Iptables: Herramienta para Controlar el Tráfico de un Servidor

Esta herramienta configurable tiene dos funciones básicas

- Bloquear el acceso no permitido desde redes externas
- Restringir las conexiones de la red local con el exterior.

¿Qué es Iptables?

Iptables es un módulo del núcleo de Linux que se encarga de filtrar los paquetes de red, determinando qué paquetes de datos llegan hasta el servidor y cuáles no.

Iptables funciona a través de **reglas**. El usuario indica mediante instrucciones el tipo de paquetes permitidos, los puertos de recepción, el protocolo utilizado y cualquier información relacionada con el intercambio de datos entre redes.

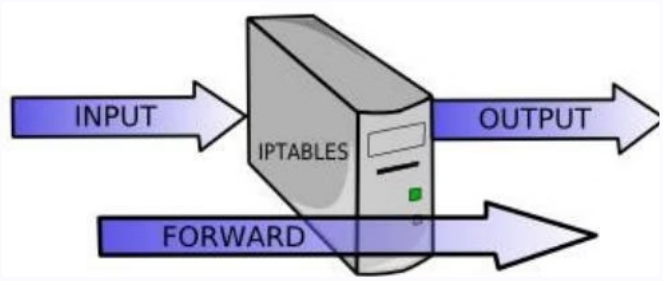
Cuando el sistema recibe o envía un paquete, se recorren las reglas en orden hasta encontrar una que cumpla las condiciones. Una vez localizada, esa regla se activa realizando la acción indicada sobre el paquete.

Tablas y Cadenas en Iptables

En iptables existen tres grandes grupos de reglas o tablas, dentro de las que se definen cadenas predefinidas. Cualquier paquete pasará por una de ellas para determinar su tratamiento.

Tabla Filter: Reglas de Filtrado

La tabla filter es donde se indican las reglas de filtrado fundamentales. Esta tabla contiene tres cadenas predefinidas que controlan el flujo de paquetes en diferentes direcciones.



INPUT

Hace referencia a los paquetes que llegan al sistema desde el exterior

OUTPUT

Tabla NAT: Traducción de Direcciones

Mediante la tabla NAT, se indican las reglas para realizar el enmascaramiento de la dirección IP del paquete, redirigir puertos o cambiar la dirección IP de origen y destino. Esta tabla es esencial para la comunicación entre redes privadas y públicas.

01

PREROUTING

Realiza una acción sobre el paquete antes de que sea enrutado justo cuando llega al cortafuegos.

02

POSTROUTING

Permite realizar una acción determinada antes de que el paquete salga del cortafuegos hacia su destino final.

03

OUTPUT

Permite modificar los paquetes generados en el propio cortafuegos antes de ser enrutados a su destino.

Estructura General de las Reglas

Una vez vistas las distintas tablas que trae predefinidas la herramienta iptables, es hora de comprender la estructura de las reglas que se pueden crear dentro de cada una de esas tablas.

> **Iptables -t [tabla] operación cadena parámetros acción**

Acciones sobre los Paquetes

Una vez definida la regla, hay que indicar la acción que realizaremos sobre aquellos paquetes que la cumplan. Para indicar esta acción, haremos uso del parámetro -j seguido de alguno de los siguientes valores.

ACCEPT

El paquete es aceptado y se permite su paso

-j ACCEPT

DROP

Se elimina el paquete sin enviar respuesta

-j DROP

REJECT

Se elimina el paquete y se envía mensaje ICMP

-j REJECT

REDIRECT

Modifica la dirección IP de la interfaz de entrada

-j REDIRECT

Operaciones sobre las Reglas

Mediante las operaciones, especificamos qué se hará con la regla en el sistema de firewall. Estas operaciones permiten gestionar el conjunto completo de reglas de iptables.

1

-A, --append

Añade una regla al final de la cadena especificada

```
iptables -A INPUT -p tcp -j DROP
```

2

-D, --delete

Elimina una regla específica del firewall

```
iptables -D INPUT -p tcp -j DROP
```

3

-I, --insert

Inserta una regla en una posición específica

```
iptables -I INPUT 4 -p tcp -j DROP
```

4

-L, --list

Lista todas las reglas de una cadena

```
iptables -L OUTPUT
```

5

-F, --flush

Borra todas las reglas de una cadena

```
iptables -F INPUT
```

Ejemplos Prácticos de Reglas (I)

Veamos ejemplos concretos de reglas de filtrado que ilustran casos de uso comunes en la administración de servidores Linux.

Reenvío entre Interfaces

Reenvío de paquetes desde la interfaz eth1 hacia la interfaz eth0

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Permitir Todo el Tráfico Entrante

Permite todo el tráfico desde cualquier dirección de la red eth1 hacia cualquier destino

```
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT
```

Denegar Tráfico de Red Local

Deniega todo el tráfico desde eth2 que intente usar direcciones IP de la red local

```
iptables -A INPUT -i eth2 -s 192.168.0.0/24 -j DROP
```

Ejemplos Prácticos de Reglas (II)

Aceptar Tráfico SMTP

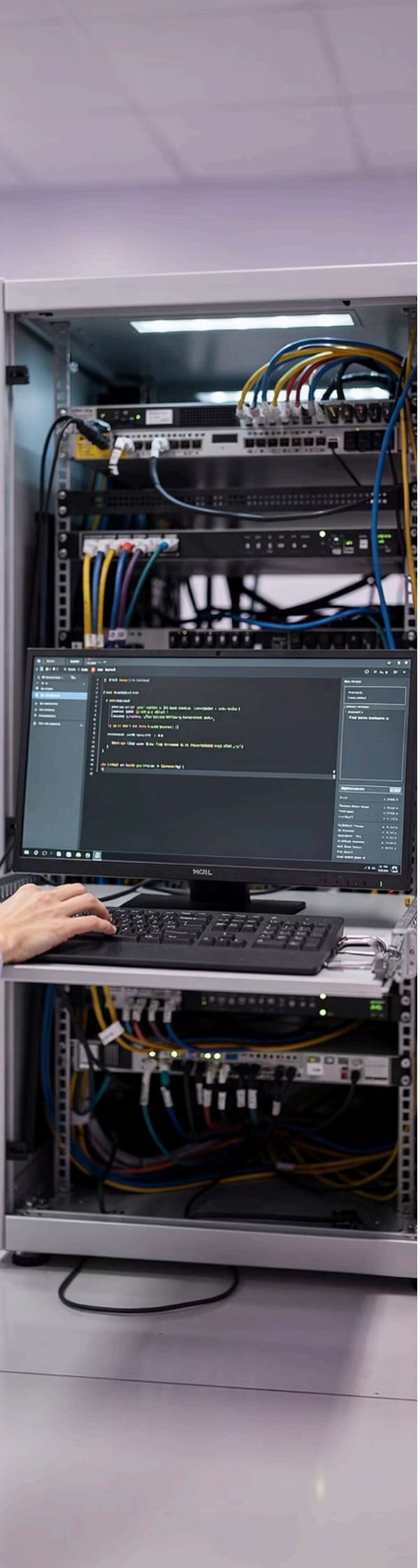
Acepta todos los paquetes enviados por el protocolo TCP por el puerto 25 (SMTP) en el servidor con IP 217.81.148.217 procedente desde cualquier sitio.

```
iptables -A INPUT -p tcp --dport 25 -s 0/0 -d 217.81.148.217 -j ACCEPT
```

Configurar NAT con MASQUERADE

Hacer NAT si la IP origen es 217.51.222.183 y sale por la interfaz eth1.

```
iptables -t nat -A POSTROUTING -s 217.51.222.183 -o eth1 -j MASQUERADE
```



Persistencia de Reglas: iptables-save

Las reglas de iptables que vayamos creando se van almacenando en memoria, por lo que cada vez que reiniciáramos el servidor, habría que volver a introducir las reglas manualmente.

Guardar Reglas

Ejecutar el comando iptables-save para almacenar las reglas en el archivo /etc/sysconfig/iptables

Reinicio del Sistema

Al iniciar el sistema, el script de inicio de iptables carga automáticamente las reglas almacenadas

Restauración Automática

Las reglas se restauran automáticamente sin intervención manual del administrador

Script Personalizado de Reglas

Otra opción para lograr la persistencia es crear un script personalizado donde escribiremos todas las reglas. Este método ofrece mayor control y flexibilidad en la gestión del firewall.

01

Crear el Script

Crear el archivo que contendrá todas las reglas y guardarlo en /etc (por ejemplo, /etc/reglas-iptables)

02

Asignar Permisos

Asignar permisos de ejecución mediante el comando: chmod +x /etc/reglas-iptables

03

Configurar Ejecución Automática

Añadir la ruta del script en /etc/rc.local para que se ejecute al iniciar el sistema

```
#!/bin/sh -e
# rc.local
/etc/reglas-iptables
exit 0
```