SEAX

Seguretat perimetral vs seguretat en servidors

Curs 2023-2024

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

Pràctica 3

Índex

Perímetre vs servidor

Objectius

- ✓ Entendre la diferència entre el que es demana a:
  - ✓ Directrius de seguretat per a la configuració dels tallafocs
  - ✓ Directrius de seguretat específiques pels servidors
- ✓ Plantejar on i com actuar en cada cas
- ✓ Presentar eines que ens poden ajudar

Escenari

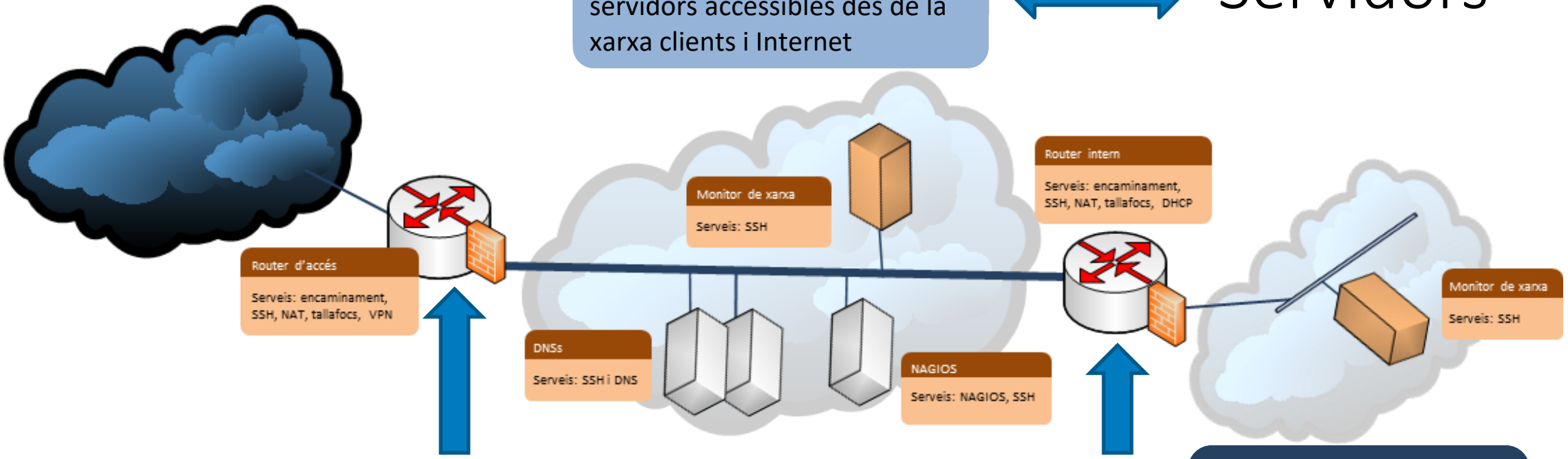
Xarxa troncal

Descripció: xarxa "real" des d'on es pot accedir a Internet

Xarxa DMZ

Descripció: xarxa amb servidors accessibles des de la xarxa clients i Internet

Servidors



Perímetre (extern i intern)

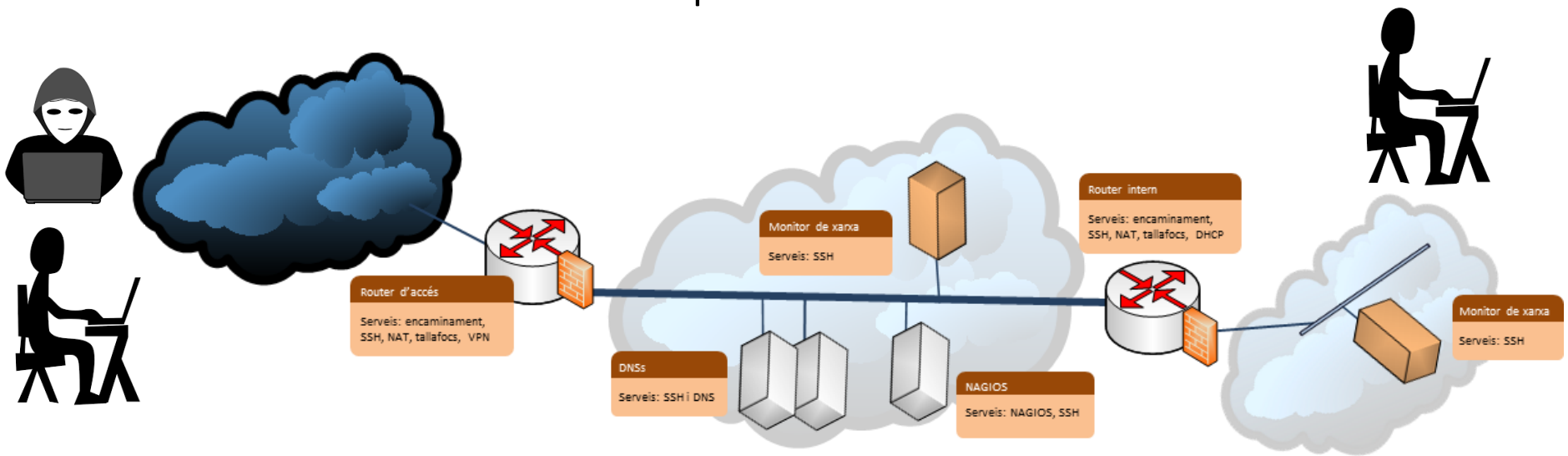
Xarxa clients

Descripció: xarxa dels usuaris

Seguretat perimetral

Tallafocs

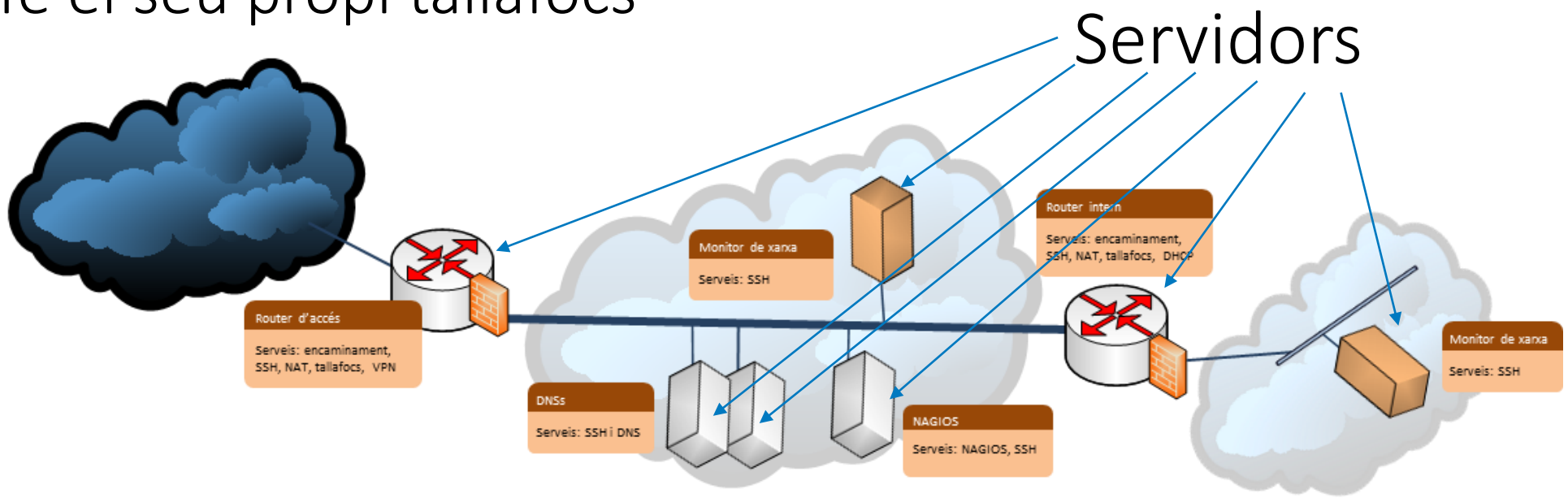
- ✓ Configuració dels tallafocs que delimiten el perímetre per:
  - ✓ Protegir l'accés a les nostres xarxes i serveis
  - ✓ Limitar l'accés a l'exterior si s'escau
  - ✓ Garantir l'accés als serveis públics



Seguretat en els servidors

Servidors

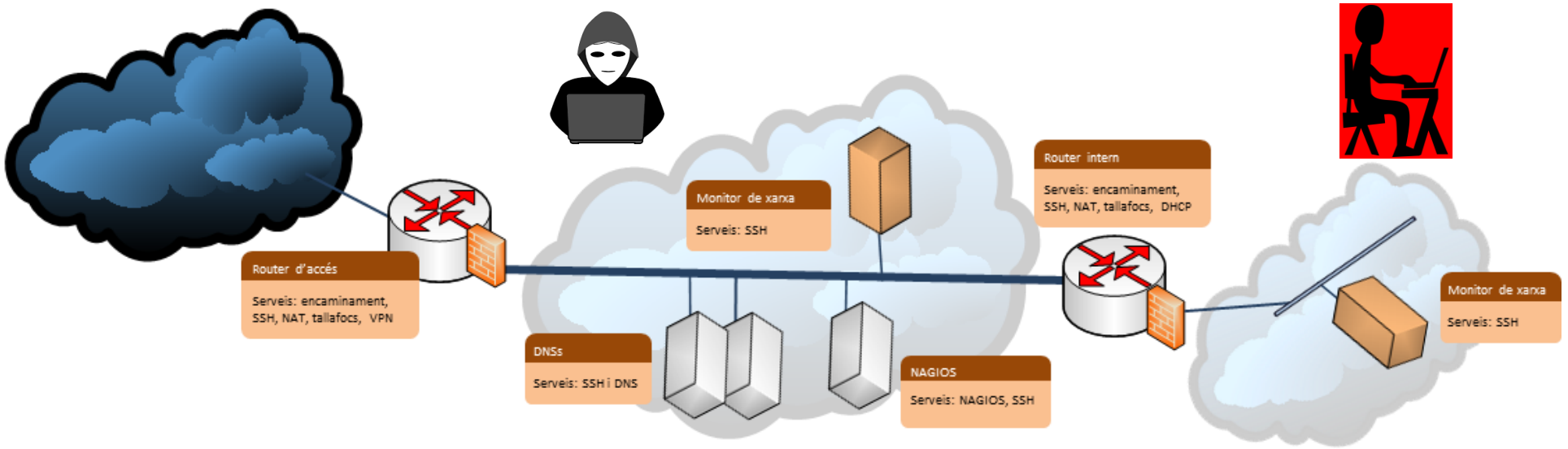
- ✓ Definirem un servidor com una màquina que:
  - ✓ Com a mínim corre un servei (SSH, DNS, Nagios, DHCP)
  - ✓ Té el seu propi tallafocs



Seguretat en els servidors (II)

Per què cal fer una protecció específica?

- ✓ Hi ha serveis que són públics (DMZ)
- ✓ No ho podem fiar tot a la seguretat perimetral (posar-nos en el pitjor cas): hacker pot trencar el perímetres & atacs interns



Seguretat en els servidors (III)

Com procedir?

- ✓ Reduir els riscos deguts a vulnerabilitats
  - ✓ Actualitzar SO i software servei
- ✓ Configurar serveis de manera adequada
  - ✓ Opcions de seguretat
- ✓ Quan el servidor no es troba en un tallafocs perimetral (cas més habitual)
  - ✓ Habilitar tallafocs personal
  - ✓ Restringir l'accés al servidor a determinats serveis i des de determinades adreces IP

Eines

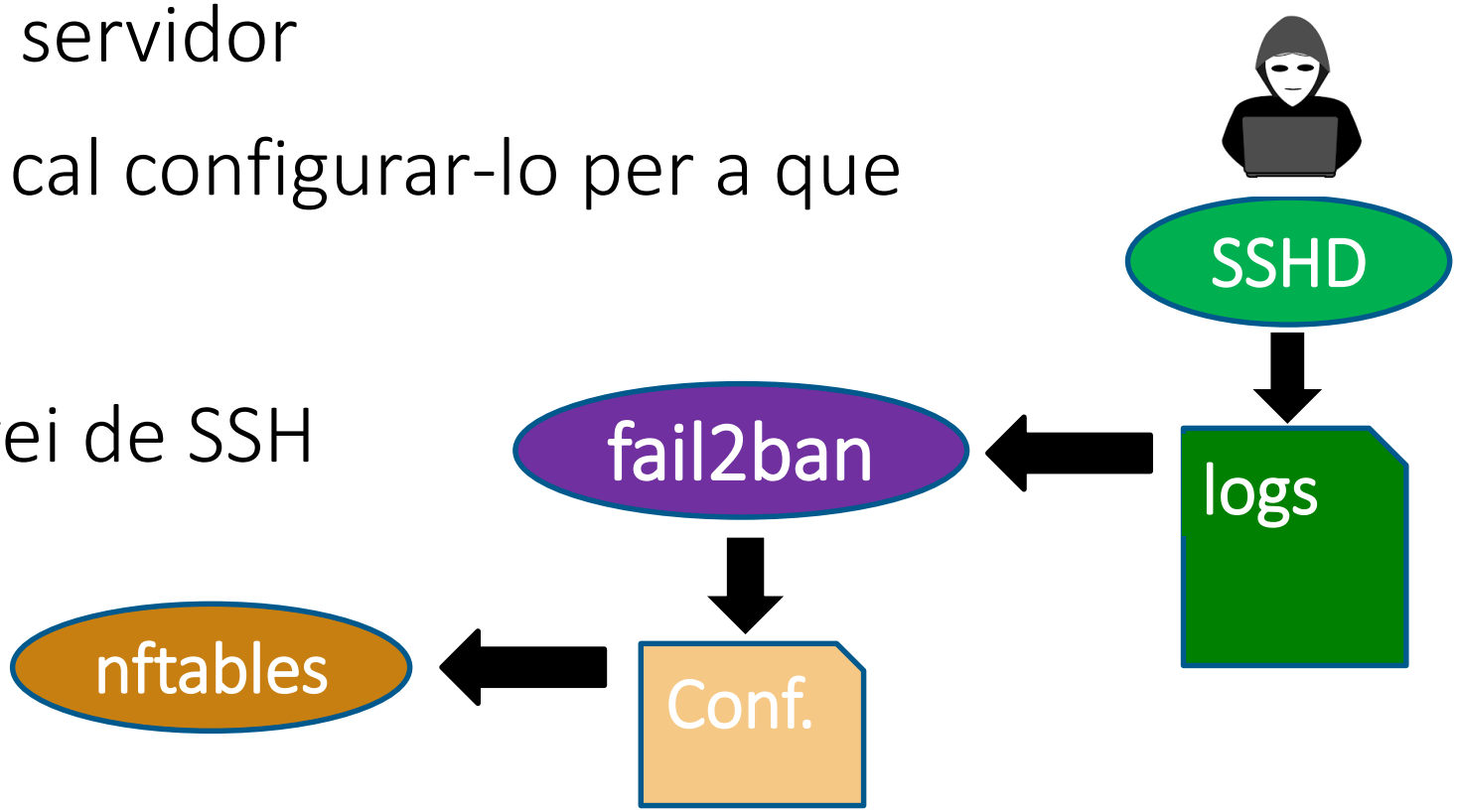
Limitar l'accés a qui no s'autentiqui correctament

- ✓ Un dels problemes més importants són els serveis que requereixen autenticació
  - ✓ Per ex. SSH
- ✓ Si no prenem mesures, l'atacant pot provar d'accedir-hi fent prova i error
  - ✓ Per ex., atacs per diccionari i enginyeria social
- ✓ Aquests atacs deixen rastre
  - ✓ Logs servidor amb IP de l'atacant

Eines

Fail2ban

- ✓ Configura dinàmicament tallafocs a partir de la lectura dels logs del servidor
- ✓ En aquesta pràctica cal configurar-lo per a que
  - ✓ Utilitzi nftables
  - ✓ Protegeixi el servei de SSH



Bibliografia

- ✓ Fail2ban: https://github.com/fail2ban/fail2ban
- ✓ Configuració: https://wiki.gbe0.com/linux/firewalling-and-filtering/nftables/fail2ban
- ✓ Bug instal·lació: https://github.com/fail2ban/fail2ban/issues/3292#issuecomment-1142503461/

Seguretat i Administració de Xarxes

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú