FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS

CARRERA INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

GUÍA 3: INSTALACIÓN Y CONFIGURACIÓN DE IPTABLES

AUTORES:

Annel Ivana Flores Reyes

Bélgica Guadalupe Delgado Suárez

DIRECTOR DE TEMA:

Ing. Edison Almeida Zambrano, Mg.

MANTA – MANABÍ – ECUADOR

2025– 2026

CONTENIDO

1. Introducción

Esta guía tiene como objetivo enseñar la instalación, configuración y verificación de iptables, una herramienta esencial para la administración de reglas de firewall en servidores Linux. A través de pasos prácticos, se explica cómo preparar el sistema, sustituir firewalld por iptables, añadir reglas de acceso a puertos específicos (como SSH y Webmin), establecer políticas de seguridad predeterminadas y guardar la configuración. Con ello, el usuario podrá asegurar su servidor mediante un control más directo y efectivo del tráfico de red

1.1 Objetivo

En esta guía aprenderás a instalar y configurar iptables en un servidor Linux, sustituyendo el firewall por defecto (**firewalld**) y estableciendo reglas específicas para mejorar la seguridad del sistema.

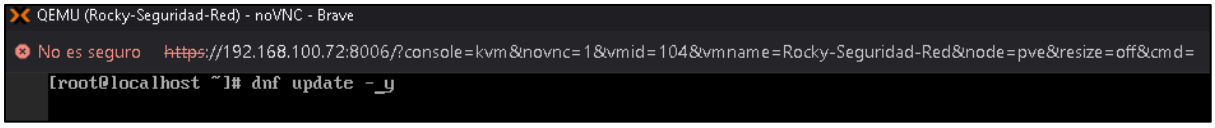
2. Actualización del Sistema

Mantener el sistema actualizado garantiza que cuente con los últimos parches de seguridad y correcciones de errores.

Comando

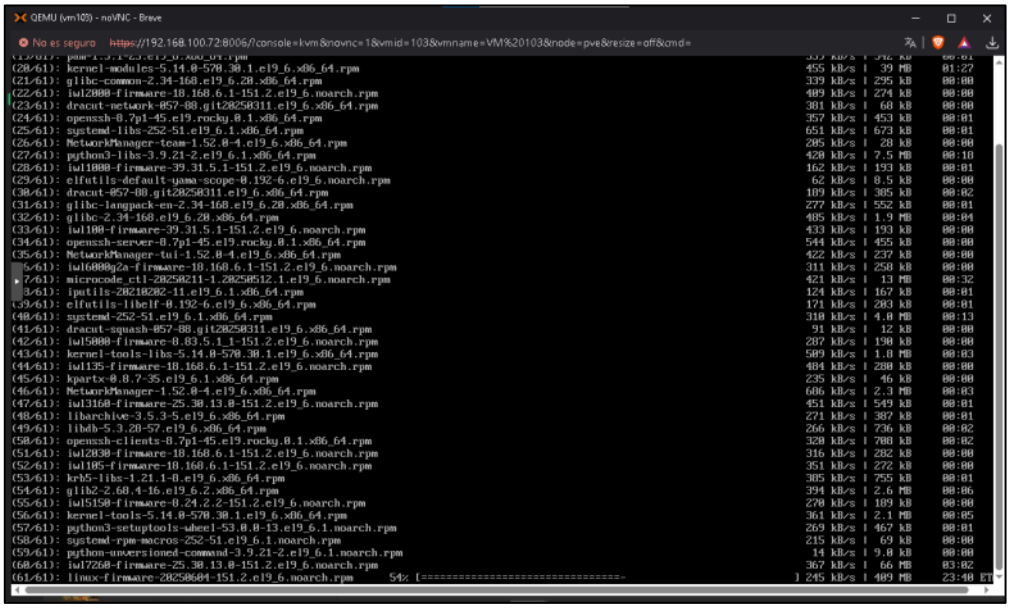
dnf update -y

Ilustración 1.*Comando de actualización del sistema*



Fuente*. Elaborado por los autores de la guía.*

Ilustración 2.*Proceso de la actualización del sistema.*



Fuente*. Elaborado por los autores de la guía.*

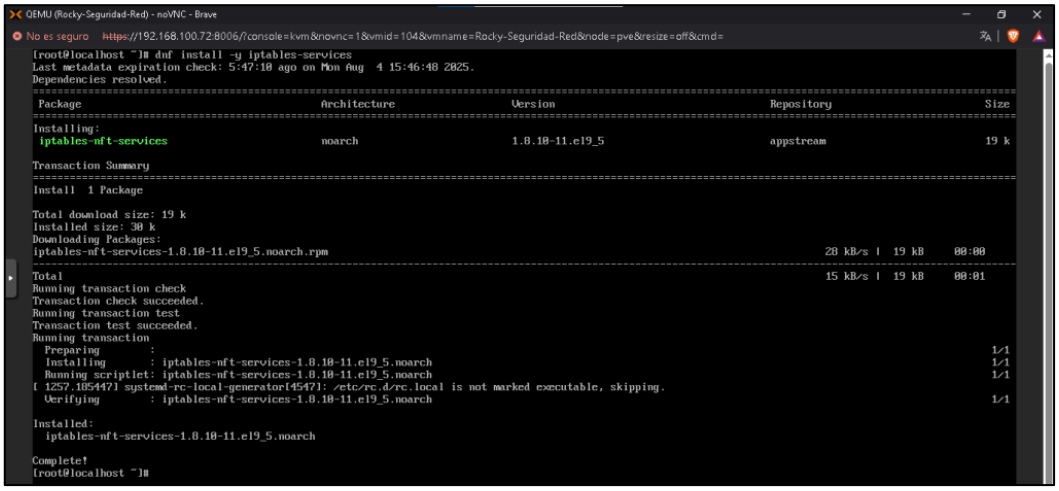
3. Instalación y Configuración de Iptables

3.1 Instalación de iptables-services

Para comenzar, instalamos el paquete que permite gestionar iptables como un servicio:

```
dnf install -y iptables-services
```

Ilustración 3.*Instalación de iptables-services*



Fuente*. Elaborado por los autores de la guía.*

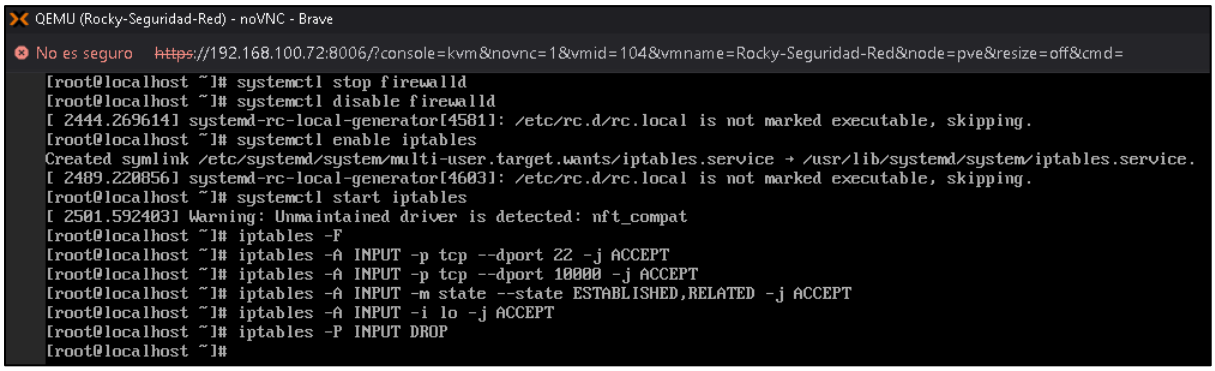
3.2 Sustituir firewalld por iptables

Dado que firewalld suele estar habilitado por defecto en muchas distribuciones, es necesario detenerlo y desactivarlo antes de usar iptables:

systemctl stop firewalld

systemctl disable firewalld

Ilustración 4.*Proceso de sustitución del firewalld por iptables.*



Fuente*. Elaborado por los autores de la guía.*

3.3 Habilitar iptables como firewall principal

- systemctl enable iptables
- systemctl start iptables

3.4 Limpieza de reglas previas

Antes de añadir nuevas reglas, se eliminan todas las existentes para evitar conflictos:

- iptables -F

4. Definición de Reglas Básicas

4.1 Permitir acceso por SSH

Esto permite conexiones remotas seguras a través del puerto 22:

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

4.2 Permitir acceso a Webmin

Si se está usando Webmin, se debe habilitar el puerto 10000:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

4.3 Permitir tráfico relacionado y establecido

Esto asegura que las conexiones legítimas en curso puedan continuar:

```
iptables -A INPUT -p tcp --dport 10000 -j ACCEPT
```

4.4 Permitir tráfico local (loopback)

```
iptables -A INPUT -i lo -j ACCEPT
```

4.5 Establecer política por defecto

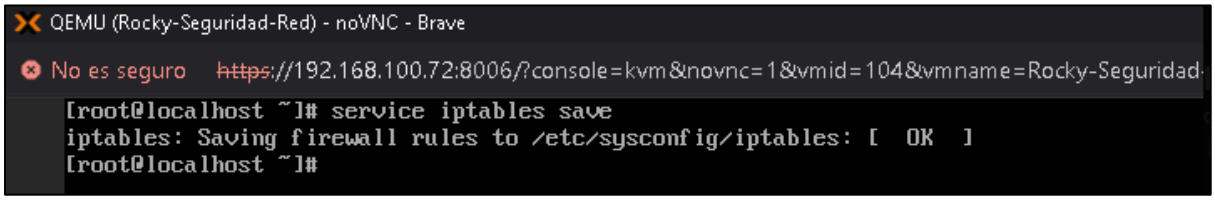
Cualquier otro tráfico no definido en las reglas será bloqueado:

```
iptables -P INPUT DROP
```

4.6 Guardar la configuración

```
service iptables save
```

Ilustración 5.*Guardado de la configuración.*



Fuente*. Elaborado por los autores de la guía.*

5. Verificación de Reglas

5.1 Comando para listar reglas

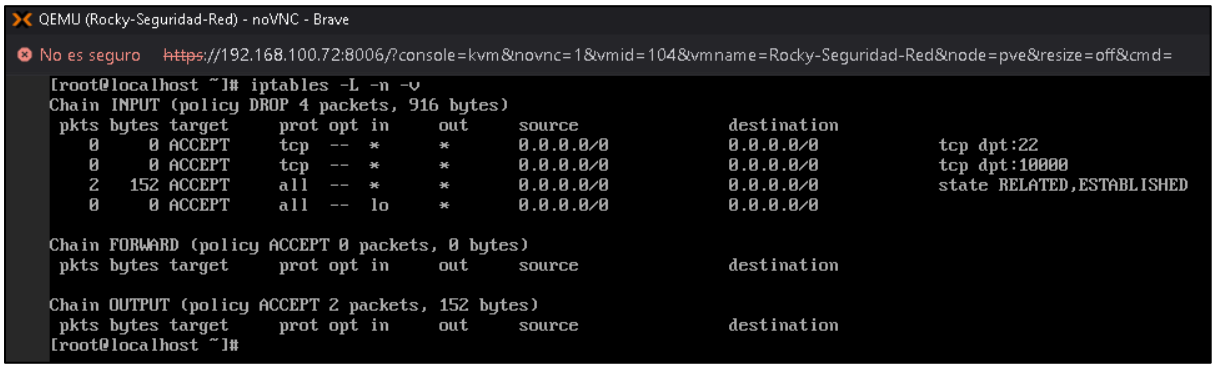
- iptables -L -n -v

5.2 Resultados esperados

Las reglas que añadiste (--dport 22 y --dport 10000) deben aparecer en la cadena INPUT.

La política de INPUT debe estar como DROP.

Ilustración 6.*Resultados esperados de la cadena.*



Fuente*. Elaborado por los autores de la guía.*

6. Conclusión

Con esta configuración, se ha reemplazado **firewalld** por **iptables**, definiendo un conjunto básico de reglas que permiten acceso por SSH y Webmin, garantizando la seguridad del servidor frente a accesos no autorizados.