1. **Iptables**

*iptables* es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema *ipchains*, un firewall de iptables no es como un servidor que iniciamos o detenemos o que se pueda caer por un error de programación. iptables está integrado en el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ello se ejecuta el comando iptables, con el que añadimos, borramos o creamos reglas.

* 1. ***Tablas y cadenas***

Utiliza las siguientes tablas:

* **Filter**: tabla utilizada para efectuar el filtrado de paquetes. Es la tabla por defecto.
* **Nat**: tabla utilizada para modificar la cabecera de los paquetes. La vamos a utilizar para hacer la redirección de paquetes.
* **Mangle**: Para alterar el estado de un paquete.

Cada una de estas tablas tiene un grupo de cadenas internas o de cortafuegos que son conjuntos de reglas utilizadas para comprobar si el paquete cumple alguna de ellas. Las cadenas determinan las acciones que ejecutará el filtro de red sobre el paquete. El orden en que se escriben estas reglas es muy importante.

Si el paquete no cumple la primera regla pasa a la siguiente. Si la cumple, la regla decide qué se hace con el paquete recibido, y si no la cumple pasa a la siguiente. Así sucesivamente, hasta que se llega a la última regla, que es la que se aplica por defecto.

En función del tipo de tabla o lista de reglas utilizadas las cadenas internas son las siguientes:

* Para la tabla **Filter:**
* **INPUT**: filtra paquetes dirigidos al firewall.
* **OUTPUT**: filtra paquetes enviados desde el propio firewall.
* **FORWARD**(reenviar): filtra paquetes recibidos por el firewall cuyo destinatario final no es él.
* Para la tabla **Nat:**
* **PREROUTING**(preenrutar) Cadena que modifica recibidos por el firewall.
* **OUTPUT**: cadena que modifica paquetes generados en la propio firewall antes de que sean dirigidos a través de un dispositivo de red.
* **POSTROUTING**(postenrutar): cadena que modifica paquetes antes de que sean enviados a través de un dispositivo de red.
  1. ***Acciones***

Las acciones de IPTABLES son las siguientes:

* **ACCEPT**(aceptar): el paquete que coincida con el objetivo accept se salta el resto de las reglas y continúa el camino hacia su destino. Se permite el paso del paquete a través del cortafuegos.
* **DROP**(eliminar) : al paquete que coincida con el objetivo drop se le niega el acceso al sistema y no se envía nada a la máquina origen del paquete.
* **REJECT**(rechazar): rechaza el paquete que coincide con el objetivo y se envía un mensaje a la máquina origen del paquete.
* **MASQUERADE**(enmascarar): Se utiliza con la tabla NAT para convertir la IP privada en pública.
* **REDIRECT**(redirigir): redirecciona un paquete . Se utiliza con la tabla NAT.
  1. ***Sintaxis***

La sintaxis de la orden IPTABLES es la siguiente:

**iptables [- t <nombre de tabla>] <comando> <nombre\_cadena> <parámetro1>/opción1 … <parámetron>/<opción>**

Donde:

**-t <nombre de tabla>**

Especifica la tabla a utilizar. Por defecto es Filter.

**<comando>**

Permite añadir o eliminar una regla dada en <nombre de cadena>

**<parámetro1>/<opcion1>**

Indica el objetivo, es decir, qué se hará cuando un paquete coincida con la regla.

**<comando> <nombre\_cadena>**

Los comandos van siempre en mayúsculas y solo puede haber un comando para cada <nombre de cadena>

* + 1. ***Comandos***

**-P** Política. Determina cuál será la política por defecto para una cadena concreta.

**iptables –P INPUT DROP**

**-F** Vaciar. Dada una cadena, con -F se eliminan las reglas de dicha cadena. Si no se indica ninguna cadena, se elimina cada regla de cada cadena.

**iptables –F OUTPUT**

**-Z** Pone ceros en los contadores de byte y de paquete en todas las cadenas de una tabla en particular.

**-A** Añadir. Dada una cadena, con –A se añade una nueva regla al final de dicha cadena.

**iptables –A INPUT –i lo –j ACCEPT**

**-D** Borrar. Borra una regla de una cadena.

**iptables –D INPUT –dport 80 –j DENY**

**-L** Listar. Lista, para la cadena dada, las reglas introducidas o vigentes en el cortafuegos.

**iptables –t filter –L INPUT**

* + 1. ***Parámetros***

**-j** Saltar. Indica al paquete qué objetivo debe ejecutar (ACCEPT, DROP, DENY, REJECT…)

**-s** Origen. Indica la IP de la máquina origen de un paquete sobre el que se evalúa la regla. Para una red se indica la máscara IP/Máscara

**-d** Destino. Indica la IP de la máquina destino de un paquete sobre el que se evalúa la regla.

**-i** Entrada. Indica la interfaz de entrada sobre la que se evalúa la regla. Se utiliza con las cadenas INPUT y FORWARD para la tabla Filter y con la cadena PREROUTING para la tabla Nat.

**-o** Salida. Igual que –i. Se utiliza con OUTPUT y FORWARD en Filter y POSTROUTING en Nat.

**-p** Protocolo. Indica el protocolo IP del paquete. Puede ser icmp, tcp o udp. La opción por defecto es all(todos los protocolos). Cada tipo de protocolo tiene sus propios modificadores.

* + 1. ***Opciones de identificación de paquetes***

Los diferentes protocolos de red proporcionan opciones especializadas de concordancia que pueden ser configurados de forma específica para identificar un paquete en particular usando dicho protocolo.

**Protocolo TCP**

Estas opciones de identificación están disponibles en el protocolo TCP (opción ***-p tcp***):

**--dport / --destination-port**

Puerto de destino del paquete. Puede utilizar o bien un nombre de servicio de red (como www o smtp), un número de puerto, o bien un rango de números de puertos para configurar esta opción. Para ver los nombres o alias de los servicios de red y los números de puertos que usan, se puede mirar el fichero /etc/services.

Para especificar un rango de números de puertos hay que separar los dos números de puertos con dos puntos (:), como en -p tcp --dport 3000:3200. El rango válido más grande es 0:65535.

También se puede usar el carácter de punto de exclamación (!) como flag tras la opción --dport para decirle a iptables que seleccione los paquetes que no usen ese servicio o puerto.

**--sport / --source-port**

Puerto de origen del paquete, usando las mismas opciones que --dport. También puede usar --source-port para especificar esta opción.

**--syn**

Provoca que todos los paquetes designados de TCP, comúnmente llamados paquetes SYN, cumplan esta regla. Cualquier paquete que esté llevando un payload de datos no será tocado. Si se sitúa un punto de exclamación (!) como flag tras la opción --syn se provoca que todos los paquetes no-SYN sean seleccionados.

**--tcp-flags**

Permite que los paquetes TCP con conjuntos de bits específicos, o flags, sean seleccionados para una regla. La opción de selección --tcp-flags acepta dos parámetros, que son los flags para los diferentes bits ordenados en una lista separada por comas. El primer parámetro es la máscara, que configura los flags que serán examinados en el paquete. El segundo parámetro se refiere a los flags que se deben configurar en el paquete para ser seleccionado. Los flags posibles son ACK, FIN, PSH, RST, SYN, y URG. Adicionalmente, se pueden usar ALL y NONE para seleccionar todos los flags o ninguno de ellos.

Por ejemplo, una regla iptables que contiene *-p tcp --tcp-flags ACK,FIN,SYN SYN* tan sólo seleccionará los paquetes TCP que tengan el flag SYN activo y los flags ACK y FIN sin activar.

Como en otras opciones, al usar el punto de exclamación (!) tras --tcp-flags invierte el efecto de la opción, de tal forma que los flags del parámetro no tendrán que estar presentes para poder ser seleccionados.

**Protocolo UDP**

Estas opciones de selección están disponibles para el protocolo UDP ***(-p udp***):

**--dport**

Especifica el puerto destino del paquete UDP usando el nombre del servicio, el número del puerto, o un rango de puertos. La opción de selección de paquetes --destination-port se puede utilizar en lugar de --dport.

**--sport**

Especifica el puerto origen del paquete UDPm usando el nombre del servicio número de puerto, o rango de puertos. La opción --source-port puede ser usada en lugar de --sport.

**Protocolo ICMP**

Los paquetes que usan el protocolo de control de mensajes de internet (Internet Control Message Protocol, ICMP) pueden ser seleccionados usando la siguiente opción cuando se especifique ***-p icmp***:

**--icmp-type**

Selecciona el nombre o el número del tipo ICMP que concuerde con la regla. Se puede obtener una lista de nombres válidos ICMP tecleando el comando iptables -p icmp -h.

**Módulos con opciones de selección adicionales**

Las opciones de selección adicionales, que no son específicas de ningún protocolo en particular están también disponibles a través de módulos que se cargan cuando el comando iptables los necesite. Para usar una de estas opciones, se deberá cargar el módulo por su nombre incluyendo *-m <nombre-módulo>* en el comando iptables que crea la regla.

Un gran número de módulos, cada uno de ellos con sus diferentes opciones de selección de paquetes, están disponibles por defecto. También es posible crear sus propios módulos que proporcionen funcionalidades de selección adicionales, puede que para requisitos específicos de su red. Existen muchos módulos, pero tan sólo los más populares serán vistos aquí.

El módulo **state**, que utiliza la opción --state, puede seleccionar un paquete con los siguientes estados de conexión particulares:

* *ESTABLISHED* El paquete seleccionado se asocia con otros paquetes en una conexión establecida.
* *INVALID* El paquete seleccionado no puede ser asociado a una conexión conocida.
* *NEW* El paquete seleccionado o bien está creando una nueva conexión o bien forma parte de una conexión de dos caminos que antes no había sido vista.
* *RELATED* El paquete seleccionado está iniciando una nueva conexión en algún punto de la conexión existente.

Estos estados de conexión se pueden utilizar en combinación con otros separándolos mediante comas como en *-m state --state INVALID,NEW*.

Para seleccionar una dirección MAC hardware de un dispositivo Ethernet en particular utilice el módulo **mac**, que acepta *--mac-source* con una dirección MAC como opción. Para excluir una dirección MAC de una regla, ponga un punto de exclamación (!) tras la opción --mac-source.

* 1. ***Esquemas de filtrado***

Es importante saber cuál es el circuito exacto que siguen los paquetes en la máquina. Cada paquete que llega a nuestro cortafuegos sigue un determinado camino en el que 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.



Cuando un paquete llega al firewall, en primer lugar, pasa por la cadena **PREROUTING,** donde podemos manipular el paquete modificando sus datos de destino, y así redirigirlo a otra máquina o a otro puerto. Esto se conoce como DNAT (Destination Network Address Translation).

Una vez dejada atrás la cadena PREROUTING, se comprueba si el paquete va dirigido al propio firewall -en cuyo caso pasa al filtro de entrada (**INPUT**)-, o bien si va dirigido a otra máquina (porque se ha hecho un cambio en PREROUTING) -en cuyo caso se dirige al filtro de reenvío (**FORWARD**)-.

Si el paquete iba destinado al propio firewall y ha pasado el filtro de entrada, se procesará localmente.

Si un proceso local genera un paquete que tiene que enviar a otro equipo (sea de la red local o no), pasará primero por el filtro de salida (**OUTPUT**).

Si el paquete ha pasado el filtro de reenvío (FORWARD), pasaría al 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; esto es conocido comúnmente como SNAT (Source Network Address Translation).

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

El orden de las reglas de un cortafuegos define su comportamiento. En la cadena, se va comparando el paquete con cada una de las reglas hasta que se encuentra una que se cumple; en ese caso, se lleva a cabo la acción que indique esa regla; 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.

También se puede dar el caso de que un paquete no haya cumplido ninguna de las reglas de una cadena. Para resolver esta situación se dispone de una política por defecto que permite indicar qué hacer con los paquetes que no hayan cumplido ninguna regla. La política por defecto se define mediante la opción "-P".

Por ejemplo:

|  |
| --- |
| **iptables -P INPUT -j ACCEPT** |

Esta línea definiría como ACEPTAR la política predeterminada de la cadena 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.

Con la política predeterminada establecida como ACEPTAR, es mucho más fácil la gestión del cortafuegos. Es útil cuando sabemos claramente qué puertos queremos proteger y el resto no nos importa. Es fácil y cómodo de implementar. Sin embargo, es peligroso dejar el tráfico aceptado por defecto. ¿Qué ocurrirá si recibimos un ataque nuevo que explota un puerto que no habíamos cerrado expresamente porque en su momento no era vulnerable?

Cuando la 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, ya que hay que tener muy claro cómo funciona el sistema y qué es lo que se tiene que aceptar. Esta configuración de cortafuegos es la recomendada de cara a asegurar una red local.

* 1. ***Enrutamiento***

Por defecto, el firewall no enruta nada; por lo tanto, lo primero que debemos hacer es activar el enrutamiento, con esta orden:

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

* 1. ***Gestión de filtros y cadenas***
     1. ***Mostrar las reglas activas de una cadena***

Para mostrar las reglas de una cadena ejecutaremos iptables con la opción -L. Por ejemplo, para mostrar todas las reglas de la tabla *filter* pondríamos:

|  |
| --- |
| **iptables -L** |

Y, para ver las de la tabla *nat*:

|  |
| --- |
| **iptables -t nat -L** |

* + 1. ***Vaciar una cadena***

Cuando queremos reiniciar una cadena para añadir reglas nuevas tenemos que borrar todas las reglas que tiene definidas; para hacerlo, tenemos que usar la opción "-F". La siguiente orden borraría toda las reglas definidas en la cadena FORWARD:

|  |
| --- |
| **iptables -F FORWARD** |

* + 1. ***Borrar una regla de una cadena***

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

|  |
| --- |
| **iptables -D INPUT numero** |

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