Tallafocs

Seguretat

- El principi bàsic dels mecanismes de seguretat dels Sistemes Informàtics és el de mantenir als intrusos fora de la xarxa
- Un dels sistemes bàsics per garantir aquest principi són els tallafocs

Seguretat

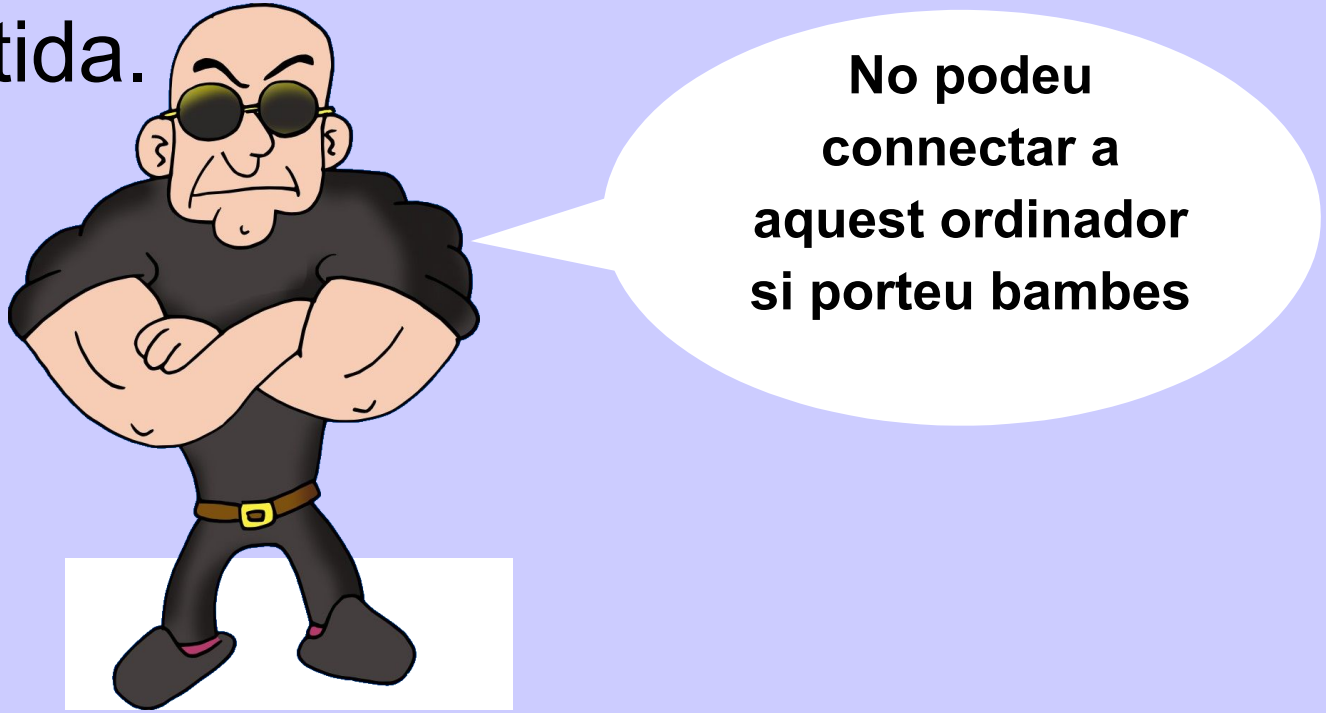
- A part dels tallafocs sempre s'ha de tenir present una de les regles bàsiques de la seguretat:

Només tenir engegats els serveis estrictament necessaris

- La idea és minimitzar l'exposició tant com sigui possible

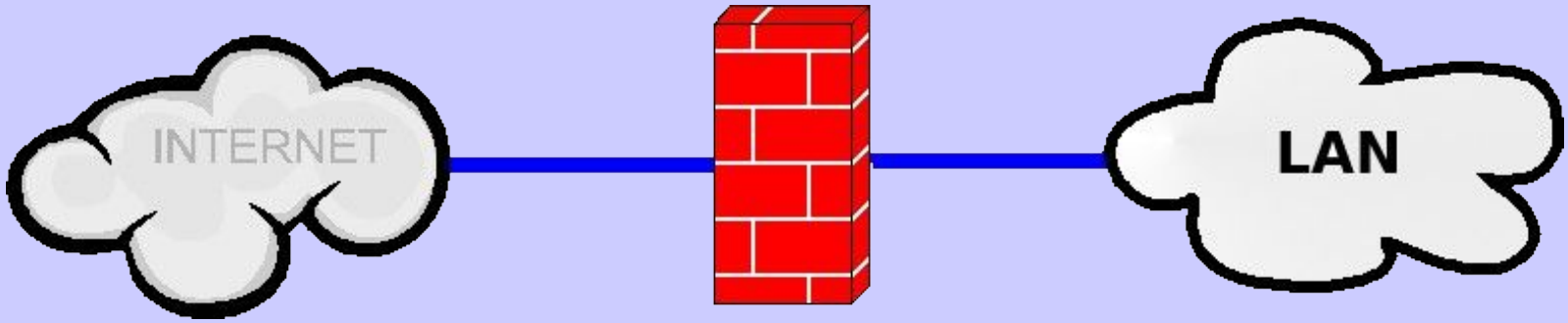
Tallafocs

- Un tallafocs és un o un grup de sistemes informàtics que controlen les vies d'accés al sistema fent el control del trànsit d'entrada i de sortida.



Tallafocs

- Separa la zona “perillosa” d'allò que volem protegir
- Bàsicament:
  - Bloqueja el trànsit de llocs no autoritzats
  - Permet el trànsit de llocs correctes



Configuració

- Hi ha dues formes de configurar els tallafocs:
  - Denegar tot i afegir-hi excepcions
    - Tancar totes les connexions possibles
    - Obrir només els ports dels serveis que volem exposar
  - Acceptar tot i afegir-hi excepcions
    - Permetre l'accés a tot
    - Tancar els serveis que no volem que siguin accessibles
- El segon sistema és més senzill de configurar però el primer és molt més segur

Polítiques dels tallafocs

- En general un tallafocs té tres formes d'actuar davant d'un intent de connexió:

1) Permetre (ACCEPT)

   Deixem passar la connexió en direcció al destí al que anava dirigit

2) Denegar (DENY)

   Denega la connexió i envia un missatge al que la iniciava

3) Ignorar (DROP)

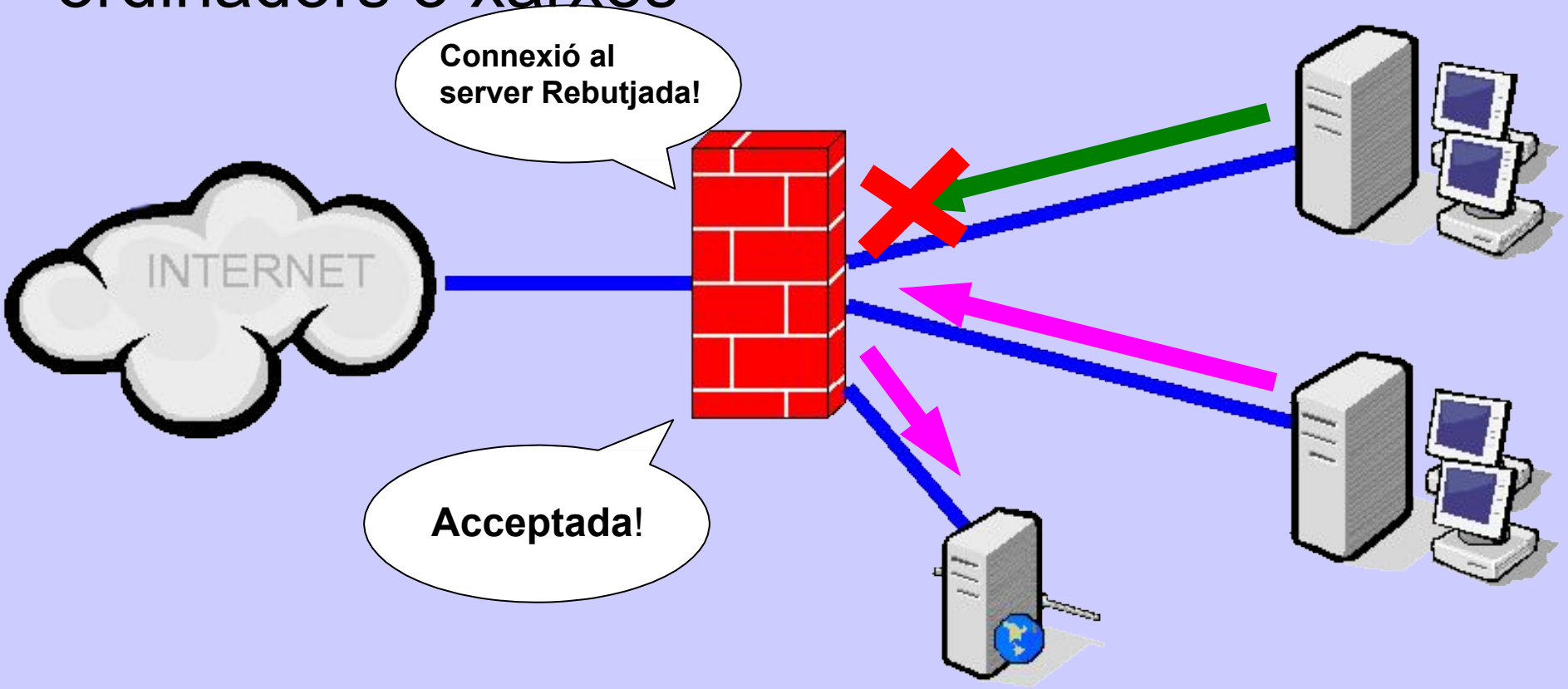
   Ignora la petició descartant el paquet

Característiques

- Per tenir un bon tallafocs hem d'aconseguir que:
  - Tot el trànsit entre la xarxa interna i externa passi pel tallafocs
  - Només el trànsit autoritzat segons la política de seguretat ha de poder passar d'una xarxa a una altra
  - El tallafocs ha de ser immune als atacs des de fora

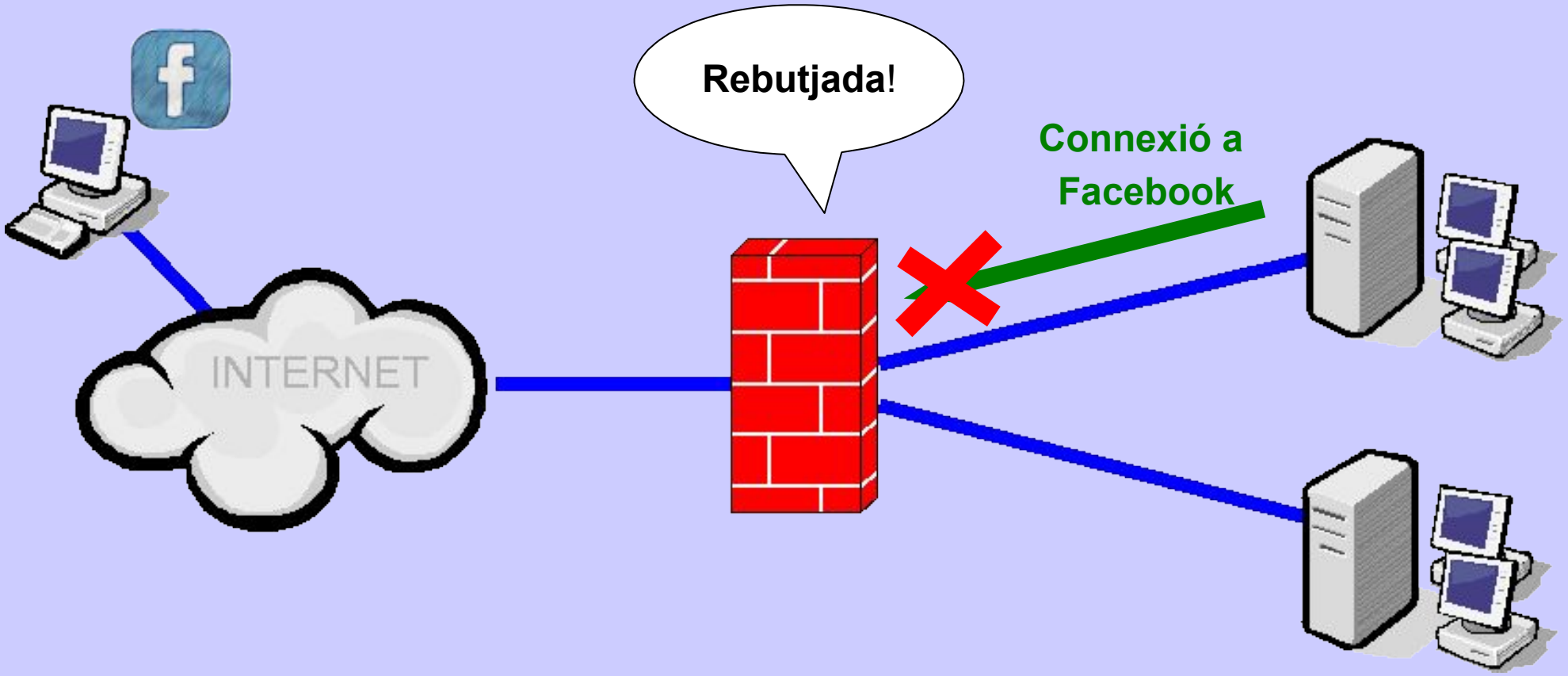
Seleccionar connexions

- Es pot fer servir el tallafocs per permetre l'accés a llocs concrets només a determinats ordinadors o xarxes



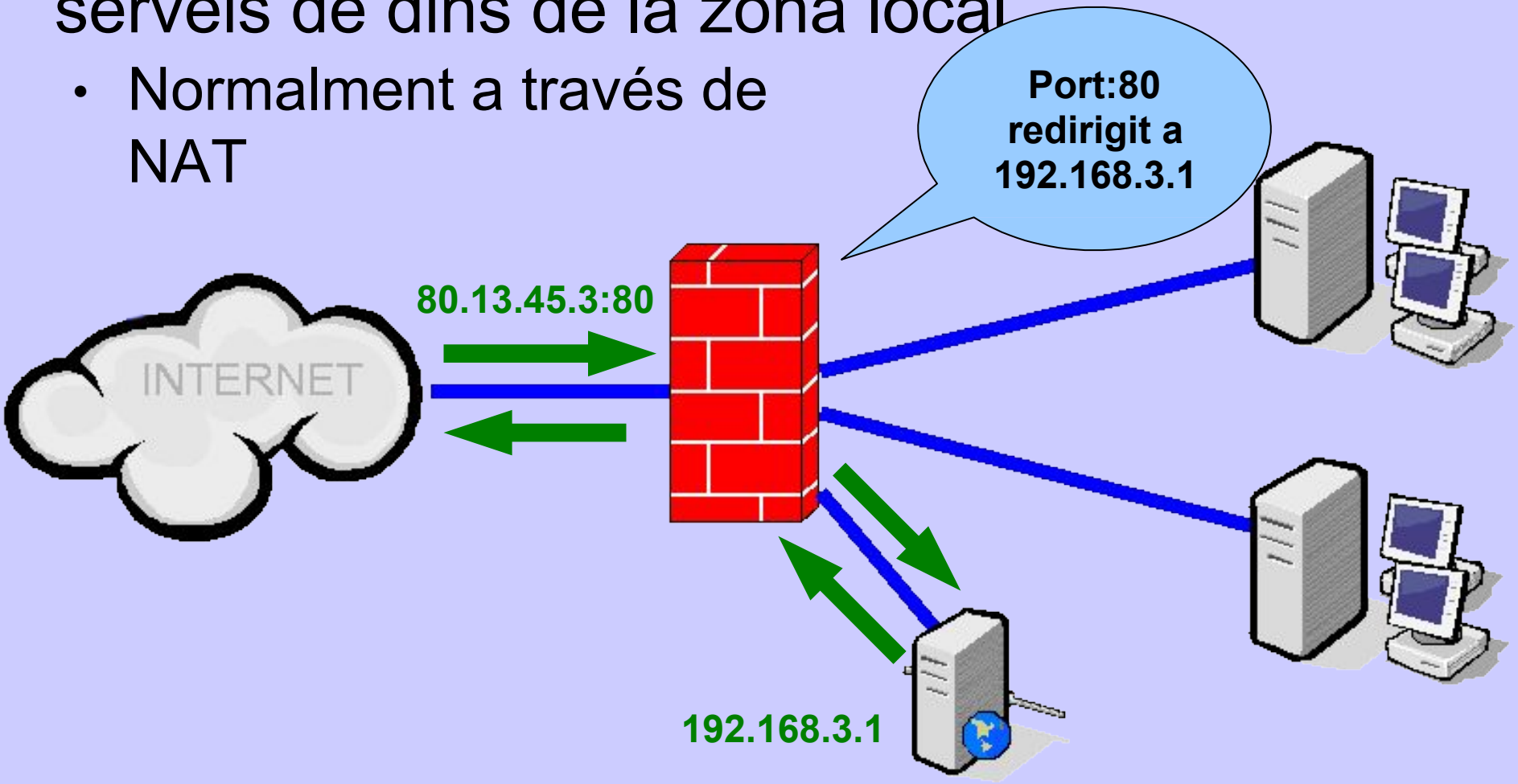
Bloquejar connexions

- Per bloquejar l'accés a determinats llocs o xarxes determinades



Permetre accés a serveis

- Per permetre que des de fora s'accedeixi a serveis de dins de la zona local
  - Normalment a través de NAT



Tallafocs

- Hi ha tallafocs tant per programari com per maquinari

  Els tallafocs de maquinari sovint també fan funcions de router

- Generalment ofereixen més serveis com VPN, control de l'estat, proxy, etc...

https://media.stockinthechannel.com/pic/Z7W6nB9qR0ezLeahwScUZw.c-r.jpg

Màquines dedicades

- Una popular alternativa als tallafocs de maquinari és dedicar un ordinador a fer de tallafocs
- Hi ha distribucions de Linux o de BSD especialitzades en aquestes tasques

https://en.wikipedia.org/wiki/List_of_router_and_firewall_distributions

Tallafocs

Tipus de tallafocs

Tipus de tallafocs

- **Tallafocs personals**

  Són sempre de programari i s'instal·len en un determinat ordinador filtrant les connexions entre aquest i la xarxa. Alguns sistemes en porten de preinstal·lat.

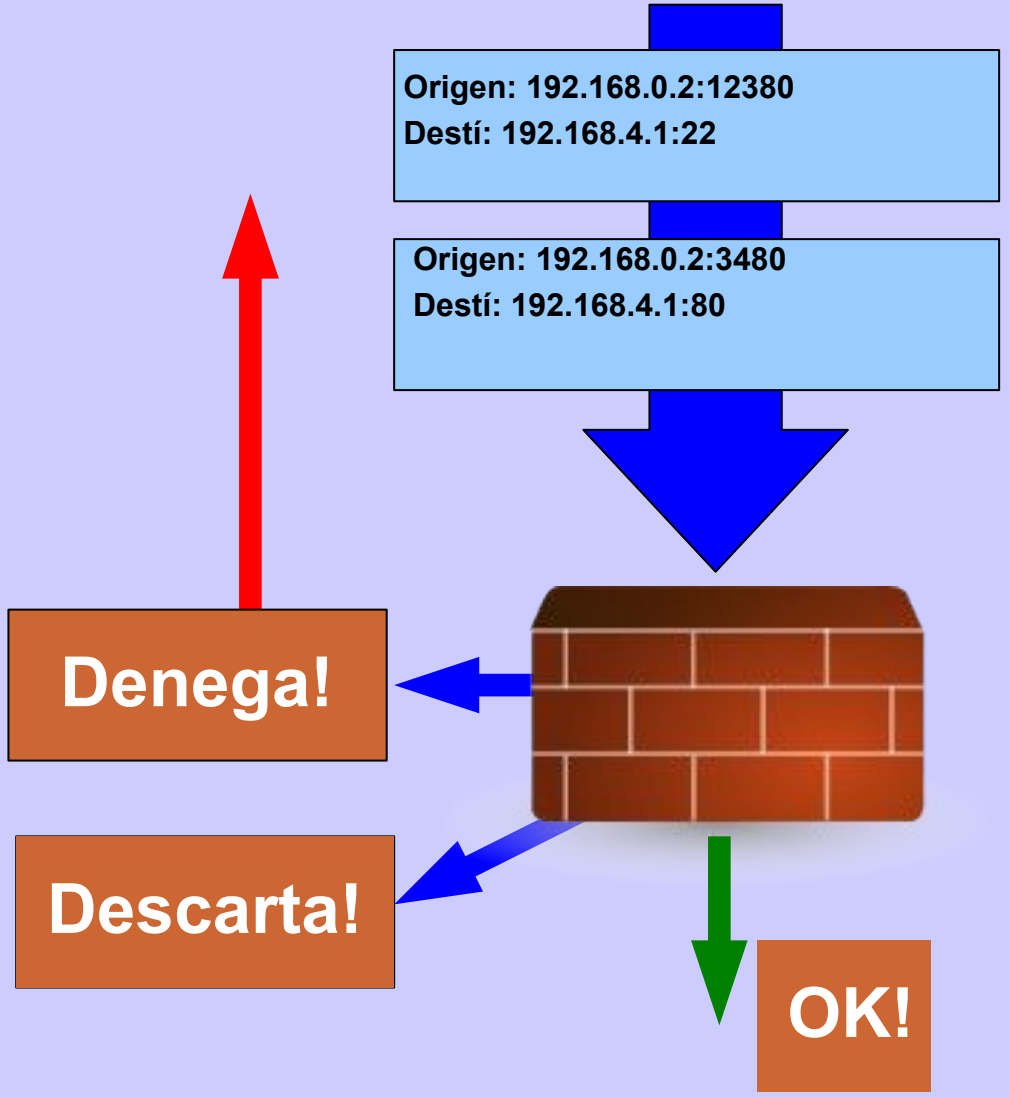
Tipus de tallafocs

Packet Filters

Va ser el primer tipus de firewall en apareixer (finals anys 80).

Explora la capa de xarxa i de transport de cada un dels paquets per observar-ne les característiques i prenent decisions.

Poden analitzar el trànsit de tota una xarxa.

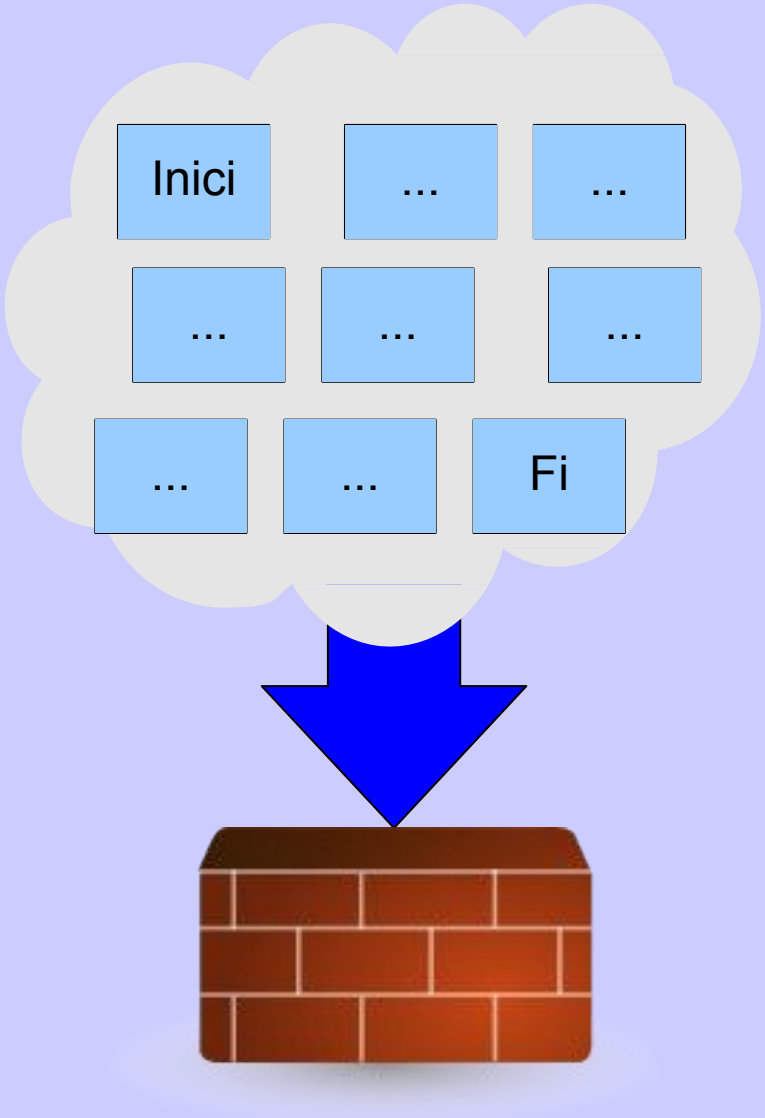


Tipus de tallafocs

- **Tallafocs de control d'estat (Stateful)**

  Firewall de segona generació (inicis anys 90)

  Mateixa capa pero analitzen una seqüència de temps que representa tota la connexió en conjunt per detectar-ne la validesa, o si en canvien propietats de forma sobtada



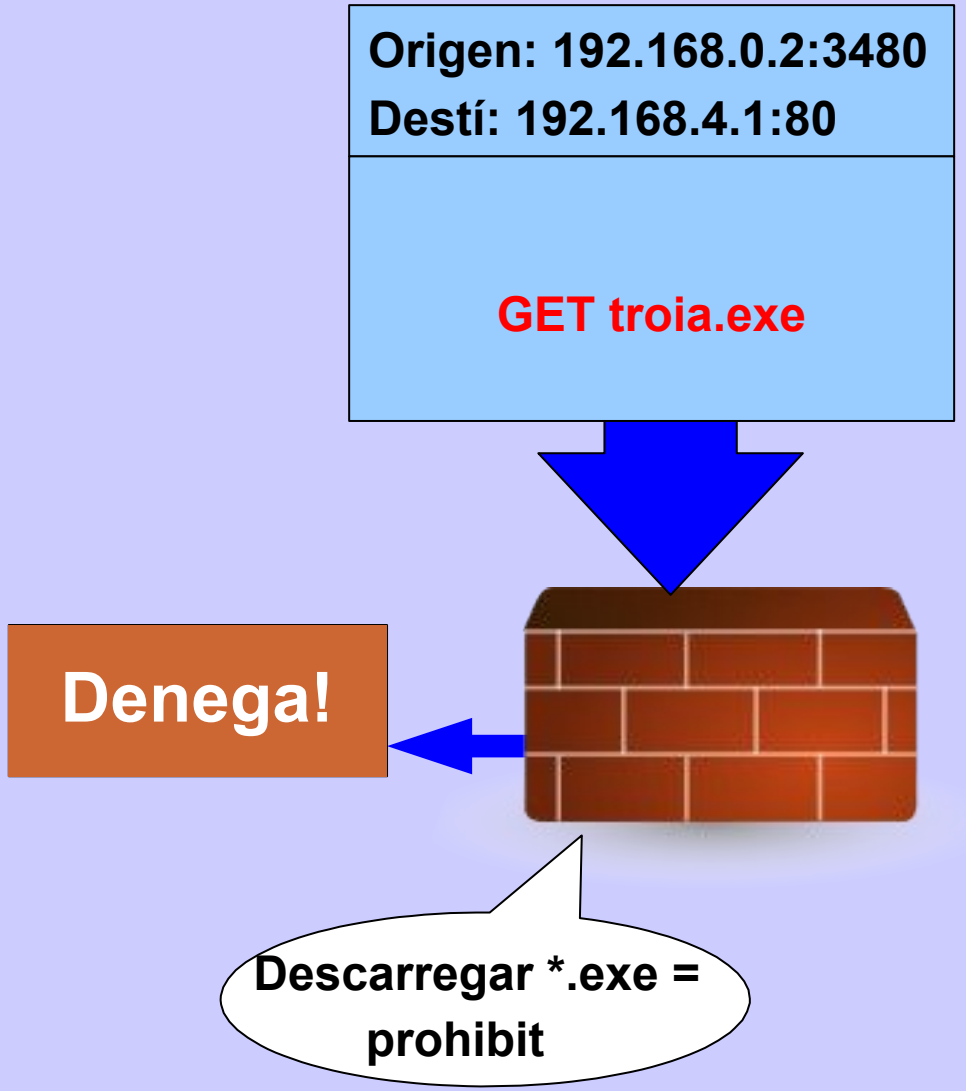
Tipus de tallafocs

- **Tallafocs de capa d'aplicació**

  “Enten” certes aplicacions i protocols de la capa d’aplicació (nivells OSI 5,6 i 7). Inspecciona el contingut dels paquets interpretant i analitzant-ne els protocols

  Sol ser més segur si es configura adequadament

  Poden detectar el pas de cucs o troians



Tallafocs

Tallafocs

Tallafocs personals

- Internet ha fet que actualment sigui un risc connectar a Internet amb un sistema sense un tallafocs personal
  - En sistemes en Windows n'hi ha molts: gratuïts, de pagament, etc..
    -
    En Linux la majoria dels tallafocs estan basat en
  - Netfilter/iptables

    - Hi ha assistents que ens faciliten la creació de regles

Tallafocs personals

- Sobretot en Windows n'hi ha molts:
  - Windows Firewall
  - Comodo Firewall Pro
  - Outpost Firewall Pro
  - ZoneAlarm Pro
  - PC Tools Firewall
  - Plus Online Armor
  - etc...

netfilter

- És el framework per desenvolupar tallafocs en Linux
- Permet filtrar paquets, fer NAT i registrar les comunicacions
- El seu component més popular és **iptables**

IPTABLES

Frontends per iptables

- IPTables pot ser cridat des de la

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh tcp  --  anywhere             anywhere             multiport dports ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-ssh (1 references)
target     prot opt source               destination

DROP       all  --  203.113.137.188      anywhere
RETURN     all  --  anywhere             anywhere
```

- Configurar-ho a mà pot ser una feina molt tediosa Per això també existeixen eines per configurar-lo com Firestarter

ufw

- *Uncomplicated Firewall* funciona sota la línia de comandes
- És el tallafocs per defecte d'Ubuntu
- Funciona
  - anomenant quin port volem obrir/tancar
  - Fent servir una plantilla

```
# ufw enable
# ufw default deny
```

```
# ufw status
active
```

```
# ufw allow Apache
```

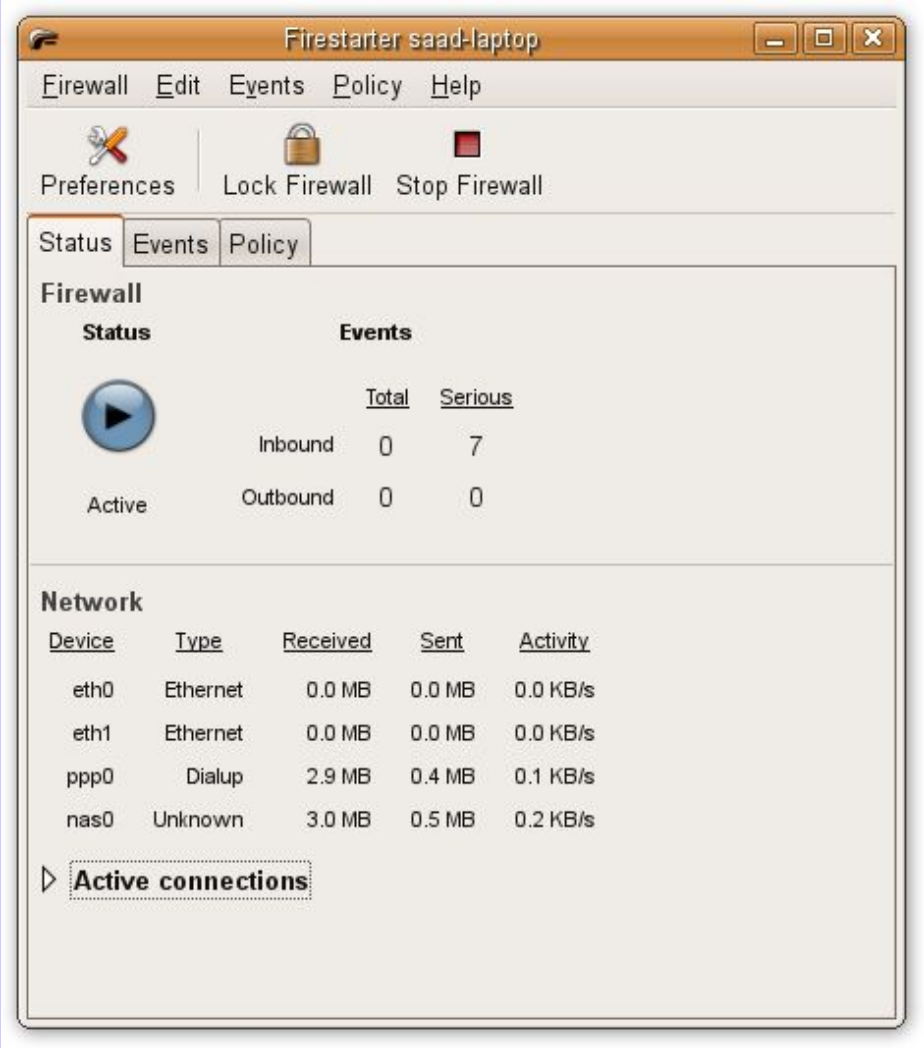
```
# ufw allow from 192.168.0.0/16 to any
```

Administració deconsola

- Des de consola també hi tenim:
  - **Shorewall**
    - Molt potent i flexible
    - S'hi interactua via fitxers de configuració
    - Per usuaris avançats
  - **Uruk**
    - Lleuger
    - Per configuracions no gaire avançades

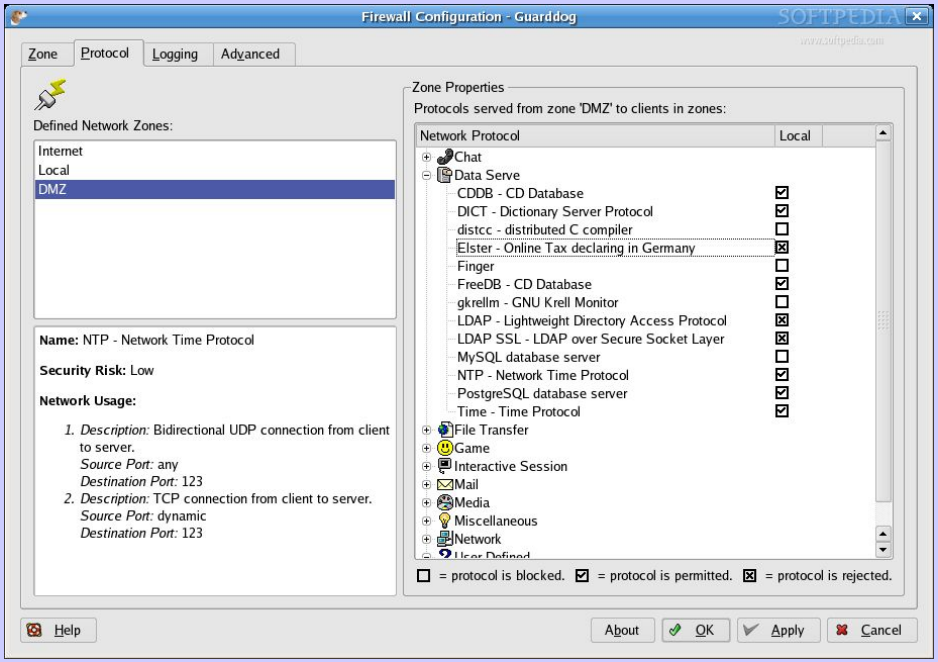
Firestarter

- És un dels més coneguts
- Entorn gràfic de GNOME
- Permet monitoritzar les entrades i sortides



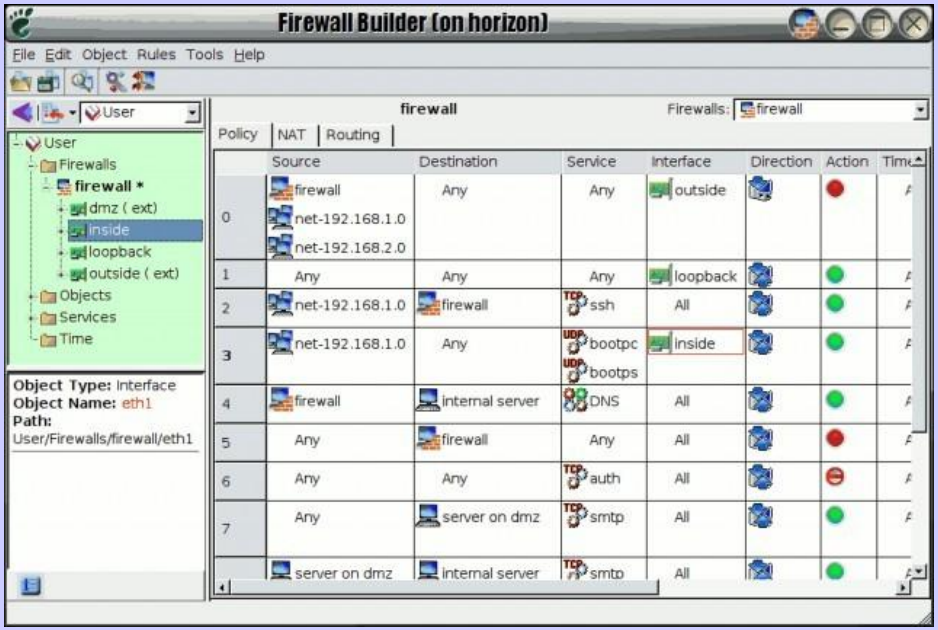
Guardog

- Pensat per escriptoris KDE
- Té possibilitat de fer configuracions senzilles i avançades
- En la versió més senzilla simplement especifiquem quins protocols permetem entre quins grups d'ordinadors



fwbuilder

- Es pot controlar des de consola
- Suporta tallafocs d'altres sistemes operatius (no té perquè ser només iptables)
- Porta plantilles per facilitar la tasca de configurar diferents tipus de tallafocs



NuFW

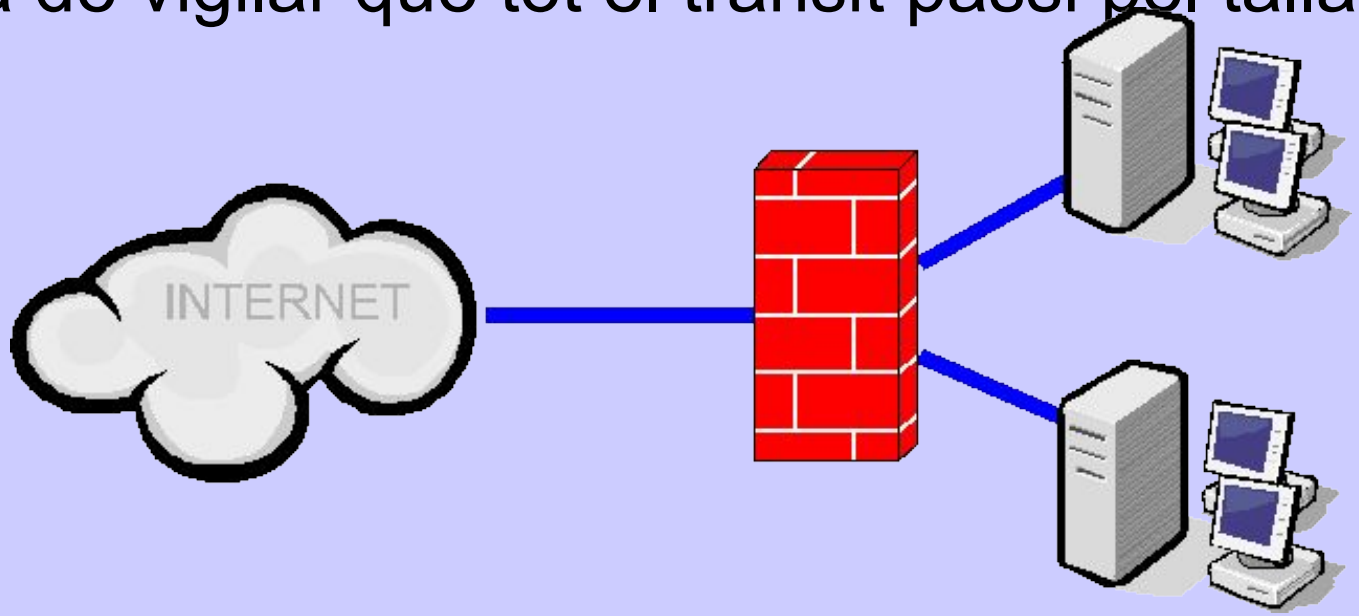
- Es tracta un tallafocs basat en Netfilter
  - A més de filtrat per IP pot fer regles basades en identificació d'usuaris
  - S'integra amb bases de dades
  - És la base de NuFirewall, del tallafocs comercial EdenWall

Tallafocs

Posicionament dels tallafocs

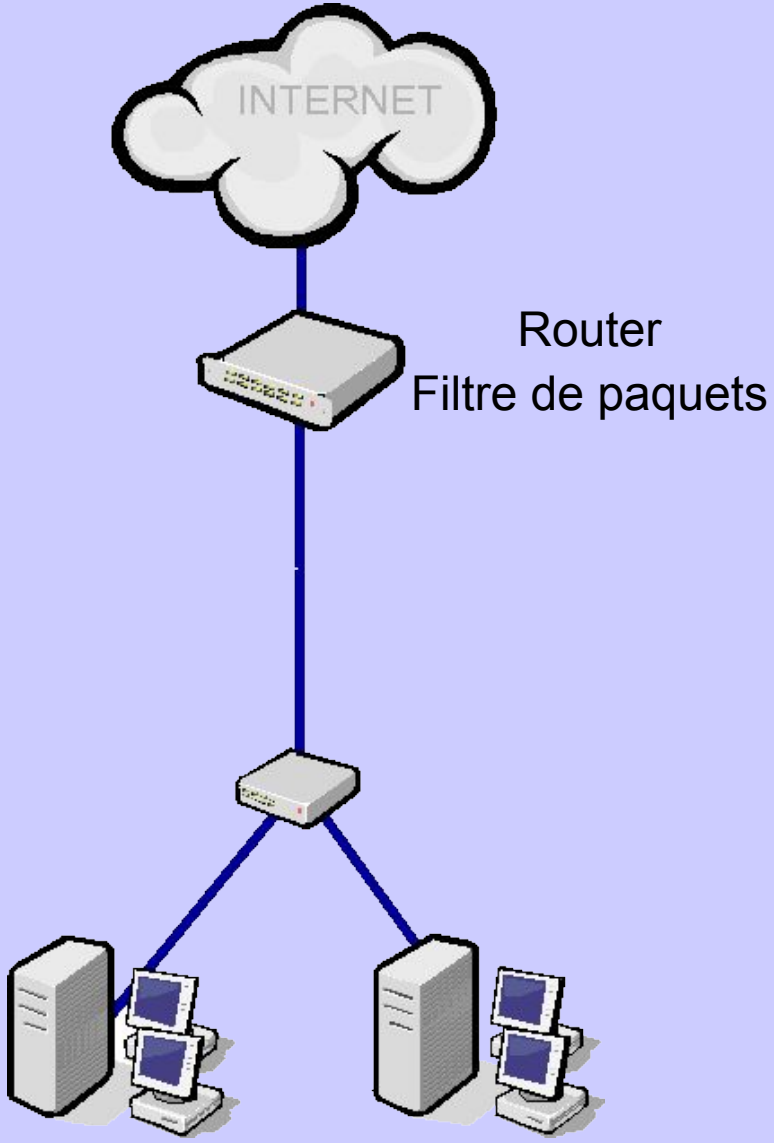
Tallafocs

- Perquè els tallafocs sigui efectius el lloc on es col·loquen és clau
- El lloc ideal és el punt que separa la nostra xarxa de la xarxa pública
- S'ha de vigilar que tot el trànsit passi pel tallafocs



Arquitectures

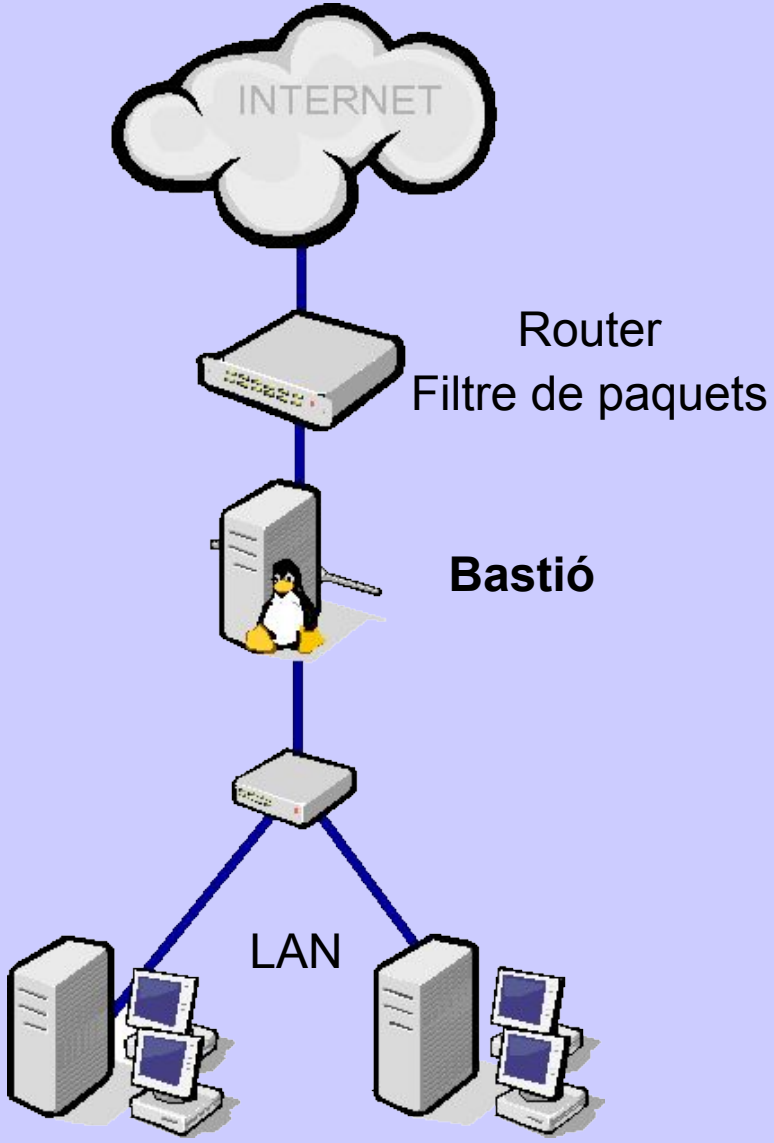
- **Filtrat de paquets**
  - Usat en xarxes petites
    - Els mòdems/routers ADSL ho solen fer
    - Es pot fer amb un ordinador en Linux
  - No solen controlar els paquets sortints
  - Sovint funcionen amb redirecció de ports



Arquitectures

- **Dual Homed Gateway**

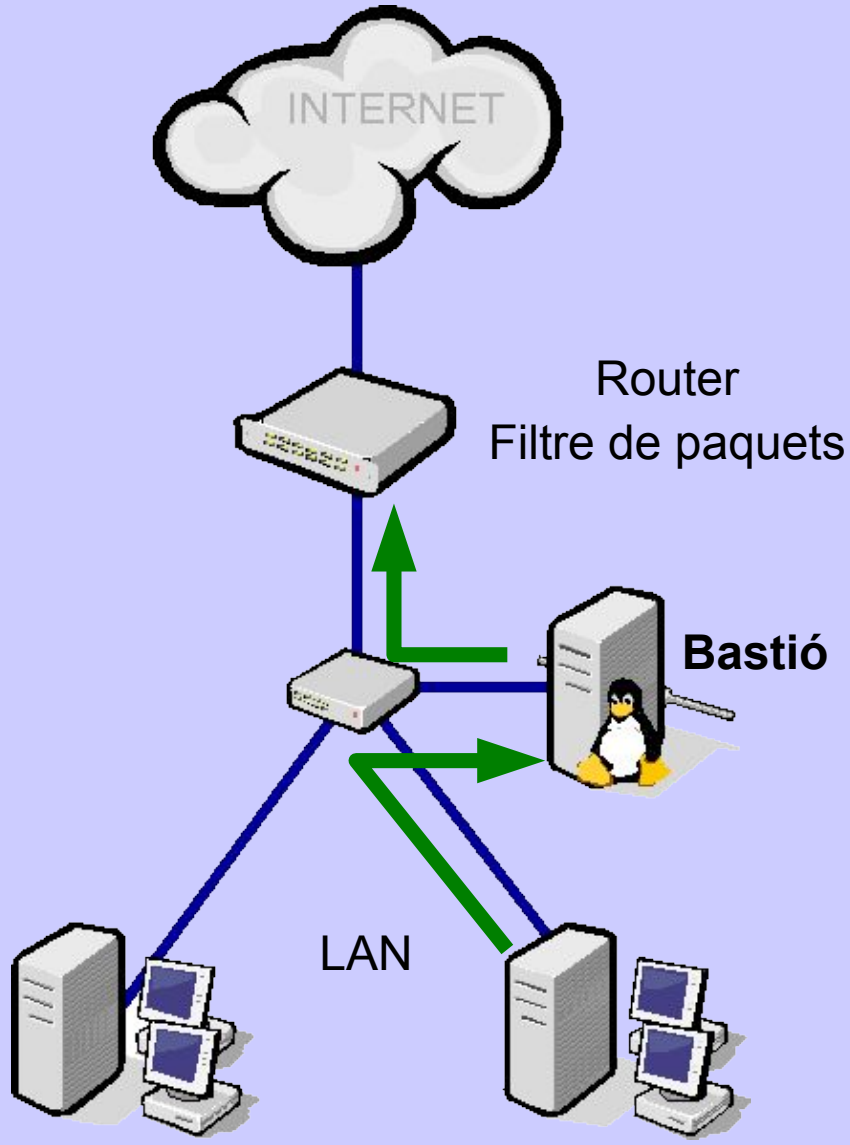
- ✔ Només es permet connectar amb l'exterior
- ✔ al Bastió que fa de proxy
- ✔ No es permeten connexions directes
- ✔ S'amaga la xarxa interna dels atacants



Arquitectures

Una alternativa consisteix en col·locar el bastió dins de la xarxa local

Es poden permetre connexions directes a hosts concrets que les necessitin però això és perillós



Arquitectures

- **Zona desmilitaritzada (DMZ)**

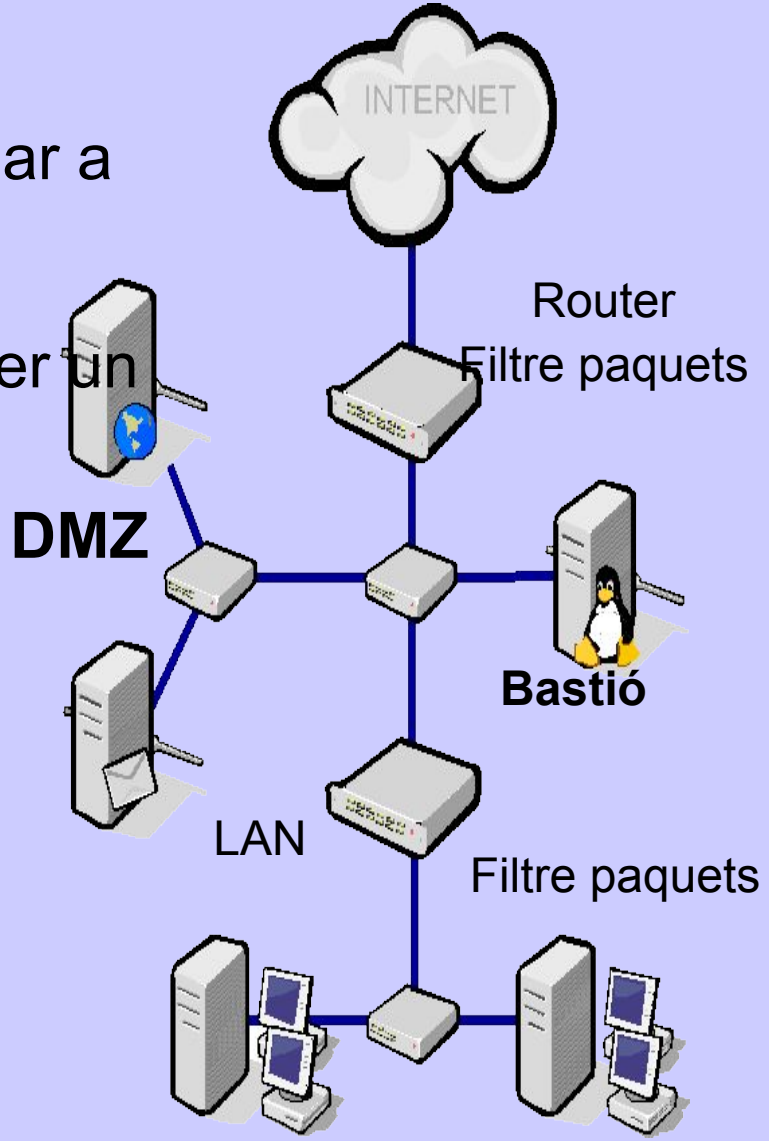
✔ Les connexions de fora només poden anar a la DMZ

✔ L'accés a la xarxa interna està protegit per un altre tallafocs

✔ Permet que la xarxa ofereixi serveis a l'exterior

✔ Encara cal que el transit sortint passi pel Bastió

✔ Es fa servir en xarxes grans



Arquitectures

Filtre Invisible

- Alguns equips permeten funcionar com bridges
- No necessiten IP
  - Per tant són més difícils d'atacar
- Al no fer de routers es poden posar en qualsevol lloc de la xarxa
- No interfereixen