Práctica 6b: Cortafuegos (firewalls)

2. Traducción de direcciones y puertos en el firewall: tabla nat

2.1. Clientes en la red privada, servidores externos

Configura un script fw1.sh en el firewall para que:

- Se borren las reglas que hubiera configuradas previamente en la tabla nat

- Se reinicien los contadores de la tabla nat

- Se realice la traducción de direcciones para el tráfico saliente de las redes privadas (SNAT) y su correspondiente tráfico de respuesta

2.1.1. Comunicaciones con TCP

Ejecuta el script fw1.sh de 2.1.

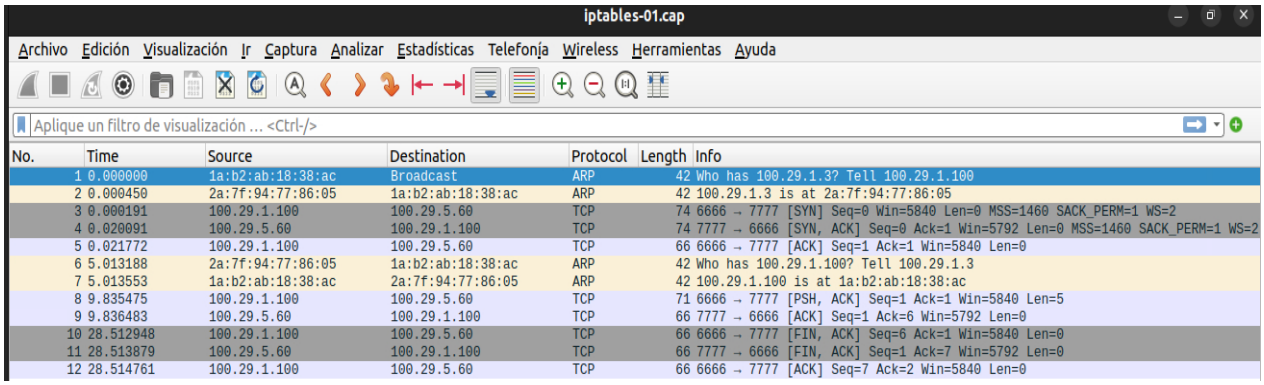
1. Captura el tráfico en r3-eth0 (iptables-01.cap) y en firewall-eth0 (iptables-02.cap) para ver los paquetes dentro de la red de la Empresa y por Internet.

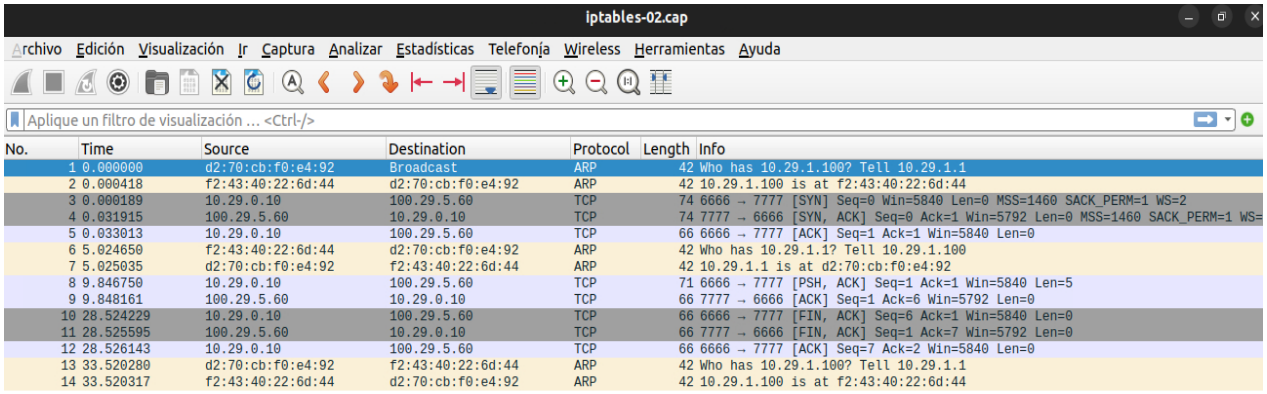
Arranca las siguientes aplicaciones:

- nc como servidor TCP en pc6, puerto 7777 = **nc –l –p 7777**

- nc como cliente TCP en pc1 = **nc –p 6666 100.29.5.60 7777**

4. Interrumpe las capturas, y estúdialas. En particular, identifica todos los paquetes que aparecen en las capturas, relacionados con la prueba que has realizado teniendo en cuenta que se trata de una conexión TCP. Identifica los mismos paquetes en las 2 capturas, y observa cómo cambian las direcciones IP de los mismos paquetes según viajen dentro de la EMPRESA o por INTERNET.

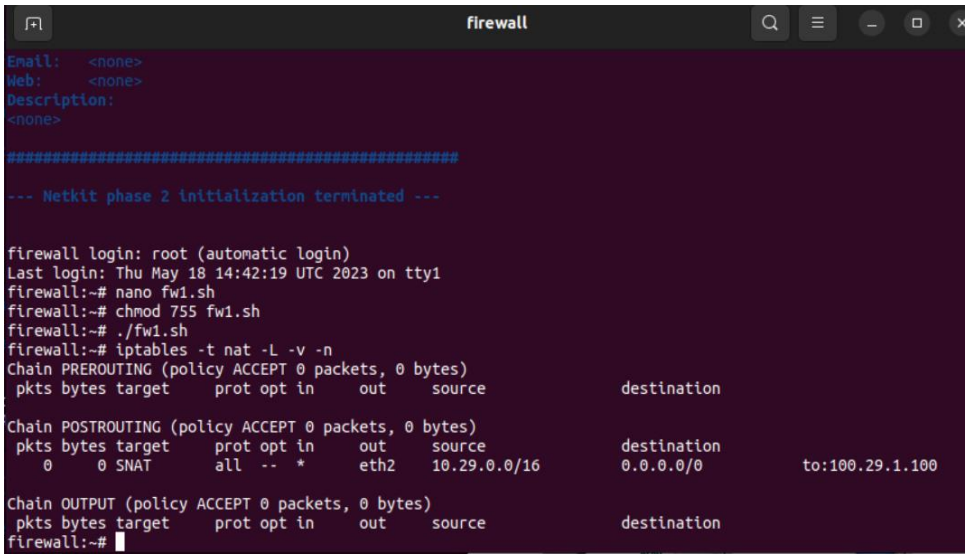




5. Consulta la lista de reglas en el firewall con

firewall:~# iptables -t nat -L -v -n

Observa qué regla(s) están cumpliendo los paquetes y cuántas veces se cumple(n).



2.1.2. Comunicaciones con UDP

Ejecuta el script fw1.sh de 2.1 para que se reinicien los contadores de paquetes de iptables, compruébalo consultando la lista de reglas del firewall.

1. Captura el tráfico en r3-eth0 (iptables-03.cap) y en firewall-eth0 (iptables-04.cap) para ver los paquetes dentro de la red de la Empresa y por Internet.

Arranca las siguientes aplicaciones:

- nc como servidor UDP en pc6, puerto 7777 = **nc –u –l –p 7777**

- nc como cliente UDP en pc2 = **nc –u –p 6666 100.29.5.60 7777**

2. Consulta la lista de reglas en el firewall, e indica cuáles se están cumpliendo y cuántas veces se cumplen

```
firewall:~# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 SNAT       all  --  *      eth2    10.29.0.0/16         0.0.0.0/0
  to:100.29.1.100

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

4. Captura de nuevo el tráfico en r3-eth0 (**iptables-05.cap**) y en firewall-eth0 (**iptables-06.cap**) para ver los paquetes dentro de la red de la Empresa y por Internet cuando tienes varios clientes desde un mismo puerto origen conectándose a un mismo servidor, para ello inicia:

- nc como servidor UDP en pc7, puerto 7777 = **nc –u –l –p 7777**

- nc como cliente UDP en pc1, puerto 6666 = **nc –u –p 6666 100.29.6.70 7777**

- nc como cliente UDP en pc2, puerto 6666 = **nc –u –p 6666 100.29.6.70 7777**

Ahora, envía una línea desde pc1 y después una línea desde pc2. Ten en cuenta que nc no funciona como las aplicaciones servidoras que pueden atender a varios clientes a la vez. La aplicación nc no está preparada para que un servidor se pueda comunicar a la vez con dos clientes, por ello el envío desde pc2 provocará que pc7 envíe un ICMP de error a pc2. Pero para lo que queremos comprobar este error no es importante, sólo queremos analizar lo que ocurre en el firewall con la traducción de direcciones IP y puertos. Interrumpe las capturas y analízalas fijándote en las direcciones IP y puertos que se utilizan en la red de la EMPRESA y en INTERNET

2.1.3. Comunicaciones con ICMP

Ejecuta el script fw1.sh de 2.1 para que se reinicien los contadores de paquetes de iptables.

1. Ejecuta el siguiente comando en pc1 (recuerda sustituir la X por el número que te corresponde): pc1:~# ping -c 2 100.X.5.60 2.

```
pc1:~# ping -c 2 100.29.5.60
PING 100.29.5.60 (100.29.5.60) 56(84) bytes of data.
64 bytes from 100.29.5.60: icmp_seq=1 ttl=60 time=38.5 ms
64 bytes from 100.29.5.60: icmp_seq=2 ttl=60 time=2.89 ms

--- 100.29.5.60 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 2.892/20.703/38.515/17.812 ms
pc1:~#
```

Consulta la lista de reglas en el firewall, y mira cuáles se están cumpliendo y cuántas veces. Ten en cuenta que cada echo request y su respuesta echo reply es realmente una comunicación diferente, aunque repitas el ping varias veces no se quedan ligadas durante todas las repeticiones las dos máquinas que se intercambian los paquetes ICMP.

```
firewall:~# ./fw1.sh
firewall:~# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 2 packets, 168 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    2   168 SNAT       all  --  *      eth2    10.29.0.0/16         0.0.0.0/0
  to:100.29.1.100

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

firewall:~#
```

2.2. Servidores en la red privada, clientes externos

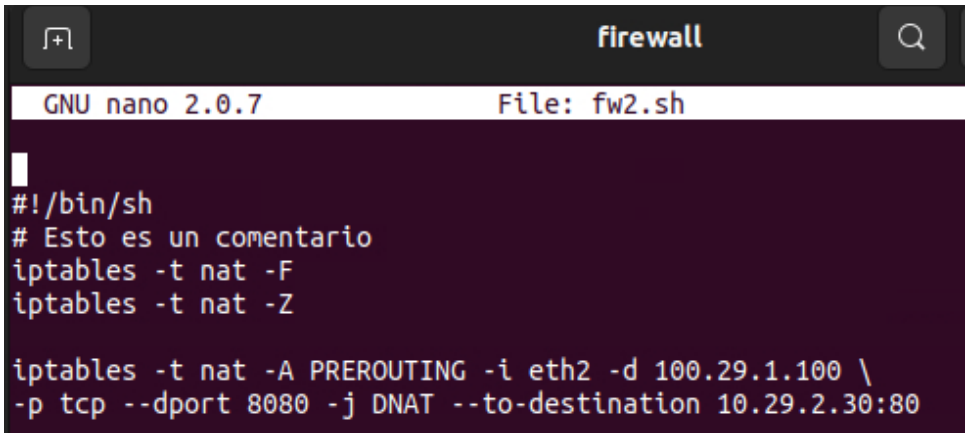
2.2.1. Apertura de puertos TCP

1. Captura el tráfico en r3-eth0 (**iptables-07.cap**) y en firewall-eth0 (**iptables-08.cap**) para ver los paquetes dentro de la red de la Empresa y por Internet.

2. Realiza un nuevo script fw2.sh en el rewall para que: se borren las reglas que hubiera configuradas previamente en la tabla nat se reinicien los contadores de la tabla nat el tráfico de entrada al firewall destinado al puerto TCP 80 sea redirigido a pc3, puerto 80. Incluye el script en la memoria

Ejecuta dicho script y arranca las siguientes aplicaciones:

- nc como servidor TCP en pc3, puerto 80 =**nc –l –p 80**
- nc como cliente TCP en pc6, de forma que su tráfico lo reciba el servidor de pc3 (NOTA: presta especial atención a los parámetros con los que debes lanzar este cliente). Indica en la memoria el comando que has usado para lanzar el cliente y explica por qué lo has hecho así. = **nc –p 6666 100.29.1.100 8080**



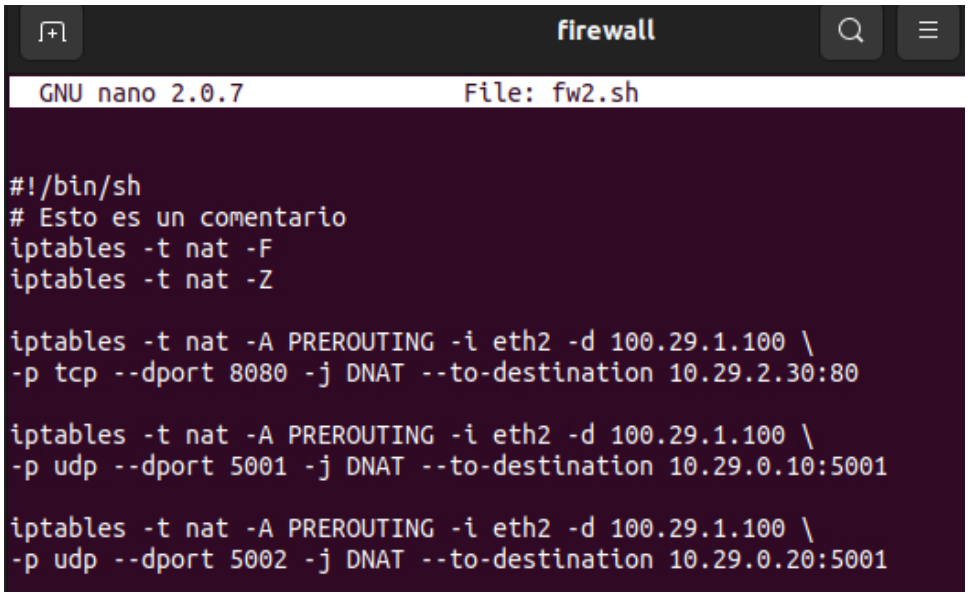
2.2.2. Apertura de puertos UDP

2. Modifica el script fw2.sh para que, adicionalmente:

El tráfico de entrada al firewall destinado al puerto UDP 5001 sea redirigido a pc1, puerto 5001

El tráfico de entrada al firewall destinado al puerto UDP 5002 sea redirigido a pc2, puerto 5001

Incluye el script en la memoria.



Ejecuta el script que acabas de modificar y arranca las aplicaciones:

- nc como servidor UDP en pc1, puerto 5001 = **nc –u –l 5001**
- nc como servidor UDP en pc2, puerto 5001 = **nc –u –l 5001**
- nc como cliente UDP en pc6, de forma que su tráfico lo reciba el servidor de pc1. Indica el comando que has utilizado para lanzar el cliente y explica por qué. = **nc –u 6666 100.29.1.100 5001**
- nc como cliente UDP en pc7, de forma que su tráfico lo reciba el servidor de pc2. Indica el comando que has utilizado para lanzar el cliente y explica por qué. = **nc –u 6666 100.29.1.100 5002**

3. Filtrado de tráfico en el firewall: tabla filter

Crea un scrip**t fw3.sh** en el firewall partiendo de la configuración de traducción de direcciones realizada en fw1.sh (clientes en la red privada, servidores externos) al que se le añada la siguiente configuración (todas en el mismo script). Descripción de las especificaciones:

1.Reiniciar la tabla filter: borrar su contenido y reiniciar sus contadores.

2.Fijar las políticas por defecto de las cadenas de la tabla filter, haciendo que por defecto se descarte todo el tráco en el firewall excepto los paquetes que cree el propio firewall (conguración habitual en un rewall).

3.Permitir el tráco de entrada dirigido a las aplicaciones que se están ejecutando en el propio firewall únicamente si este tráco tiene su origen en las subredes privadas de la empresa.

4.Permitir todo el tráco saliente desde las subredes privadas hacia Internet y el tráco de respuesta al saliente. Ten en cuenta que como has partido del script fw1.sh, en dicho script ya tenías las reglas de la tabla nat para la traducción de la dirección IP de origen de los paquetes que reenvía el firewall y los paquetes del tráco entrante de respuesta a éste.

5.Permitir desde Internet únicamente el tráco entrante nuevo hacia la zona DMZ según las siguientes reglas:

- acceso a un servidor echo existente en pc4 (UDP, puerto 7). El servidor de echo es un servidor que al enviarle una cadena de caracteres, devuelve la misma cadena que se le ha enviado. Para comprobar el acceso a este servidor utiliza nc como cliente desde otra máquina.

- acceso a un servidor daytime existente en pc5 (UDP, puerto 13). El servidor daytime es un servidor que al enviarle algo, devuelve la fecha y hora de la máquina donde está instalado. Para comprobar el acceso a este servidor utiliza nc como cliente desde otra máquina.

6.Permitir únicamente la comunicación entre la red privada y la zona DMZ de la siguiente forma: acceso desde pc1 a un servidor de echo (TCP, puerto 7) existente en pc4.

7.Desde la zona DMZ no se debe permitir iniciar ninguna comunicación con la red privada ni con el propio firewall.