# **Configurar iptables**

1. Enrutamiento con NAT y registro o log de paquetes FORWARD y PREROUTING. Se crea

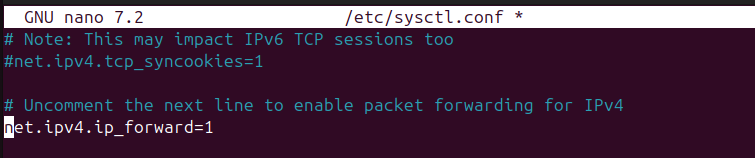
un registro en /var/log/iptables.log para tener un control de lo que entra y sale de

nuestros cortafuegos.

* Habilitamos el enrutamiento de paquetes



Lo ponemos permanente



Guardamos cambios



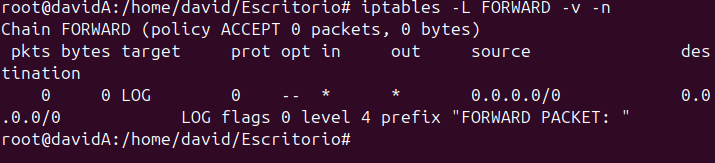
* Habilitamos MASQUEREADING para hacer que los paquetes salgan



* Ejecutamos un comando para monitorear los paquetes que pasan por un firewall entre otras dos redes



* Verificamos la regla ejecutada



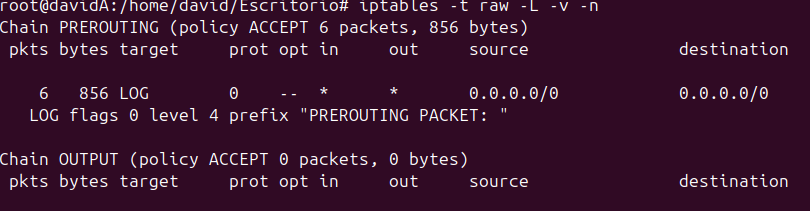
* Para hacerlo con PREROUTING debemos cargar el módulo ipt\_LOG



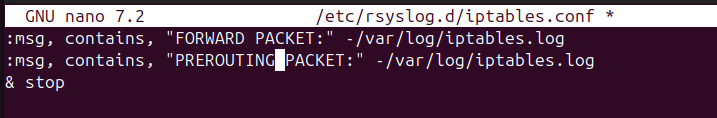
* Ahora ejecutamos el comando, que nos permitiría ver qué paquetes están llegando al firewall antes de aplicar NAT



* Verificamos la regla ejecutada de nuevo



* Configuramos el fichero /etc/rsyslog-d/iptables.conf y añadimos las siguientes líneas



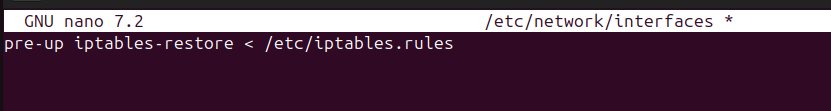
Lo que hemos puesto es para filtrar los registros de FORWARD y PREROUTING (que hemos definido previamente) y la última línea para evitar que estos aparezcan en otros archivos de log del sistema

* Reiniciamos RSYSLOG



* Guardamos las reglas locales y las configuramos para que se apliquen automáticamente al iniciar el equipo





2. Reglas que permita el acceso a los protocolos HTTP, DNS y FTP en Internet, pero solo a

dos direcciones IP determinadas desde una red local (192.168.2.100 y 192.168.2.114),

todos los demás equipos no tendrán acceso.

* Protocolo HTTP



* Protocolo DNS





* Protocolo FTP



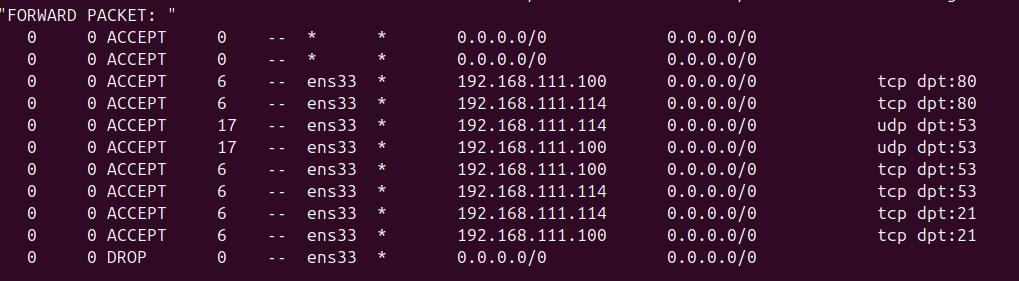
* Denegar el tráfico restante



* Guardamos las reglas



* Comprobamos esas reglas que estén bien configuradas tal y como se pide

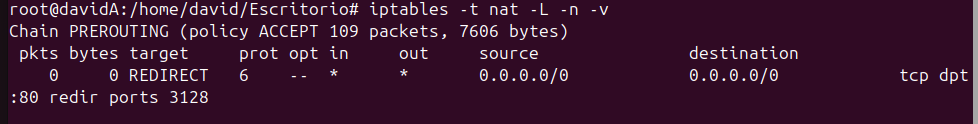


3. Redirección del tráfico web en el puerto 80 por el puerto 3128 (Proxy).

* Creo y ejecuto la regla. Lo que voy hacer es redirigir el tráfico que llega al puerto 80 / HTTP al puerto 3128 que es el que escucha el proxy



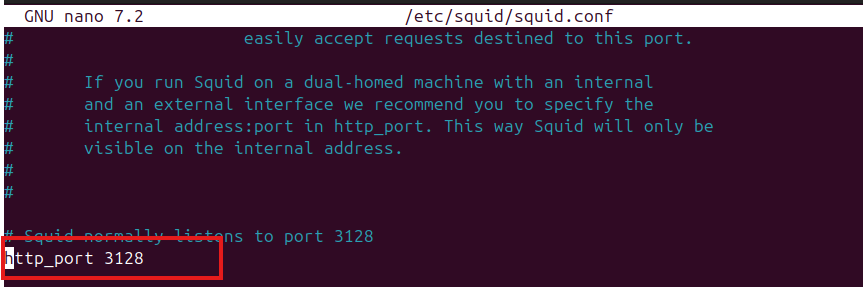
* Verificamos que se hayan aplicado las reglas



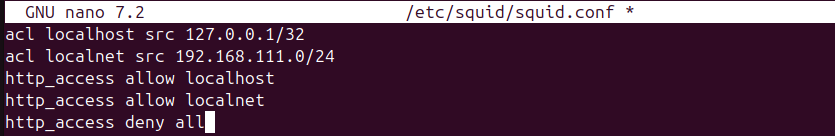
* Guardamos las reglas en el archivo ‘/etc/iptables/rules.v4’



* Ahora usare el proxy llamado Squid para ello en su fichero de configuración debo configurar una línea relacionada con el puerto 3128, que por defecto viene descomentada



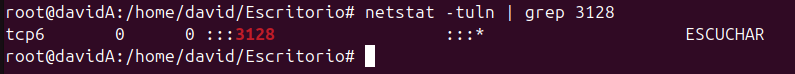
* Configuramos arriba del todo unas reglas de acceso para permitir a mi IP que acceda al proxy y el http\_access controla el tráfico de mi IP para que acceda al proxy



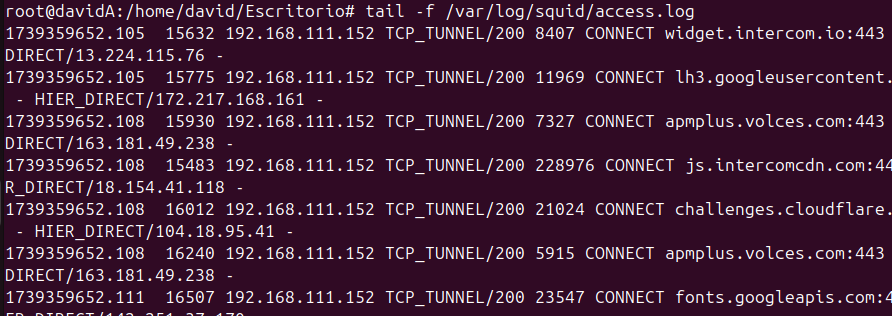
* Reiniciamos squid y vemos su estado



* Vemos que squid este escuchando en el puerto deseado



* Aquí vemos que todo el tráfico pasar a través de Squid y están registradas en el log por lo que funciona correctamente



4. Haz todo lo que está abajo y adjunta pantallazos para probarlo

# 

