I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Manual IPTables

1 Cortafuegos e iptables

Un cortafuegos es un conjunto de reglas de filtrado de paquetes que regulan y controlan el tráfico entre dos redes (o el tráfico individual de un equipo). Este conjunto de reglas se pueden establecer en un hadware específico o bien establecerlo en un ordenador, con linux en nuestro caso.

Iptables es la utilidad que vamos a utilizar para crear e insertar en el núcleo las distintas reglas de filtrado que vamos a establecer sobre los paquetes.

1.1 Tipos de filtros de paquetes

Podemos distinguir varios tipos de paquetes IP en la máquina cortafuegos:

Paquetes con origen remoto y destino remoto: son los paquetes, que actuando como gateway, nuestra máquina tiene que reenviar. Estos paquetes se analizan mediante el filtro de reenvío, llamado FORWARD. Para que una máquina pueda reenviar paquetes tenemos que activar esta caractaarística mediante

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Paquetes con origen remoto y destino local: son los paquetes que las máquinas de cualquier red envían a nuestra máquina. Estos paquetes se analizan mediante el filtro de entrada, llamado INPUT.

Paquetes con origen local y destino remoto: son los paquetes que nuestra máquina envía a otras computadoras. Estos paquetes se analizan mediante el filtro de salida, llamado OUTPUT.

Generalizando un poco los tipod de filtos pueden ser:

MANGLE: reglas de manipulación de paquetes.

NAT: reglas PREROUTING, POSTROUTING de traducción de direcciones. (NAT network address translation).

FILTER: reglas INPUT, OUTPUT, FORWARD de filtrado de paquetes que ya habíamos descrito.

1.1.1 Cadenas

Vamos a denominar cadena al conjunto de reglas asociados con un determinado tipo de filtro. Iptables también dispone de la posibilidad de que un usuario pueda definir sus

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

propias cadenas y asignarle un nombre. Los nombres de cadenas predefinidos son INPUT, OUTPUT y FORWARD.

1.2 Acciones sobe un paquete

Como vimos anteriormente, las decisiones que puede tomar un cada regla de un filtro de paquetes pueden ser, dejar pasar el paquete (ACCEPT), responderle al emisor educadamente que ese paquete no puede pasar (REJECT) o bien simplemente descartarlo como si no hubiera llegado (DROP o DENY).

Observamos que la diferencia entre REJECT y DROP consiste en que mediante REJECT se le contesta que el servicio no está disponible (icmp destination port unrechable) evitando así demoras en la conexión y mediante DROP no se le contesta nada por lo cual el sistema remoto no corta la conexión hasta que ha transcurrido el tiempo de espera de la contestación con la consiguiente ralentización. Para la red local es aconsejable usar REJECT aunque cada administrador tiene que estudiar su situación.

Por los mismos motivos tenemos que tener cuidado con el protocolo ICMP.

También tenemos la acción LOG que origina un registro de los paquetes que verifican la regla.

En un paso un poco más complicado, también se podría manipular el paquete y cambiarle ciertas características a nuestra conveniencia.

Estas opciones se la vamos a especificar a iptables con la opción "-j".

1.3 Características básicas de un paquete

Las características básicas de un paquete, que van a servir para identificarlo son:

1.3.1 Dirección de origen

Indica quien es el emisor del paquete, de qué ordenador viene. Lo podremos especificar con una dirección IP, un nombre de host o una dirección de red en formato CIDR (192.168.0.0/24) o en notación clasica (192.168.0.0/255.255.255.0). En iptables podemos especificar la dirección origen con la opción "-s". Si en una regla omitimos la dirección origen equivale a poner 0/0 es decir cualquier dirección. Por ejemplo "-s 192.168.0.0/24" indicaría cualquier dirección con origen en la red de clase C (24 bits de red) 192.168.0.0. Si delante de la dirección añadimos "!" entonces hacemos referencia a cualquier dirección salvo la especificada, es decir, que no sea esa dirección.

1.3.2 Dirección de destino

Indica a quien va dirigido el paquete, a qué ordenador via. También lo podremos especificar con una dirección IP, un nombre de host o una dirección de red en formato CIDR (192.168.0.0/24) o en notación clasica (192.168.0.0/255.255.255.0). En iptables podemos especificar la dirección destino con la opción "-d". Si en una regla omitimos la dirección origen equivale a poner 0/0 es decir cualquier dirección. Por ejemplo "-s 192.168.0.0/24" indicaría cualquier dirección con destino a la red de clase C (24 bits de

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

red) 192.168.0.0. Si delante de la dirección añadimos "!" entonces hacemos referencia a cualquier dirección salvo la especificada, es decir, que no sea esa dirección.

1.3.3 Protocolo

Podemos establecer filtros sobre protocolos concretos, será obligatorio si además especificamos algún puerto. La opción para especificar un protocolo es "-p" y los valores posibles son TDP, UDP e ICMP. El signo "!" antes del nombre del protocolo también se utiliza para negar.

1.3.4 Interfaz de entrada

Podemos especificar un dispositivo de entrada de red concreto con la opción "-i". Por ejemplo "-i eth0" indicaría un paquete que proviene de eth0. Se puede usar un "!". Evidentemente no podremos usar un interfaz de entrada con una regla de salida (OUTPUT).

1.3.5 Interfaz de salida

Podemos especificar un dispositivo de salida de red concreto con la opción "-o". Por ejemplo "-o eth0" indicaría un paquete que sale por eth0. Se puede usar un "!". Evidentemente no podremos usar un interfaz de salida con una regla de entrada (INTPUT).

1.3.6 Puerto origen

Mediante la opción "--sport" podemos especificar un puerto o un rango de puertos si los separamos por ":", por ejemplo [1024:65535] indicaría desde 1025 hasta 65535. Los puertos los podemos especificar por su número o también por el nombre asociado en el fichero /etc/services. Es necesario especificar -p TCP o -p UDP para poder especificar un pueerto origen.

1.3.7 Puerto destino

Mediante la opción "--dport" podemos especificar un puerto o un rango de puertos. Las consideraciones son iguales que para el puerto origen.

1.4 Definición de reglas

Para definir una nueva regla sólo tenemos que decirle a iptables si tiene que insertar la nueva regla en alguna posición (-I numero) o bien simplemente añadirla al final (-A) y la descripción de la regla. Vemos algunos ejemplos:

Ejemplo 1:

```
iptables -A INPUT -s 192.168.0.0/24 -d 192.168.5.0 -p tcp --dport 80 -
j ACCEPT
```

Estaría añadiendo (-A) una regla de entrada (INPUT) que indica que todos los paquetes originados en la red 192.168.0.0 (-s 192.168.0.0/24) y dirigidos a la la red 192.168.5.0 (

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

-d 192.168.5.0) y dirigidos al puerto 80 (--dport 80) tienen que dejarse pasar (-j ACCEPT).

Ejemplo 2:

```
iptables -A FORWARD -s 192.168.0.7 -j REJECT
```

Estaría añadiendo (-A) una regla de reenvío (FORWARD) que indica que todo el tráfico proveniente del ordenador 192.168.0.7 (-s 192.168.0.7) se rechaza (-j REJECT). Es decir estamos cortando a este equipo la salida fuera de la red.

Ejemplo 3:

```
iptables -A OUTPUT -o eth0 -j ACCEPT
```

Permitimos culquier salida por la interfaz de red eth0.

Desde aquí suponemos que el lector está familiarizado con los números de puertos y servicios.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

2 Esquemas de filtrado

Es importante saber cual es el circuito exacto que siguen los paquetes en la máquina. Cada paquete que llega a nuestro cortafuegos sigue un determinado camino donde se le aplican una determinadas reglas de filtrado. Si el paquete no ha verificado ninguna de las reglas de aceptar o denegar entonces también deberemos tomar una decisión final con ese paquete.

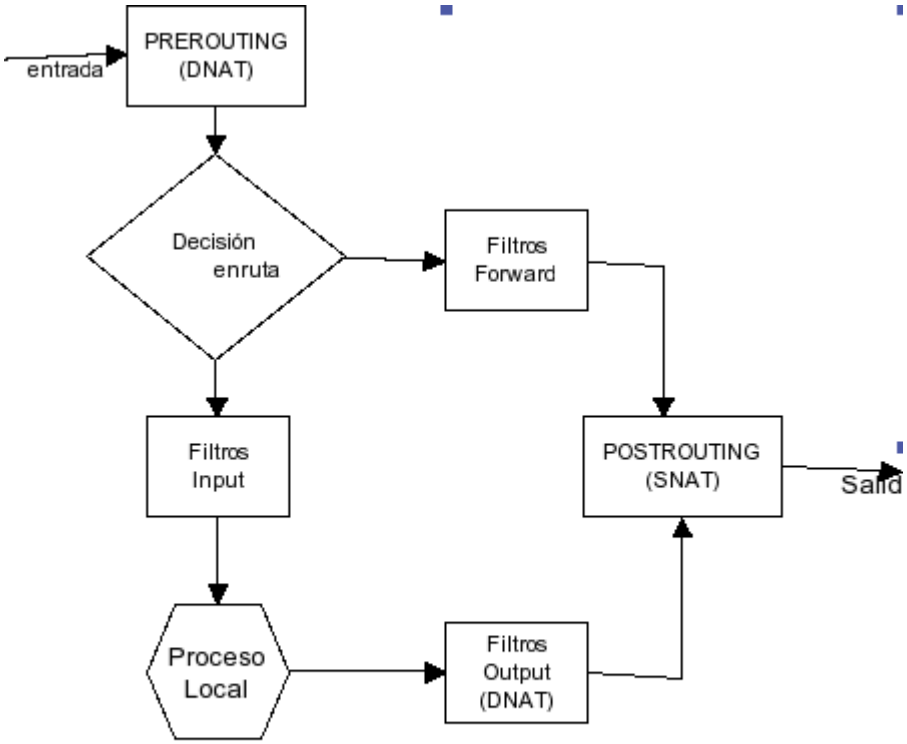

Figura 1. Esquema de filtrado

2.1 Circuito de filtrado.

Cuando un paquete llega a nuestro cortafuegos primero pasa unos filtros.

En primer lugar pasamos al filtro de PREROUTING donde podemos manipular el paquete modificando sus datos de destino, por ejemplo redirigir a otra máquina o a otro puerto. Esto se conoce como DNAT (destination network address translation).

Una vez que el paquete de entrada está preparado se comprueba si va dirigido al propio ordenador en cuyo caso pasa al filtro de entrada (INPUT), o bien si va dirigido a otra máquina, en cuyo caso se dirige al filtro de reenvío (FORWARD).

Si el paquete iba destinado a la máquina local y ha pasado el filtro de entrada se le entrega al proceso local que lo solicitó.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Si un proceso local genera un paquete que tiene que enviar a la red primero pasa por el filtro de salida (OUTPUT). El filtro de salida podría manipular el paquete modificando el destino.

Si el paquete ha pasado el filtro de reenvío (FORWARD) pasaría el filtro de POSTROUTING. Igualmente si el paquete local pasa el filtro de salida también pasa al filtro de POSTROUTING).

En el filtro de POSTROUTING se pueden manipular los datos de origen de un paquete. En esta fase podemos realizar SNAT (source network address translation), es decir, manipular los datos de origen del paquete.

Cada vez que tengamos que configurar un filtro tenemos que tener muy en cuenta este esquema.

2.2 Orden de la reglas

El orden de las reglas de un cortafuegos define su comportamiento. El filtro de va comparando el paquete con cada una de las reglas hasta que se encuentra una que verifica y en ese caso se lleva a cabo lo que indique esa regla (aceptar o denegar); una vez realizada la acción no se comprueban más reglas. Si ponemos reglas muy permisivas entre las primeras del cortafuegos, puede que las siguientes no se apliquen y no sirvan de nada.

2.3 Política predeterminada

También se puede dar el caso de que un paquete no haya verificado ninguno de los filtros una vez que ha los ha comprobado todos. En este caso no sabemos si tenemos que aceptar o rechazar este paquete. Para resolver esta situación iptables dispone de una política predeterminada que permite indicar qué hacer con los paquetes que no hayan verificado ninguna regla. La política predeterminada será algunas de las acciones que hemos definido y se define con la opción "-P".

Por ejemplo:

```
iptables -P INPUT -j ACCEPT
```

Definiría como aceptar la política predeterminada del filtro INPUT.

La política predeterminada define un esquema distinto de cortafuegos. Si la política predeterminada es aceptar entonces tendremos que denegar todo aquello que no nos interese. Si la política predeterminada es denegar entonces entremos que permitir todo aquello que nos interese.

Cada uno de los modelos de cortafuegos tiene sus ventajas e inconvenientes. En el primer caso, con la política predeterminada de aceptar es mucho más fácil la gestión del cortafuegos. En este caso es útil cuando sabemos claramente qué puertos queremos proteger y el resto no importa y se acepta. El problema que plantea es no poder controlar qué tenemos abierto o que en un momento dado se instale un software nuevo,

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

un troyano por ejemplo, que abra un puerto determinado, o que no sepamos que determinados paquetes ICMP son peligrosos. Si la política predeterminada es ACEPTAR y no se protege explícitamente el sistema puede ser inseguro.

Cuando política predeterminada es DENEGAR todo lo que no aceptemos explícitamente será denegado por lo que el sistema puede fallar por despiste o desconocimiento en lo que estamos permitiendo. Es más complicado establecer este tipo de cortafuegos, hay que tener muy claro como funciona el sistema y qué es lo que se tiene que aceptar sin caer en la tentación de intorducir reglas muy perpermisivas. Esta configuración de cortafuegos es la recomendada, aunque no es aconsejable usarla si no se domina mínimamente el sistema.

2.4 Otros criterios de definición de filtros

2.4.1 Registro de paquetes

Se utiliza con el objetivo LOG (-j LOG) y dispone de las siguientes opciones:

--*log-level* nivel (nombre o número de nivel) define el nnivel de registro. Los nombres válidos son (distingue mayúsculas/minúsculas) «debug», «info», «notice», «warning», «err», «crit», «alert», «emerg», que corresponden a los números 7 a 0.

--*log-prefix* cadena Especifica una cadena de hasta 30 caracteres que se escriben la comienzo del registro para identificarlos con posterioridad.

Este módulo se puede asociar con «limit» para evitar que los registros de conexión se hagan excesivamente voluminosos en los ficheros de registro.

2.4.2 Extensiones TCP

Las extensiones TCP se cargan automáticamente si especificamos "-p tcp" y habilitan las algunas opciones de especificación más:

--*tcp-flags* tomo como argumento dos cadenas de indicadores que permiten filtrar según ciertos indicadores de TCP. En primer lugar especificamos la máscara: una lista de los indicadores que desea examinar. En segundo lugar indicamos cuales deben estar activos. "--tcp-flags" puede ir seguido por una «!» opcional Por ejemplo,

```
# iptables -A INPUT --protocol tcp --tcp-flags ALL SYN,ACK -j DENY
```

Esto indica que se deben examinar todos los indicadores («ALL» es sinónimo de «SYN,ACK,FIN,RST,URG,PSH»), pero sólo deben estar activos SYN y ACK. Hay otro argumento llamado «NONE», que significa «ningún indicador».

--*syn* es equivalente a --tcp-flags SYN,RST,ACK SYN. Esta condición la verifican sólo los paquetes que treten de iniciar una conexión con un servidor. Ese indicador permite controlar quien inicia conexión. Puede incluir "!".

--*sport* y --*dport* ya las hemos descrito anteriormente.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

son lo mismo que lo anterior, sólo que especifican el puerto de destino, en lugar del de origen.

2.4.3 Extensiones ICMP

Esta extensión se carga de forma automática si se especifica «-p icmp». Proporciona sólo una opción nueva:

--icmp-type seguida de un «!» opcional, y a continuación el nombre de un tipo icmp (p.ej. «host-unreachable»), un tipo numérico («3»), o un tipo numérico y un código separados por «/» («3/3»). Puede ver una lista de los nombres de los tipos icmp disponibles usando «-p icmp --help».

2.4.4 Otras extensiones de coincidencia (match)

Otras extensiones del paquete netfilter se pueden invocar con la opción «-m».

2.4.5 Extensión mac

Este módulo se debe especificarde forma explícita con «-m mac» o «--match mac». Se usa para coincidencias en las direcciones Ethernet (MAC) de los paquetes entrantes, y por tanto sólo son útiles para los paquetes que pasan por las cadenas PREROUTING e INPUT. Proporciona sólo una opción:

--*mac-source* seguida de un «!» opciona, y luego una dirección ethernet en notación hexadecimal separada por «:», por ejemplo «--mac-source B0:70:99:AD:DC:B4».

2.4.6 limit

Este módulo de debe especificar de forma explícita con «-m limit» o «--match limit». Se usa para restringir la tasa de coincidencias, como por ejemplo para suprimir mensajes de registro. Sólo se activará un número dado de veces por segundo (por defecto, 3 coincidencias por hora, a ráfagas de 5). Tiene dos argumentos opcionales:

--*limit* seguido por un número; especifica el número máximo de coincidencias de media por segundo a permitir. El número puede especificar unidades de forma explícita, usando «/second», «/minute», «/hour», o «/day», o abreviadas (de manera que «5/second» es lo mismo que «5/s»).

--*limit-burst* seguido de un número, indica la ráfaga más larga que se puede producir antes de comprobar el límite.

Este tipo de coincidencias se suele usar con el objetivo LOG para producir registros limitados por una tasa. Para comprender cómo funciona esto, veamos la siguiente regla, que registra los paquetes con los parámetros de limitación por defecto:

```
iptables -A FORWARD -m limit -j LOG
```

La primera vez que se alcanza esta regla, se registra el paquete; en realidad, como la ráfaga por defecto es de 5, se registrarán los primeros cinco paquetes. Después, pasarán

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

veinte minutos antes de que vuelva a registrarse un paquete con esta regla. Además, cada veinte minutos que pasen sin que un paquete alcance la regla, la ráfaga «recuperará» un paquete; si no sucede nada durante 100 minutos, la ráfaga quedará completamente «recargada»; de vuelta entonces a la situación inicial.

Ahora mismo no se pueden crear reglas con un tiempo de recarga mayor a 59 horas, de manera que si establece una tasa de recarga de un paquete por día, entonces el número de paquetes por ráfaga deberá ser menor que 3.

También puede usar este módulo para evitar varios ataques por denegación de servicio (DoS) con una tasa más rápida para incrementar la respuesta.

Protección contra Syn-flood (inundación mediante Syn):

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

Furtivo buscando puertos (port scanner):

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --
limit 1/s -j ACCEPT
```

2.4.7 state

Cuando se combina este módulo con el seguimiento de conexiones, podremos tener acceso al estado de seguimiento de un paquete. Este módulo de debe especificar de forma explícita con «-m state». Este módulo porporciona un opción

--*state state*, donde indicamos una lista de estados de conexión separada por comas. Los valores posibles para el esado «INVALID» lo que significa que el paquete no se puede identifcar por alguna razón, como por ejemplo falta de memoria o errores ICMP que no corresponden a ninguna conexión conocida. Otro posible estado es «ESTABLISHED» que se asocia con una conexión que ya ha tenido tráfico en ambas direcciones.. El estado «NEW» significa que el paquete inicia una nueva conexión o asociado con una conexión que aun no ha tenido paquetes en ambas direcciones. Por último «RELATED» indica que el paquete comienza una nueva conexión, pero está asociado con una conexión previa existente, por ejemplo una transferenia FTP o un error ICMP.

2.4.8 owner

El módulo owner se utiliza para fitrar según el propietario del paquete, del propietario del proceso que origina el paquete y sólo tiene sentido para los paquetes generados forma local y sólo es válido para la cadena OUTPUT. Cuando activamos este módulo disponemos de las siguientes opciones:

--*uid-owner* idusuario que se verifica cuando el proceso que originó el paquete es proiedad del usuario con el UID indicado.

iptables -A OUTPUT -m owner -uid-owner 203 -j ACCEPT

--*uid-owner* idgrupo es equivalente a la anterior opción pero con grupos.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

--*pid-owner* idproceso Permite especificar el PID del proceso que origina el paquete.

--*sid-owner* idproceso Permite espcificar el GID del proceso que genera el paquete.

2.5 Módulos de iptables

Iptables necesita tener en el núcleo diversos módulos para, qur en primer lugar funciones iptables y en segundo lugar para añadir nuevas funcionalidades, como por ejemplo las que veíamos en el punto anterior. Para comprobar los módulos que tenemos activos en el núcleo podemos ejecutar lsmod y entre otras cosas aparece:

```
ipt_multiport           1176   0  (autoclean)
ipt_conntrack           1688   0  (autoclean)
iptable_mangle          2776   0  (autoclean) (unused)
ipt_MASQUERADE          2200   2  (autoclean)
iptable_nat            21848   1  (autoclean) [ipt_MASQUERADE]
ip_conntrack           28552   2  (autoclean) [ipt_conntrack
ipt_MASQUERADE iptable_nat]
ipt_REJECT              4248   1  (autoclean)
ipt_LOG                 4248   2  (autoclean)
iptable_filter          2444   1  (autoclean)
ip_tables              15136  10  [ipt_multiport ipt_conntrack
iptable_mangle ipt_MASQUERADE iptable_nat ipt_REJECT ipt_LOG
iptable_filter]
```

En el directorio /lib/modules/version/kernel/net/ipv4/netfilter podremos encontrar todos los módulos necesarios.

Si algún módulo necesario no se carga automáticamente tendremos que hacerlo explícitamente.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

3 Manipulación de filtros

Resulta evidente que de alguna forma tendermos que namipular los filtros y cadenas que utiliza iptables. La manipulación se basará en instrucciones como añadir o insertar una regla, que ya hemos visto al definir una regla, borrar una regla, borrar todas las reglas de una cadena, crear y borrar una cadena de usuario, etc

3.1 Gestión de filtros y cadenas

3.1.1 Mostrar las reglas activas de una cadena

Para mostrar las reglas de una cadena ejecutaermos ipatables con la opción -L. Por ejemplo para mostar todas las reglas de la cadena INPUT podríamos:

```
iptables -L input
```

Para ver todas las reglas NAT pondríamos

```
iptables -t nat -L
```

Iptables va a tratar de resolver los nombres de las direcciones IP resultantes. Si esto demora el proceso podemos ejecutarlo con la opción "-n" para que diectamente muestre los números:

```
iptables -L input -n
```

3.1.2 Vaciar una cadena

Cuando queremos reiniciar una cadena para añadir reglas nuevas tenemos qeu borrar todas las reglas que tiene definidas. para hacerlo tenemos que usar la opción "-F". Si ponemos

```
iptables -F FORWARD
```

eliminaría toda las reglas de FORWARD definidas.

3.1.3 Borrar una regla de una cadena

Cuando tengamos que borrar una cadena tenemos que usar la opción "-D" de iptables. Esta opción la podemos uar de dos formas,

```
iptables -D  INPUT numero
```

y eliminaríamos de la cadena INPUT la regla que ocupa la opsición especificada.

También podemos poner

iptables -D descripcion de la cadena

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

y borrarría la cadena que verificara de forma exacta esa descripción.

3.2 Cadenas de usuario

iptables permite definir cadenas propias de usuario para facilitar la gestión. Una cadena de usuario es un conjunto de reglas asociadas una acción definida por el usuario.

3.2.1 Crear una cadena de usuario

Con la opción "-N" de iptables un usuario puede definir una cadena propia a la cual asociarle posteriormente un conjunto de reglas de la misma forma que se hace con las cadenas predefinidas.

En el siguiente ejemplo vamos a definir una cadena llamada TLT que se va a ejecutar, con todas sus reglas cada vez que llegue un paquete dirigido al puerto 23.

```
iptables -N TLT

iptables -A TLT -s 192.168.1.0/24 -p tcp --dport 23  -j ACCEPT
iptables -A TLT -s 192.168.0.37 -p tcp --dport 23  -j ACCEPT
iptables -A TLT -s 192.168.0.0/24 -p tcp --dport 23  -j REJECT

iptables -A INPUT -p tcp --dport 23 -j TLT
```

La última línea indica que si un paquete llega para el puerto 23 tiene que pasar todas las reglas correspondientes a TLT.

3.2.2 Borrar una cadena de usuario

Una cadena de usuario se elimina con la opción "-X". Para poder borrar la cadena tiene que estar vacía de reglas. Si quisiéramos borrar una cadena llamada TLT tendríamos que hacer:

iptables -F TLT

iptables -X TLT

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

4 Seguimiento de conexiones

4.1 Qué es el seguimiento de conexiones

Ya hemos visto que mediante el módulo state (-m state) podemos tomar decisiones a partir del estado del paquete. A continuación podemos ver qué partido podemos sacar de esta posiblidad. Alguna muestra ya se ha incluido en los ejemplos anteriores.

El seguimiento de la conexión se refiere a la posiblidad demantener información sobre el estado de la conexión en memoria. Se guarda información del tipo direcciones ip origen o destino junto a su puertos correspondientes, protocolos, estado de la conexión, etc. Esta posibilidad agrega una interesantes posibilidaades a al configuración de un cortafuegos.

El seguimiento de conexiones se realiza en las cadenas PREROUTING u OUTPUT.

El número máximo de conexiones se guarda en /proc/sys/net/ipv4/ip_conntrack_max y su valor predefinido dependerá del tamaño de la memoria.

Es necesario tener instalado el módulo ip_conntrack.

4.2 Realizar seguimiento

El esquema de seguimiento se realiza en el siguiente orden: Primero si el paquete forma parte de alguna conexión existente (ESTABLISHED). Si es tráfico icmp, puede estar relacionado (RELATED) a otra conexión udp/tcp existente. El paquete puede estar inicianod una nueva (NEW) conexión o puede no tener relación con ninguna conexión en cuyo caso se considera inválido (INVALID).

4.2.1 UDP

Udp es un protocolo no orientado a conexión, no obstante se puede realizar un seguimiento. Por ejemplo, si tenemos qu cortafuegos con una política predeternidada de denegar podemos abrir las conexiones clientes udp con:

```
iptables -A INPUT     -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
```

4.2.2 TCP

Tcp es una comunicación orientada a conexión que se inicia con el intercambio de paquetes SYN y ACK (que figuran en las cabeceras de los paquetes). Por ejemplo, si tenemos qu cortafuegos con una política predeternidada de denegar podemos abrir las conexiones clientes tdp con:

```
iptables -A INPUT     -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

4.2.3 icmp

En el mismo caso anterior tendremos, para icmp:

```
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT     -p icmp -m state --state ESTABLISHED,RELATED  -j
ACCEPT
```

4.2.4 Conexión ftp

Para activar un conexión FTP podríamos poner:

```
iptables -A INPUT     -p icmp -m state --state ESTABLISHED,RELATED  -j
ACCEPT
iptables -A INPUT     -p tcp --sport 21 -m state --state ESTABLISHED -
j ACCEPT
iptables -A OUTPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED
-j ACCEPT
```

En el caso de ftp activo el cliente envía un número de puerto alto al servidor FTP y el servidor devuelvel a conexión desde el puerto 20 a este puerto para comenzar a enviar datos. Obsevamos que esta segunda conexión va en sentido contrario, el servidor inicia una conexión con el cliente. Para permitir una conexión ftp activa pondremos:

```
iptables -A INPUT -p tcp --sport 20 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p tcp --dport 20 -m state --state ESTABLISHED -j
ACCEPT
```

En el caso de ftp pasivo el cliente también envía un número de puerto al servidor, pero ahora es el cliente el que inicia la conexión con el servidor:

```
iptables -A INPUT -p tcp --sport 1024: --dport 1024: -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 1024: --dport 1024:  -m state --
state ESTABLISHED,RELATED -j ACCEPT
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

5 Cortafuegos básicos

A continucación vemos unos ejemplos de cortafuegos básicos. No son cortafuegos hechos para cortar y pegar, la idea es proponer diversos ejemplos para que puedas sacar tus propias conclusiones y establecer el cortafuegos de acuerdo con sus propios intereses. Cada cortafuegos debería adaptarse a unas necesidades concretas.

5.1 Proteger la propia máquina I

El primer ejemplo define un ejemplo de cortafuegos para una máquina individual:

```
## Vaciamos las reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos politicas predeterminada
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD ACCEPT
 iptables -t nat -P PREROUTING ACCEPT
 iptables -t nat -P POSTROUTING ACCEPT

# Aceptamos todo de localhost
 /sbin/iptables -A INPUT -i lo -j ACCEPT

# A nuestra IP le dejamos todo
 iptables -A INPUT -s 192.168.0.1 -j ACCEPT

# Permitimos una conexión a ssh y telnet (22 y 23) desde un equipo
 iptables -A INPUT -s 192.168.0.37 -p tcp --dport 22:23 -j ACCEPT

# A otro le permitimos acceso FTP
 iptables -A INPUT -s 192.168.0.45 -p tcp -dport 20:21 -j ACCEPT

# El puerto 80 (www) abierto, para un servidor web.
 iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# Y el resto, lo cerramos
 iptables -A INPUT -p tcp --dport 20:21 -j DROP
 iptables -A INPUT -p tcp --dport 22:23 -j DROP
 iptables -A INPUT -p tcp --dport 6001 -j DROP
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Proteger la propia máquina II

```
## Vaciamos las reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos politica predeterminadas
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD ACCEPT
 iptables -t nat -P PREROUTING ACCEPT
 iptables -t nat -P POSTROUTING ACCEPT

## creamos una nueva cadena
 iptables -N filtro

## definimos las reglas dela nueva cadena
 iptables -A filtro -m state --state ESTABLISHED,RELATED -j ACCEPT
 iptables -A filtro -m state --state NEW -i ! eth0 -j ACCEPT
 iptables -A filtro -j DROP

# Aceptamos conexiones internas
 /sbin/iptables -A INPUT -i lo -j ACCEPT

## Ir a la cadena filtro desde las cadenas INPUT y FORWARD.
 iptables -A INPUT -j block
 iptables -A FORWARD -j block
```

Proteger la propia máquina III

```
## Vaciamos las reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos politica predeterminadas
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD ACCEPT
 iptables -t nat -P PREROUTING ACCEPT
 iptables -t nat -P POSTROUTING ACCEPT

# Aceptamos todo de localhost
 /sbin/iptables -A INPUT -i lo -j ACCEPT

# A nuestra IP le dejamos todo
 iptables -A INPUT -s 192.168.0.1 -j ACCEPT

# Permitimos una conexión a telnet y ssh (puerto 22 y 23) desde un
equipo
 iptables -A INPUT -s 192.168.0.37 -p tcp --dport 22:23 -j ACCEPT

# A otro le permitimos acceso FTP
 iptables -A INPUT -s 192.168.0.45 -p tcp -dport 20:21 -j ACCEPT

# El puerto 80 (www) debe estar abierto, ya  que es un servidor web.
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

```
 iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# Cerramos rango de los puertos privilegiados. Cuidado con este tipo
de
# barreras, antes hay que abrir a los que si tienen acceso.
 iptables -A INPUT -p tcp --dport 1:1024 -j DROP
 iptables -A INPUT -p udp --dport 1:1024 -j DROP

# impedimos iniciar conexión en los puertos altos
# (puede que ftp no funcione)
 iptables -A INPUT -p tcp --syn --dport 1025:65535 -j DROP

# Cerramos otros puertos que estan abiertos
 iptables -A INPUT -p tcp --dport 3306 -j DROP
 iptables -A INPUT -p tcp --dport 10000 -j DROP
```

Red local con salida a internet

Una red local con salida a a internet necesita una regla que haga NAT hacia fuera (enmascaramiento en iptables).

```
# Activamos el reenvío para que FORWARD funcione
 echo 1 > /proc/sys/net/ipv4/ip_forward

## FLUSH de reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos politica por defecto
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD ACCEPT
 iptables -t nat -P PREROUTING ACCEPT
 iptables -t nat -P POSTROUTING ACCEPT

 ## Nota: eth0 es el interfaz conectado a internet y eth1 a la LAN
 # acceso localhost
 /sbin/iptables -A INPUT -i lo -j ACCEPT

# Al firewall tenemos acceso desde las redes locales
 iptables -A INPUT -s 192.168.0.0/24 -i eth1 -j ACCEPT

# Ahora hacemos enmascaramiento de la red local
 iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j
MASQUERADE

# Cerramos el rango de puerto bien conocido
 iptables -A INPUT -s 0/0 -p tcp -dport 1:1024 -j DROP
 iptables -A INPUT -s 0/0 -p udp -dport 1:1024 -j DROP

# Cerramos un puerto de gestión: webmin
 iptables -A INPUT -s 0/0 -p tcp -dport 10000 -j DROP
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Dos redes locales con salida a internet

Ahora tenemos dos redes locales y una salida a a internet. Ahora necesitamos dos reglas que hagan NAT hacia fuera (enmascaramiento en iptables) y además las reglas de enrutado entre redes.

```
# Activamos el reenvío para que FORWARD funcione
 echo 1 > /proc/sys/net/ipv4/ip_forward

## FLUSH de reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos politica por defecto
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD ACCEPT
 iptables -t nat -P PREROUTING ACCEPT
 iptables -t nat -P POSTROUTING ACCEPT

 ## Nota: eth0 es el interfaz conectado a internet y eth1 a la LAN
 # acceso localhost
 /sbin/iptables -A INPUT -i lo -j ACCEPT

# Al firewall tenemos acceso desde las redes locales
 iptables -A INPUT -s 192.168.0.0/24 -i eth1 -j ACCEPT
 iptables -A INPUT -s 192.168.1.0/24 -i eth2 -j ACCEPT

# Ahora hacemos enmascaramiento de las redes locales
 iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j
MASQUERADE
 iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j
MASQUERADE

# Abrimos el puerto del servidor web
 iptables -A INPUT -s 0/0 -p tcp -dport 80 -j ACCEPT

# Abrimos el puerto del servidor DNS
 iptables -A INPUT -s 0/0 -p tcp -dport 53 -j ACCEPT
 iptables -A INPUT -s 0/0 -p udp -dport 53 -j ACCEPT

# Cerramos el rango de puerto bien conocido
 iptables -A INPUT -s 0/0 -p tcp -dport 1:1024 -j DROP
 iptables -A INPUT -s 0/0 -p udp -dport 1:1024 -j DROP

# Cerramos un puerto de gestión: webmin
 iptables -A INPUT -s 0/0 -p tcp -dport 10000 -j DROP

# configuramos el tráfico entre redes
# permitimos el tráfico para el puerto 445
 iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -p tcp -dport
445 -j ACCEPT
 iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -p tcp -dport
445 -j ACCEPT

# denegamos el resto del tráfico
 iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -j REJECT
 iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -j REJECT
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

5.1.1 Cortafuegos con política FORWARD predeterminada DROP

Esta es la forma aconsejada para configurar un cortafuegos si queremos poner énfasis en la seguridad.

```
## Vaciado de reglas
 iptables -F
 iptables -X
 iptables -Z
 iptables -t nat -F

## Establecemos politica predeterminada: DROP
 iptables -P INPUT ACCEPT
 iptables -P OUTPUT ACCEPT
 iptables -P FORWARD DROP


## Acceso desde la red
## Servidores WEB
 # Acceso a puertos 80
 iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 80 -j ACCEPT

 # Acceso a puertos 20 y 21 para ftp
 iptables -A FORWARD -p tcp --dport 20:21 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 20:21 -j ACCEPT

 # Acceso a DNS
 iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 53 -j ACCEPT
 iptables -A FORWARD -p udp --dport 53 -j ACCEPT
 iptables -A FORWARD -p udp --sport 53 -j ACCEPT

## correo electrónico
 # Acceso a puerto 25, 110 y 143
 iptables -A FORWARD -p tcp --dport 25 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 25 -j ACCEPT

 iptables -A FORWARD -p tcp --dport 110 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 110 -j ACCEPT

 iptables -A FORWARD -p tcp --dport 143 -j ACCEPT
 iptables -A FORWARD -p tcp --sport 143 -j ACCEPT
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

5.1.2 Cortafuegos con política predeterminada DROP

```
## Vaciamos las reglas
 iptables -F
 iptables -X
 iptables -t nat -F

## Establecemos predeterminada
 iptables -P INPUT DROP
 iptables -P OUTPUT DROP
 iptables -P FORWARD DROP

# permitimos el tráfico loopback
 iptables -A INPUT -i lo -j ACCEPT
 iptables -A OUTPUT -o lo -j ACCEPT

# Configuramos el acceso a nuestra IP
 iptables -A INPUT -s 192.168.0.0/24 -j ACCEPT
 iptables -A INPUT -s 0/0 -p tcp --sport 1:1024 -j ACCEPT
 iptables -A INPUT -s 0/0 -p tcp --dport 1025:65535 ! --syn -j ACCEPT
 iptables -A INPUT -s 0/0 -p udp --sport 1:1024 -j ACCEPT
 iptables -A OUTPUT -d 192.168.0.0/24 -j ACCEPT
 iptables -A OUTPUT -d 0/0  -p tcp --sport 1025:65535 -j ACCEPT

 iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
 iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT

 iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
 iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
 iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT

# El cortafuegos es también un servidor web
 iptables -A INPUT -p tcp --dport 80 -j ACCEPT
 iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

# El cortafuegos es también un servidor smtp
 iptables -A INPUT -p tcp --dport 25 -j ACCEPT
 iptables -A OUTPUT -p tcp --sport 25 -j ACCEPT
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

6 Manipulación de paquetes

Ya hemos visto algo sobre manipulación de paquetes cuando en el ejemplo de cortafuegos incluíamos una regla para enmascarar los paquetes de la red local hacia internet. En ese caso, cada paquete procedente de la red local se modifica para sustituir su IP privada por la IP pública del gateway de forma que el paquete ya sea válido para internet.

El enmascaramiento es sólo un pequeño ejemplo de todo lo que se puede hacer y forma parte de lo que hemos denominado NAT (network address translation), aunque son posibles otras formas de manipulación.

La manipulación se podrá hacer en las cadenas PREROUTING, POSTROUTING y OUTPUT.

En el caso de PREROUTING podremos modifcar los datos destino de la conexión según nos interese y antes de tomar la deción de enrutamiento. Así podremos desviar paquetes que vayan destinados al host local hacia otro host y viceversa. Sólo tiene sentido en el interfaz de entrada. Esto lo vamos a llamar DNAT (destination NAT)..

El mismo caso se puede aplicar a la cadena OUTPUT y podermos modificar llos datos de destino de los paquetes paquetes que salen de un proceso local. En este caso sólo es aplicable en el interfaz de salida.

Cuando utilizamos la cadena POSTROUTING podremos modificar los paquetes justo antes de devolverlos a la red. Podremos modificar los datos de origen, porque el destino ya se ha decidido en una de las cadenas previas FOWRARD o OUTPUT. Como hemos visto anteriormente, este es el caso de MASQUERADE. Sólo tiene sentido en el interfaz de salida. Esto lo vamos a denominar SNAT (source NAT).

6.1 Cambios de destino (DNAT)

Los cambios de destino corresponden a cadena PREROUTING cuando entra el paquete para que estas modificaciones ya se pueda aplicar al decidir si el paquete se eenvía o va dirigido el sistema local. Sólo, como ya hemos visto anteriormente, se puede utilizar la opción «-i» (interfaz de entrada).

Si el paquete tiene origen local el cambio de destino tendremos que hacerlo en la cadena OUTPUT.

En pimer lugar, para el cambio de destino tenemos que usar la opción «-j DNAT», y los argumentos que dispone esta opción, «--to» para especificar una dirección y un puerto opcional. Podremos también especificar rangos de direcciones.

Vemos algunos ejemplos:

```
## Cambiar la dirección de destino por 192.168.0.254
iptables -t nat -A PREROUTING -i eth1 -j DNAT --to 192.168.0.254
```

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

```
## Cambia la dirección de destino por 192.168.0.11 ,192.168.0.12 o
192.168.0.13
 iptables -t nat -A PREROUTING -i eth1 -j DNAT --to 192.168.0.11-
192.168.0.13
```

6.1.1 Configuración de un proxy

Suponemos que tenemos un proxy en la dirección 192.168.0.1 y el puerto 3128 para las conexiones a servidores web de internet: Con la siguiente regla en el gateway redirigiremos todas las peticiones que se realicen hacia un servidor web (puerto 80) hacia el puerto 3128 de la máquina 192.168.0.1:

```
## Cambia la dirección de destino del tráfico web por 192.168.0.1 en
el puerto 3128
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to
192.168.0.1:3128
```

6.1.2 Servidor web con proxy

Ahora suponemos que tenemos un servidor web, pero que para acelerar las conexiones todas las peticiones que se hagan las va a resolver el proxy que está en el mismo equipo pero en el puerto 3128.

Envía el tráfico que entra dirigido al puerto 80 (web) al proxy squid (transparente)

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128

6.1.3 Poner un servidor web en una IP privada

Suponemos que tenemos una red con un gateway con la única dirección IP pública y nos interesa tener un servidor web en el interior de la red local, en el equipo 192.168.0.78. Entonces tendremos que poner:

Envía el tráfico que entra dirigido al puerto 80 (web) al servidor web local (transparente)

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to 192.168.0.78

6.2 Cambio de Origen

Los cambios de destino corresponden a cadena POSTROUTING, justo antes de que el paquete sea enviado y para que estas modificaciones no se vean afectadas por la cadena FORWARD, en su caso. Este es un detalle importante, ya que significa que cualquier otro servicio de la máquina Linux (encaminamiento, filtrado de paquetes) verá el paquete sin cambiar. Sólo podremos usar «-o» (interfaz de salida).

En pimer lugar, para el cambio de destino tenemos que usar la opción «-j SNAT», y los argumentos que dispone esta opción, «--to» para especificar una dirección y un puerto opcional. Podremos también especificar rangos de direcciones.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es
C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

```
## Cambiar la dirección de origen por 192.168.0.4
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.4

## Cambiar la dirección de origen a 192.168.0.4, 192.168.0.5 ó
192.168.0.6
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.4-
192.168.0.6

## Cambiar la dirección de origen por 192.168.0.4, puertos 1-1023
iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to
192.168.0.4:1-1023
```

6.2.1 Enmascaramiento

El caso más utilizado de SNAT el el que denominamos «enmascaramiento» (masquerading), que se utiliza para ocultar las direcciones privadas de una red local en el acceso a internet.

No es necesario escribir la dirección de origen de forma explícita con el enmascaramiento:

```
## Enmascarar todo lo que salga por eth0 proveniente de la red local.
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```