Tallafocs i iptables

Índex

1. Introducció als tallafocs

Un **tallafoc** (*firewall*) és un sistema de seguretat que controla el trànsit de xarxa entrant i sortint basant-se en un conjunt de regles predefinides. Actua com a barrera entre xarxes de confiança (xarxa interna) i xarxes no fiables (Internet).

1.1. Tipus de tallafocs

Tipus	Descripció
Filtratge de paquets	Analitza cada paquet de manera independent (IP, port, protocol)
Stateful (amb estat)	Segueix l'estat de les connexions (NEW, ESTABLISHED, RELATED, INVALID)
Proxy / capa d'aplicació	Analitza el contingut (capa 7 OSI), com ara HTTP, FTP, DNS
NGFW (Next-Generation)	Combina filtratge, IDS/IPS, inspecció profunda de paquets (DPI)
WAF (Web Application)	Especialitzat en trànsit HTTP/HTTPS per protegir aplicacions web

1.2. Tallafocs per maquinari vs. programari

- **Maquinari:** dispositius dedicats (Cisco ASA, Fortinet, pfSense en maquinari dedicat). Alta disponibilitat i rendiment.
- **Programari:** s'executen al sistema operatiu (iptables, nftables, ufw, firewalld). Més flexibles i econòmics.

2. El subsistema Netfilter

Netfilter és el marc de filtratge de paquets integrat al nucli (*kernel*) de Linux. Totes les eines de tallafoc de Linux (iptables, nftables, ufw, firewalld) interaccionen amb Netfilter.

2.1. Punts d'ancoratge (hooks)

El trànsit de xarxa passa per diferents punts del kernel on Netfilter pot interceptar-lo.

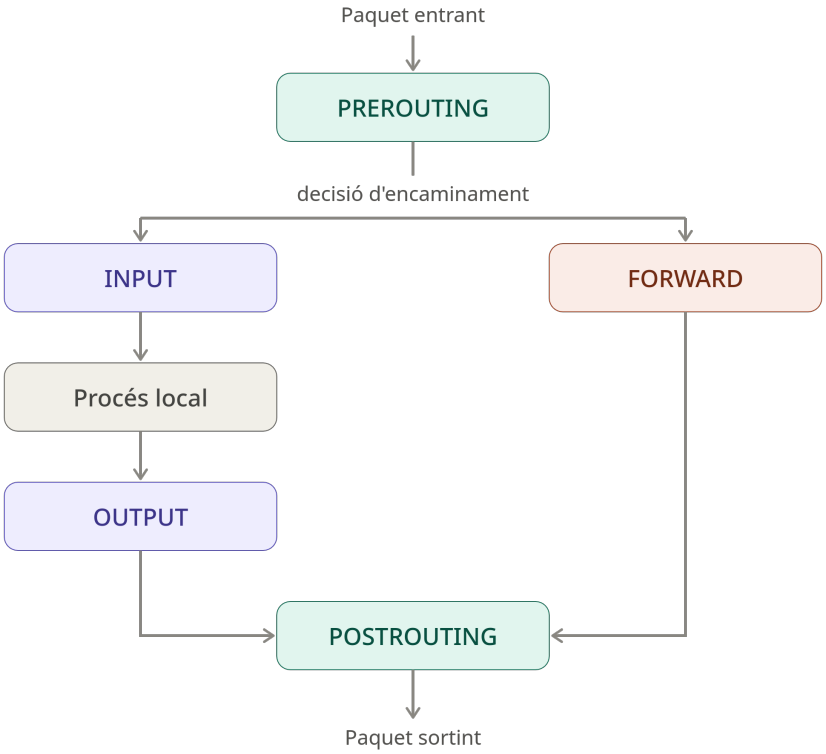

Figura 1: Flux de paquets Netfilter

3. `iptables`

3.1. Descripció

`iptables` és la interfície d'espai d'usuari clàssica per configurar les regles de Netfilter a Linux. Treballa amb **taules**, **cadenes** i **regles**.

> **Nota:** En sistemes moderns, `iptables` ha estat substituït per `nftables`, però segueix sent àmpliament usat i present a la majoria de distribucions.

3.2. Instal·lació

```
# Debian/Ubuntu
sudo apt install iptables iptables-persistent

# Fedora/RHEL
sudo dnf install iptables iptables-services

# Arch/Manjaro
sudo pacman -S iptables
```

3.3. Taules

`iptables` organitza les regles en **taules** segons la seva funció:

Taula	Funció
`filter`	Filtratge de paquets (per defecte). Cadenes: INPUT, OUTPUT, FORWARD
`nat`	Traducció d'adreces (NAT). Cadenes: PREROUTING, OUTPUT, POSTROUTING
`mangle`	Modificació de capçaleres de paquets. Totes les cadenes
`raw`	Processament abans del seguiment de connexions
`security`	Etiquetes SELinux en paquets

3.4. Cadenes predefinides

Cada taula conté cadenes on s'apliquen les regles:

Cadena	On s'aplica
`INPUT`	Paquets destinats al sistema local
`OUTPUT`	Paquets originats al sistema local
`FORWARD`	Paquets que passen pel sistema (encaminament)
`PREROUTING`	Paquets en arribar, abans de la decisió d'encaminament
`POSTROUTING`	Paquets en sortir, després de la decisió d'encaminament

3.5. Polítiques per defecte (targets)

Target	Acció
`ACCEPT`	Accepta el paquet
`DROP`	Descarta el paquet silenciosament
`REJECT`	Rebutja el paquet enviant un missatge d'error
`LOG`	Registra el paquet al log del sistema
`MASQUERADE`	NAT dinàmic (per a IP dinàmiques)
`SNAT`	Source NAT (canvia IP origen)
`DNAT`	Destination NAT (canvia IP destí, port forwarding)
`RETURN`	Torna a la cadena pare

4. Sintaxi d'`iptables`

```
iptables [-t taula] ORDRE cadena [criteris] [-j target]
```

4.1. Ordres principals

Ordre	Descripció
`-A cadena`	Afegeix una regla al final de la cadena
`-I cadena [n]`	Insereix una regla a la posició n (per defecte 1)
`-D cadena n`	Elimina la regla número n de la cadena
`-D cadena regla`	Elimina la regla especificada
`-R cadena n`	Substitueix la regla número n
`-L [cadena]`	Llista les regles
`-F [cadena]`	Buida totes les regles de la cadena
`-X [cadena]`	Elimina una cadena personalitzada
`-Z [cadena]`	Posa a zero els comptadors
`-P cadena target`	Estableix la política per defecte
`-N cadena`	Crea una nova cadena personalitzada
`-n`	No resol noms (mostra IP i ports numèrics)
`-v`	Mode verbose (mostra comptadors)

4.2. Criteris (condicions de la regla)

```
-p protocol          # tcp, udp, icmp, all
-s adreça            # IP o xarxa origen
-d adreça            # IP o xarxa destí
-i interfície        # Interfície d'entrada (eth0, lo...)
-o interfície        # Interfície de sortida
--sport port         # Port origen
--dport port         # Port destí
--dport port1:port2  # Rang de ports
-m state --state ESTATS  # Estat de la connexió
```

```
-m multiport --dports p1,p2,p3  # Múltiples ports
-m limit --limit N/s  # Limitar freqüència
! -s adreça          # Negació
```

5. Exemples pràctics

5.1. Consultar les regles actuals

```
# Llistar regles de la taula filter
sudo iptables -L
sudo iptables -L -n -v         # Amb comptadors i sense resolució de
 ↪  noms
sudo iptables -L -n -v --line-numbers  # Amb números de línia

# Llistar una cadena concreta
sudo iptables -L INPUT -n -v

# Llistar taula NAT
sudo iptables -t nat -L -n -v
```

5.2. Polítiques per defecte

```
# Política restrictiva: denegar tot per defecte
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT

# Política permissiva (menys segura)
sudo iptables -P INPUT ACCEPT
sudo iptables -P OUTPUT ACCEPT
```

5.3. Regles bàsiques d'acceptació

```
# Permetre trànsit de loopback (imprescindible)
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT

# Permetre connexions establertes i relacionades
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Permetre ICMP (ping)
sudo iptables -A INPUT -p icmp -j ACCEPT

# Permetre SSH (port 22)
```

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

# Permetre SSH només des d'una xarxa
sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 -j ACCEPT

# Permetre HTTP i HTTPS
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# Permetre DNS
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
```

5.4. Bloqueig de trànsit

```
# Bloquejar una IP concreta
sudo iptables -A INPUT -s 192.168.1.100 -j DROP

# Bloquejar un rang d'IPs
sudo iptables -A INPUT -s 10.0.0.0/8 -j DROP

# Bloquejar un port
sudo iptables -A INPUT -p tcp --dport 23 -j DROP   # Telnet

# Bloquejar trànsit sortint cap a un host
sudo iptables -A OUTPUT -d 93.184.216.34 -j DROP
```

5.5. Registre de paquets (LOG)

```
# Registrar i després descartar
sudo iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix
 ↪  "SSH_INTENT: " --log-level 4
sudo iptables -A INPUT -p tcp --dport 22 -j DROP

# Registrar intents de connexió denegats
sudo iptables -A INPUT -j LOG --log-prefix "IPTABLES_DROP: "
 ↪  --log-level 4
sudo iptables -A INPUT -j DROP
```

Els logs apareixen a `/var/log/kern.log` o via `journalctl -k`.

5.6. Limitació de connexions (protecció DDoS bàsica)

```
# Limitar intents de connexió SSH (màx. 3 per minut)
sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW \
    -m limit --limit 3/min --limit-burst 3 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP

# Protecció contra SYN flood
sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst
 ↪  3 -j ACCEPT
sudo iptables -A INPUT -p tcp --syn -j DROP
```

5.7. NAT i encaminament

```
# Activar l'encaminament IP al kernel
echo 1 > /proc/sys/net/ipv4/ip_forward
# O de manera permanent a /etc/sysctl.conf:
# net.ipv4.ip_forward = 1

# MASQUERADE: NAT per a connexions a Internet (IP dinàmica)
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# SNAT: NAT amb IP estàtica
sudo iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source
 ↪  203.0.113.1

# DNAT: port forwarding (redirigir port 80 extern al port 8080 intern)
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT
 ↪  --to-destination 192.168.1.10:8080

# Permetre el trànsit encaminat
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state
 ↪  ESTABLISHED,RELATED -j ACCEPT
```

5.8. Cadenes personalitzades

```
# Crear cadena personalitzada
sudo iptables -N BLOQUEIG_ESPIA

# Afegir regles a la cadena
sudo iptables -A BLOQUEIG_ESPIA -s 192.168.1.50 -j DROP
sudo iptables -A BLOQUEIG_ESPIA -s 192.168.1.51 -j DROP

# Cridar la cadena des d'INPUT
sudo iptables -A INPUT -j BLOQUEIG_ESPIA
```

6. Persistència de les regles

Les regles d'`iptables` es perden en reiniciar el sistema. Per fer-les persistents:

Debian/Ubuntu

```
# Guardar les regles actuals
sudo iptables-save > /etc/iptables/rules.v4
sudo ip6tables-save > /etc/iptables/rules.v6

# Restaurar manualment
sudo iptables-restore < /etc/iptables/rules.v4

# Amb iptables-persistent (es restauren automàticament en arrencar)
sudo apt install iptables-persistent
sudo netfilter-persistent save
```

Fedora/RHEL

```
sudo systemctl enable --now iptables
sudo service iptables save
# Les regles es desen a /etc/sysconfig/iptables
```

Arch Linux

```
# Desar regles
sudo iptables-save > /etc/iptables/iptables.rules

# Habilitar el servei de restauració
sudo systemctl enable --now iptables
```

7. Script de tallafoc complet

```
#!/bin/bash
# firewall.sh --- Configuració bàsica de tallafoc amb iptables

set -e

IPT="iptables"

echo "Aplicant regles de tallafoc..."
```

```
# --- Buidar regles existents ---
$IPT -F
$IPT -X
$IPT -t nat -F
$IPT -t nat -X
$IPT -t mangle -F
$IPT -t mangle -X

# --- Política per defecte: denegar tot ---
$IPT -P INPUT DROP
$IPT -P FORWARD DROP
$IPT -P OUTPUT ACCEPT

# --- Loopback ---
$IPT -A INPUT -i lo -j ACCEPT

# --- Connexions establertes ---
$IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# --- ICMP (ping) ---
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

# --- SSH (limitat a la xarxa local) ---
$IPT -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 \
     -m state --state NEW -j ACCEPT

# --- Web ---
$IPT -A INPUT -p tcp --dport 80 -j ACCEPT
$IPT -A INPUT -p tcp --dport 443 -j ACCEPT

# --- Log i descart del trànsit no permès ---
$IPT -A INPUT -j LOG --log-prefix "FW_DROP: " --log-level 4
$IPT -A INPUT -j DROP

echo "Tallafoc configurat correctament."
```

8. `nftables`: el successor d'`iptables`

`nftables` substitueix `iptables`, `ip6tables`, `arptables` i `ebtables` en una sola eina amb sintaxi unificada.

```
# Instal·lació
sudo apt install nftables      # Debian/Ubuntu
sudo dnf install nftables      # Fedora

# Veure les regles actuals
sudo nft list ruleset

# Exemple de configuració bàsica
sudo nft add table inet filter
```

```
sudo nft add chain inet filter input { type filter hook input priority
 ↪  0 \; policy drop \; }
sudo nft add rule inet filter input iif lo accept
sudo nft add rule inet filter input ct state established,related
 ↪  accept
sudo nft add rule inet filter input tcp dport 22 accept
sudo nft add rule inet filter input tcp dport { 80, 443 } accept
```

Fitxer de configuració: `/etc/nftables.conf`

9. Frontends per a `iptables`/`nftables`

9.1 `ufw` (Uncomplicated Firewall)

Frontend senzill per a Ubuntu/Debian:

```
sudo apt install ufw

# Habilitar/deshabilitar
sudo ufw enable
sudo ufw disable
sudo ufw status verbose

# Política per defecte
sudo ufw default deny incoming
sudo ufw default allow outgoing

# Permetre serveis
sudo ufw allow ssh
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow from 192.168.1.0/24 to any port 22

# Denegar
sudo ufw deny 23/tcp

# Eliminar regla
sudo ufw delete allow 80/tcp

# Logs
sudo ufw logging on
```

9.2 `firewalld`

Frontend dinàmic usat a Fedora, RHEL, CentOS:

```
sudo systemctl enable --now firewalld

# Zones disponibles (public, home, work, trusted, drop...)
firewall-cmd --list-all-zones
firewall-cmd --get-active-zones

# Zona per defecte
firewall-cmd --get-default-zone
firewall-cmd --set-default-zone=home

# Permetre serveis
firewall-cmd --permanent --add-service=ssh
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https

# Permetre port
firewall-cmd --permanent --add-port=8080/tcp

# Eliminar regla
firewall-cmd --permanent --remove-service=http

# Aplicar canvis permanents
firewall-cmd --reload

# Veure configuració de la zona activa
firewall-cmd --list-all
```

9.3 `fail2ban`

Complementa el tallafoc bloquejant IP amb massa intents fallits:

```
sudo apt install fail2ban

# Configuració: /etc/fail2ban/jail.local
[sshd]
enabled = true
port    = ssh
filter  = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime  = 3600
findtime = 600
```

10. ip6tables: IPv6

```
# Mateixa sintaxi que iptables però per a IPv6
sudo ip6tables -L -n -v
sudo ip6tables -P INPUT DROP
sudo ip6tables -A INPUT -i lo -j ACCEPT
sudo ip6tables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo ip6tables -A INPUT -p tcp --dport 22 -j ACCEPT
```

11. Bones pràctiques

1. **Política restrictiva per defecte:** `DROP` a INPUT i FORWARD; `ACCEPT` a OUTPUT.
2. **Loopback sempre permès:** les aplicacions locals el necessiten.
3. **Connexions ESTABLISHED primer:** per no tallar connexions actives.
4. **SSH abans de tancar tot:** evitar quedar-se sense accés remot.
5. **Provar amb `--dry-run` o en sessió local** abans d'aplicar canvis remots.
6. **Persistència:** desar les regles per sobreviure reinicis.
7. **Revisar regularment** les regles i eliminar les obsoletes.
8. **Logs:** registrar els paquets denegats per detectar intents d'atac.
9. **IPv6:** no oblidar configurar `ip6tables` / nftables per a IPv6.
10. **Principi de mínims privilegis:** obrir només els ports estrictament necessaris.

12. Comparativa d'eines

Eina	Basat en	Complexitat	Distros principals	Estat
`iptables`	Netfilter	Mitjana	Totes	Llegat
`nftables`	Netfilter	Mitjana	Totes (modern)	Actual
`ufw`	iptables/nft	Baixa	Ubuntu, Debian	Actiu
`firewalld`	nftables/ipt	Baixa-mitjana	Fedora, RHEL, CentOS	Actiu
`fail2ban`	iptables/nft	Baixa	Totes	Actiu
`pf`	BSD	Mitjana	FreeBSD, OpenBSD, macOS	Actiu (BSD)

13. Resum d'ordres

```
# Llistar regles
iptables -L -n -v --line-numbers

# Buidar tot
iptables -F && iptables -X

# Afegir regla (al final)
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
# Inserir regla (al principi)
iptables -I INPUT 1 -p tcp --dport 80 -j ACCEPT

# Eliminar regla per número
iptables -D INPUT 3

# Política per defecte
iptables -P INPUT DROP

# Desar regles
iptables-save > /etc/iptables/rules.v4

# Restaurar
iptables-restore < /etc/iptables/rules.v4

# NAT bàsic
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Port forwarding
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to
 ↪  192.168.1.10:80
```

14. Referències

- `man iptables` --- Manual complet
- `man iptables-extensions` --- Mòduls i extensions
- `man nft` --- Manual de nftables
- Netfilter.org --- Projecte oficial
- Arch Wiki: iptables
- Arch Wiki: nftables
- Arch Wiki: ufw
- Arch Wiki: firewalld

Versions d'aquest document

- HTML - iptables.html
- PDF - iptables.pdf
- ODT - iptables.odt
- MD - iptables.md