Práctica 7

Cortafuegos y PNAT

7.1. Introducción

En esta práctica utilizaremos tres máquinas virtuales para poner de manifiesto el funcionamiento de los cortafuegos (*firewalls*) perimetrales y del mecanimo de traducción de direcciones PNAT (*Port and Network Address Translation*).

Para el desarrollo utilizaremos la topología mostrada en la figura 7.1.

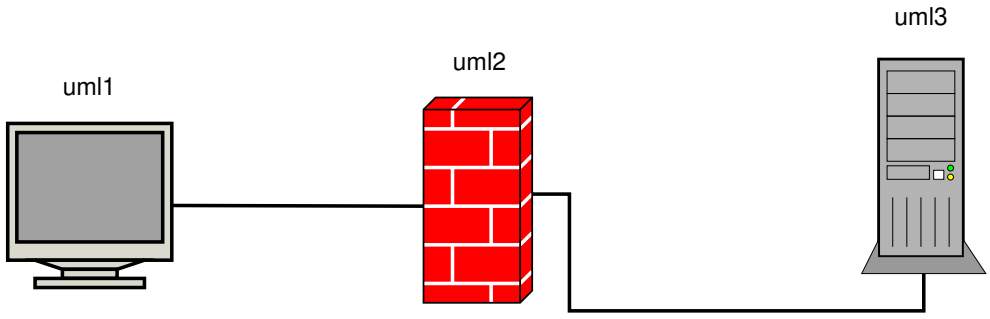

FIGURA 7.1: Topología virtual

7.2. Cortafuegos

Emplearemos `iptables` para desplegar un cortafuegos perimetral en la máquina `uml2`, que es la que actúa de encaminador. La máquina `uml3` será un servidor dentro de la red que queremos proteger (red interna), mientras que la máquina `uml1` estará en la red `198.51.100.0/24`

`Se deben establecer las reglas adecuadas en el cortafuegos de manera que:`

- `Se permitan las conexiones a uml3 (entrantes) sólo a los puertos TCP 80 y 22.`

- Se permiten las conexiones desde uml3 (salientes) sólo al puerto TCP 443 y UDP 53 hacia cualquier dirección externa.
- Se permite el tráfico ICMP tanto entrante como saliente.

Para comprobar el funcionamiento, se puede emplear la orden netcat, nc, con las opciones: -l para especificar el modo *listen* (servidor); -p <puerto> para el número de puerto, y -u para indicar protocolo UDP (si no se pone esta opción, se supone TCP). Por ejemplo:

```
nc -l -p 80
nc -l -u -p 53
```

En el lado del cliente se puede utilizar la misma orden nc <ip_servidor> <puerto>:

```
nc 198.51.100.2 80
```

Se puede encontrar más información sobre el funcionamiento de netcat en la página del manual (orden man netcat).

7.3. NAT: Network Address Translation

La idea de NAT es "ocultar" toda una red, que puede estar formada por un buen número de computadores, detrás de unas pocas direcciones IP, que son las direcciones *públicas* por las que se conoce dicha red. El caso más habitual es ocultar toda la red tras una única dirección IP pública. Las máquinas que están dentro de la red poseen direcciones *privadas*. Recordemos que IANA ha reservado 3 rangos de direcciones privadas con este propósito:

- 10.0.0.0/8 (1 red de clase A)
- 172.16.0.0/12 (16 redes de clase B)
- 192.168.0.0/16 (256 redes de clase C)

Estas direcciones son **no encaminables**, es decir, no existen rutas para alcanzarlas dentro de Internet. Por eso sólo tienen sentido dentro de la red local donde están definidas.

Por otro lado, según el RFC-5737, los siguientes bloques de direcciones se pueden emplear sólo con fines de documentación, y serán los ejemplos que emplearemos aquí como direcciones públicas:

- 192.0.2.0/24 (TEST-NET-1),
- 198.51.100.0/24 (TEST-NET-2),
- 203.0.113.0/24 (TEST-NET-3)

Cuando un datagrama abandona la red interna y sale a Internet, su dirección origen es la que define a dónde deberá ir dirigida la posible respuesta. Por tanto, esa dirección debe ser válida, es decir, debe ser **encaminable**. Por ello, la pasarela NAT reemplaza la dirección origen del datagrama original por la dirección IP pública. Cuando llega la respuesta, lo hace dirigida a la dirección pública. En la pasarela NAT se deshace ahora el cambio, reenviando el datagrama a la máquina destino dentro de la red interna.

Para que este proceso pueda llevarse a cabo sin problemas, la pasarela NAT debe recordar los datagramas que ha enviado a Internet para, cuando ve regresar el datagrama de respuesta asociado, pueda deshacer el cambio. Para ello no basta con recordar sólo las direcciones IP origen y destino de los datagramas, pues varias máquinas de la red interior podrían enviar datagramas simultáneamente a las mismas máquinas en Internet. Por ejemplo, en la figura 7.2, las máquinas A y B pueden realizar sendas peticiones de conexión con el servidor web externo WEB_Server, con lo que NAT debe ser capaz de identificar correctamente ambas conexiones. Para ello, además de modificarse la dirección origen de los datagramas salientes, también se modifica el puerto TCP o UDP origen, como se muestra en la tabla 7.1.

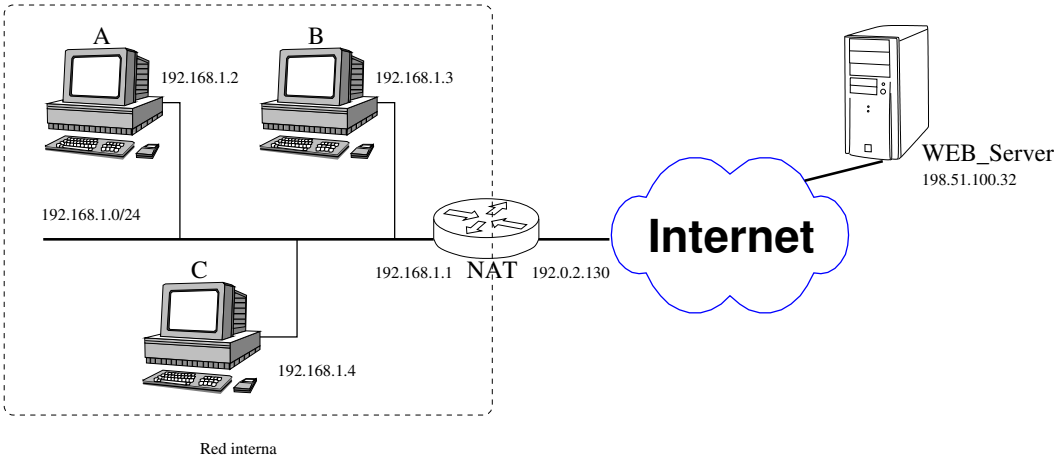

FIGURA 7.2: Ejemplo de red interna con NAT

IP origen	Puerto origen	IP destino	Puerto destino		IP origen	Puerto origen	IP destino	Puerto destino
Saliente								
192.168.1.2	30754	198.51.100.32	80	→	192.0.2.130	12300	198.51.100.32	80
192.168.1.3	45342	198.51.100.32	80	→	192.0.2.130	12301	198.51.100.32	80
Entrante								
198.51.100.32	80	192.168.1.2	30754	←	198.51.100.32	80	192.0.2.130	12300
198.51.100.32	80	192.168.1.3	45342	←	198.51.100.32	80	192.0.2.130	12301

TABLA 7.1: Mecanismo de traducción NAT

El gran problema de NAT es que rompe el paradigma de conexión extremo-a-extremo de TCP, por lo que muchos protocolos de aplicación, sobre todo los relacionados con transmisión de datos en tiempo real (VoIP, P2P...) dejan de funcionar correctamente.

7.3.1. Desarrollo de la práctica

Empleando la misma topología de la figura 7.1, en la red interna (uml3) utilizaremos direcciones privadas en el rango 192.168.0.0/24. Como dirección pública en uml2 emplearemos la dirección 198.51.100.2/24. La máquina uml1 usará la dirección 198.51.100.1/24.

PNAT

En uml2, que es la máquina que actúa como encaminador y cortafuegos, deben definirse las reglas iptables apropiadas para permitir conexiones desde el exterior a la máquina interna a los puertos 22 y 80 en TCP y al puerto 53 en UDP.

El tráfico hacia el exterior no está restringido.

Iniciar el inspector de tráfico wireshark en la máquina uml2 y comprobar el funcionamiento de la traducción de direcciones y puertos. Establecer una conexión TCP desde la máquina uml3 al puerto 9000 de la máquina uml1 y rellenar una tabla como la mostrada en 7.1 con las direcciones IP y puertos empleados.

IP origen	Puerto origen	IP destino	Puerto destino		IP origen	Puerto origen	IP destino	Puerto destino
				Saliente				
				←				
				←				
				Entrante				
				→				
				→				

Repetir el ejercicio con una conexión desde uml1 al puerto 80 de uml3.

IP origen	Puerto origen	IP destino	Puerto destino		IP origen	Puerto origen	IP destino	Puerto destino
				Entrante				
				→				
				→				
				Saliente				
				←				
				←				

7.3.2. Destino LOG

En el cortafuegos, definir las reglas apropiadas para guardar una traza de los intentos de conexión entrantes (segmentos con bit SYN activado). Consultar la página del manual (man

iptables) para las opciones adecuadas.

Para examinar el archivo de traza del sistema, podemos ejecutar la siguiente orden:

```
tail -F /var/log/syslog
```

y comprobar que aparecen los avisos definidos en iptables.

7.4. Cortafuegos con IPv6

Se puede utilizar la orden ip6tables para configurar el cortafuegos adecuado a IPv6. Repetir la práctica del apartado 7.2 pero empleando las direcciones de red con prefijos 2001:db8:1::/64 para la red interna (uml3) y 2001:db8:ffff::/64 para la red externa (uml1).