



Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

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	3
1.1 Objetivo.....	3
2. Actualización del Sistema	3
3. Instalación y Configuración de Iptables	4
3.1 Instalación de iptables-services.....	4
3.2 Sustituir firewalld por iptables.....	5
3.3 Habilitar iptables como firewall principal	5
3.4 Limpieza de reglas previas.....	5
4. Definición de Reglas Básicas.....	6
4.1 Permitir acceso por SSH	6
4.2 Permitir acceso a Webmin.....	6
4.3 Permitir tráfico relacionado y establecido	6
4.4 Permitir tráfico local (loopback).....	6
4.5 Establecer política por defecto.....	6
4.6 Guardar la configuración	6
5. Verificación de Reglas	7
5.1 Comando para listar reglas.....	7
5.2 Resultados esperados	7
6. Conclusión	8

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

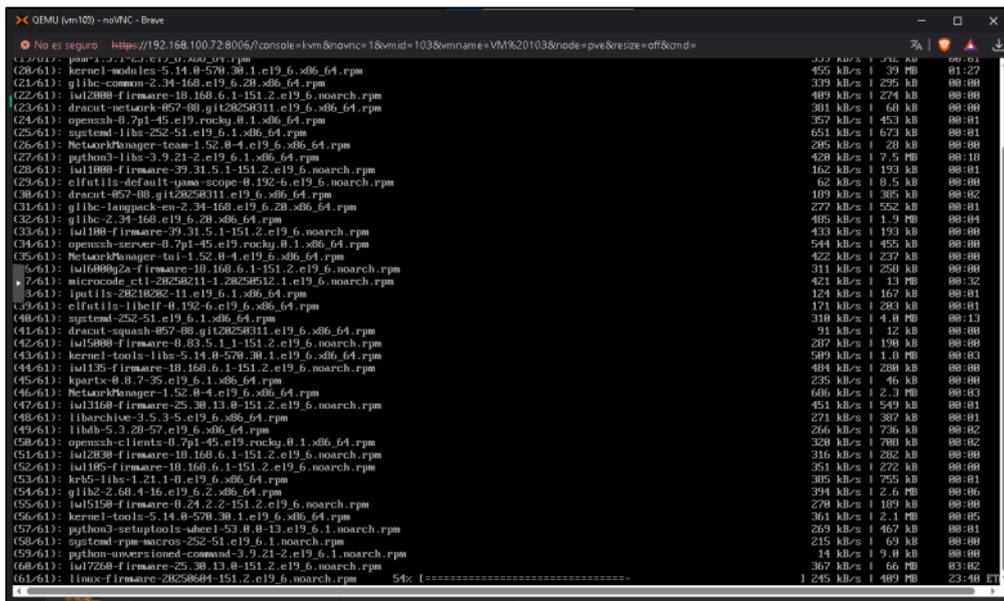
```
dnf update -y
```

Ilustración 1. Comando de actualización del sistema



Fuente. Elaborado por los autores de la guía.

Ilustración 2. Proceso de la actualización del sistema.



```
QEMU (vm107) - noVNC - Brave
No es seguro https://192.168.100.72:8006/?console=1&vmid=103&vmname=VM%20103&node=pve&resize=off&cmd=
(120/61): pam-1.4.2-1.e19.6.noarch.rpm 207 kB/s | 196 kB 00:01
(121/61): kernel-modules-5.14.8-579.30.1.e19.6.x86_64.rpm 455 kB/s | 39 MB 01:27
(122/61): glibc-common-2.34-168.e19.6.20.x86_64.rpm 339 kB/s | 295 kB 00:00
(123/61): iwl2000-firmware-18.168.6.1-151.2.e19.6.noarch.rpm 489 kB/s | 274 kB 00:00
(124/61): dracut-network-857-88.git28258311.e19.6.x86_64.rpm 381 kB/s | 60 kB 00:00
(125/61): openssl-0.7p1-45.e19.rocky.0.1.x86_64.rpm 257 kB/s | 453 kB 00:01
(126/61): systemd-libs-252-51.e19.6.1.x86_64.rpm 651 kB/s | 673 kB 00:01
(127/61): NetworkManager-team-1.52.0-4.e19.6.x86_64.rpm 295 kB/s | 20 kB 00:00
(128/61): python3-libs-3.9.21-2.e19.6.1.x86_64.rpm 428 kB/s | 7.5 MB 00:10
(129/61): iwl1000-firmware-39.31.5.1-151.2.e19.6.noarch.rpm 162 kB/s | 193 kB 00:01
(130/61): elfutils-default-yama-scope-0.132-6.e19.6.noarch.rpm 62 kB/s | 8.5 kB 00:00
(131/61): dracut-857-88.git28258311.e19.6.x86_64.rpm 109 kB/s | 305 kB 00:02
(132/61): glibc-langpack-en-2.34-168.e19.6.20.x86_64.rpm 277 kB/s | 552 kB 00:01
(133/61): glibc-2.34-168.e19.6.20.x86_64.rpm 485 kB/s | 1.9 MB 00:04
(134/61): iwl100-firmware-39.31.5.1-151.2.e19.6.noarch.rpm 433 kB/s | 193 kB 00:00
(135/61): openssl-server-0.7p1-45.e19.rocky.0.1.x86_64.rpm 544 kB/s | 455 kB 00:00
(136/61): NetworkManager-tui-1.52.0-4.e19.6.x86_64.rpm 422 kB/s | 237 kB 00:00
(137/61): iwl6000g2a-firmware-18.168.6.1-151.2.e19.6.noarch.rpm 311 kB/s | 250 kB 00:00
(138/61): microcode_ctl-28258211-1.28258512.1.e19.6.noarch.rpm 421 kB/s | 13 MB 00:32
(139/61): iputils-20210302-11.e19.6.1.x86_64.rpm 124 kB/s | 167 kB 00:01
(140/61): elfutils-libelf-0.192-6.e19.6.x86_64.rpm 171 kB/s | 293 kB 00:01
(141/61): systemd-252-51.e19.6.1.x86_64.rpm 318 kB/s | 4.8 MB 00:13
(142/61): dracut-squash-857-88.git28258311.e19.6.x86_64.rpm 91 kB/s | 12 kB 00:00
(143/61): iwl5000-firmware-0.83.5.1-1-151.2.e19.6.noarch.rpm 287 kB/s | 190 kB 00:00
(144/61): kernel-tools-libs-5.14.8-579.30.1.e19.6.x86_64.rpm 595 kB/s | 1.0 MB 00:03
(145/61): iwl135-firmware-18.168.6.1-151.2.e19.6.noarch.rpm 484 kB/s | 288 kB 00:00
(146/61): kpartx-0.8.7-35.e19.6.1.x86_64.rpm 235 kB/s | 46 kB 00:00
(147/61): NetworkManager-1.52.0-4.e19.6.x86_64.rpm 606 kB/s | 2.3 MB 00:03
(148/61): iwl802-firmware-25.38.13.0-151.2.e19.6.noarch.rpm 451 kB/s | 549 kB 00:01
(149/61): libarchive-3.5.3-5.e19.6.x86_64.rpm 271 kB/s | 387 kB 00:01
(150/61): libb2-5.3.20-57.e19.6.x86_64.rpm 266 kB/s | 736 kB 00:02
(151/61): openssl-clients-0.7p1-45.e19.rocky.0.1.x86_64.rpm 328 kB/s | 700 kB 00:02
(152/61): iwl2030-firmware-18.168.6.1-151.2.e19.6.noarch.rpm 276 kB/s | 282 kB 00:00
(153/61): iwl105-firmware-18.168.6.1-151.2.e19.6.noarch.rpm 351 kB/s | 272 kB 00:00
(154/61): krb5-libs-1.21.1-0.e19.6.x86_64.rpm 305 kB/s | 755 kB 00:01
(155/61): glib2-2.68.4-16.e19.6.2.x86_64.rpm 394 kB/s | 2.6 MB 00:06
(156/61): iwl5150-firmware-0.24.2-2-151.2.e19.6.noarch.rpm 276 kB/s | 189 kB 00:00
(157/61): kernel-tools-5.14.8-579.30.1.e19.6.x86_64.rpm 361 kB/s | 2.1 MB 00:05
(158/61): python3-setuptools-wheel-53.0.8-13.e19.6.1.noarch.rpm 269 kB/s | 467 kB 00:01
(159/61): systemd-rpm-macros-252-51.e19.6.1.noarch.rpm 215 kB/s | 69 kB 00:00
(160/61): python-universiconn-command-3.9.21-2.e19.6.1.noarch.rpm 14 kB/s | 9.0 kB 00:00
(161/61): iwl7260-firmware-25.38.13.0-151.2.e19.6.noarch.rpm 367 kB/s | 66 MB 03:02
(162/61): linux-firmware-20258694-151.2.e19.6.noarch.rpm 54% [=====] 1.245 kB/s | 489 MB 23:40 ET
```

Fuente. Elaborado por los autores de la guía.

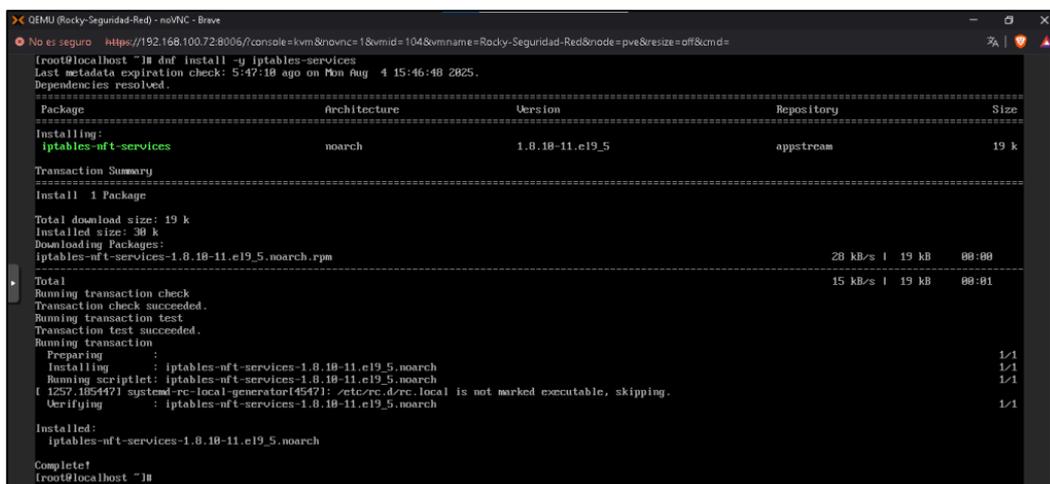
3. Instalación y Configuración de Iptables

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



```
QEMU (Rocky-Seguridad-Red) - noVNC - Brave
No es seguro https://192.168.100.72:8006/?console=1&vmid=104&vmname=Rocky-Seguridad-Red&node=pve&resize=off&cmd=
[root@localhost ~]# dnf install -y iptables-services
Last metadata expiration check: 5:47:18 ago on Mon Aug 4 15:46:48 2025.
Dependencies resolved.
=====
Package                architecture  Version      Repository  Size
-----
Installing:
iptables-services      noarch       1.0.10-11.e19_5  appstream  19 k
Transaction Summary
-----
Install 1 Package
Total download size: 19 k
Installed size: 38 k
Downloading Packages:
iptables-nft-services-1.0.10-11.e19_5.noarch.rpm 28 kB/s | 19 kB 00:00
-----
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction:
Preparing                :
Installing                : iptables-nft-services-1.0.10-11.e19_5.noarch 1/1
Running scriptlet: iptables-nft-services-1.0.10-11.e19_5.noarch 1/1
(1557/10547) systemd-rc-local-generator(45471): etc/rc.d/udev.local is not marked executable, skipping.
Verifying                 : iptables-nft-services-1.0.10-11.e19_5.noarch 1/1
Installed:
iptables-nft-services-1.0.10-11.e19_5.noarch
Complete!
[root@localhost ~]#
```

Fuente. Elaborado por los autores de la guía.

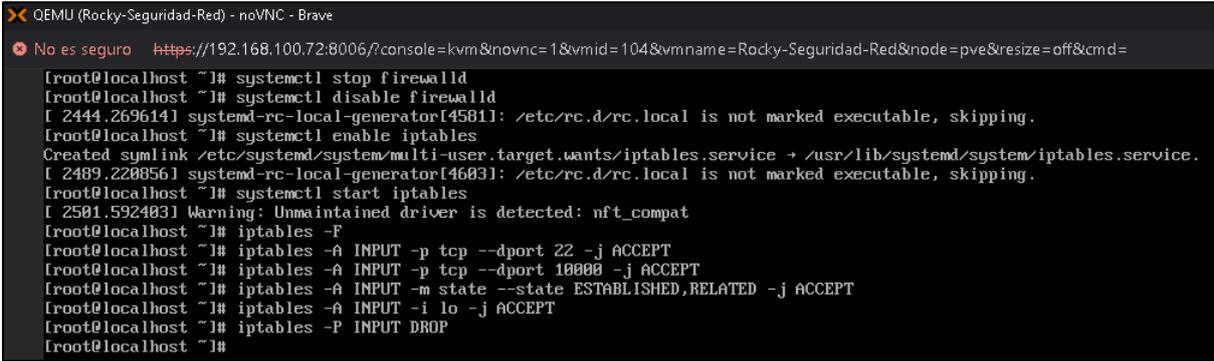
3.2 Sustituir firewalld por iptables

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.



```
QEMU (Rocky-Seguridad-Red) - noVNC - Brave
No es seguro https://192.168.100.72:8006/?console=kvm&novnc=1&vmid=104&vmname=Rocky-Seguridad-Red&node=pve&resize=off&cmd=
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# systemctl disable firewalld
[ 2444.269614] systemd-rc-local-generator[45811]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@localhost ~]# systemctl enable iptables
Created symlink /etc/systemd/system/multi-user.target.wants/iptables.service → /usr/lib/systemd/system/iptables.service.
[ 2489.220856] systemd-rc-local-generator[46031]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@localhost ~]# systemctl start iptables
[ 2501.592403] Warning: Unmaintained driver is detected: nft_compat
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --dport 10000 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
[root@localhost ~]# iptables -A INPUT -i lo -j ACCEPT
[root@localhost ~]# iptables -P INPUT DROP
[root@localhost ~]#
```

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.

```
QEMU (Rocky-Seguridad-Red) - noVNC - Brave
No es seguro https://192.168.100.72:8006/?console=kvm&novnc=1&vmid=104&vmname=Rocky-Seguridad-Red
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables: [ OK ]
[root@localhost ~]#
```

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.

```
QEMU (Rocky-Seguridad-Red) - noVNC - Brave
No es seguro https://192.168.100.72:8006/?console=kvm&novnc=1&vmid=104&vmname=Rocky-Seguridad-Red&node=pve&resize=off&cmd=
[root@localhost ~]# iptables -L -n -v
Chain INPUT (policy DROP 4 packets, 916 bytes)
 pkts bytes target    prot opt in     out     source            destination
  0     0 ACCEPT    tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:22
  0     0 ACCEPT    tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:10000
  2   152 ACCEPT    all  --  *     *     0.0.0.0/0         0.0.0.0/0         state RELATED,ESTABLISHED
  0     0 ACCEPT    all  --  lo    *     0.0.0.0/0         0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target    prot opt in     out     source            destination
[root@localhost ~]#
```

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.