
RA4. Implantació de tallafocs

Índex

Introducció	1
1. Característiques, tipus i funcions dels tallafocs	2
1.1. Què és un tallafocs	2
1.2. Tipus de tallafocs	2
1.3. Funcions principals	2
2. Nivells de filtratge de trànsit	3
3. Planificació de la instal·lació de tallafocs	4
3.1. Ubicació dins la xarxa	4
3.2. Arquitectures típiques amb DMZ	4
3.3. Criteris de planificació	5
4. Configuració de filtres a partir d'un llistat de regles	5
4.1. Regles de filtratge: estructura general	5
4.2. Exemple amb nftables (Linux)	5
4.3. Exemple equivalent en un tallafocs perimetral (pfSense/OPNsense)	7
5. Revisió dels registres d'esdeveniments	8
5.1. Per què cal revisar els logs	8
5.2. On i com consultar-los	8
5.3. Què buscar	8
6. Proves de funcionament: opcions de programari i maquinari	9
6.1. Programari vs. maquinari	9
6.2. Sondeig i proves	9
7. Diagnòstic de problemes de connectivitat provocats pel tallafocs	10
7.1. Reproduir i acotar el problema	10
7.2. Comprovar la connectivitat capa a capa	10
7.3. Consultar els registres del tallafocs (enllaç directe amb 4.5)	11
7.4. Causes habituals de problemes de connectivitat provocats pel tallafocs	11
8. Documentació del tallafocs	11
8.1. Continguts mínims de la documentació	11
8.2. Exemple de plantilla de fitxa de regla	12

Cicle formatiu: Administració de sistemes informàtics en xarxa (ASIX)

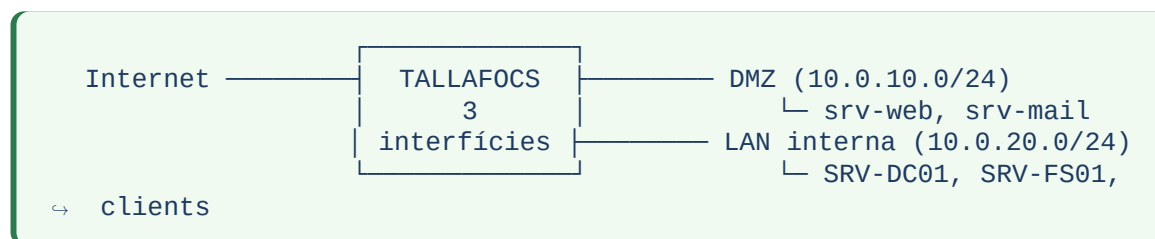
Mòdul: 0378. Seguretat i alta disponibilitat

Introducció

Un tallafocs (*firewall*) és l'element de seguretat perimetral més bàsic i, alhora, més crític de qualsevol infraestructura de xarxa. La seva funció és senzilla d'explicar, però delicada de configurar bé: decidir, paquet a paquet o connexió a connexió, què pot entrar i sortir d'una xarxa (o d'una màquina) i què no.

En aquesta unitat treballarem els vuit criteris d'avaluació del RA4, des de la teoria (tipus, nivells de filtratge) fins a la pràctica (regles amb `nftables` i amb un tallafocs perimetral tipus `pfSense/OPNsense`), passant per l'anàlisi de registres, les proves de funcionament i el diagnòstic d'incidències.

Com a escenari de referència farem servir un muntatge típic de xarxa docent, similar al del nostre laboratori **THOS.LOCAL**:



NOTA

Aquest disseny amb tres zones (Internet / DMZ / LAN) és el que farem servir com a fil conductor en tots els exemples pràctics de la unitat.

1. Característiques, tipus i funcions dels tallafocs

1.1. Què és un tallafocs

Un tallafocs és un sistema (maquinari, programari o una combinació dels dos) situat en un punt de la xarxa que **inspecciona el trànsit que hi circula i aplica una política de seguretat** definida per l'administrador, que permet o denega connexions segons un conjunt de regles.

Característiques bàsiques que ha de complir:

- **Tot el trànsit que ha de ser controlat hi ha de passar obligatòriament.** Si existeix una via alternativa (un mòdem 4G connectat a un equip intern, una xarxa Wi-Fi no controlada...), el tallafocs deixa de ser efectiu.
- **Només ha de deixar passar el trànsit autoritzat**, seguint el principi de **mínim privilegi** (denegar per defecte, permetre només el necessari).
- **Ha de ser resistent als atacs**, ja que és un dels elements més exposats de la infraestructura.
- No protegeix contra amenaces que no passen per ell: atacs interns, dispositius USB infectats, enginyeria social, etc.

1.2. Tipus de tallafocs

Tipus	Descripció	Exemple
Tallafocs de filtratge de paquets	Analitza capçaleres IP/TCP/UDP (IP origen/destí, ports, flags) sense mantenir estat de la connexió	iptables en mode <i>stateless</i> , ACL de router
Tallafocs d'estat (<i>stateful</i>)	Manté una taula d'estats de les connexions actives i permet respostes legítimes sense regla explícita	nftables, pf, la majoria de tallafocs actuals
Tallafocs d'aplicació / proxy (<i>application-layer</i>)	Actua a nivell 7, entén el protocol (HTTP, FTP, SMTP...) i pot filtrar continguts	Squid, WAF, proxy SMTP amb antispam
Tallafocs personal (<i>host-based</i>)	S'executa a la mateixa màquina que protegeix	Windows Defender Firewall, ufw/firewalld
Tallafocs perimetral (<i>network-based</i>)	Dispositiu dedicat entre xarxes, sol tenir diverses interfícies	pfSense, OPNsense, FortiGate, Cisco ASA
UTM / NGFW (<i>Next-Generation Firewall</i>)	Integra filtratge, IDS/IPS, antivirus, VPN, control d'aplicacions en un sol dispositiu	FortiGate, Palo Alto, Sophos XG

1.3. Funcions principals

1. **Filtratge de trànsit** segons adreces IP, ports, protocols o aplicacions.
2. **Traducció d'adreces (NAT/PAT)**, imprescindible per compartir una única IP pública.
3. **VPN** (terminació de túnels IPsec/WireGuard/OpenVPN per a accés remot o interconnexió de seus).
4. **Registre i auditoria** (logging) del trànsit permès i denegat.
5. **Balanceig de càrrega i alta disponibilitat** en els models més avançats (failover entre dos tallafocs).
6. **IDS/IPS integrat** per detectar i bloquejar signatures d'atac conegudes.

2. Nivells de filtratge de trànsit

El filtratge es pot fer a diferents capes del model OSI/TCP-IP. Com més amunt es filtra, més informació té el tallafocs però més cost de procés i més complexitat:

Capa	Exemples de criteri de filtratge	Tecnologia típica
Enllaç (2)	Adreça MAC	Filtratge MAC en switches/AP
Xarxa (3)	IP origen/destí, ICMP	ACL de router, iptables -s/-d
Transport (4)	Port TCP/UDP, flags TCP (SYN, ACK...), estat de connexió	Tallafocs <i>stateful</i> (nftables, pf)
Aplicació (7)	Contingut del protocol: URL, capçaleres HTTP, adjunts de correu, comandes FTP	Proxy, WAF, DPI (<i>Deep Packet Inspection</i>)

En la pràctica, un tallafocs modern combina diversos nivells alhora:

- **Filtratge de paquets (packet filtering):** decisió paquet a paquet, sense memòria de connexions anteriors. Ràpid, però limitat (no distingeix una resposta legítima d'un paquet fals amb el mateix port).
- **Filtratge amb inspecció d'estat (*stateful inspection*):** el tallafocs recorda les connexions que ell mateix ha permès i només cal obrir regla d'entrada per a les noves connexions; les respostes es permeten automàticament (estat ESTABLISHED, RELATED).
- **Filtratge a nivell d'aplicació:** entén el protocol i pot prendre decisions més fines (per exemple, permetre HTTP però bloquejar només certs URL, o permetre FTP però inspeccionar el canal de dades dinàmic obert pel mode passiu).

NOTA

És fonamental saber identificar a quin nivell es demana filtrar quan es dissenya una regla. Per exemple, "bloquejar l'accés a xarxes socials" no es pot resoldre només amb IP/port (moltes usen els mateixos CDN que altres serveis legítims): cal filtratge de capa 7 (per domini/SNI) o un proxy amb llistes de categories.

3. Planificació de la instal·lació de tallafocs

3.1. Ubicació dins la xarxa

La decisió d'on col·locar el tallafocs és tan important com la configuració de les regles. Els punts habituals són:

1. **Perímetre (Internet ↔ xarxa corporativa):** el més bàsic i imprescindible. Separa la xarxa interna d'Internet.
2. **Entre zones internes de diferent nivell de confiança** (per exemple, xarxa d'administració vs. xarxa d'aules, o xarxa de servidors vs. xarxa de clients). Aplica el principi de **segmentació**: si un segment es compromet, el tallafocs interior limita la propagació (moviment lateral).
3. **Davant d'una DMZ (zona desmilitaritzada):** xarxa intermèdia on es col·loquen els serveis que han de ser accessibles des d'Internet (web, correu, DNS públic) però que no han de tenir accés directe a la LAN interna.
4. **A escala d'amfitrió (host-based):** cada servidor o client amb el seu propi tallafocs local, com a capa addicional de seguretat (*defensa en profunditat*).

3.2. Arquitectures típiques amb DMZ

a) Tallafocs amb tres interfícies (arquitectura més habitual en centres educatius i pimes):

```
Internet — [WAN] TALLAFOCS [DMZ] — srv-web, srv-mail
                        [LAN] — xarxa interna
```

Un únic dispositiu amb tres (o més) interfícies físiques o VLANs, cadascuna amb la seva política. És l'arquitectura més senzilla d'administrar.

b) Doble tallafocs (arquitectura “back-to-back”):

```
Internet — TALLAFOCS EXTERN — DMZ — TALLAFOCS INTERN — LAN
```

Més segura (dos productes/fabricants diferents redueixen el risc que una vulnerabilitat afecti els dos alhora), però més cara i complexa de mantenir. Habitual en entorns d'alta seguretat.

3.3. Criteris de planificació

Abans de desplegar cal documentar:

- **Inventari de zones i actius:** quines xarxes existeixen, quins serveis corren a cada màquina, quins ports necessiten.
- **Matriu de fluxos:** qui ha de parlar amb qui i per quin port (origen, destí, protocol, port, justificació). Aquesta matriu és la base de les regles que es configuraran a 4.4.
- **Política per defecte:** recomanada *default deny* (es denega tot i només es permet el trànsit explícitament necessari), més segura que *default allow*.
- **Redundància:** si el tallafocs falla, cau tota la connectivitat que hi passa. Cal valorar un clúster actiu-passiu (per exemple amb CARP a pfSense/OPNsense o VRRP amb keepalived en Linux).
- **Dimensionament:** throughput necessari, nombre de connexions simultànies esperades, si cal inspecció SSL/TLS (consumeix molta CPU).

4. Configuració de filtres a partir d'un llistat de regles

4.1. Regles de filtratge: estructura general

Independentment del producte, una regla de tallafocs sol tenir aquests camps:

Interfície | Direcció | Protocol | IP origen | Port origen | IP destí
| Port destí | Acció | Log

Les accions habituals són **ACCEPT/PASS**, **DROP** (descarta sense avisar) i **REJECT** (descarta i respon amb un missatge d'error, per exemple ICMP *port unreachable*).

NOTA

DROP és preferible a REJECT en un tallafocs perimetral perquè no revela informació a un possible atacant (l'origen no sap si el port està tancat o filtrat). REJECT és útil en xarxes internes, on la resposta ràpida d'error facilita el diagnòstic als usuaris legítims.

4.2. Exemple amb nftables (Linux)

Suposem el tallafocs de l'escenari amb tres interfícies: eth0 (WAN), eth1 (DMZ, 10.0.10.0/24) i eth2 (LAN, 10.0.20.0/24).

```
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # Trànsit ja establert o relacionat, sempre permès
```

```

    ct state established,related accept
    ct state invalid drop

    # Loopback
    iif lo accept

    # Gestió del propi tallafocs només des de la LAN, per SSH
    iif eth2 tcp dport 22 accept

    # Registre de la resta abans de descartar
    log prefix "INPUT-DROP: " drop
}

chain forward {
    type filter hook forward priority 0; policy drop;

    ct state established,related accept
    ct state invalid drop

    # Internet -> DMZ: només HTTP/HTTPS al servidor web i
    ↪ SMTP/IMAP al de correu
    iif eth0 oif eth1 ip daddr 10.0.10.10 tcp dport { 80, 443 }
    ↪ accept
    iif eth0 oif eth1 ip daddr 10.0.10.20 tcp dport { 25, 143, 993
    ↪ } accept

    # LAN -> Internet: navegació i DNS
    iif eth2 oif eth0 tcp dport { 80, 443 } accept
    iif eth2 oif eth0 udp dport 53 accept

    # LAN -> DMZ: administració del servidor web des de la LAN
    iif eth2 oif eth1 ip daddr 10.0.10.10 tcp dport 22 accept

    # La DMZ MAI ha d'iniciar connexions cap a la LAN
    iif eth1 oif eth2 drop

    log prefix "FORWARD-DROP: " drop
}

chain output {
    type filter hook output priority 0; policy accept;
}
}

```

Punts clau d'aquest exemple:

- La política per defecte (policy drop) de les cadenes input i forward implementa el principi *default deny*.
- ct state established,related accept és el que permet el filtratge amb estat: no cal obrir regla d'entrada per a les respostes.
- La regla iif eth1 oif eth2 drop és explícita per **deixar constància** de la decisió de disseny (la DMZ és una zona no confiable i mai ha d'iniciar trànsit cap a la LAN), encara que la política per defecte ja ho denegaria.

- Cada bloc que descarta trànsit no esperat es registra (log prefix) abans de fer drop, per poder-ho revisar després (vegeu 4.5).

4.3. Exemple equivalent en un tallafocs perimetral (pfSense/OPNsense)

En aquest tipus de producte les regles es defineixen per interfície, amb interfície gràfica, però segueixen la mateixa lògica. Per a la interfície **WAN**:

#	Protocol	Origen	Port origen	Destí	Port destí	Acció
1	TCP	*	*	10.0.10.10 (web)	80, 443	Pass
2	TCP	*	*	10.0.10.20 (mail)	25, 143, 993	Pass
3	*	*	*	*	*	Block (implícita)

Per a la interfície **LAN**:

#	Protocol	Origen	Port origen	Destí	Port destí	Acció
1	UDP	LAN net	*	Aquest tallafocs	53	Pass
2	TCP	LAN net	*	*	80, 443	Pass
3	TCP	LAN net	*	10.0.10.10	22	Pass
4	*	*	*	*	*	Block (implícita)

NOTA

A pfSense/OPNsense les regles s'avaluen **de dalt cap avall i s'atura en la primera coincidència** (com a iptables), i sempre hi ha una regla implícita final de *block* a cada interfície. Cal tenir molt present aquest ordre: una regla massa genèrica situada abans pot “tapar” regles més específiques posades després.

5. Revisió dels registres d'esdeveniments

5.1. Per què cal revisar els logs

Configurar les regles no és suficient: cal **verificar que fan el que es pretenia**. Els registres (logs) del tallafocs permeten:

- Confirmar que el trànsit legítim passa i el no autoritzat es bloqueja.
- Detectar intents d'accés no autoritzat (escanejos de ports, força bruta) o mala configuració (una regla massa restrictiva que bloqueja trànsit vàlid).
- Fer forense després d'un incident.
- Complir requisits normatius d'auditoria (ENS, RGPD en el que sigui aplicable).

5.2. On i com consultar-los

A **Linux (nftables/iptables)**, els paquets marcats amb log es registren via `journald/syslog`:

```
# Veure en temps real
journalctl -k -f | grep 'FORWARD-DROP'

# Comptar quants intents s'han bloquejat per IP origen en l'última
↪ hora
journalctl -k --since "-1 hour" | grep 'INPUT-DROP' | grep -oP
↪ 'SRC=\K[\d.]+' | sort | uniq -c | sort -rn
```

A **pfSense/OPNsense**, l'apartat *Status* → *System Logs* → *Firewall* mostra taula amb interfície, acció, origen/destí i regla que ha coincidit, amb possibilitat de filtrar en temps real.

Centralització: en un entorn amb diversos tallafocs (o simplement per no dependre de logs locals que roten), és recomanable enviar-los a un **servidor de logs centralitzat** (syslog remot, Wazuh, Graylog...) per correlacionar-los amb altres fonts (IDS, servidors) i generar alertes.

5.3. Què buscar

Patró als logs	Possible interpretació
Molts DROP des d'una mateixa IP origen a ports consecutius en poc temps	Escaneig de ports (nmap)
DROP repetit del mateix client cap al mateix servei intern	Regla mal configurada bloquejant trànsit legítim → revisar
Pics sobtats de trànsit ACCEPT cap a un port poc habitual	Possible exfiltració o servei no autoritzat aixecat sense permís
Molts intents SSH/RDP fallits des de l'exterior	Atac de força bruta → valorar fail2ban, canvi de port o VPN obligatòria

6. Proves de funcionament: opcions de programari i maquinari

6.1. Programari vs. maquinari

	Programari (nftables, pf, ufw...)	Maquinari dedicat (Fortigate, Cisco ASA, aparell pfSense)
Cost	Baix (sovint lliure), aprofita maquinari genèric	Alt, però rendiment garantit pel fabricant
Rendiment	Depèn del maquinari on s'instal·la; pot patir amb molt trànsit o inspecció TLS	ASIC/hardware dedicat per a xifratge i inspecció a alta velocitat
Flexibilitat	Molt alta, totalment personalitzable, s'integra amb scripts	Limitada a les funcions del fabricant, encara que sol ser molt completa
Manteniment	Requereix més coneixement tècnic intern	Suport oficial del fabricant, actualitzacions de firmware
Cas d'ús típic	Laboratoris, entorns amb personal tècnic, virtualització	Entorns de producció crítics, requisits de certificació

En un centre educatiu és habitual combinar totes dues coses: un tallafocs perimetral (programari com OPNsense sobre maquinari genèric, o un aparell comercial) i tallafocs locals a cada servidor (firewall, Windows Defender Firewall) com a capa addicional.

6.2. Sondeig i proves

Un cop desplegades les regles, cal **provar-les activament**, no donar per fet que funcionen:

Des de fora cap al tallafocs (comprovar que només s'obre el necessari):

```
# Escaneig de ports TCP contra la IP pública/WAN
nmap -sS -p 1-1000 <IP_WAN>

# Comprovar un port concret
nmap -p 443 <IP_WAN>

# Petició real al servei per confirmar que respon correctament
curl -I https://<IP_WAN>
```

Des de la LAN cap a l'exterior o la DMZ (comprovar que el permès funciona i el prohibit es bloqueja):

```
# Ha de funcionar (permès a la matriu de fluxos)
curl -I https://www.exemple.cat

# Ha de fallar/bloquejar-se (LAN -> DMZ per un port no autoritzat)
nc -zv -w2 10.0.10.10 21
```

Comprovació de l'estat de les connexions al mateix tallafocs:

```
# nftables: veure la taula d'estats de connexió
cat /proc/net/nf_conntrack | wc -l
conntrack -L | grep ESTABLISHED
```

Auditoria automatitzada de la configuració: eines com `nmap --script firewall-bypass` o revisions manuals de la política contra la matriu de fluxos prevista ajuden a detectar regles obsoletes o massa permissives (per exemple, una regla `any any any` oblidada d'una prova).

7. Diagnòstic de problemes de connectivitat provocats pel tallafocs

Quan un usuari reporta “no tinc accés a X”, el tallafocs sol ser el primer sospitós (i sovint, amb raó). Metodologia recomanada:

7.1. Reproduir i acotar el problema

- Des de quina IP/xarxa falla? Falla també des d'altres xarxes?
- Quin port/protocol/servei concret? (no és el mateix “no puc navegar” que “no puc enviar correu”)
- És total (cap paquet passa) o parcial (connecta, però es talla, va molt lent)?

7.2. Comprovar la connectivitat capa a capa

```
# Capa 3: hi ha ruta i respon l'equip?
ping <IP_desti>

# Capa 3/4: hi ha un salt (el tallafocs) que talla el camí?
traceroute <IP_desti>          # Linux
tracert <IP_desti>             # Windows

# Capa 4: el port concret és accessible?
nc -zv <IP_desti> <port>
telnet <IP_desti> <port>
```

Si el ping (ICMP) falla, però el servei real funciona (o a l'inrevés), sovint és perquè hi ha una regla que tracta l'ICMP de manera diferent del trànsit TCP/UDP --- un error de disseny relativament habitual.

7.3. Consultar els registres del tallafocs (enllaç directe amb 4.5)

Els logs solen donar la resposta immediata: buscar l'entrada DROP/REJECT corresponent a l'origen, destí i port del problema, i identificar quina regla (o la política per defecte) l'ha generat.

7.4. Causes habituals de problemes de connectivitat provocats pel tallafocs

Síntoma	Causa freqüent
Un servei intern deixa de ser accessible des de fora just després d'un canvi	Ordre de regles: una regla nova o modificada coincideix abans que l'específica (a <code>nftables/pfSense</code> , la primera coincidència guanya)
Les connexions s'obren, però es tallen als pocs segons	Temps d'espera (<i>timeout</i>) de la taula d'estats massa curt per a connexions de llarga durada
Un protocol amb port dinàmic (FTP actiu, SIP, algunes VPN) no funciona tot i tenir el port de control obert	Falta el mòdul d'ajuda de connexió (<i>connection tracking helper</i> , p. ex. <code>nft_conntrack_ftp</code>) que entengui el protocol i obri dinàmicament els ports necessaris
Funciona intern però no des d'Internet (o a l'inrevés)	Confusió entre regles de WAN/LAN/DMZ o entre INPUT (tràfic cap al mateix tallafocs) i FORWARD (trànsit que el travessa)
Alguns usuaris sí i altres no, mateix servei	Regla basada en IP origen concreta en lloc de xarxa/subxarxa, o resta d'una regla temporal de proves no eliminada
Tot funciona per IP però no per nom	No és problema del tallafocs sinó de resolució DNS; cal descartar-ho abans de "culpar" les regles

8. Documentació del tallafocs

Un tallafocs sense documentar és un risc de seguretat en si mateix: si la persona que el va configurar marxa, ningú sap per què existeix cada regla, i això porta a no gosar tocar-lo mai (regles obsoletes que s'acumulen) o a eliminar regles necessàries per error.

8.1. Continguts mínims de la documentació

1. **Esquema de xarxa** amb totes les zones, interfícies, VLANs i adreçament IP.
2. **Matriu de fluxos** (la treballada a 4.3), amb justificació de negoci/servei de cada flux permès.
3. **Llistat de regles** amb, per a cadascuna: propòsit, data d'alta, responsable de la petició i data de revisió/caducitat prevista (especialment important en regles "temporals").
4. **Procediment de gestió de canvis**: com se sol·licita, aprova i desplega un canvi a les regles (evita canvis improvisats sense registre).
5. **Procediment de còpia de seguretat i restauració** de la configuració del tallafocs.
6. **Procediment davant d'incidents**: què fer si es detecta un atac o una regla compromesa, a qui escalar-ho.
7. **Registre de canvis (cronologia)**: qui ha canviat què i quan (idealment amb control de versions si la configuració és fitxers de text, com en el cas de `nftables`).

8.2. Exemple de plantilla de fitxa de regla

```
### Regla: WEB-DMZ-HTTPS-01
- **Zones:** WAN -> DMZ
- **Origen:** any
- **Destí:** 10.0.10.10 (srv-web)
- **Port/Protocol:** TCP/443
- **Acció:** ACCEPT
- **Justificació:** publicació del web corporatiu
- **Sol·licitat per:** Direcció / Comunicació
- **Data d'alta:** 2026-02-10
- **Revisió prevista:** anual
```

NOTA

Per a la unitat, els mateixos fitxers de configuració comentats (nftables, regles de pfSense exportades en XML) ja constitueixen part de la documentació tècnica, sempre que es mantinguin sota control de versions (per exemple amb Git) i s'acompanyin de l'esquema de xarxa i la matriu de fluxos en un document a part.

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)