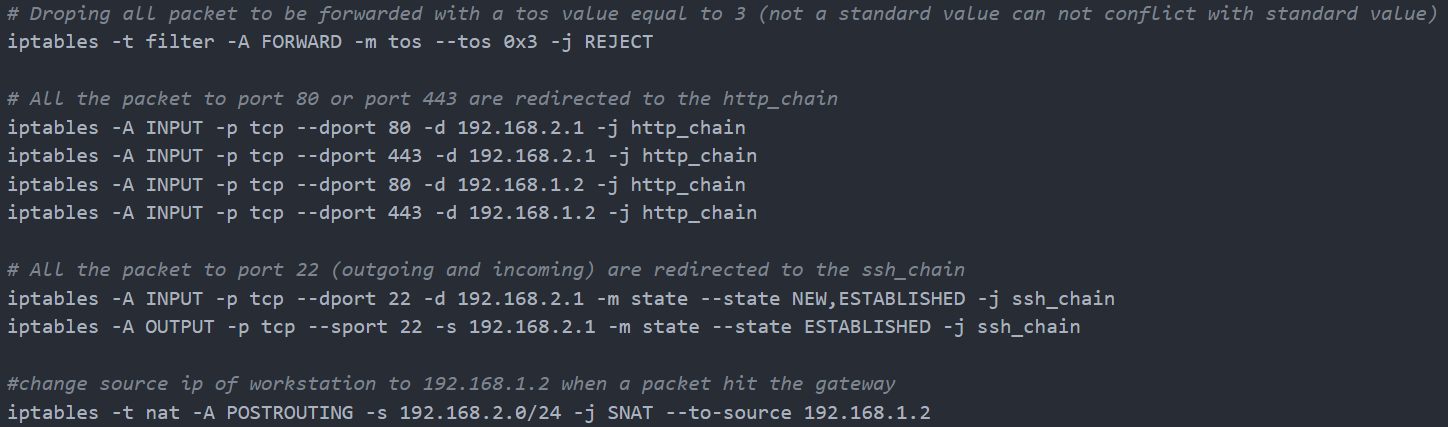
Los workstations son capaz de generar logs diferentes dependiente del usuario que navega sobre la internet. Por eso marcamos todos los paquetes emitidos con el owner con un uid igual a 998 (user2) con un 2, 999 (user1) con un 1 y con 0 (root) con un 0.

Desde aquí, las siguientes reglas dicen que cuando un paquete es marcado con un 0, hacemos un log con el prefix: “UID 0 : [contenido del log]”, y hacemos lo mismo para los otros usuarios.

La última regla nos permite marcar los paquetes emitidos por el user2 (UID = 998), utilizamos el campo tos y lo ponemos con un valor de 3. Este valor no es unas del valor oficialmente utilizado por la tos encabezada, por eso no entramos en conflicto con el funcionamiento de TCP/IP.

Después, veremos que todos los paquetes con una tos encabezada igual a 3, el Gateway va descartarse de ellos.

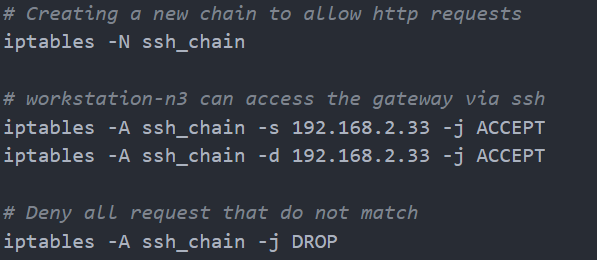
## Configuracion de iptables del Gateway



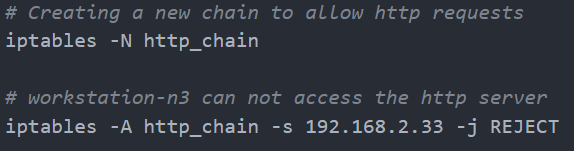
La primera regla nos sirve para que el Gateway se descarta de todos los paquetes con un tos valor igual a 3. Este valor no es utilizado en la implementación original del tos, entonces el Gateway no se descartara de ninguno paquetes accidentalmente.

Para que los paquetes emitidos por los workstation sean visto sobre internet como emitidos por el Gateway, hemos añadido la última regla que nos permite cambiar el ip de origen por el ip del Gateway.

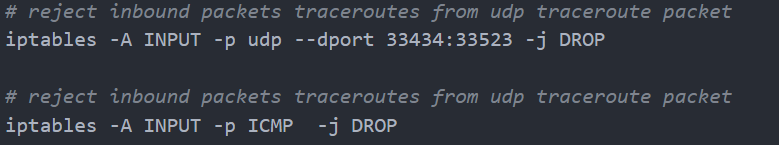
Las otras reglas permiten cuando un paquete utiliza el protocol http o https (puerto 80, 443) enviarlo a la cadena http\_chain. Y lo mismo para el protocol ssh (puerto 22).



Aquí creamos una nueva cadena “ssh\_chain” y en esta cadena, por defecto rechazamos todo los requests porque queremos implementar una white list. Despuès hemos añadido las reglas que permite aceptar las conexionas ssh desde y hacia la maquina Workstation (n3).



En este fichero, creamos la cadena “http\_chain”, esta cadena nos permite implementar un black list, en este black list, decimos que la maquina Workstation (n3) no puede acceder al servidor http del Gateway.



Para terminar, hemos definido un script para rechazar los requests de traceroute. Traceroute utiliza el protocol icmp en su Linux implementación, pero en su Windows implementación, utiliza el protocol udp y una serie de puertos que van desde 33 434 hacia el puerto 33 523.

Entonces, bloquemos todos los requests udp que utilizan un numero de puerto entre 33 434 y 33 523 para blocar los paquetes traceroute de Windows et para los de Linux, bloquemos los paquetes utilizando el protocol icmp.