

Docker, restricción IP

docker

Docker manipula iptables directamente y sus reglas se evalúan antes que las de UFW. Si publicas el puerto con `-p 2222:22` (o `ports: «2222:22»` en compose), **el puerto quedará abierto a todo Internet aunque UFW diga lo contrario**. La regla de arriba no restringe nada por sí sola en ese caso.

enfoques

- no es posible limitar el acceso desde docker-compose:

```
ports:
  - "<IP_PUBLICA>:2222:22"
```

- usar iptables con la cadena DOCKER-USER
- usar ufw-docker
 - requiere fijar las direcciones IPs de los contenedores
 - requiere añadir un servicio en systemctl para volver a activar la regla tras reinicio
- usar iptables en combinación con ipset

iptables + ipset

- IPSET: [Linux tcp/ip ipset](#)
- añadir regla IPTABLES con IPSET (sftp_allowed):

```
sudo iptables -I DOCKER-USER -i eth0 -p tcp -m conntrack --ctorigdstport 2222
--ctdir ORIGINAL -m set ! --match-set sftp_allowed src -j DROP # añadir
```

```
sudo iptables -D DOCKER-USER -i eth0 -p tcp -m conntrack --ctorigdstport 2222
--ctdir ORIGINAL -m set ! --match-set sftp_allowed src -j DROP # quitar
sudo iptables -L DOCKER-USER -n --line-numbers
sudo iptables -D DOCKER-USER <número>
```

- modificación de IPs: [Linux tcp/ip ipset](#)
- persistencia:

[/etc/systemd/system/docker-sftp-filter.service](#)

```
[Unit]
Description=Restringir puerto 2222 a IPs autorizadas
After=docker.service
Requires=docker.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/ipset create -exist sftp_allowed hash:ip
ExecStart=/sbin/ipset add -exist sftp_allowed 88.26.243.132
ExecStart=/sbin/ipset add -exist sftp_allowed 203.0.113.10
ExecStart=/sbin/iptables -I DOCKER-USER -i eth0 -p tcp -m conntrack --
ctorigdstport 2222 --ctdir ORIGINAL -m set ! --match-set sftp_allowed src
```

```
-j DROP
ExecStop=/sbin/iptables -D DOCKER-USER -i eth0 -p tcp -m conntrack --
ctorigdstport 2222 --ctdir ORIGINAL -m set ! --match-set sftp_allowed src
-j DROP
ExecStop=/sbin/ipset destroy sftp_allowed

[Install]
WantedBy=multi-user.target
```

```
sudo systemctl daemon-reload
sudo systemctl enable --now docker-sftp-filter.service # primera vez
sudo systemctl restart docker-sftp-filter.service # modificación servicio
```

- despersistir:

```
sudo systemctl stop docker-sftp-filter.service      # ejecuta ExecStop: borra
la regla y el set
sudo systemctl disable docker-sftp-filter.service  # que no vuelva a
aplicarse al arrancar
```

iptables

1 IP

- **sudo iptables -I DOCKER-USER -i eth0 -p tcp -m conntrack --ctorigdstport 2222 --ctdir ORIGINAL ! -s 88.26.243.132 -j DROP**

- [/etc/systemd/system/docker-sftp-filter.service](#)

```
[Unit]
Description=Restringir puerto 2222 a IP autorizada
After=docker.service
Requires=docker.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/iptables -I DOCKER-USER -i eth0 -p tcp -m conntrack --
ctorigdstport 2222 --ctdir ORIGINAL ! -s 88.26.243.132 -j DROP
ExecStop=/sbin/iptables -D DOCKER-USER -i eth0 -p tcp -m conntrack --
ctorigdstport 2222 --ctdir ORIGINAL ! -s 88.26.243.132 -j DROP

[Install]
WantedBy=multi-user.target
```

- **sudo systemctl daemon-reload**
sudo systemctl enable --now docker-sftp-filter.service

+ 1 IP

Primero el DROP general del puerto 2222

```
sudo iptables -I DOCKER-USER 1 -i eth0 -p tcp -m conntrack --ctorigdstport 2222 --ctdir ORIGINAL -j DROP
```

Después, por encima, cada IP autorizada

```
sudo iptables -I DOCKER-USER 1 -i eth0 -p tcp -m conntrack --ctorigdstport 2222 --ctdir ORIGINAL -s 88.26.243.132 -j RETURN
```

```
sudo iptables -I DOCKER-USER 1 -i eth0 -p tcp -m conntrack --ctorigdstport 2222 --ctdir ORIGINAL -s 203.0.113.10 -j RETURN
```

diagnósticos

```
nc -zv <IP_SERVIDOR> 2221
```

```
sftp -vvv -P 2221 clienteA@<IP_SERVIDOR>
```

```
sudo ss -tlnp | grep -E '2221'
```

From:

<https://matebcn.eu/> - miguel angel torres egea

Permanent link:

<https://matebcn.eu/tech:docker:restriccion-ip>

Last update: **29/09/2026 12:41**

