Unidad 14. Servidor Proxy

1. Instale el servidor proxy squid en su equipo. Repase la configuración por defecto (ojo, es MUY larga). Configure el navegador y compruebe si funciona sin hacer ningún cambio. Revise los logs que ha dejado y los archivos de la caché.

2. Pruebe a cambiar en el proxy el puerto de escucha de peticiones http. Compruebe el cambio. Deje finalmente dos puertos de escucha, el que trae por defecto y el nuevo. Compruebe el cambio.

3. Ya sabemos los puertos, pero ... ¿en que IP's/interfaces está escuchando el proxy? Cambielo para que sólo escuche en localhost y compruebelo. Cambielo para que escuche sólo por el interfaz eth0.

4. Configure el control de acceso, para permitir acceso desde unos equipos de la LAN y rechazar el acceso desde otros. Realice las pruebas de ambos casos conectandose desde otros equipos. Revise los logs.

5. Prohiba el acceso a un determinado dominio de internet, por ejemplo microsoft.com. Pruebe con varias de las directivas comunes que permiten hacerlo. Haga la prueba y revise los logs.

6. Mantenga la restricción del ejercicio 5, pero permita ahora el acceso al mismo dominio sólo desde un equipo de la red. Compruebe los casos de acceso y de rechazo.

Unidad 15. NAT/Firewall con netfilter.

1. Familiarícese con tcpdump. Escuche el tráfico en las interfaces disponibles. Genere tráfico, pings, navegación, etc... y estudie los resultados. Si hay demasiada información/tráfico para analizar, pruebe a poner reglas más concretas, para mostrar sólo el tráfico realmente interesante en cada momento.

2. Pruebe ethereal. Elija el interfaz eth0, dele a capturar y espere unos segundos antes de detenerlo. En ese tiempo, puede generar algún tráfico si lo desea. Estudie la información que se le muestra. Filtre para obtener sólo el tráfico www y pruébelo.

3. Limite el tráfico ICMP en su equipo por la interfaz eth0. Compruebe el resultado desde otro equipo y con tcpdump/ethereal. Pruebe tanto reglas de INPUT como de OUTPUT. ¿Qué diferencia hay? ¿Cual es más adecuado?

4. Compruebe los servicios disponibles en su equipo. Limite el acceso por eth0 a algún servicio (www, smtp, etc...) y compruebe el resultado. ¿Y tcpdump que dice?

5. Permita el acceso desde un único equipo a ese servicio limitado en el ejercicio 4. Finalmente limite el acceso -en salida- a la www.

6. Elimine todas las reglas. Pongase de acuerdo con un compañero y ponga que ahora su equipo es el gateway de la LAN, plantee reglas para limitar el acceso a la LAN... Limite el tráfico de salida de los equipos de esa LAN. NOTA: Para hacer las pruebas configure adecuadamente el gateway por defecto en el equipo vecino y compruebe las reglas obtenidas. Observe el tráfico con tcpdump en ambos equipos.

7. Configure Squid como proxy transparente de la LAN. Haga las pruebas desde otros equipos según el punto anterior (sin configurar el proxy en el navegador!). Revise los logs de squid para ver si realmente están pasando las peticiones www por el proxy transparente.

8. Siguiendo con el ejercicio 6, donde un equipo es el gateway de la LAN, configure en ese equipo a su vez el gateway 10.1.15.121 y elimine todas las reglas de iptables. Haga ahora NAT para el acceos a internet de la LAN. ¿Es SNAT o DNAT? ¿Es recomendable usar Masquerade o NAT? Haga las pruebas, de nuevo desde equipos vecinos, mediante pings a otros equipos y observe con tcpdump los resultados [tcpdump en el equipo “origen”, en el gateway y en el equipo “destino”]. No se olvide activar el forwarding en el kernel, si no lo está.

9. Elimine todas las reglas. Cambie las políticas por defecto para que no permita nada. Vaya abriendo algún servicio en INPUT y compruebelo. Igualmente piense en reglas restrictivas respecto a la chain de OUTPUT y asignelas. ¿Necesita el FORWARD para algo? Esta es la mejor forma de ir planteando un 'firewall real'.

10. Elimine las reglas y pruebe firestarter. Pruebe a añadir alguna restricción. Observe las reglas que ha creado, con iptables. Pruebe a detener el firewall y a 'bloquear' ¿que hacen?