SEAX

Encaminament, tallafocs i NAT

Curs 2023-2024

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

Pràctica 3

Índex

- Objectius
- Escenari de la pràctica 3
  - Fases de configuració i test
- Encaminament estàtic
- Tallafocs i NAT amb nftables
  - Conceptes i exemples
  - Problema i solució

Encaminament, tallafocs i NAT

Objectius

- ✓ Construir la infraestructura de xarxa on s'allotjaran
  - ✓ Servidors, monitors i els hipotètics usuaris i administradors
- ✓ Configurar aquesta infraestructura d'acord amb unes certes polítiques de seguretat
- ✓ Comprovar el funcionament de l'escenari (connectivitat, polítiques de seguretat, accessibilitat als serveis)

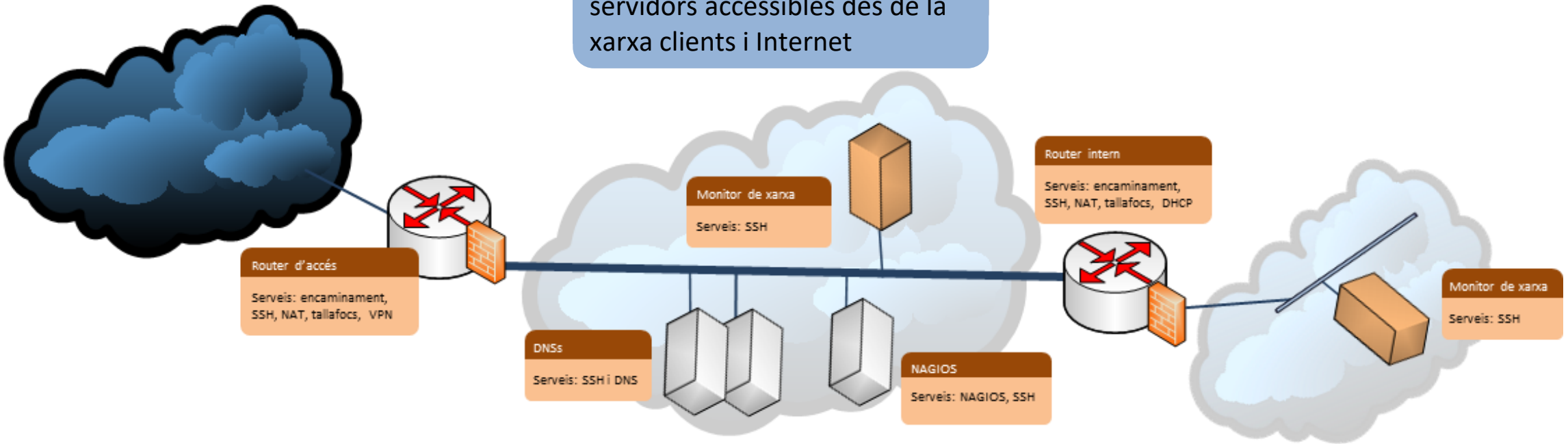
Escenari

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



Xarxa clients

Descripció: xarxa dels usuaris

Fases de configuració

Fase 0 - Anàlisis

- ✓ Identificar les VMs que cal crear
  - ✓ Tipus: router o monitor
  - ✓ Nº de interfícies de xarxa i tipus
- ✓ Penseu una estratègia eficient per a crear aquestes VMs
  - ✓ Clonació
    - ✓ Abans o després de configurar el sistema operatiu?

Fases de configuració

Fase 1 - Encaminament

- ✓ Crear les VMs dels 2 routers
- ✓ Configurar-les per a que (a) puguin reenviar paquets i (b) sàpiguen arribar a totes les xarxes
- ✓ Fer proves de connectivitat entre ells
- ✓ Automatitzar la càrrega de la seva configuració
- ✓ Introduir un monitor en cadascuna de les xarxes i fer proves de connectivitat amb tots els routers

Tingueu en compte que en aquest punt només el "router d'accés" te accés a Internet. La resta de màquines no

En aquest punt, podeu garantir que teniu connectivitat en tot l'escenari

Fases de configuració

Fase 2 – NAT (I)

- ✓ Identificar en quins routers cal configurar el NAT
- ✓ Començar configurant la sortida a Internet
- ✓ Fer proves per a comprovar que els routers i el monitor (en qualsevol de les xarxes) poden sortir a Internet

En un escenari en producció primer faríeu la fase 4 (tallafocs) i després la resta. Aquí ho fem així per assegurar que el tallafocs no interfereix

En aquest punt, podeu garantir que teniu connectivitat a Internet per tot l'escenari

Fases de configuració

Fase 3 – NAT (II)

- ✓ Identificar en quins routers cal configurar el NAT
- ✓ Configurar-lo per a permetre l'accés des de fora als servidors DNS i SSH de la DMZ
- ✓ Fer les proves corresponents per a comprovar aquest accés

Feu les proves per SSH. Les proves amb DNS ja les fareu a la sessió 3

En aquest punt, podeu garantir que els servidors de la DMZ (DNS i SSH) són accessibles també des d'Internet

Fases de configuració

Fase 4 – Tallafocs

- ✓ Identificar les polítiques de seguretat i de registre d'incidents
- ✓ Identificar en quin router s'han d'aplicar
- ✓ Traduir aquestes polítiques en regles de les taules IP
- ✓ Provar la implementació de les regles utilitzant el monitor i alguna màquina més interna o externa
- ✓ Automatitzar la càrrega de les regles
- ✓ Verificació de la configuració

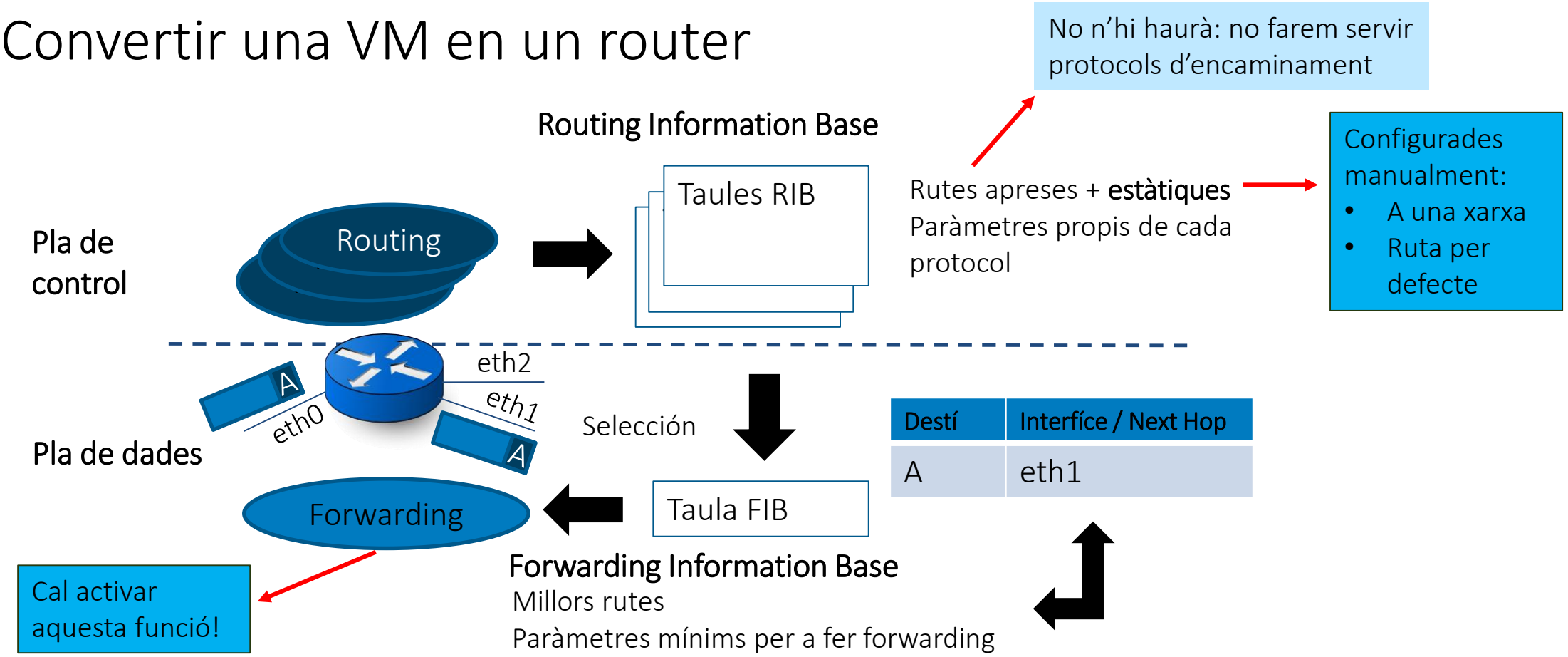
Es recomana desactivar el tallafocs quan proveu els serveis de les sessions 3-5. Activeu-lo quan hagueu comprovat que funcionen correctament

En aquest punt, podeu garantir que l'escenari està protegit d'acord amb els requeriments de la pràctica

Encaminament estàtic

Què cal fer?

✓ Convertir una VM en un router



Encaminament estàtic

Com ho fem?

- ✓ Caldrà esbrinar com activar la funció de forwarding
- ✓ Caldrà assegurar-se que la taula d'encaminament de cada router permet arribar a totes les xarxes i a Internet (quan el NAT estigui activat)
  - ✓ Com podeu veure la taula d'encaminament?
- ✓ Caldrà esbrinar com carregar aquesta informació de manera automàtica a l'arrencar el router
  - ✓ En quins fitxers posem la configuració?

Conceptes

- ✓ Taules
- ✓ Cadenes
  - ✓ Hooks
  - ✓ Política per defecte
- ✓ Regles
  - ✓ Patrons & accions
  - ✓ Amb estat o sense

nftables - Conceptes

Taules

- ✓ Nftables contempla diferents tipus de taules
  - ✓ 3 tipus de taules IP
    - ✓ **ip**: configuració tallafocs per paquets IPv4
    - ✓ **ip6**: configuració tallafocs per paquets IPv6
    - ✓ **inet**: configuració del tallafocs per paquets IPv4&IPv6
  - ✓ Altres taules
    - ✓ arp, bridge & netdev
- ✓ La configuració de les taules es realitza en base a cadenes

Important

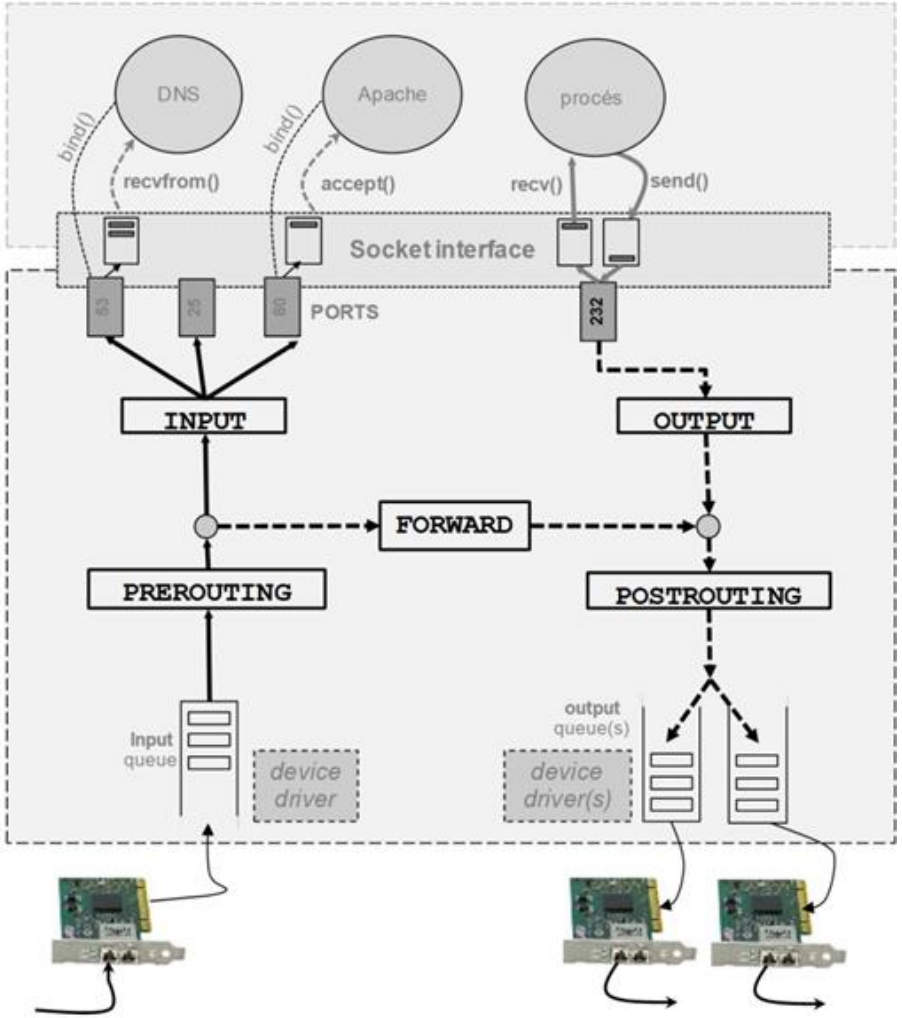
Només utilitzarem les taules IP per IPv4&IPv6

Taula IP

nftables - Conceptes

Cadenes-Hooks

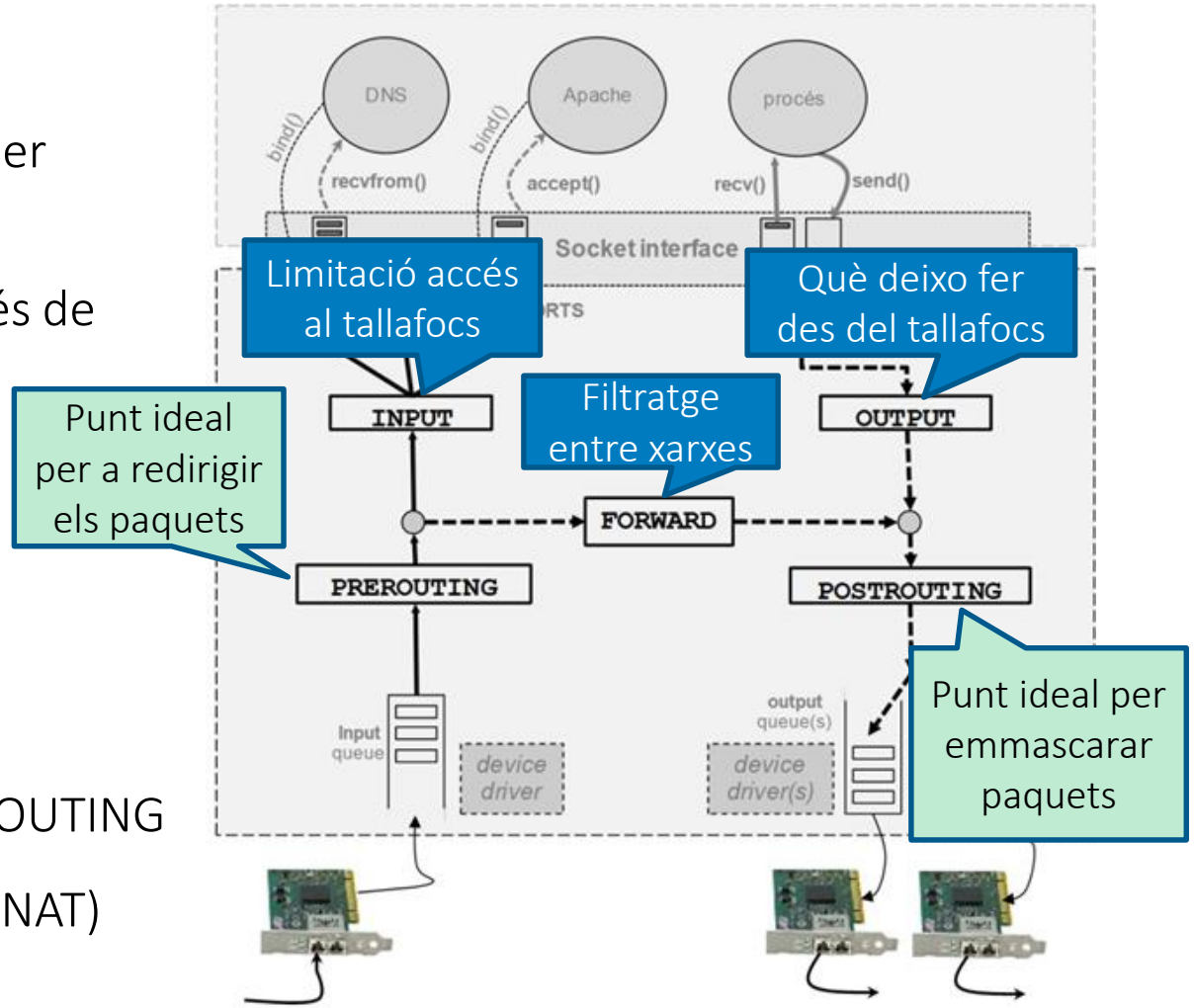
- ✓ Les cadenes s'apliquen en diferents punts de processat dels paquets IP. És el que es coneix com *hooks*:
  - ✓ **INPUT**: paquets que tenen per destí el FW
  - ✓ **OUTPUT**: paquets que tenen per origen el FW
  - ✓ **FORWARD**: paquets que han de travessar el FW
  - ✓ **PREROUTING**: paquets que arriben al FW, abans de ser encaminats
  - ✓ **POSTROUTING**: paquets que surten del FW, després de ser encaminats



nftables - Conceptes

Cadenes-Hooks (II)

- ✓ Tots els paquets que arriben al tallafocs, passen per PREROUTING
- ✓ En funció de l'adreça IP de destí que tingui després de passar per PREROUTING
  - ✓ Se li pot canviar l'original (DNAT)
- ✓ el paquet passarà per INPUT o FORWARD
- ✓ Els paquets que surten del tallafocs provenen de FORWARD o OUTPUT
- ✓ Abans de ser enviats a la xarxa passen per POSTROUTING
  - ✓ Els podem manipular, per ex. la IP d'origen (SNAT)



nftables - Conceptes

Cadenes

- ✓ Per les taules IP tenim les següent cadenes:
  - ✓ **filter**. Com filtrarem el paquets
    - ✓ Hooks: INPUT, OUTPUT & FORWARD
  - ✓ **nat**. Com modificarem certs camps dels paquets
    - ✓ Hooks: PRE/POSTROUTING & OUPUT
  - ✓ **route.** Re-encaminar paquets

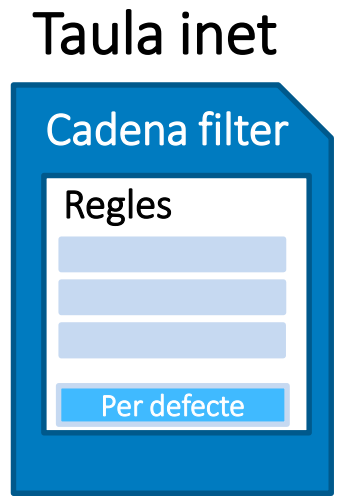
Important

Només utilitzarem les cadenes filter i nat

nftables - Conceptes

Cadenes-Configuració

- ✓ La configuració de les cadenes es realitza en base a regles
- ✓ Per cada cadena cal definir una política per defecte (policy)
  - ✓ Acció que es realitzarà si no s'acompleix cap de les regles definides
    - ✓ Típicament **ACCEPT** (deixar passar), o l'oposada, **DROP.**



nftables - Conceptes

Regles

- ✓ S'apliquen segons l'ordre en què s'han creat
- ✓ Estan formades per 4 parts:
  - ✓ Taula
  - ✓ Cadena & hook
  - ✓ Patró (*matches*)
  - ✓ Acció (*statement*)
- ✓ Exemple:
  - ✓ `nft add rule inet filter input tcp dport 22 accept`

L'ordre és molt important!

Per ex., no té sentit 1er eliminar els paquets TCP i després permetre l'accés a pàgines Web

nftables - Conceptes

Patró

- ✓ Condicions que ha de complir un paquet i que s'apliquen en una determinada taula i cadena
- ✓ Paràmetres típics:
  - ✓ Interfície de xarxa d'entrada (iif) o de sortida (oif)
  - ✓ Adreça IP o port de destí (daddr, dport) o origen (saddr, sport)
  - ✓ Protocol que transporta el paquet IP (tcp, udp, icmp,...)
- ✓ Exemples:
  - ✓ `nft add rule inet filter input` **`iif eth0 icmp type echo-request`** `accept`
  - ✓ `nft add rule inet filter output` **`ip daddr 172.22.0.0/16 tcp sport 22`** `accept`

Els patrons han de ser precisos

nftables - Conceptes

Patró (II)

Faciliten la configuració del tallafocs

- ✓ Paràmetres amb estat (per ex.):
  - ✓ El paquet és una resposta a un altre (established)
  - ✓ Es tracta d'una connexió associada a un altre (related)
  - ✓ Exemple:
    - ✓ `nft add rule inet filter forward ip daddr 172.22.0.0/16 tcp sport 22` **`ct state established`** `accept`

nftables - Conceptes

Acció

- ✓ El que se li fa al paquet si aquest coincideix amb el patró de la regla
  - ✓ Es pot combinar més d'una acció però només una pot ser terminal
- ✓ Exemples:
  - ✓ **accept / drop**
  - ✓ **reject**: permet generar un msg. ICMP d'avís
  - ✓ **dnat**: canviar adreça o port de destí
  - ✓ **snat**: canviar adreça o port d'origen
  - ✓ **log**: apuntar el pas del paquet
  - ✓ **counter**: comptabilitza paquets

S'aplica l'acció i surt de la cadena

Exemple:

```
nft add rule inet filter
output inet daddr
172.22.0.0/16 tcp sport
22 counter accept
```

nftables - Conceptes

Trucs interessants

- ✓ Donar més d'un valor a un paràmetre
  - ✓ `nft add rule inet filter forward ip daddr 172.22.0.0/16 tcp sport { 22, 80, 443 } accept`
- ✓ Esborrar una regla
  - ✓ Cal conèixer el seu *handle*, numero intern que identifica una regla
  - ✓ `nft -a list table inet filter` # per veure les regles de la taula filtre amb en seu handle
  - ✓ `nft delete rule inet filter output handle 5` # esborra la regla 5 del hook output a la taula filter

nftables - Problema

Interacció amb d'altres serveis

- Per defecte, nftables s'executa abans que d'altres serveis de xarxa
- Això genera una situació molesta
  - Els canvis de nom de les interfícies de xarxa s'apliquen un cop nftables està arrencat
  - Si nftables fa servir noms d'interfícies de xarxa diferents dels originals, donarà error
  - Un dels motius per fer servir noms d'interfícies de xarxa modificats és facilitar l'enteniment de la configuració dels tallafocs

nftables - Solució

Interacció amb d'altres serveis

- Cal configurar l'ordre d'arrencada dels serveis
- Cada servei té el seu fitxer de configuració a `/etc/systemd/system/`
  - L'ordre es controla mitjançant les directives
    - **Before**: el servei s'ha d'executar abans que els indicats
    - **After**: el contrari, s'executarà després dels que s'indiquin
- Si volem que el canvi de nom de les interfícies de xarxa tingui lloc abans que arrenqui nftables podem fer
  - Editar `/etc/systemd/system/network-online.target.wants/networking.service`
  - Afegir a "Before" "nftables.service"

Bibliografia

- ✓ Wiki Debian: https://wiki.debian.org/nftables
- ✓ Wiki nftables: https://wiki.nftables.org/wiki-nftables/

Seguretat i Administració de Xarxes

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú