

# IPTABLES TASK

Ivana Sánchez Pérez

# Introducción

Iptables es una herramienta ampliamente utilizada en sistemas Linux para gestionar y configurar reglas de cortafuegos a nivel de red. Se basa en la funcionalidad del marco de Netfilter en el kernel de Linux y permite a los administradores definir políticas de seguridad detalladas para el tráfico de red que entra y sale de un sistema.

## ¿Qué es iptables?

Iptables es una utilidad en la línea de comandos que permite a los administradores definir reglas para controlar el tráfico de red. Estas reglas se aplican a los paquetes de datos que pasan a través de las interfaces de red del sistema. iptables es extremadamente flexible y poderoso, lo que lo convierte en una elección popular para la seguridad de red en entornos Linux.

## Funciones Principales de iptables

1. **Filtrado de Paquetes:** Permite definir reglas para permitir o bloquear paquetes basándose en criterios como direcciones IP de origen y destino, puertos, y protocolos.
2. **Redirección de Tráfico:** Puede redirigir el tráfico de un puerto a otro o de una dirección IP a otra, lo cual es útil para balanceo de carga y proxy inverso.
3. **Control de Acceso:** Define políticas de acceso para diferentes servicios y segmentos de red, garantizando que solo el tráfico autorizado pueda pasar.
4. **Registro y Monitoreo:** Las reglas pueden ser configuradas para registrar información sobre el tráfico, lo cual es útil para monitoreo de seguridad y diagnóstico de problemas.

## Componentes de iptables

- **Tablas:** iptables organiza las reglas en diferentes tablas, cada una diseñada para un propósito específico:
  - **filter:** La tabla predeterminada para el filtrado de paquetes.
  - **nat:** Utilizada para la traducción de direcciones de red (NAT).
  - **mangle:** Permite modificar paquetes en el nivel de red.
  - **raw:** Utilizada para tareas especializadas que requieren acceso directo a los paquetes.

- **Cadenas:** Dentro de cada tabla, las reglas se organizan en cadenas, que son conjuntos de reglas que se aplican en un orden específico. Las cadenas más comunes incluyen:
  - INPUT: Reglas que se aplican a los paquetes que entran al sistema.
  - OUTPUT: Reglas que se aplican a los paquetes que salen del sistema.
  - FORWARD: Reglas que se aplican a los paquetes que pasan a través del sistema hacia otro destino.
- **Reglas:** Cada regla en una cadena define una acción a tomar para los paquetes que coinciden con ciertos criterios. Las acciones pueden ser permitir (ACCEPT), rechazar (REJECT), o descartar (DROP) el paquete, entre otras.

## Scrip de configuración

Configuro dos VM Debian en modo interno. Una que será el servidor (DebianSeguridad) y la segunda será el cliente (DebianEjercicios).

```

GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
address 192.168.0.10
netmask 255.255.255.0
gateway 192.168.0.1
  
```

```

GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
address 192.168.0.11
netmask 255.255.255.0
gateway 192.168.0.1
  
```

En el servidor/firewall, crearé un script de configuración de iptables al que le agregaré reglas para permitir DNS y otras funciones esenciales.

```
GNU nano 7.2
#!/bin/bash

# Habilitar el enrutamiento IP
echo 1 > /proc/sys/net/ipv4/ip_forward
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
sysctl -p

# Limpiar reglas previas de iptables
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X

# * Reemplaza 'enp0s3' con la interfaz correcta *
IFACE_WAN="enp0s3" # Interfaz con salida a Internet
IFACE_LAN="enp0s8" # Interfaz de la red interna

# Permitir tráfico de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# * Reglas DNS (consultas y respuestas)
iptables -A OUTPUT -o $IFACE_WAN -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i $IFACE_WAN -p udp --sport 53 -j ACCEPT

# * Permitir tráfico HTTP/HTTPS (para navegación web)
iptables -A FORWARD -i $IFACE_LAN -o $IFACE_WAN -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $IFACE_LAN -o $IFACE_WAN -p tcp --dport 443 -j ACCEPT

# * Configurar NAT para permitir salida a Internet
iptables -t nat -A POSTROUTING -o $IFACE_WAN -j MASQUERADE

# * Permitir respuestas de tráfico establecido
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

# * Bloquear todo lo demás (politica por defecto)
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Guardar configuración
iptables-save > /etc/iptables.rules
echo " Configuración de iptables aplicada exitosamente."
```

Este script permite:

- DNS (UDP PUERTO 53)
- Navegación web (HTTP/HTTPS – puertos 80/443)
- NAT para que la VM2 tenga acceso a Internet

Le concedo permisos con **sudo chmod**

**+x configuración iptables.sh**

```
Actividades Terminal 2 de feb 17:40
ivana@debian: ~
ivana@debian:~$ sudo su
[sudo] contraseña para ivana:
root@debian:/home/ivana# ls
configuracion_iptables.sh Documentos Imágenes Plantillas Vídeos
Descargas Escritorio Música Público
root@debian:/home/ivana# nano configuracion_iptables.sh
root@debian:/home/ivana# chmod +x configuracion_iptables.sh
root@debian:/home/ivana#
```

Ejecutamos el script

```
debianSeguridad [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 2 de feb 20:52
ivana@debian: ~
root@debian:/home/ivana# ./configuracion_iptables.sh
net.ipv4.ip_forward = 1
net.ipv4.ip_forward = 1
net.ipv4.ip_forward = 1
Configuración de iptables aplicada exitosamente.
root@debian:/home/ivana#
```

Como al ejecutar el script, me ha cerrado todo acceso a internet, he creado un nuevo script para abrir todo lo que se ha cerrado. Lo ejecuto igualmente después de haberle dado los permisos +x.

```
Actividades Terminal 2 de feb 17:57
ivana@debian: ~
GNU nano 7.2 abrirTodo_iptables.sh *
#!/bin/sh
## SCRIPT de IPTABLES -FIREWALL PARA LA RED 192.168.8.0/24
##
echo -n Aplicando Reglas de Firewall...

## INICIALIZACIÓN
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

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

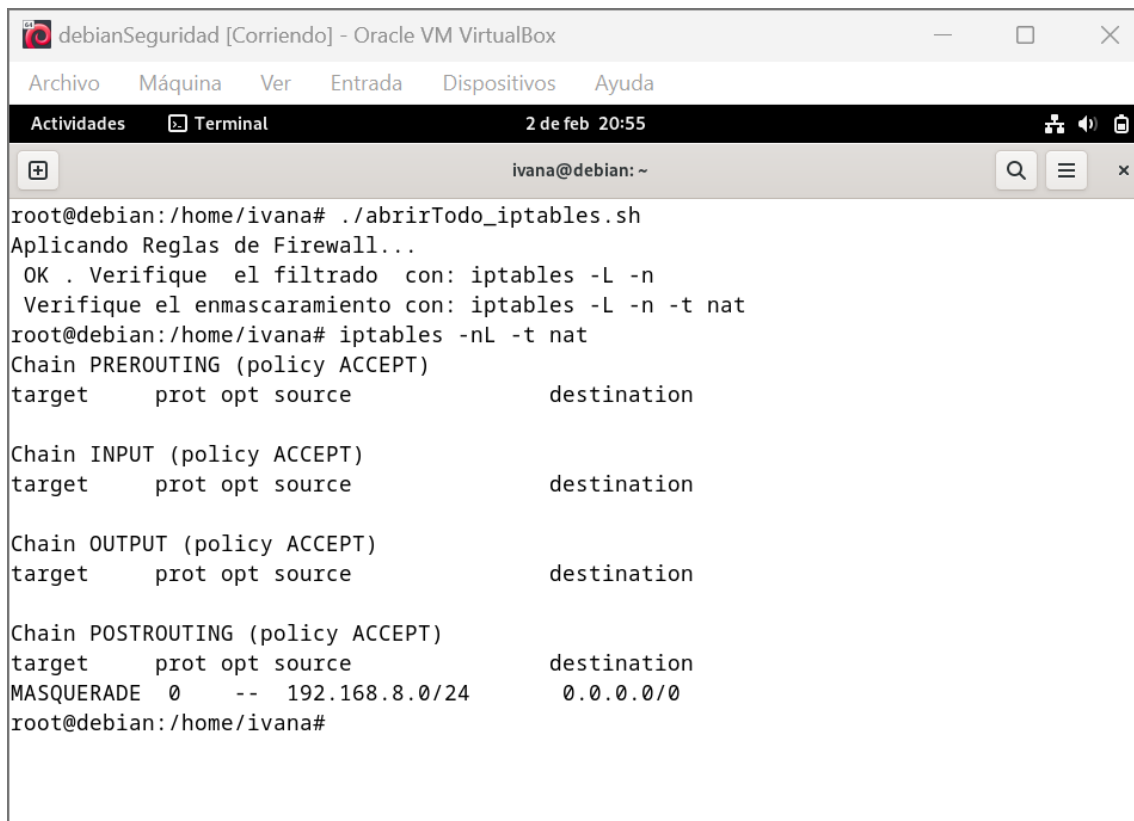
### Política de INPUT (servicios locales)

# Política de FORWARD (acceso a Internet y otras redes)

# Enmascaramiento
iptables -t nat -A POSTROUTING -s 192.168.8.0/24 -o enp0s3 -j MASQUERADE

#Activar forwarding (reenvío de paquetes)
echo 1 > /proc/sys/net/ipv4/ip_forward

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  ^M-U Deshacer  ^M-A Poner
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea  ^M-E Rehacer   ^M-G Copiar
```



debianSeguridad [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 2 de feb 20:55

ivana@debian: ~

```
root@debian:/home/ivana# ./abrirTodo_iptables.sh
Aplicando Reglas de Firewall...
OK . Verifique el filtrado con: iptables -L -n
Verifique el enmascaramiento con: iptables -L -n -t nat
root@debian:/home/ivana# iptables -nL -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

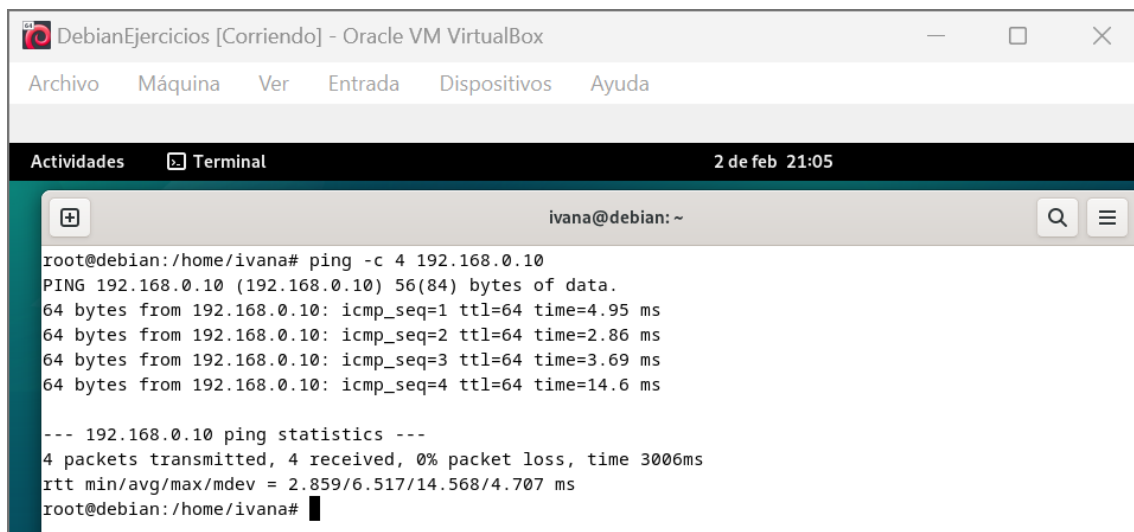
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE 0    --  192.168.8.0/24        0.0.0.0/0
root@debian:/home/ivana#
```

## Consultas y respuestas

Verificamos la conectividad entre ambas máquinas



DebianEjercicios [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 2 de feb 21:05

ivana@debian: ~

```
root@debian:/home/ivana# ping -c 4 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=4.95 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=2.86 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=64 time=3.69 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=64 time=14.6 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.859/6.517/14.568/4.707 ms
root@debian:/home/ivana#
```

Comprobamos DNS

```
Actividades Terminal 2 de feb 21:06
ivana@debian: ~
root@debian:/home/ivana# nslookup google.com
Server:          212.166.132.110
Address:         212.166.132.110#53

** server can't find google.com: NXDOMAIN

root@debian:/home/ivana# dig google.com

;<<>> DiG 9.18.28-1~deb12u2-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35284
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: ea410b95e4670a78bed6a03b679fd026ed5769ac88d78428 (good)
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 42      IN      A      142.250.184.174

;; Query time: 28 msec
;; SERVER: 212.166.132.110#53(212.166.132.110) (UDP)
;; WHEN: Sun Feb 02 21:05:58 CET 2025
;; MSG SIZE rcvd: 83

root@debian:/home/ivana#
```

Probamos la navegación Web

```
ivana@debian: ~
root@debian:/home/ivana# curl -I -L http://google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-shkgp5X_q4Clo0lz7GN_JQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Date: Sun, 02 Feb 2025 20:34:52 GMT
Expires: Tue, 04 Mar 2025 20:34:52 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-LETo3PRHkr817_s5m2Lv7w' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Date: Sun, 02 Feb 2025 20:34:53 GMT
Server: gws
```

