

♦ **nftables** es el **reemplazo moderno de iptables** en Linux.

♦ **iptables**

- Herramienta clásica de firewall en Linux (años 2000 en adelante).
 - Trabaja con **tablas y cadenas** (filter, nat, mangle).
 - Cada regla se procesa de manera **lineal**, lo que puede ralentizar con muchas reglas.
 - Ha sido la base en la mayoría de distribuciones Linux durante años.
-

♦ **nftables**

- Introducido en el **kernel 3.13 (2014)** como sucesor de iptables.
 - Diseñado para unificar: **iptables, ip6tables, arptables y ebtables** → un solo framework.
 - Sintaxis más clara y **más compacta** (menos reglas redundantes).
 - Usa un **único binario (nft)** para todo.
 - Permite **estructuras más eficientes** (conjuntos, mapas) → mejor rendimiento con muchas reglas.
 - Compatible con IPv4 e IPv6 de forma unificada.
-

♦ **Situación actual**

- **Distribuciones modernas (Debian, Ubuntu, Fedora, RHEL, Parrot OS)** ya incluyen **nftables como sistema por defecto**.
 - Aun así, iptables sigue presente por **compatibilidad**, pero internamente muchas veces es una “capa” que traduce reglas a nftables (ej: iptables-nft).
 - El **futuro** es nftables → iptables quedará en desuso.
-

♦ **Fichero de configuración**

- nftables → /etc/nftables.conf
 - iptables → /etc/iptables/rules.v4 (en Debian/Ubuntu) o /etc/sysconfig/iptables (en RHEL/CentOS).
-

Ejercicios básicos con nftables

1 Ver configuración actual

Enunciado: Muestra las reglas activas en el firewall.

Solución:

sudo nft list ruleset

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > sudo nft list ruleset
# Warning: table ip filter is managed by iptables-nft, do not touch!
table ip filter {
    chain ufw-before-logging-input {
    }

    chain ufw-before-logging-output {
    }

    chain ufw-before-logging-forward {
    }

    chain ufw-before-input {
        iifname "lo" counter packets 6 bytes 300 accept
        ct state related,established counter packets 12685 bytes 19856840 accept
        ct state invalid counter packets 7 bytes 420 jump ufw-logging-deny
        ct state invalid counter packets 7 bytes 420 drop
        ip protocol icmp icmp type destination-unreachable counter packets 0 bytes 0 accept
        ip protocol icmp icmp type time-exceeded counter packets 0 bytes 0 accept
        ip protocol icmp icmp type parameter-problem counter packets 0 bytes 0 accept
        ip protocol icmp icmp type echo-request counter packets 0 bytes 0 accept
        udp sport 67 udp dport 68 counter packets 2 bytes 656 accept
        counter packets 556 bytes 449897 jump ufw-not-local
        ip daddr 224.0.0.251 udp dport 5353 counter packets 0 bytes 0 accept
        ip daddr 239.255.255.250 udp dport 1900 counter packets 0 bytes 0 accept
        counter packets 556 bytes 449897 jump ufw-user-input
    }
}
```

2 Limpiar reglas

Enunciado: Borra todas las reglas del firewall para empezar limpio.

Solución:

sudo nft flush ruleset

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft flush ruleset
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft list ruleset
```

3 Crear una tabla y cadena de filtrado

Enunciado: Crea una tabla llamada filtro para IPv4 con una cadena entrada.

Solución:

sudo nft add table inet filtro

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add table inet filtro
```

sudo nft add chain inet filtro entrada { type filter hook input priority 0; }

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add chain inet filtro entrada '{ type filter hook inp
ut priority 0; }'
```

4 Permitir SSH (puerto 22) y bloquear todo lo demás

Enunciado: Configura nftables para aceptar solo conexiones SSH entrantes.

Solución:

```
sudo nft add rule inet filtro entrada tcp dport 22 accept
```

```
sudo nft add rule inet filtro entrada drop
```

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add rule inet filtro entrada tcp dport 22 accept
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add rule inet filtro entrada drop
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft list ruleset
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        drop
    }
}
```

5 Permitir tráfico local

Enunciado: Asegura que el tráfico de lo (loopback) siempre está permitido.

Solución:

```
sudo nft add rule inet filtro entrada iif lo accept
```

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add rule inet filtro entrada iif lo accept
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft list ruleset
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        drop
        iif "lo" accept
    }
}
```

6 Permitir navegación web

Enunciado: Permite tráfico entrante a puertos HTTP (80) y HTTPS (443).

Solución:

`sudo nft add rule inet filtro entrada tcp dport {80, 443} accept`

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft add rule inet filtro entrada 'tcp dport {80, 443, 50}
accept'

~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft list ruleset
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        drop
        iif "lo" accept
        tcp dport { 50, 80, 443 } accept
    }
}
```

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept # handle 2
        drop # handle 3
        iif "lo" accept # handle 4
        tcp dport { 50, 80, 443 } accept # handle 6
    }
}
```

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft delete rule inet filtro entrada handle 3

~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft list ruleset
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        iif "lo" accept
        tcp dport { 50, 80, 443 } accept
    }
}
```

7 Bloquear acceso desde una IP concreta

Enunciado: Bloquea todo el tráfico entrante desde la IP 192.168.1.50.

Solución:

```
sudo nft add rule inet filtro entrada ip saddr 192.168.1.50 drop
```

```
~ > ss -tupnlis seguridad_informatica_2025 main ?1 > sudo nft delete rule inet filtro entrada
Netid:Stateax erRecv-QSend-Qed droLocalAddress:Porte  Peer Address:Port Process
udp:UNCONNinet0filtro0entrada drop 0.0.0.0:39344 0.0.0.0:*
udp ESTAB 0 0 192.168.0.121%eth0:68 192.168.0.1:67
udp UNCONN 0 0 127.0.0.1:18120 0.0.0.0:*
udp:UNCONNcios0seguri0ad_informatica_200.0.0.0:1812 sudo nft 0.0.0.0:*net filtro e
udp:UNCONNx error, unexpected inet 0.0.0.0:1813 0.0.0.0:*
udp:UNCONNfiltro0 entrada drop [::]:1812 [::]:*
udp UNCONN 0 0 [::]:1813 [::]:*
udp UNCONN 0 0 [::]:38847 [::]:*
tcp:LISTENcios0seguri128_informatica_200.0.0.0:22 sudo nft 0.0.0.0:*filtro entra
tcp:ESTABax error, unexpected str192.168.0.121:59006 54.171.145.158:443 users:(
tcp:TIME-WAIT0rada drop 192.168.0.121:39718 104.18.32.47:443
tcp TIME-WAIT 0 0 192.168.0.121:32776 34.36.137.203:443
tcp ESTAB 0 0 192.168.0.121:22 192.168.0.65:32743
```

```
PS C:\Users\2-DAW> ssh csubires@192.168.0.121
The authenticity of host '192.168.0.121 (192.168.0.121)' can't be established.
ED25519 key fingerprint is SHA256:ZfpsKoPyRh/gaHixWsr18ggjAH0VqVxBh9TYI69b2w.
This host key is known by the following other names/addresses:
  C:\Users\2-DAW/.ssh/known_hosts:1: 192.168.0.78
  C:\Users\2-DAW/.ssh/known_hosts:4: 192.168.0.41
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.121' (ED25519) to the list of known host
csubires@192.168.0.121's password:
Last login: Mon Sep 29 14:50:40 CEST 2025 from ::1 on ssh
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 29 14:50:40 2025 from ::1
(csubires@ kali)-[~]
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft insert rule inet filtro entrada ip saddr 192.168.0.65 drop
~/Documents/Ejercicios_seguridad_informatica_2025 main ?1 > sudo nft -a list chain inet filtro entrada
table inet filtro {
  chain entrada { # handle 1
    type filter hook input priority filter; policy accept;
    ip saddr 192.168.0.65 drop # handle 10
    tcp dport 22 accept # handle 2
    iif "lo" accept # handle 4
    tcp dport { 50, 80, 443 } accept # handle 6
  }
}
```

```
PS C:\Users\2-DAW> ssh csubires@192.168.0.121
ssh: connect to host 192.168.0.121 port 22: Connection timed out
PS C:\Users\2-DAW>
```


8 Registrar intentos bloqueados

Enunciado: Añade una regla para que los intentos de conexión denegados queden registrados en el log del sistema.

Solución:

```
sudo nft add rule inet filtro entrada log prefix "Bloqueado: " flags all
```

```
sudo nft add rule inet filtro entrada drop
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada 'log prefix "Bloqueado: " flags ip options'
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft list ruleset
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        iif "lo" accept
        tcp dport { 50, 80, 443 } accept
        log prefix "Bloqueado: " flags ip options
    }
}
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft insert rule inet filtro entrada drop
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        drop # handle 14
        tcp dport 22 accept # handle 2
        iif "lo" accept # handle 4
        tcp dport { 50, 80, 443 } accept # handle 6
        log prefix "Bloqueado: " flags ip options # handle 13
    }
}
```

clear

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > dmesg | grep "Bloqueado:"
[ 3701.780296] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=52 TOS=0x00 PREC=0x00
TTL=242 ID=50612 DF PROTO=TCP SPT=443 DPT=49814 WINDOW=194 RES=0x00 ACK URGP=0
[ 3701.900058] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=142.250.200.67 DST=192.168.0.121 LEN=125 TOS=0x00 PREC=0x00
TTL=116 ID=46615 PROTO=TCP SPT=443 DPT=55998 WINDOW=1048 RES=0x00 ACK PSH URGP=0
[ 3703.122570] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:2c:41:38:ac:7d:1c:08:00 SRC=192.168.0.60 DST=192.168.1.255 LEN=32 TOS=0x00 PREC=0x00 TT
L=128 ID=10314 PROTO=UDP SPT=61628 DPT=2000 LEN=12
[ 3713.917993] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:2c:41:38:ac:7d:1c:08:00 SRC=192.168.0.60 DST=192.168.1.255 LEN=32 TOS=0x00 PREC=0x00 TT
L=128 ID=10315 PROTO=UDP SPT=53411 DPT=2000 LEN=12
[ 3717.784728] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=52 TOS=0x00 PREC=0x00
TTL=242 ID=50613 DF PROTO=TCP SPT=443 DPT=49814 WINDOW=194 RES=0x00 ACK URGP=0
[ 3718.591214] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:da:3a:ec:84:9f:88:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=346 TOS=0x10 PREC=0x00 TTL=
64 ID=0 DF PROTO=UDP SPT=68 DPT=67 LEN=326
[ 3719.618711] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:da:3a:ec:84:9f:88:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=356 TOS=0x10 PREC=0x00 TTL=
64 ID=0 DF PROTO=UDP SPT=68 DPT=67 LEN=336
[ 3724.702118] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:2c:41:38:ac:7d:1c:08:00 SRC=192.168.0.60 DST=192.168.1.255 LEN=32 TOS=0x00 PREC=0x00 TT
L=128 ID=10316 PROTO=UDP SPT=58438 DPT=2000 LEN=12
[ 3733.793329] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=52 TOS=0x00 PREC=0x00
TTL=242 ID=50614 DF PROTO=TCP SPT=443 DPT=49814 WINDOW=194 RES=0x00 ACK URGP=0
[ 3735.576213] Bloqueado: IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:2c:41:38:ac:7d:1c:08:00 SRC=192.168.0.60 DST=192.168.1.255 LEN=32 TOS=0x00 PREC=0x00 TT
L=128 ID=10317 PROTO=UDP SPT=56450 DPT=2000 LEN=12
[ 3742.510277] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=52 TOS=0x00 PREC=0x00
TTL=242 ID=10829 DF PROTO=TCP SPT=443 DPT=49806 WINDOW=111 RES=0x00 ACK URGP=0
[ 3742.510375] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=98 TOS=0x00 PREC=0x00
TTL=242 ID=10830 DF PROTO=TCP SPT=443 DPT=49806 WINDOW=111 RES=0x00 ACK PSH URGP=0
[ 3744.700801] Bloqueado: IN=eth0 OUT= MAC=08:00:27:d1:f8:5d:00:a0:26:d2:68:9a:08:00 SRC=54.171.145.158 DST=192.168.0.121 LEN=113 TOS=0x00 PREC=0x00
```

9 Guardar configuración

Enunciado: Haz que las reglas persistan tras reiniciar.

Solución:

```
sudo sh -c "nft list ruleset > /etc/nftables.conf"
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept # handle 2
        iif "lo" accept # handle 4
        tcp dport { 50, 80, 443 } accept # handle 6
    }
}

~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft delete rule inet filtro entrada handle 6

~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada 'tcp dport {80, 443} accept'

~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada 'udp dport {53} accept'

~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept # handle 2
        iif "lo" accept # handle 4
        tcp dport { 80, 443 } accept # handle 16
        udp dport 53 accept # handle 17
    }
}
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo sh -c "nft list ruleset > /etc/nftables.conf"

~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo cat /etc/nftables.conf
table inet filtro {
    chain entrada {
        type filter hook input priority filter; policy accept;
        tcp dport 22 accept
        iif "lo" accept
        tcp dport { 80, 443 } accept
        udp dport 53 accept
    }
}
```

10 Ejercicio final

Enunciado:

Configura nftables para que tu servidor:

- Permita tráfico de loopback (lo).
- Acepte SSH (22), HTTP (80), HTTPS (443).
- Bloquee todo lo demás y registre intentos.

Solución (resumen):

```
sudo nft flush ruleset
```

```
sudo nft add table inet filtro
```

```
sudo nft add chain inet filtro entrada { type filter hook input priority 0; }
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list tables
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft flush ruleset
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add table inet filtro
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add chain inet filtro entrada '{ type filter hook input priority 0; }'
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
    }
}
```

```
sudo nft add rule inet filtro entrada iif lo accept
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada iif lo accept
```

```
sudo nft add rule inet filtro entrada tcp dport {22,80,443} accept
```

```
sudo nft add rule inet filtro entrada log prefix "Bloqueado: " flags all
```

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada 'tcp dport {22, 80, 443} accept'
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada 'log prefix "Bloqueado: " flags all'
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        iif "lo" accept # handle 2
        tcp dport { 22, 80, 443 } accept # handle 4
        log prefix "Bloqueado: " flags all # handle 5
    }
}
```


sudo nft add rule inet filtro entrada drop

```
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft add rule inet filtro entrada drop
~/Documents/Ejercicios_seguridad_informatica_2025 main > sudo nft -a list chain inet filtro entrada
table inet filtro {
    chain entrada { # handle 1
        type filter hook input priority filter; policy accept;
        iif "lo" accept # handle 2
        tcp dport { 22, 80, 443 } accept # handle 4
        log prefix "Bloqueado: " flags all # handle 5
        drop # handle 6
    }
}
```

