**Universidad Nacional Autónoma de Nicaragua**

**UNAN-León**

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**V año**

****

**Componente: Redes de Área Extensa**

**Tema: Practica de Iptables**

**Realizado por:**

**Br. Jhonatan Uziel Espinoza Ortega Carnet: 15-00737-0**

**Dirigido a:**

**M.Sc. Aldo Martínez**

**León, Nicaragua lunes 8 de Julio del 2019.**

Contenido

[1. Escenario para la configuración de un firewall 3](#_Toc14196118)

[2. Traducción de direcciones y puertos en el firewall: tabla NAT 3](#_Toc14196119)

[2.1.1. ICMP 4](#_Toc14196120)

[2.1.2. UDP 5](#_Toc14196121)

[2.1.3. TCP 10](#_Toc14196122)

[2.2. Servidor en la red privada, cliente externo 12](#_Toc14196123)

[2.2.1. UDP 12](#_Toc14196124)

[2.2.2. TCP 14](#_Toc14196125)

[3. Filtrado en el firewall: tabla filter 17](#_Toc14196126)

[3.2. Configuración de las reglas de filtrado en el firewall 17](#_Toc14196127)

[3.3. Pruebas de la configuración del firewall 19](#_Toc14196128)

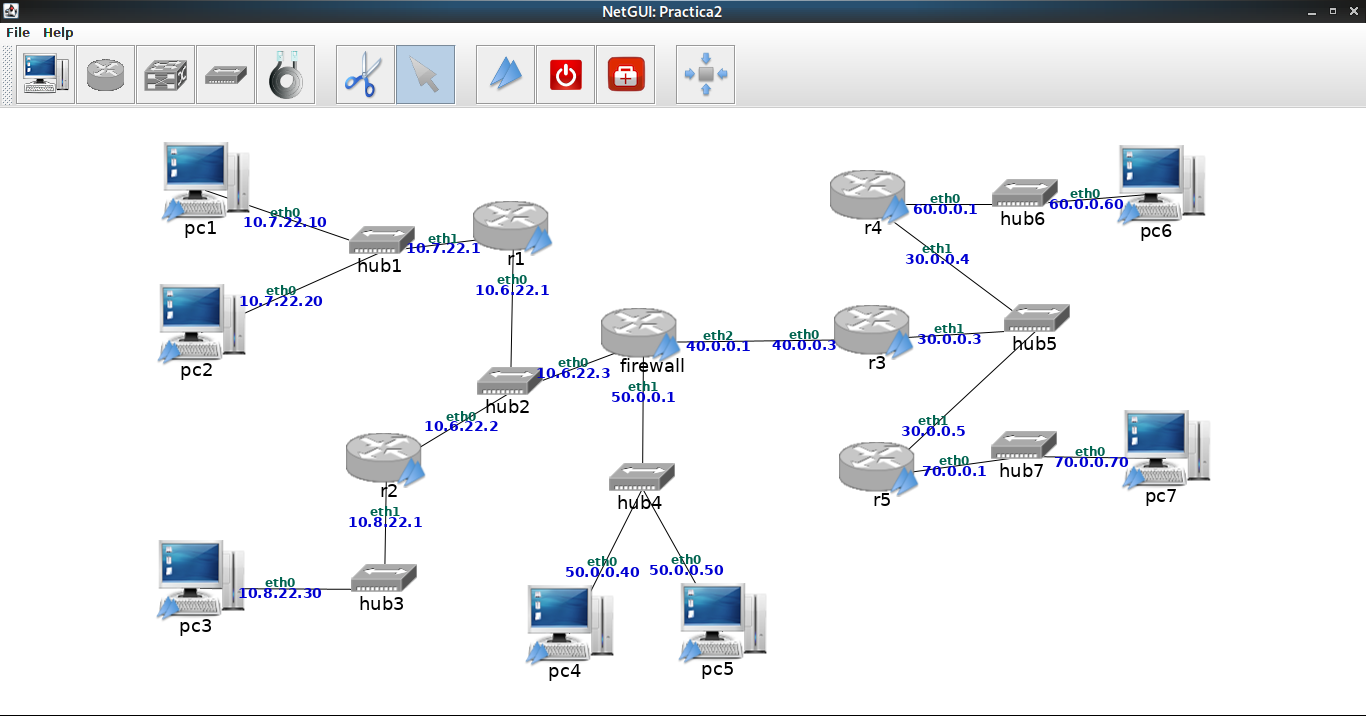
# 1. Escenario para la configuración de un firewall

Arranca de una en una todas las máquinas de la figura.

Configura las direcciones IP en cada una de las máquinas, asignándoles una dirección IP válida en

la subred a la que pertenecen. Configura las rutas que sean necesarias en cada uno de los routers para que todas las máquinas de las subredes privadas se puedan comunicar entre ellas y todas las máquinas de las subredes públicas se puedan comunicar entre ellas. Hasta que no se configuren las reglas NAT en el firewall no se podrán comunicar las máquinas de las subredes privadas con las de Internet. El router r3 sólo puede tener rutas a las subredes públicas: subred 1, subred 2, subred 3,

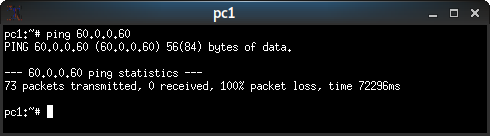
subred 4 y subred 5. No puedes configurarle una ruta por defecto.

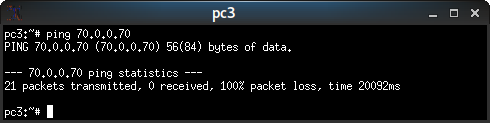


# 2. Traducción de direcciones y puertos en el firewall: tabla NAT

Comprueba que no funciona un ping desde las máquinas internas de las redes privadas (pc1, pc2

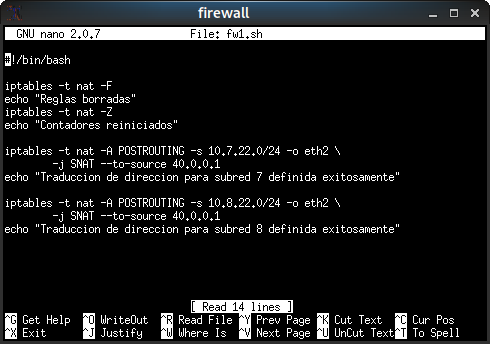
y pc3) a destinos de Internet como pc6 o pc7.





1. Configura un script fw1.sh en el firewall para que primero borre las reglas que hubiera configuradas previamente en la tabla nat y reinicie los contadores de dicha tabla, y a continuación

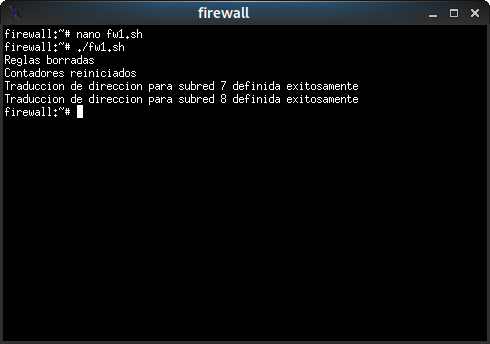
realice la traducción de direcciones en el tráfico saliente de las redes privadas (SNAT) y en su correspondiente tráfico de respuesta. Explica para qué subredes has tenido que realizar la configuración de SNAT. Incluye el script fw1.sh en la memoria y explı́calo.



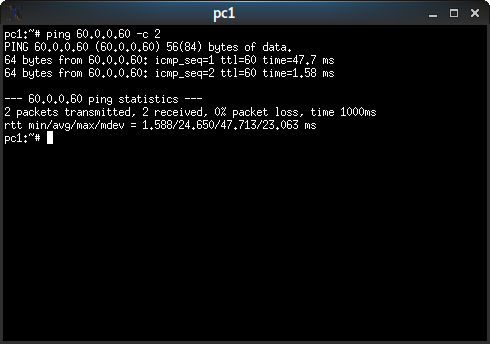
Se ha realizado la configuracion de SNAT para la subred 7 en las cuales se encuentran la pc1 y la pc2, tambien para la subred 8 en la cual se encuentra la maquina 3.

### 2.1.1. ICMP

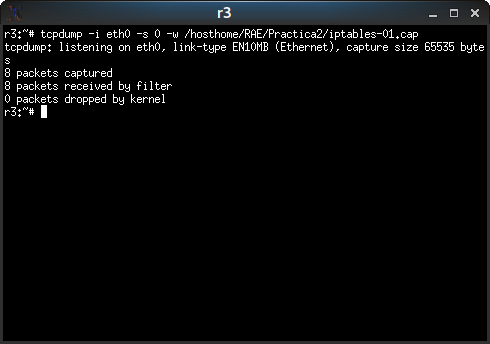
Ejecuta el script fw1.sh de 2.1.



1. Realiza una captura de tráfico en r3 (iptables-01.cap). Ejecuta un ping desde pc1 a pc6 con la opción que permite enviar sólo 2 paquetes ICMP echo request (-c 2).

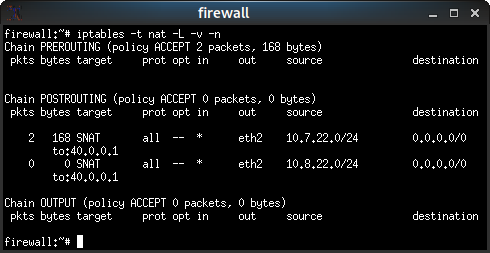


Interrumpe la captura de tráfico. Explica las direcciones IP que se usan en la captura.



Se usa la ip del firewall de la interfaz eth2 (que tiene direccionamiento publico) y la ip de la pc6, que es a la que desde pc1 se le ha hecho ping.

2. Explica qué significa el resultado de la ejecución del siguiente comando en firewall:



Qué regla/s está/n cumpliendo los paquetes ICMP echo request e ICMP echo response y cuántas

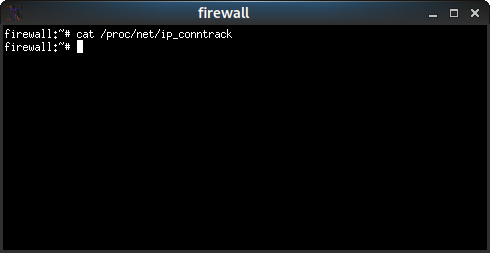
veces se cumple/n. Indica qué polı́ticas por defecto se están cumpliendo de las cadenas de la tabla

nat y cuantos paquetes las han cumplido.

- Se cumple la regla que fue definida para la subred 7 y se cumple 2 veces debido a que fueron 2 ping los que se le hicieron a la pc6,

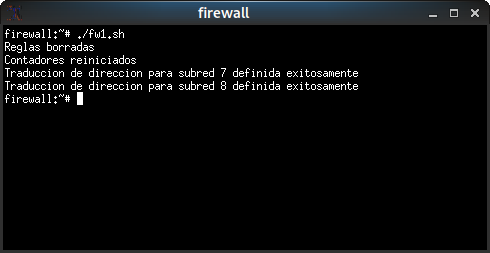
3. Consulta la información de seguimiento de conexiones del módulo ip\_conntrack del firewall

y explica el resultado.



### 2.1.2. UDP

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



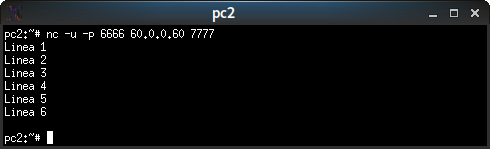
1. Ejecuta nc en modo servidor UDP en pc6 y nc en modo cliente UDP en pc2. Simultáneamente realiza una captura en r3 (iptables-02.cap) y consulta la información ip\_conntrack de firewall.

Escribe 5 lı́neas en el terminal de pc2 para que se las envı́e a pc6 (con cada lı́nea, es decir cada

vez que pulsas una cadena de caracteres y <Enter>, se envı́a un paquete UDP nuevo). Observa el

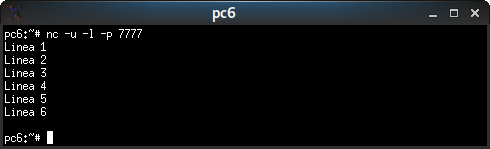
estado de ip\_conntrack. Escribe una lı́nea en pc6 para que se la envı́e a pc2. Observa el estado

de ip\_conntrack.



Enviada por servidor

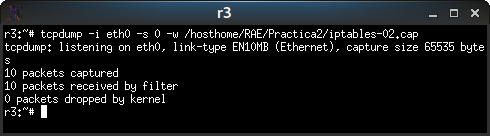






Interrumpe la captura y las ejecuciones de nc, explica la captura y cómo ésta se relaciona con

la información que has visto en ip\_conntrack.

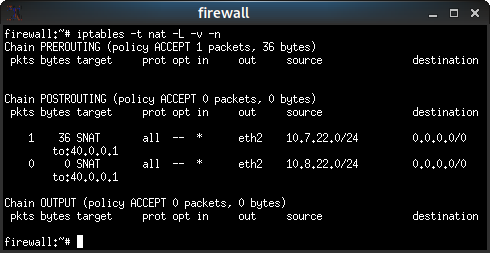


Se reflejan los paquetes udp enviados (las lineas ingresadas) desde el cliente al servidor y viceversa cuando del servidor se envio una linea al cliente, tambien se puede ver como se traduce la ip de pc1 a la ip del firewall eth2 y pc6 no sabe que en realidad es de pc1 que vienen esos mensajes, asi mismo es por ello que pc6 a quien envia la linea cuando se realiza el envio de servidor a cliente lo hace a la ip de eth2 del firewall.

2. Explica lo que muestra el contenido de la tabla nat del firewall. Indica qué regla/s están

cumpliendo los paquetes y cuántas veces se cumple/n. Indica qué polı́ticas por defecto se están

cumpliendo de las cadenas de la tabla nat y cuantos paquetes las han cumplido.



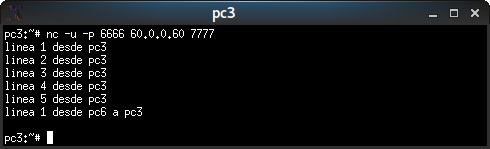
Se cumple la regla definida para la subred 7 y la cumple un paquete.

3. Vuelve a repetir la misma prueba anterior pero iniciando el servidor UDP en pc6 y el cliente

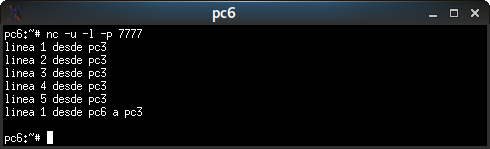
UDP en pc3. Escribe 5 lı́neas en el terminal de pc3 para que se las envı́e a pc6. Observa el

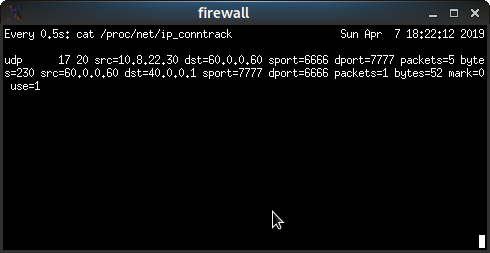
estado de ip\_conntrack. Escribe una lı́nea en pc6 para que se la envı́e a pc3. Observa el estado

de ip\_conntrack.

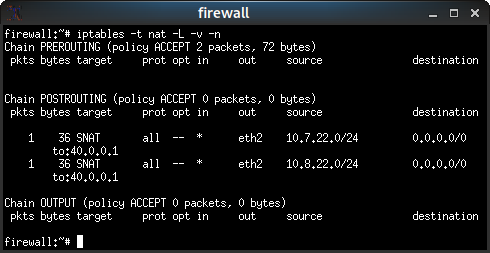








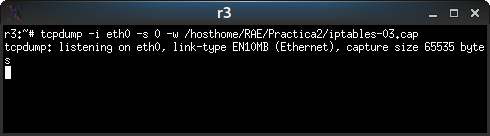
Interrumpe las ejecuciones de nc, explica lo que muestra el contenido de la tabla nat del firewall. Indica qué regla/s están cumpliendo los paquetes y cuántas veces se cumple/n. Indica qué polı́ticas por defecto se están cumpliendo de las cadenas de la tabla nat y cuantos paquetes las han cumplido.

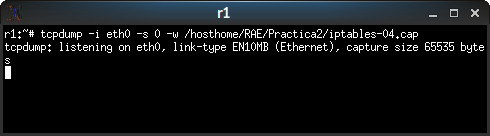


Esta vez se cumplio la regla que fue definida para la subred 8, y se cumple una vez.

4. Primero inicia una captura en r3 (iptables-03.cap) para capturar todo el tráfico que atraviese

este router e inicia otra captura en r1-eth0 (iptables-04.cap).





Ejecuta una aplicación servidor UDP escuchando en el puerto 7777 en pc7 con el comando nc.



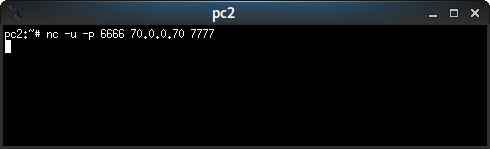
Ejecuta en pc1 una aplicación cliente UDP que utilice localmente el puerto 6666 y que se comu-

nique con ese servidor anterior de la siguiente manera:



Y ejecuta en pc2 una aplicación cliente UDP que utilice localmente el puerto 6666 y que se

comunique con ese servidor anterior de la siguiente manera:



Consulta la información de ip\_conntrack en firewall, dado que todavı́a no se han enviado

datos, no deberı́a aparecer nada.

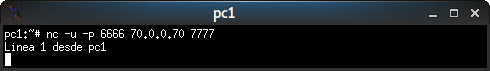


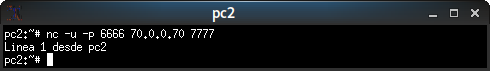
Escribe una cadena de caracteres a través de la entrada estándar de pc1 y pulsa <Enter>. A

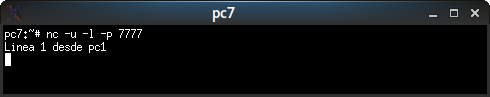
continuación introduce una cadena de caracteres a través de la entrada estándar de pc2 y pulsa

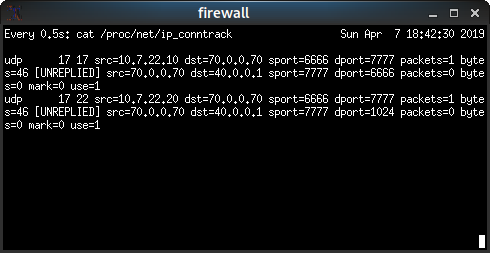
<Enter>. Interrumpe las dos capturas y explica qué ocurre con la traducción de direcciones y

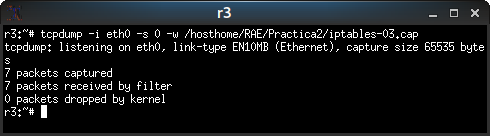
puertos.

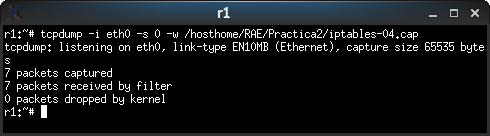








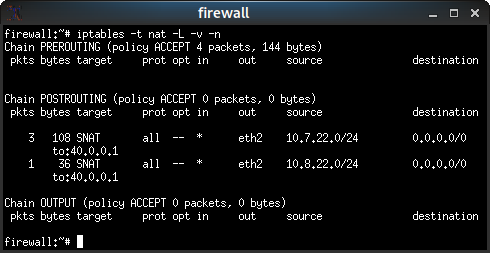




En la captura del router de la red privada que ambos mensajes de las pc de esta red van con la ip privada y con los puertos especificados como clientes, y en la captura realizada en la zona publica el puerto con el que se realiza el envio del mensaje desde el ciente ya no es el mismo que la captura en la zona privada, esto es porque se ha hecho una traduccion y en este flujo de datos se tomo un puerto que estuviera libre en el firewall para hacer el envio como cliente, ya que el 6666 especificado por pc2 a la hora de hacer el envio ya habia sido ocupado primero por pc1 al haber establecido una conexión primero ellos.

5. Consulta la tabla nat del firewall y explica cuántas veces se han cumplido las reglas de tra-

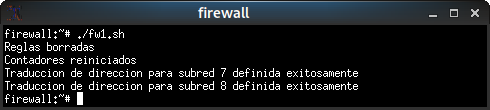
ducción de direcciones.



Se han cumplido hasta el momento 4 veces.

### 2.1.3. TCP

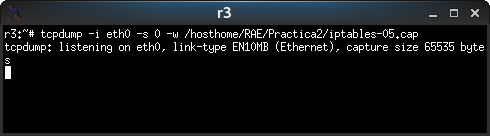
Ejecuta el script fw1.sh de 2.1 para que reinicie los contadores de paquetes de iptables.



1. Para este apartado vamos a usar nc en modo TCP.

Primero inicia una captura en r3 (iptables-05.cap) para capturar todo el tráfico que atraviese

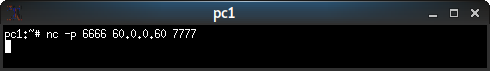
este router.



Ejecuta una aplicación servidor TCP escuchando en el puerto 7777 en pc6 con el comando nc.

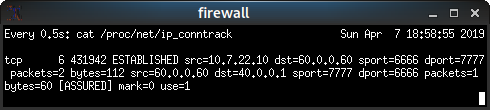


Y ejecuta en pc1 una aplicación cliente TCP que se comunique con el servidor anterior.



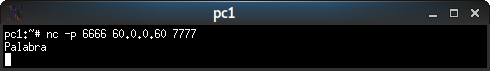
Simultáneamente consulta ip\_conntrack del firewall cada medio segundo. Explica el número

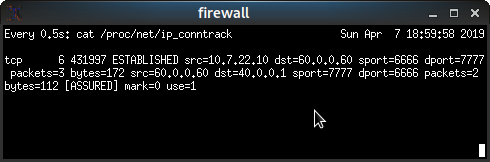
de paquetes que se han observado en cada sentido, razonando la respuesta.



2. Introduce una palabra en la entrada estándar de pc1, pulsa <Enter> y explica razonadamente

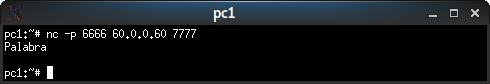
lo que observas en ip\_conntrack.

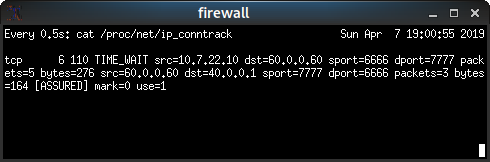


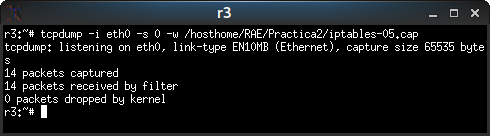


3. Realiza un Ctrl+C en el terminal de pc1 para interrumpir la ejecución de nc. Interrumpe la

captura en r3 y contrasta lo que observas en la captura con lo que muestra ip\_conntrack.

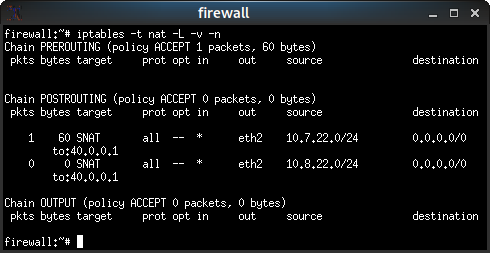






En el ip\_conntrack se muestran las ip origen y destino primero antes y despues de la traduccion realizada por el firewall y esto mismo es comprobado en la captura de trafico, como efectivamente en la zona publica las ip reales de la zona privada no se conocen.

4. Consulta la tabla nat del firewall y explica cuántas veces se han cumplido las reglas de traducción de direcciones. Indica qué polı́ticas por defecto se están cumpliendo de las cadenas de la tabla nat y cuantos paquetes las han cumplido.



Se ha cumplido una las reglas definidas y la polı́tica aplicada es la que fue definida para la subred 7 y el paquete tcp enviado es el que la ha cumplido.

## 2.2. Servidor en la red privada, cliente externo

### 2.2.1. UDP

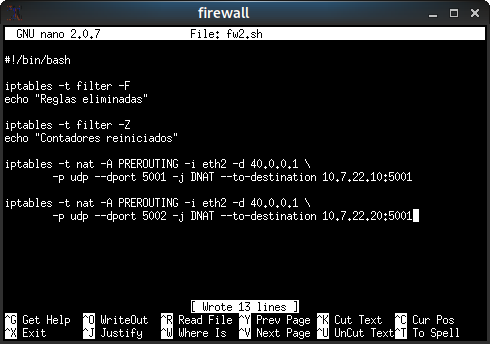
Realiza un nuevo script de iptables fw2.sh en firewall que primero borre las reglas que hubiera

configuradas previamente en la tabla nat y reinicie los contadores de dicha tabla, y a continuación

realice la siguiente traducción de direcciones:

El tráfico de entrada al firewall destinado al puerto UDP 5001 debe ser redirigido a pc1, puerto 5001.

El tráfico de entrada al firewall destinado al puerto UDP 5002 debe ser redirigido a pc2, puerto 5001.



1. Explica el nuevo script.

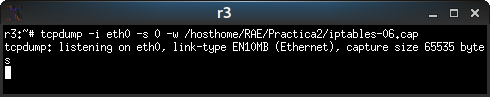
En el shellscript fw2.sh se ejecutan 4 ordenes en las cuales primeramente se eliminan todas las reglas antes definidas que puede haber tenido el firewall, en la siguiente reinicia los contadores del uso de las reglas que se eliminaron con la primer orden. En la tercer orden se direcciona todo el trafico entrante a la red privada a traves del firewall por el puerto 5001 de udp a la pc 1 a su puerto 5001 udp y en la ultima se hace lo mismo. El trafico entrante esta vez por el puerto 5002 udp del firewall se direcciona al puerto 5001 udp de la pc2.

2. Inicia una captura de tráfico en r3 (iptables-06.cap). Lanza nc en modo servidor UDP en

pc1 y pc2, escuchando en ambos casos en el puerto 5001.Lanza nc en modo cliente UDP en pc6

y pc7 de tal forma que el tráfico generado en pc6 lo reciba pc1 y el tráfico generado en pc2 lo

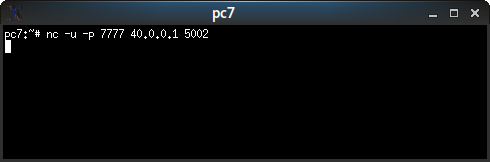
reciba pc7. Explica cómo has arrancado los dos clientes nc en pc6 y pc7.





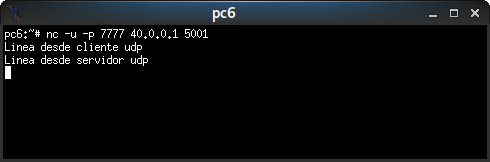


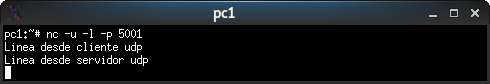


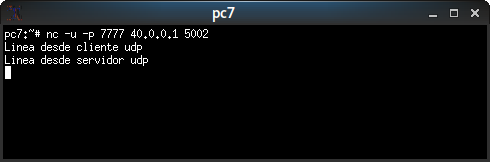


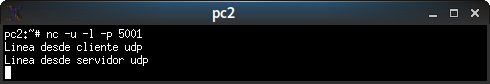
3. Escribe una lı́nea en cada uno de los terminales involucrados (pc1, pc2, pc6 y pc7). Interrumpe los clientes y servidor con Ctrl+C. Interrumpe la captura de tráfico. Explica el resultado observado

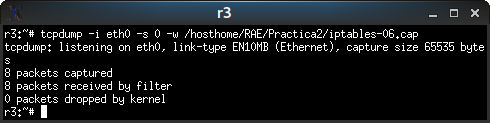
en ip\_conntrack y la traducción de direcciones IP y puertos realizada.











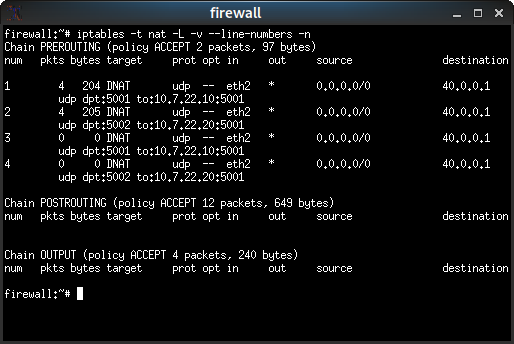


En la captura en el ip\_conntrack se puede ver que los paquetes llevan como destino la eth2 del firewall y los puertos destinos son del firewall y el firewall es el encargo de hacer la traduccion y el que sabe cual es la correspondiente a cada una.

4. Consulta la tabla nat del firewall y explica cuántas veces se han cumplido las reglas de tra-

ducción de direcciones. Indica qué polı́ticas por defecto se están cumpliendo de las cadenas de

la tabla nat y cuantos paquetes las han cumplido.



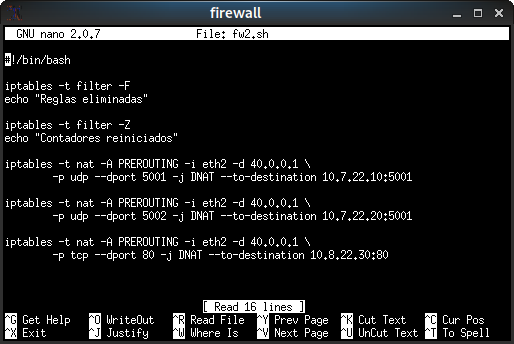
Se han cumplido 2 veces las reglas y han sido las definidas para las traducciones de direcciones y puertos del trafico entrante desde internet a la red privada.

### 2.2.2. TCP

Añade la siguiente configuración de traducción de direcciones al script fw2.sh de iptables de firewall:

El tráfico de entrada al firewall destinado al puerto TCP 80 debe ser redirigido a pc3, puerto

80.

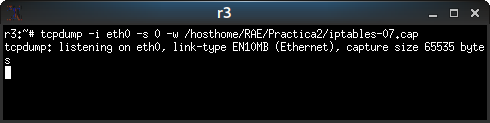


1. Explica las modificaciones del script.

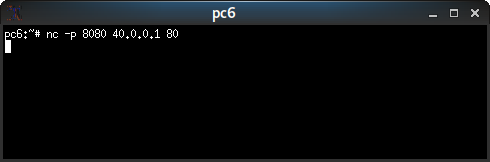
Hemos agregado una nueva orden en la cual el trafico que entra a la red privada atraves del puerto 80 tcp del firewall sea direccionado al puerto 80 de la pc3.

2. Inicia una captura de tráfico en r3 (iptables-07.cap). Lanza nc en modo servidor TCP en pc3

escuchando en el puerto 80. Lanza nc en modo cliente TCP en pc6 de tal forma que el tráfico generado en pc6 lo reciba pc3. Explica cómo has arrancado el cliente de nc en pc6.





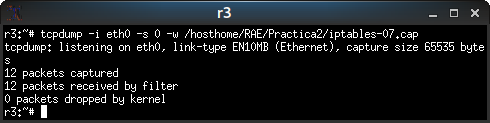


Se ha lanzado el cliente con la ip del firewall y especificando el puerto, esto es porque en internet no se conoce la existencia de la red privada, el firewall es el encargado de hacer la traduccion con la regla que se ha definido en el.

3. Interrumpe el cliente y el servidor con Ctrl+C. Interrumpe la captura de tráfico. Explica el

resultado observado en ip\_conntrack y la traducción de direcciones IP y puertos realizada.





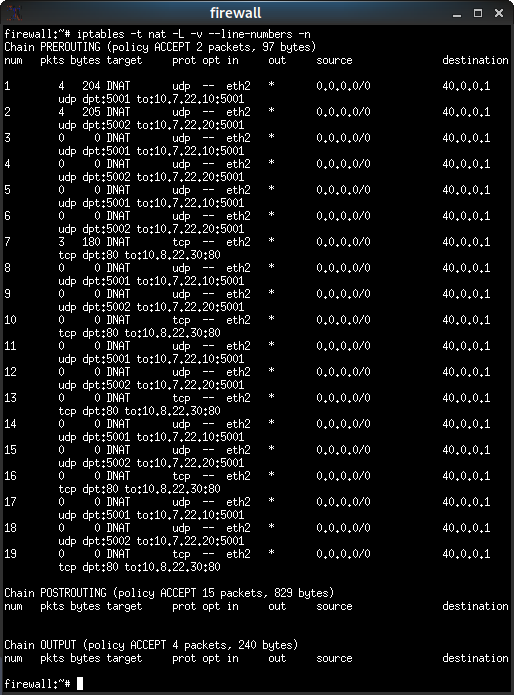


Efectivamente a como se observa en el ip\_contrack tambien se ve en la captura como aparentemente la conexión cliente-servidor se establece utilizando la ip del firewall como si estuviera ejecutandose el servidor en el.

4. Consulta la tabla nat del firewall y explica cuántas veces se han cumplido las reglas de tra-

ducción de direcciones. Indica qué polı́ticas por defecto se están cumpliendo de las cadenas de

la tabla nat y cuantos paquetes las han cumplido.



# 3. Filtrado en el firewall: tabla filter

## 3.2. Configuración de las reglas de filtrado en el firewall

1. Crea un script en el firewall fw3.sh partiendo de la configuración de traducción de direcciones IP y puertos realizada en fw1.sh que añada la siguiente configuración:

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

b) Fijar las polı́ticas por defecto de las cadenas de la tabla filter, haciendo que por defecto

se descarte todo el tráfico en el firewall excepto los paquetes de salida.

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

d ) Permitir todo el tráfico saliente desde las subredes privadas hacia Internet y el tráfico de respuesta al saliente. Ten en cuenta que como has partido del script fw1.sh, en dicho script ya tenı́as las reglas de la tabla nat de modificación de la dirección IP de origen de los paquetes que reenvı́a el firewall y los paquetes del tráfico entrante de respuesta al saliente.

e) Permitir desde Internet únicamente el tráfico entrante nuevo hacia la zona DMZ según las

siguientes reglas y su correspondiente tráfico de salida: un servidor echo instalado en pc4 (UDP, puerto 7). Debes configurar inetd en pc4para que arranque este servidor. Utiliza nc para probar la comunicación como cliente desde una máquina de Internet y el tráfico de respuesta. un servidor daytime instalado en pc5 (UDP, puerto 13). Debes configurar inetd en pc5 para que arranque este servidor. Utiliza nc para probar la comunicación como cliente desde una máquina de Internet y el tráfico de respuesta.

f ) Permitir únicamente la comunicación entre la red privada y la zona DMZ de la siguiente

forma: Conexión de telnet (TCP, puerto 23) desde pc1 a pc5. Debes configurar inetd en pc5

para que arranque este servidor. Para poder probar esta comunicación, desde pc1 ejecuta:

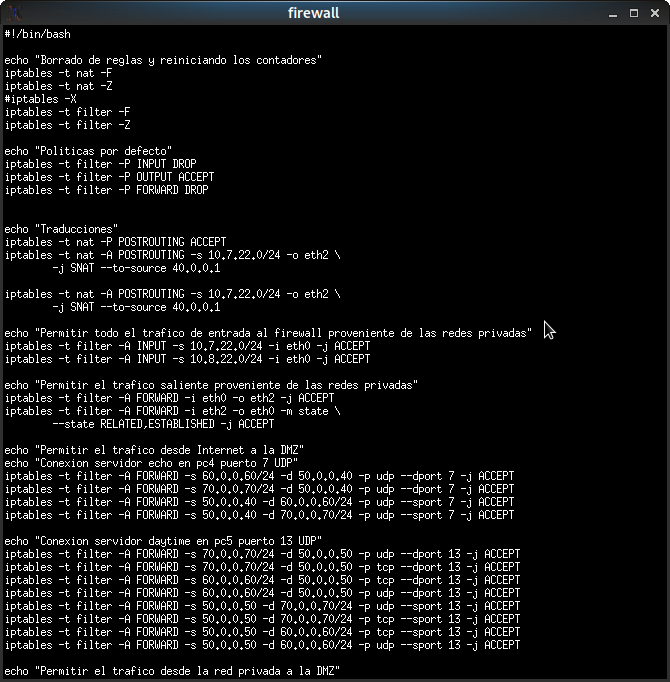
telnet <dir\_IP\_pc5> Podrás entrar de forma remota en pc5 utilizando usuario: root, clave: root.

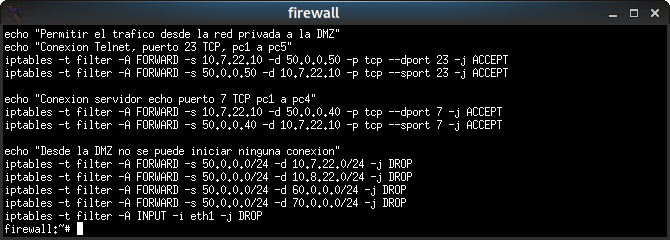
Conexión al servidor de echo (TCP, puerto 7) desde pc1 a pc4. Debes configurar inetd en pc4 para que arranque este servidor. Utiliza nc para probar la comunicación como cliente desde pc1.

g) Desde la zona DMZ no se puede iniciar ninguna comunicación con la red privada, ni con el firewall.

Incluye el script fw3.sh en la memoria y explı́calo.

Este script tiene como base el fw1.sh en el cual estan configuradas las traducciones nat y snat. Se añadieron nuevas reglas en las cuales lo que hace es permitir o negar trafico. Primero se reiniciaron los contadores de la tabla filter y fueron definidas las politicas por defecto de la tabla filter donde se descarta cualquier cosa execto los paquetes de salida. Despues se le da acceso a la red privada al firewall, se permite el trafico de la red privada a internet y su trafico de respuesta correspondiente. A la DMZ se le niega el acceso al firewall y se le niega el trafico a la red privada, se permite conexiones desde red privada a servidores de la zona DMZ con ip y puertos especificos, asi como tambien desde internet a la DMZ.

****

****

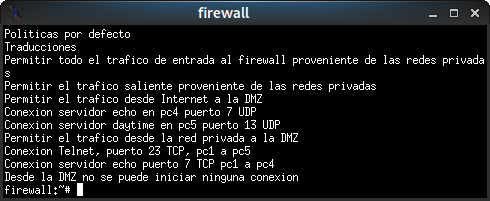
## 3.3. Pruebas de la configuración del firewall

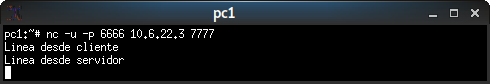
Para poder comprobar qué reglas se están aplicando a cada caso que pruebas, añade a cada regla otra regla con las misma condiciones y acción LOG de forma que quede una anotación en el fichero de log cada vez que se cumpla cada condición.

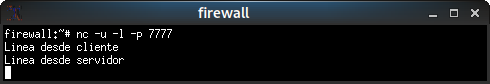
**Pruebas**

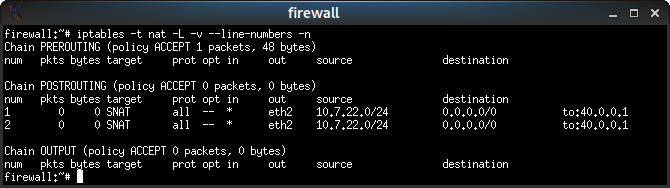
a) Si se arranca una aplicación servidor (TCP o UDP) en la máquina firewall sólo podrá aceptar tráfico de un cliente que envı́e mensajes desde una de las máquinas de las subredes privadas. Asegúrate de que antes de lanzar cliente y servidor has ejecutado fw3.sh para que reinicie los contadores de iptables. Por ejemplo arranca un servidor UDP en firewall y arranca un cliente UDP en pc1 que se comunique con dicho servidor (escribe alguna lı́nea en cada uno de los terminales para que haya tráfico UDP).

Explica en la memoria: las reglas en las tablas nat y filter que se han cumplido y el número de veces. las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.



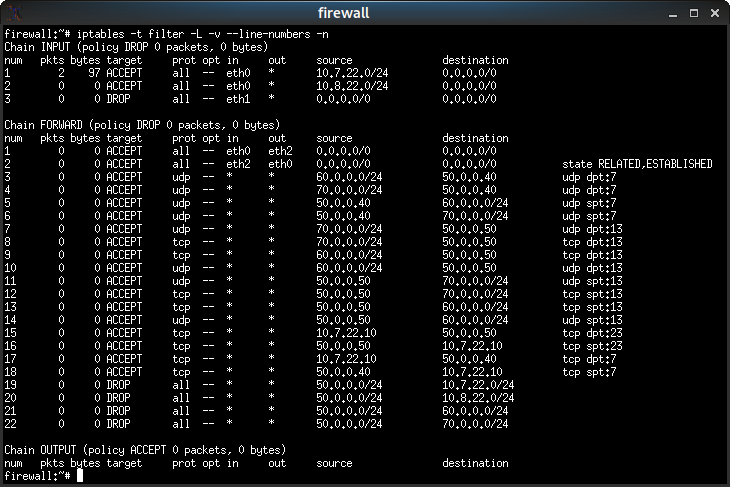






En la tabla NAT se puede ver que no se han requerido ninguna de estas reglas debido a que ningun paquete ha salido del firewall.

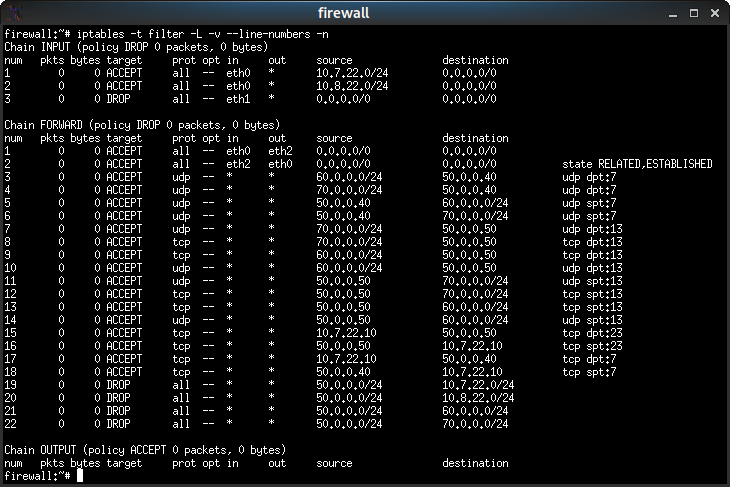
En la tabla filter si se puede ver que 2 paquetes han llegado efectivamente al firewall y fueron aceptados.

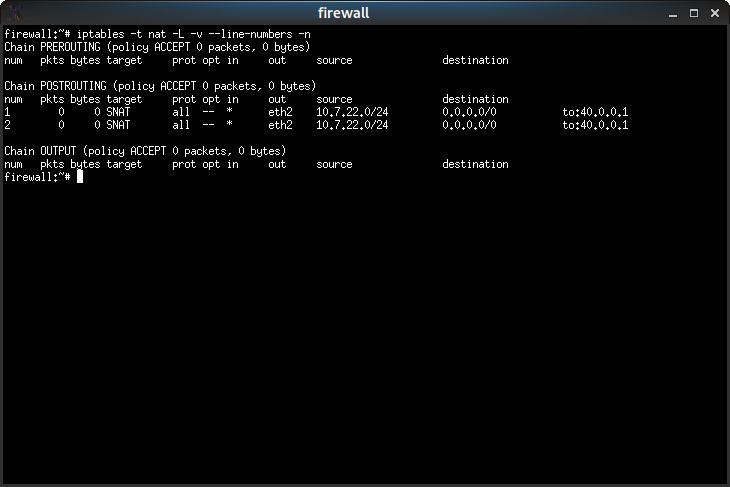
b) No podrá aceptar tráfico desde aplicaciones cliente lanzadas en otras subredes diferentes. Asegúrate de que antes de lanzar cliente y servidor has ejecutado fw3.sh para que reinicie los contadores de iptables. Por ejemplo, arranca un servidor UDP en firewall y arranca un cliente UDP en pc6 que se comunique con dicho ser vidor (escribe alguna lı́nea en cada uno de los terminales para que haya tráfico UDP).





Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.



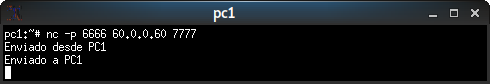
2. Permitir todo el tráfico saliente desde las subredes privadas hacia Internet, modificando la dirección IP de origen de los paquetes que reenvı́a el firewall, y el tráfico entrante de respuesta al saliente.

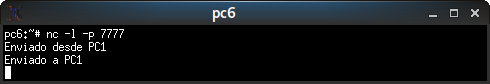
**Pruebas:**

a) Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de Internet y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de las subredes internas, el tráfico debe poder enviarse del cliente al servidor y del servidor al cliente, observando que el tráfico que sale del firewall con destino a la máquina de Internet no tiene como dirección IP origen la dirección de la máquina que pertenece a la subred privada, sino que lleva la

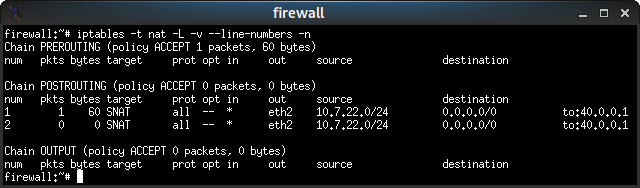
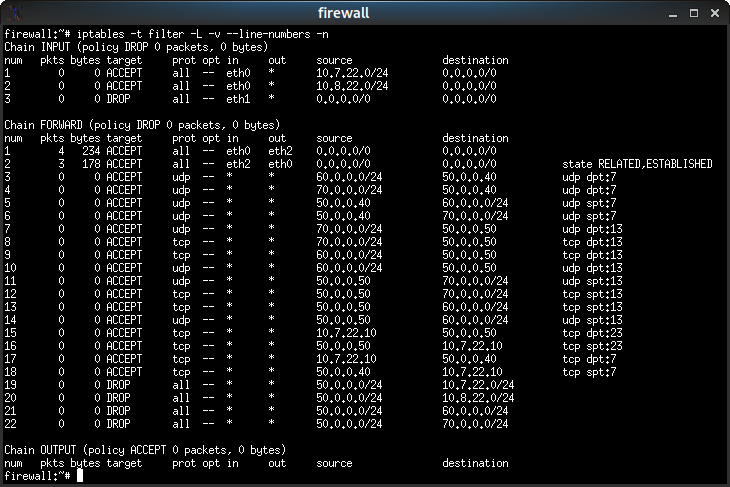
dirección pública del firewall de la interfaz que le conecta con Internet. Ejecuta la misma prueba que en el apartado 2.1.3. Asegúrate de que antes de lanzar cliente y servidor has ejecutado fw3.sh para que reinicie los contadores de iptables. Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces. las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.



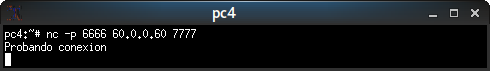


En este caso se puede ver en ambas tablas que los paquetes han cruzado el firewall en ambos sentidos y se ha hecho uso de las reglas definidas tanto para la traduccion asi como para el respectivo enrutamiento.

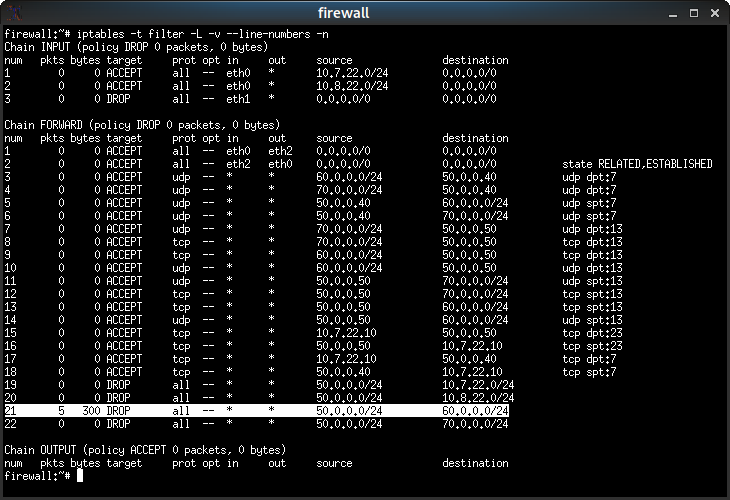


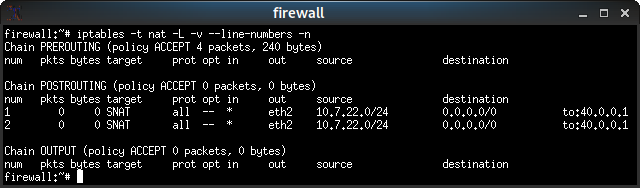
b) Si se arranca una aplicación cliente en pc4 o pc5 para comunicarse con el servidor que se haya arrancado en una de las máquinas de Internet, el firewall no deberı́a permitir reenviar ese tráfico hacia Internet. Asegúrate de que antes de lanzar cliente y servidor has ejecutado fw3.sh para que reinicie los contadores de iptables. Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces. las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.





A como se puede observar la conexión se realiza debido a que los paquetes del establecimiento de la conexión se eliminan al llegar al router a como se ve en la tabla filter.



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

- Un servidor echo instalado en pc4 (UDP, puerto 7).

Pruebas:

a) Desde una máquina de Internet se deberı́a poder acceder a ese servidor de echo de pc4. Ejecuta el siguiente comando desde una máquina de Internet:

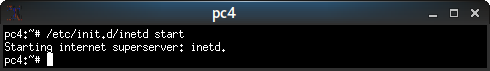
nc -u <dir\_IP\_pc4> 7

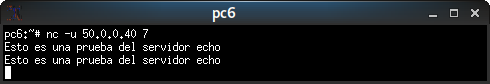
Asegúrate de que antes de lanzar el cliente desde una máquina de Internet has ejecutado fw3.sh para que reinicie los contadores de iptables.

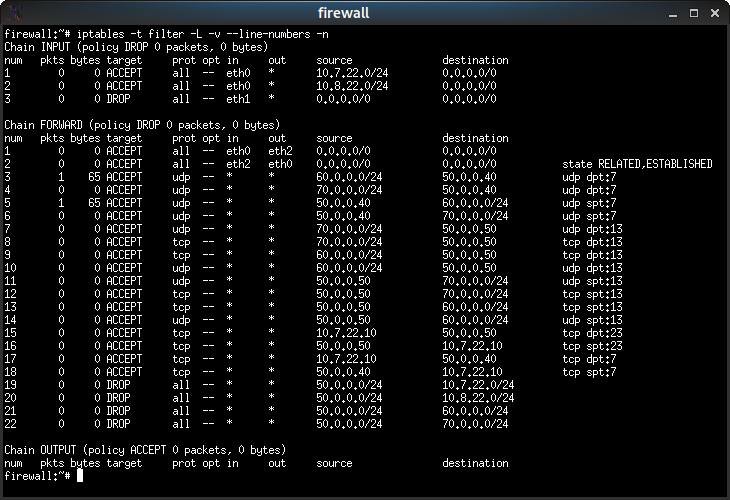
Explica en la memoria:

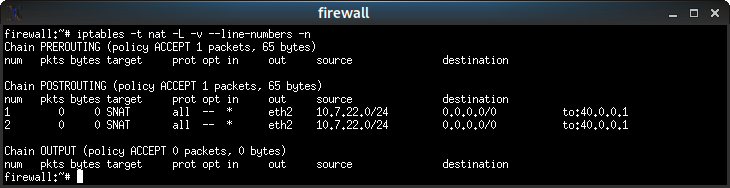
• las reglas en las tablas nat y filter que se han cumplido y el número de veces.

• las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.









A como se ve en la tabla filter se cumplen 2 reglas en las cuales esta definido el permitir ese tipo de conexión y su trafico de respuesta. En la tabla nat no se refleja ningun cambio por lo que la conexión es desde Internet a la DMZ y no es necesario ningun tipo de traduccion.

b) Si se prueba lo mismo arrancando el comando anterior desde pc3 y se manda una cadena de caracteres, no se deberı́a obtener respuesta. Asegúrate de que antes de lanzar el cliente de pc3 has ejecutado fw3.sh para que reinicie los contadores de iptables.

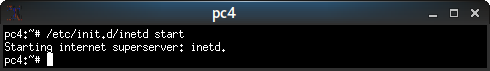
Explica en la memoria:

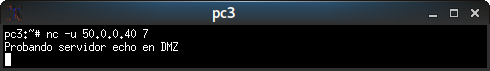
• las reglas en las tablas nat y filter que se han cumplido y el número de

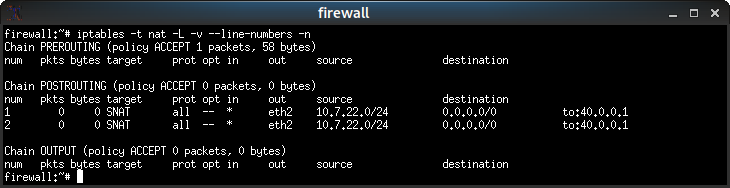
veces.

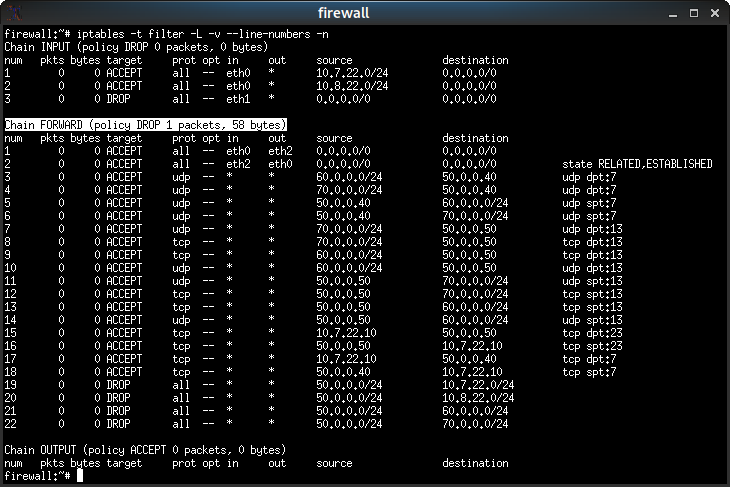
• las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y

filter y el número de veces que se ejecutan.









Como vemos no se tiene respuesta del servidor por lo que la conexión no se realiza debido a que en el firewall no hay definida una regla para permitir esta conexión, sin embargo tampoco hay una que la niegue, pero por defecto es eliminada en la configuracion de las politicas por defecto.

- Un servidor daytime instalado 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.

Pruebas:

a) Desde una máquina de Internet se deberı́a poder obtener la hora de pc5. Ejecuta el siguiente comando desde una máquina de Internet:

nc -u <dir\_IP\_pc5> 13

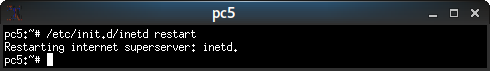
Pulsa < Enter > en el terminal de nc y deberı́a obtenerse la hora que le envı́a pc5.

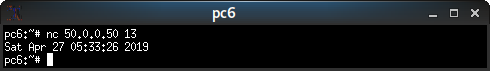
Asegúrate de que antes de lanzar el cliente en pc5 has ejecutado fw3.sh para que reinicie los contadores de iptables.

Explica en la memoria:

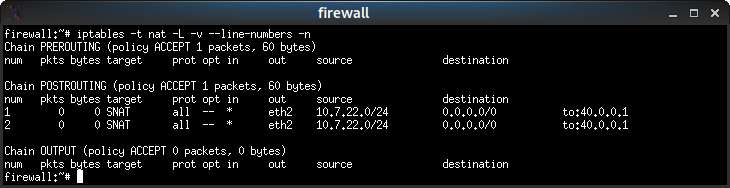
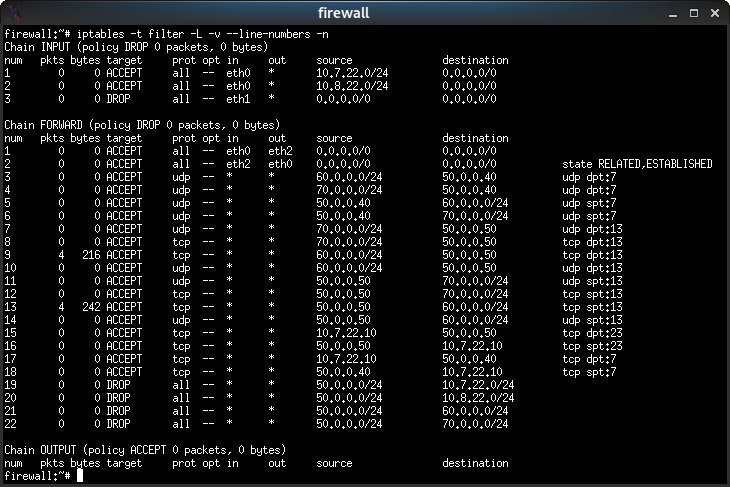
• las reglas en las tablas nat y filter que se han cumplido y el número de veces.

• las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan...





**Nota: HE REALIZADO LA PRUEBA DEL SERVIDOR DAYTIME CON EL PUERTO TCP PORQUE CON UDP NO ME CONECTA AUN SIN HABER APLICADO ALGUNA RESTRICCION EN EL FIREWALL**



b) No se debe permitir otro tipo de tráfico desde Internet a DMZ. Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de DMZ y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de Internet, el tráfico no deberı́a poder enviarse del cliente al servidor ni del servidor al cliente.

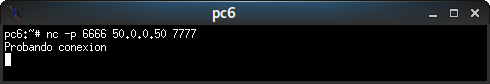
Haz una prueba para este tipo de tráfico y explica que prueba estás haciendo.

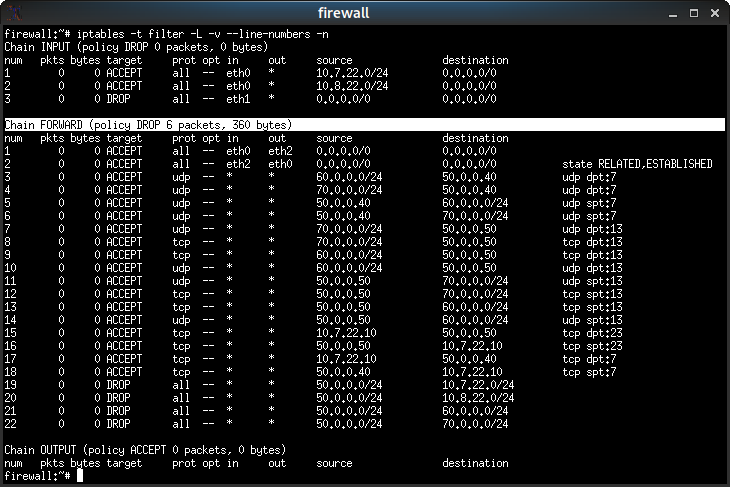
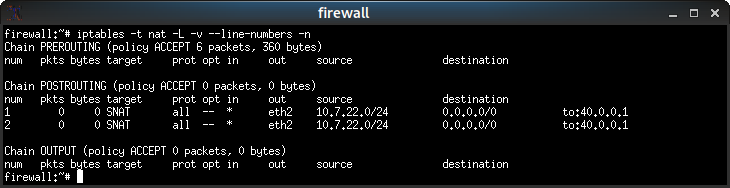
Asegúrate de que antes de lanzar el cliente has ejecutado fw3.sh para que reinicie los contadores de iptables. Explica en la memoria:

• las reglas en las tablas nat y filter que se han cumplido y el número de veces.

• las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.





La conexión no se ha realizado, los paquetes fueron eliminados esto debido al establecer las politicas por defecto y no tener ninguna regla adicional que permita la conexión.

4. Permitir únicamente la comunicación entre la red privada y la zona DMZ de la siguiente forma:

a) Conexión de telnet (TCP, puerto 23) desde pc1 a pc5. La conexión de telnet permite a un usuario conectarse de forma remota a otra máquina.

Pruebas

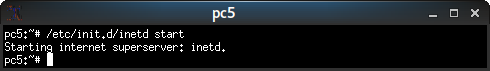
1) Asegúrate de que antes de lanzar el cliente en pc1 has ejecutado fw3.sh para que reinicie los contadores de iptables. Desde pc1 ejecuta el cliente de telnet:

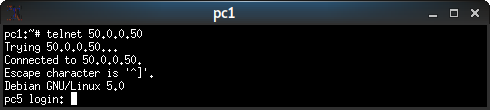
telnet <dir\_IP\_pc5>

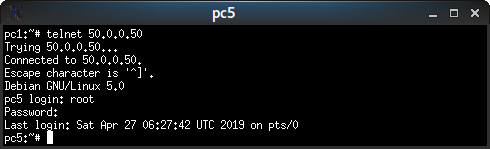
podrás entrar de forma remota en pc5 utilizando usuario: root, clave: root. Explica en la memoria:

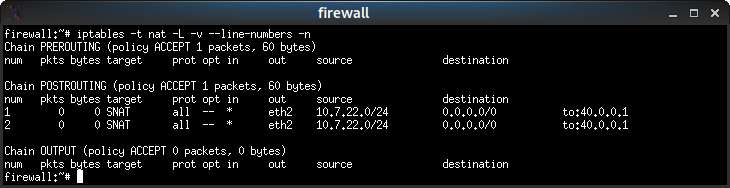
Las reglas en las tablas nat y filter que se han cumplido y el número de veces.

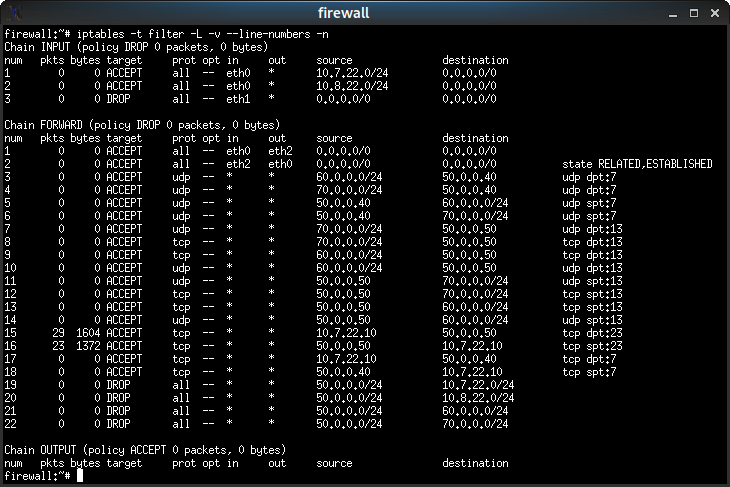
Las polı́ticas por defecto se ejecutan en las cadenas de las tablas nat y filter y el número de veces.











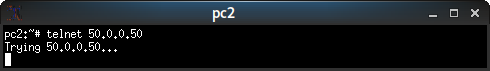
2) Si se prueba lo mismo arrancando el cliente de telnet desde pc2 o pc3 o cualquier máquina de Internet no deberı́a permitir la conexión. Haz una prueba para este tipo de tráfico y explica qué prueba estás haciendo. Asegúrate de que antes de lanzar el cliente has ejecutado fw3.sh para que

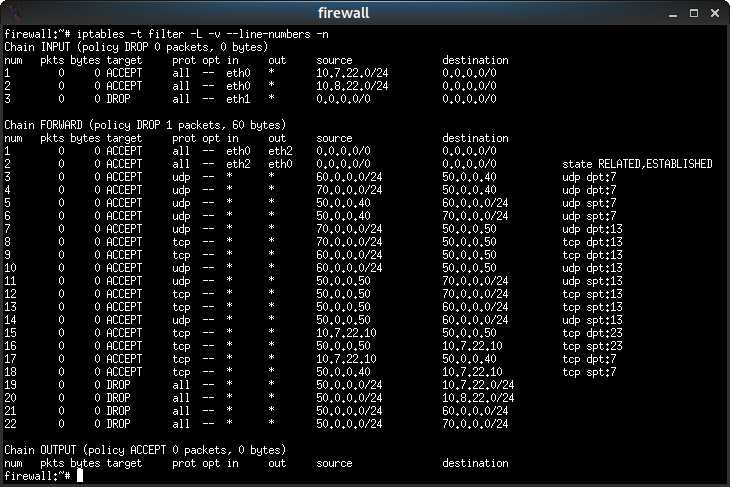
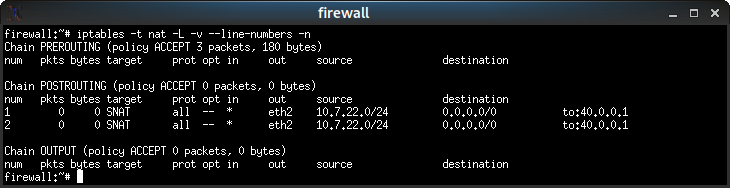
reinicie los contadores de iptables.

Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces.

las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.





b) Conexión al servidor de echo (TCP, puerto 7) desde pc1 a pc4.

Si se arranca cualquier otra aplicación servidor (TCP o UDP) en una de las máquinas de la DMZ y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de las subredes privadas, el tráfico no deberı́a poder enviarse del cliente al servidor ni del servidor al cliente.

Pruebas

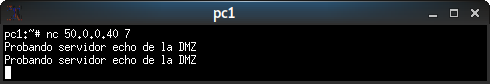
1) Asegúrate de que antes de lanzar el cliente en pc1 has ejecutado fw3.sh para que reinicie los contadores de iptables. Desde pc1 se deberı́a poder conectarse al servidor de echo de pc4:

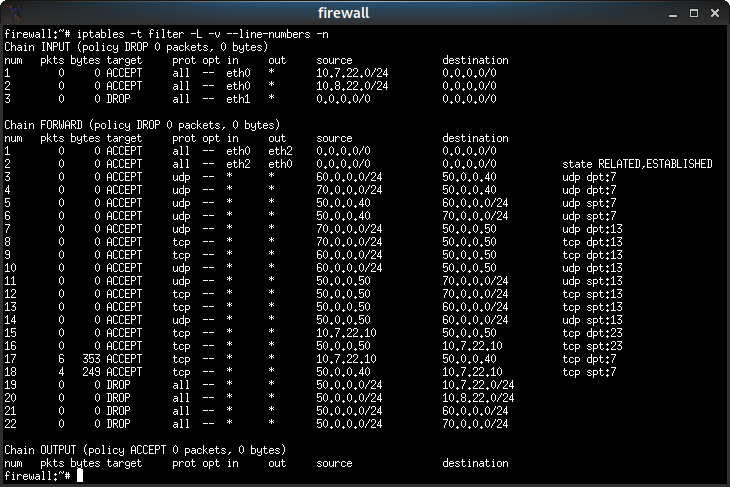
nc <dir\_IP\_pc4> 7

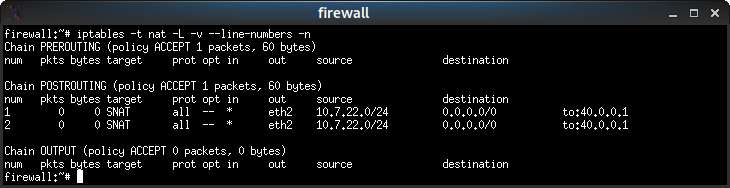
Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces.

Las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.







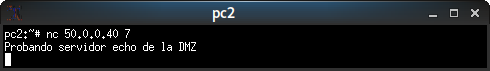
2) Si se prueba lo mismo arrancando nc desde pc2 o pc3 no deberı́a conectarse.

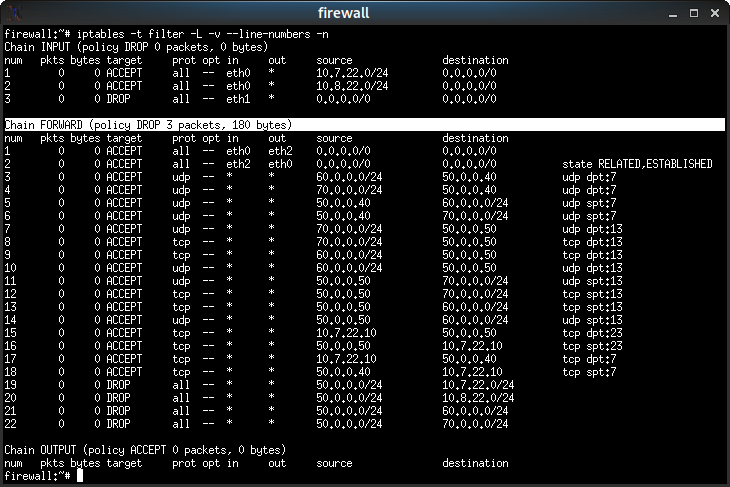
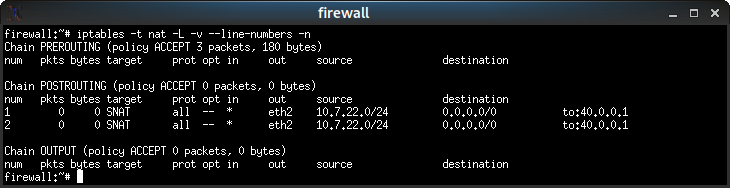
Haz una prueba para este tipo de tráfico y explica qué prueba estás haciendo. Asegúrate de que antes de lanzar el cliente has ejecutado fw3.sh para que reinicie los contadores de iptables.

Explica en la memoria:

las reglas en las tablas nat y filter que se han cumplido y el número de veces.

las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.





5. Desde la zona DMZ no se puede iniciar ninguna comunicación con la red privada, ni con el firewall.

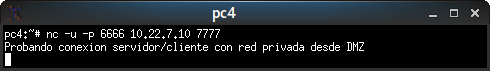
Pruebas

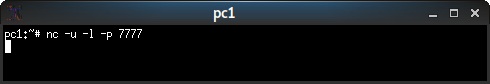
a) Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de las subredes privadas y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de DMZ, el tráfico no deberı́a poder enviarse del cliente al servidor ni del servidor al cliente.

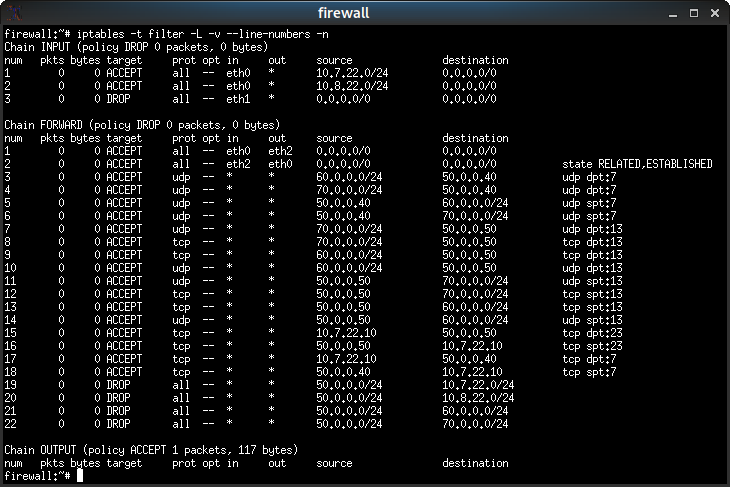
Haz una prueba para este tipo de tráfico y explica qué prueba estás haciendo. Asegúrate de que antes de lanzar el cliente has ejecutado fw3.sh para que reinicie los contadores de iptables.

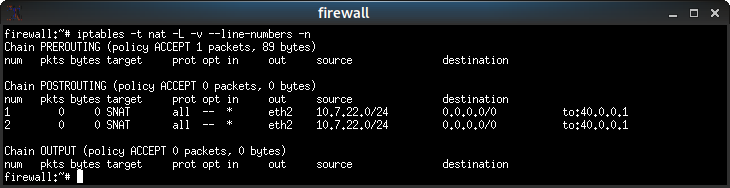
Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces.









b) Si se arranca una aplicación servidor (TCP o UDP) en el firewall y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de DMZ, el tráfico no deberı́a poder enviarse del cliente al servidor ni del servidor al cliente.

Haz una prueba para este tipo de tráfico y explica qué prueba estás haciendo.

Asegúrate de que antes de lanzar el cliente has ejecutado fw3.sh para que reinicie los contadores de iptables.

Explica en la memoria:

Las reglas en las tablas nat y filter que se han cumplido y el número de veces.

las polı́ticas por defecto que se ejecutan en las cadenas de las tablas nat y filter y el número de veces que se ejecutan.

