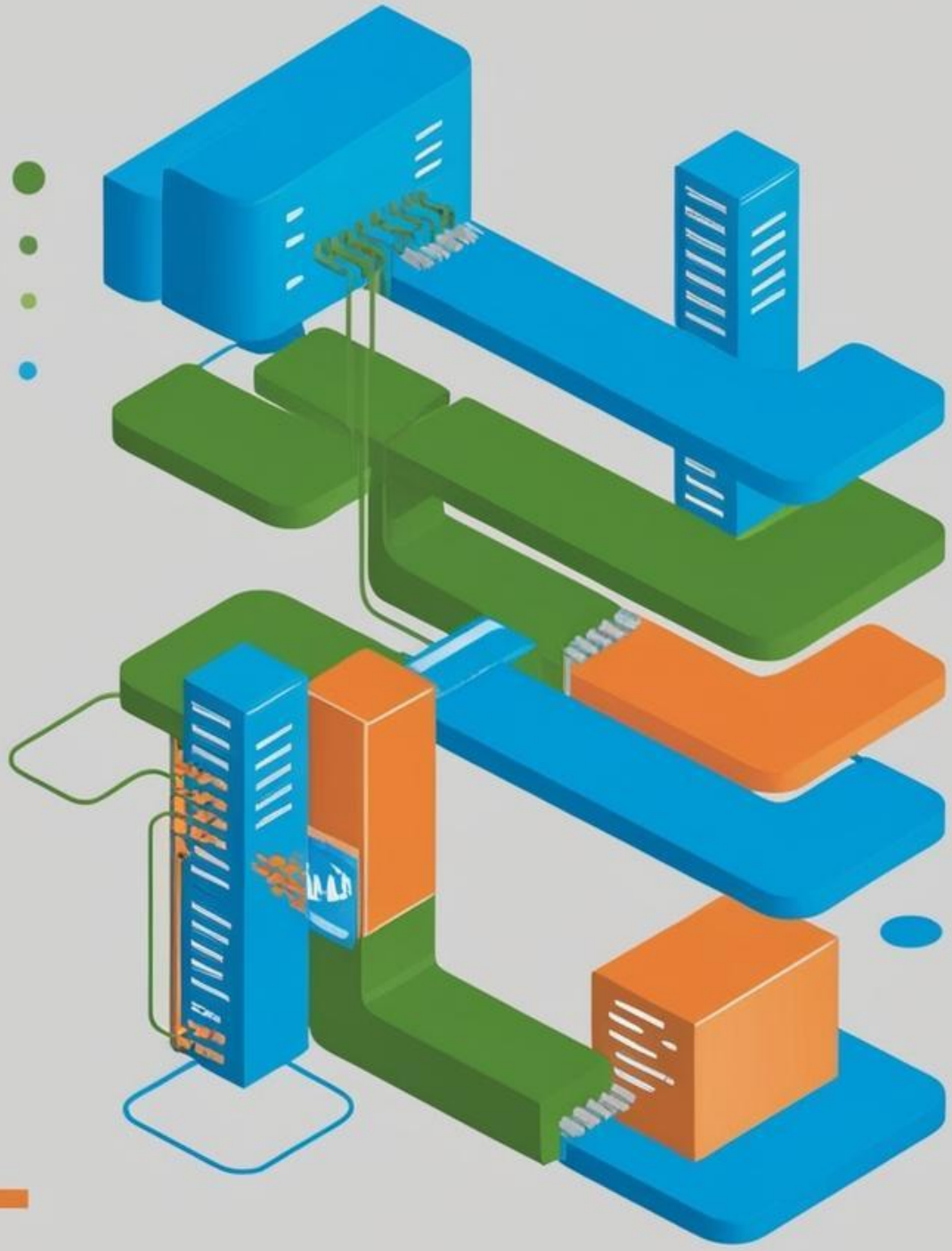


IPTABLES TASK

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.

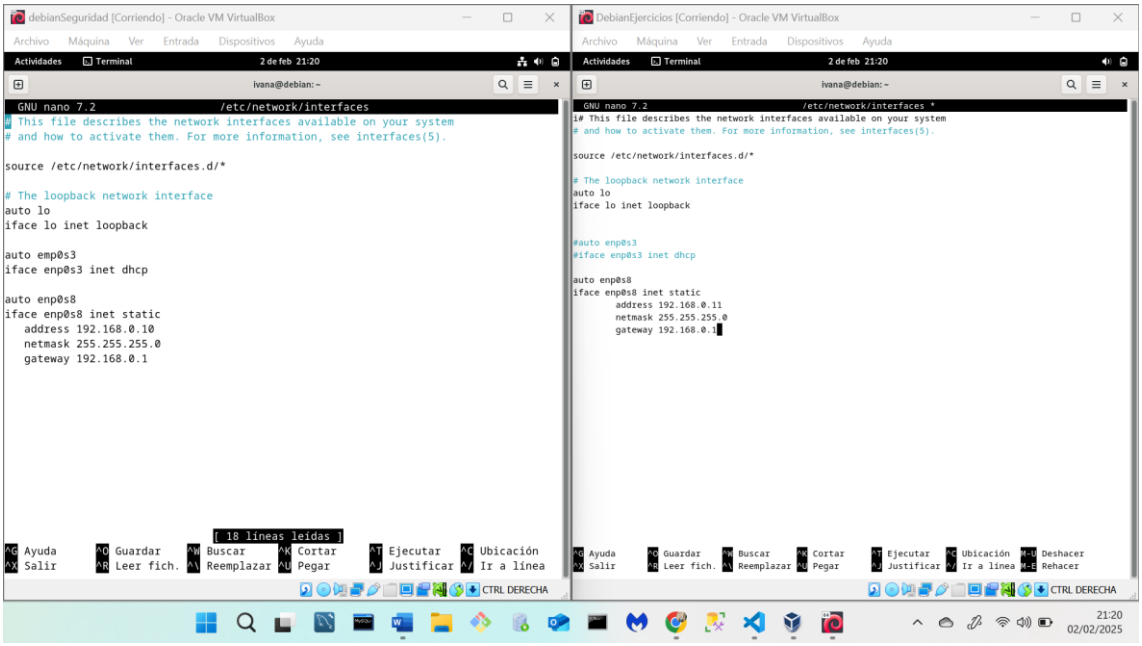
Componentes de iptables

- **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, entreotras.

Scrip de configuración

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



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

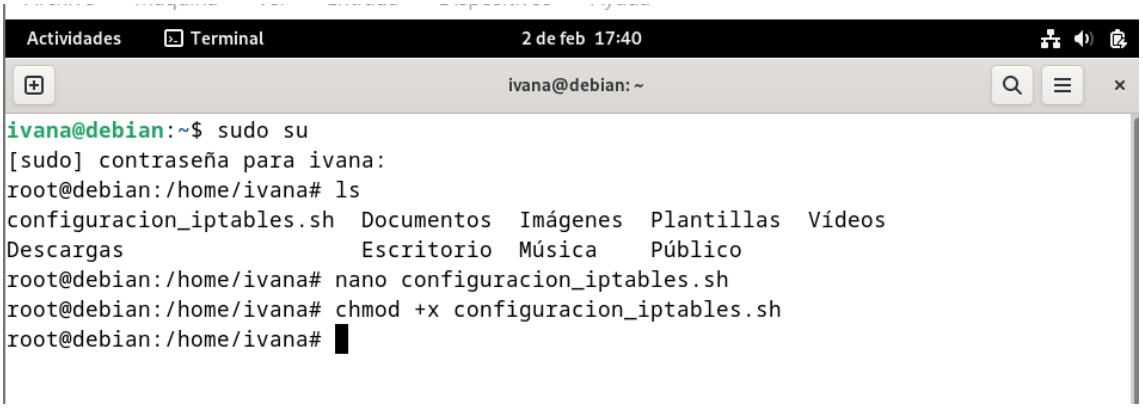
```
  GNU nano 7.2
#!/bin/bash

# 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 (política 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:

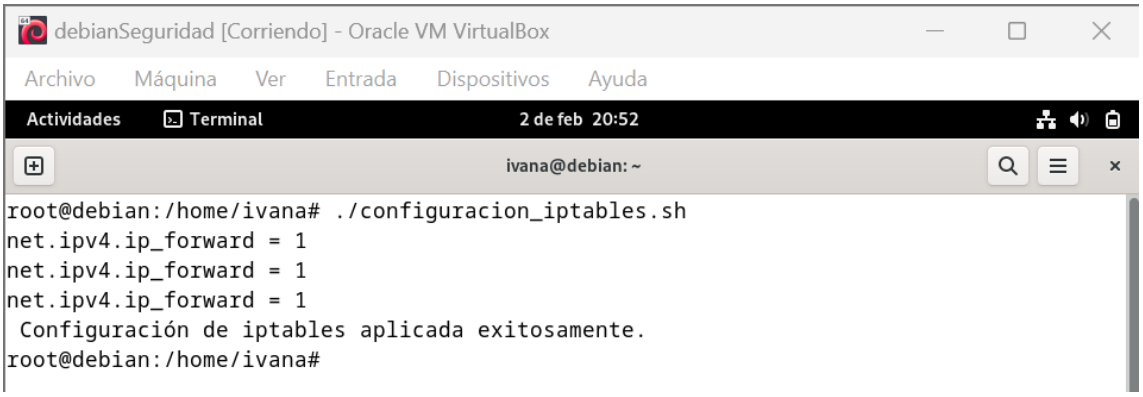
- DNS (UDP PUERTO 53)
- Navegación web (HTPP/HTPPS – puertos 80/443)
- NAT para que la VM2 tenga acceso a Internet

Le concedo permisos con ***sudo chmod***

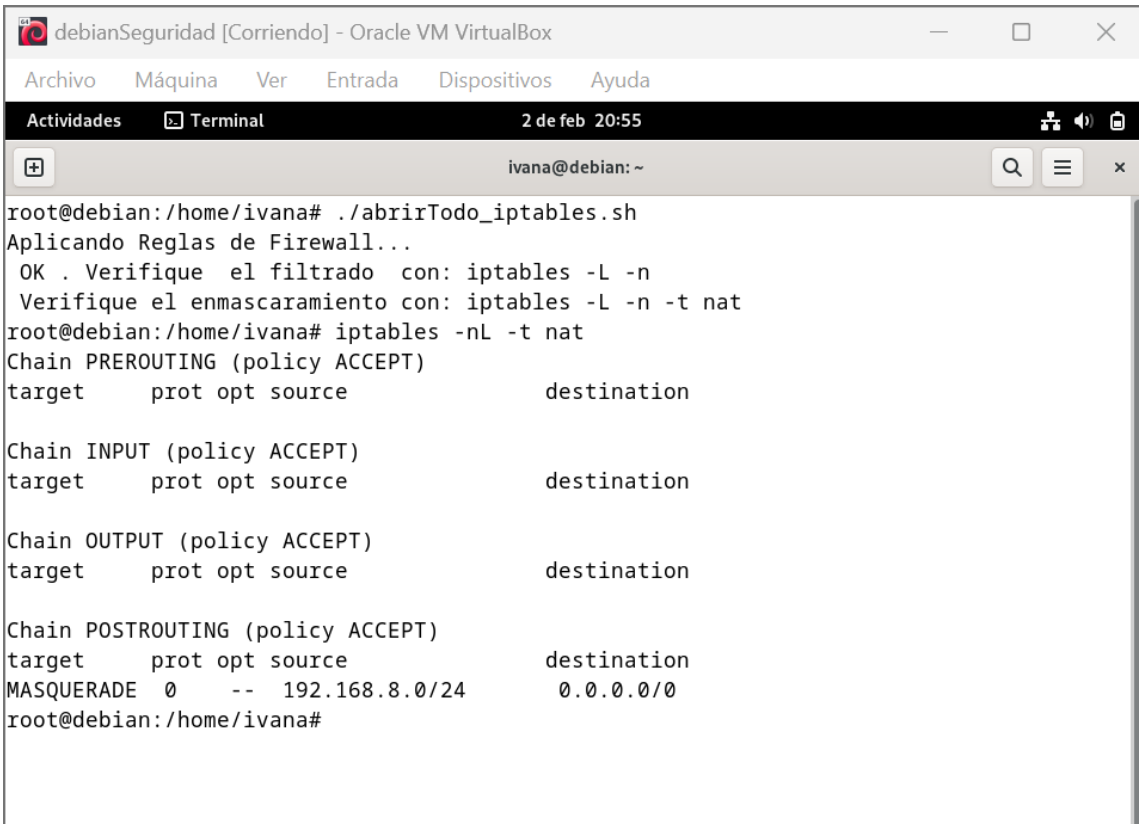
+x configuración_iptables.sh



Ejecutamos el script

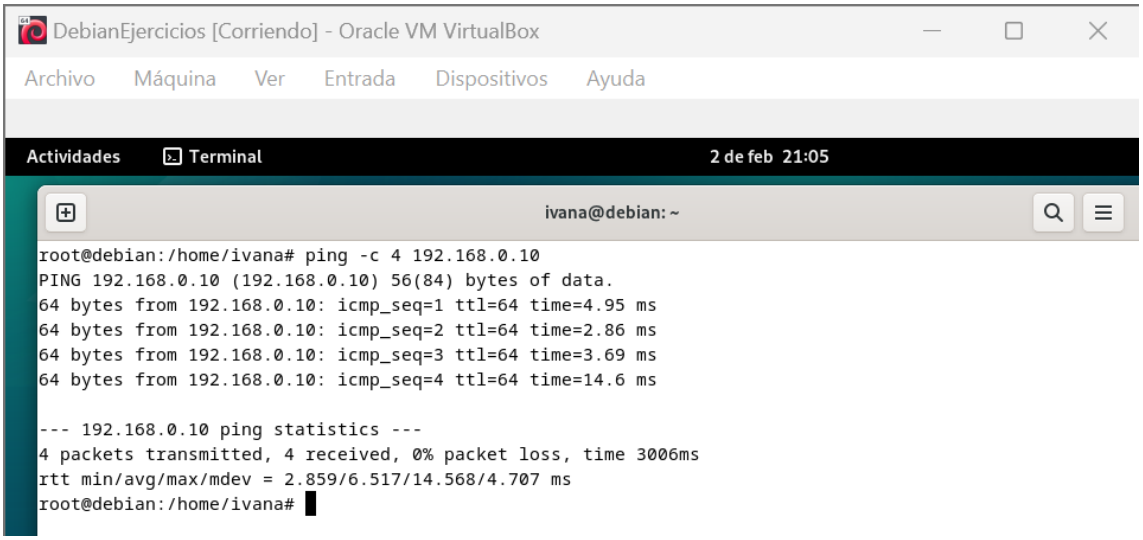


Como al ejecutar el script, me ha cerrado todo acceso a internet, he creado un nuevo script para abrir todo lo que se ha cerrado. Lo ejecuto igualmente después de haberle dado los permisos +x.

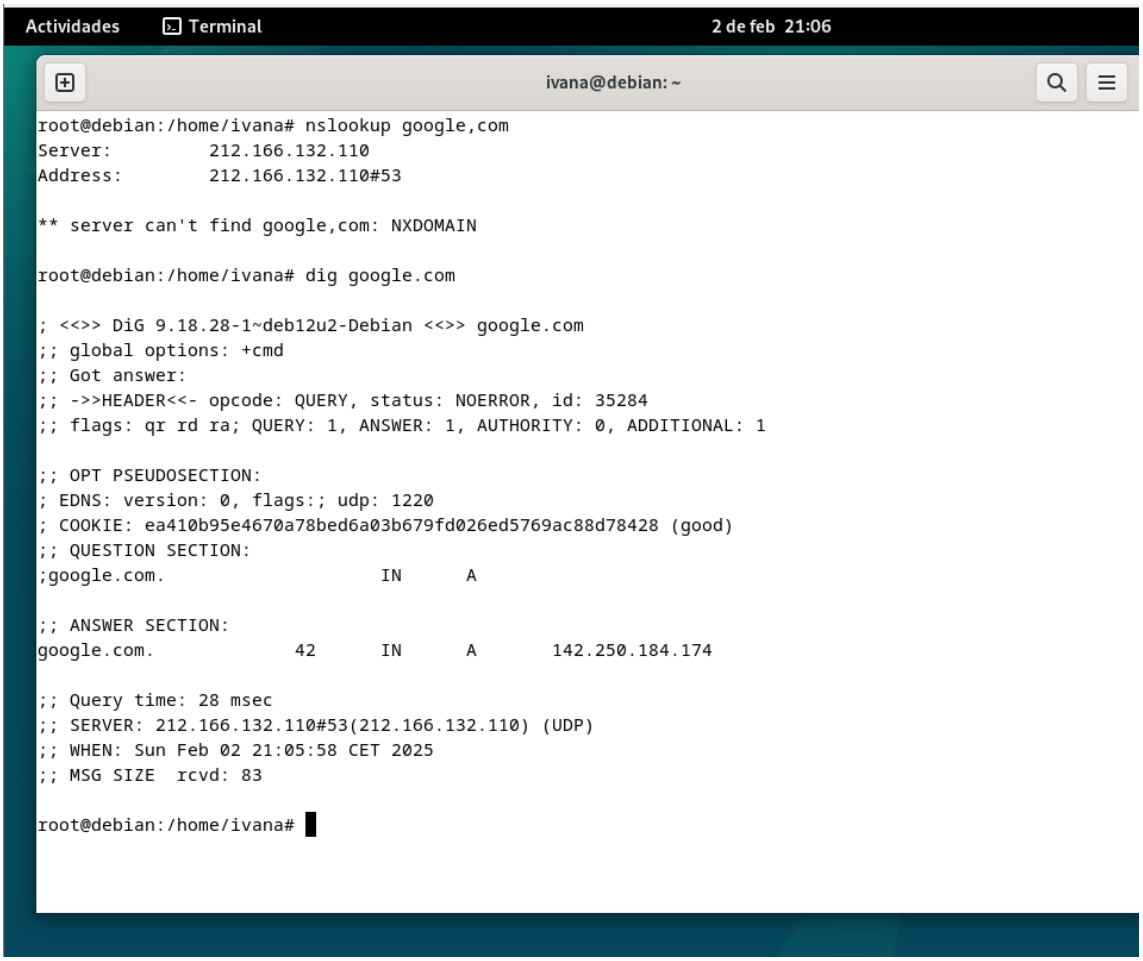


Consultas y respuestas

Verificamos la conectividad entre ambas máquinas



Comprobamos DNS



Probamos la navegación Web