📝 AF 1.1.3 - Publicar un servidor web d'una xarxa interna mitjançant NAT

Què farem en aquesta activitat?

En aquesta activitat es publicarà un servidor web Apache que es troba dins d'una **xarxa interna de VirtualBox**.

El servidor web no serà accessible directament des de l'ordinador amfitrió. Per aconseguir-ho, es configuraran **dues redireccions de ports consecutives**:

1. Una redirecció en el NAT de **VirtualBox**, per fer arribar la connexió fins al router Ubuntu.
2. Una redirecció **DNAT** en el router Ubuntu, per enviar la connexió fins al servidor Apache de la xarxa interna.

El recorregut final serà:

```
ORDINADOR AMFITRIÓ
localhost:8080
       |
       | Port Forwarding
       | VirtualBox NAT
       ▼
UBUNTU SERVER - ROUTER
enp0s3:8080
       |
       | DNAT
       ▼
XARXA INTERNA
192.168.XY.2:80
       |
       ▼
APACHE
```

Per tant, encara que Apache estarà escoltant realment en:

```
192.168.XY.2:80
```

des de l'ordinador amfitrió s'accedirà utilitzant:

```
http://localhost:8080
```

L'objectiu és entendre com es pot **publicar un servei que està darrere d'un router**, combinant NAT, encaminament i redirecció de ports.

Adreçament de la pràctica

Cada alumne disposa d'una xarxa interna diferent segons la seua posició a l'aula.

S'utilitzarà el següent criteri:

```
X = número de filera comptant des del professor
Y = número d'ordinador comptant des de la finestra
```

La xarxa de cada alumne serà:

```
192.168.XY.0/24
```

El router utilitzarà sempre la primera adreça útil:

```
192.168.XY.1
```

i el servidor web:

```
192.168.XY.2
```

Exemples:

```
Filera 1, ordinador 2

Xarxa  → 192.168.12.0/24
Router → 192.168.12.1
Apache → 192.168.12.2
```

```
Filera 3, ordinador 4

Xarxa  → 192.168.34.0/24
Router → 192.168.34.1
Apache → 192.168.34.2
```

> La part `XY` s'ha de substituir sempre pel número corresponent al lloc que ocupa cada alumne.

---

1. Preparar el servidor web

La màquina de la xarxa interna actuarà com a servidor web.

La seua configuració serà:

```
IP:       192.168.XY.2/24
Gateway:  192.168.XY.1
```

Per exemple, per a la xarxa `192.168.12.0/24`:

```
IP:       192.168.12.2/24
Gateway:  192.168.12.1
```

Instal·lar Apache:

```
sudo apt update
sudo apt install apache2
```

Comprovar que el servei està funcionant:

```
systemctl status apache2
```

També es pot provar directament:

```
curl http://localhost
```

---

2. Crear una pàgina fàcil d'identificar

Modificar la pàgina inicial:

```
sudo nano /var/www/html/index.html
```

Introduir, per exemple:

```
<h1>Servidor web de la xarxa interna</h1>

<p>Si pots llegir açò, la redirecció NAT funciona correctament.</p>
```

Comprovar:

```
curl http://localhost
```

---

3. Comprovar la comunicació des del router

Abans de configurar cap redirecció, cal comprovar que el router pot arribar al servidor Apache.

Des del router Ubuntu:

```
curl http://192.168.XY.2
```

Per exemple:

```
curl http://192.168.12.2
```

Hauria d'aparéixer la pàgina creada anteriorment.

> Si aquesta prova falla, **no s'ha de continuar amb la configuració NAT**. Primer s'ha de revisar la xarxa interna.

Es pot comprovar la configuració amb:

```
ip addr
ip route
```

---

4. Primera redirecció: NAT de VirtualBox

La interfície exterior del router Ubuntu està connectada a una xarxa **NAT de VirtualBox**.

Per defecte, VirtualBox permet que la màquina virtual isca a Internet, però no permet iniciar connexions directament des de l'amfitrió cap a la màquina virtual.

Per això es crearà una regla de **Port Forwarding**.

Amb la màquina Ubuntu Server apagada:

```
VirtualBox
   ↓
Configuració
   ↓
Xarxa
   ↓
Adaptador connectat a NAT
   ↓
Avançat
   ↓
Redirecció de ports
```

Crear aquesta regla:

Camp	Valor
Nom	WEB
Protocol	TCP
IP amfitrió	127.0.0.1
Port amfitrió	8080
IP convidat	deixar buit
Port convidat	8080

Aquesta regla significa:

```
127.0.0.1:8080
        ↓
VirtualBox NAT
        ↓
Ubuntu Server:8080
```

---

5. Entendre què falta

En aquest moment, VirtualBox ja és capaç d'enviar una connexió fins al router Ubuntu:

```
localhost:8080
       ↓
Ubuntu Server:8080
```

Però Apache **no està instal·lat en el router**.

Apache està escoltant en:

```
192.168.XY.2:80
```

Per tant, encara falta una segona redirecció:

```
Ubuntu Server:8080
       ↓
192.168.XY.2:80
```

Aquesta redirecció es farà amb **DNAT**.

6. Revisar el NAT que ja existeix

En activitats anteriors ja es va configurar el router perquè la xarxa interna poguera accedir a Internet.

La configuració es troba en:

```
sudo nano /etc/ufw/before.rules
```

Ja ha d'existir una secció `*nat` amb una regla semblant a:

```
*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -s 192.168.XY.0/24 -o enp0s3 -j MASQUERADE

COMMIT
```

Aquesta regla permet:

```
XARXA INTERNA
      ↓
POSTROUTING
MASQUERADE
      ↓
INTERNET
```

Aquesta configuració **no s'ha d'eliminar**.

Ara s'afegirà una nova regla dins de la mateixa secció.

---

7. Crear la regla DNAT

Editar:

```
sudo nano /etc/ufw/before.rules
```

Afegir la cadena:

```
:PREROUTING ACCEPT [0:0]
```

i la regla:

```
-A PREROUTING -i enp0s3 -p tcp --dport 8080 -j DNAT --to-destination
192.168.XY.2:80
```

La secció NAT quedarà semblant a:

```
*nat

:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]

# Redirecció cap al servidor Apache
-A PREROUTING -i enp0s3 -p tcp --dport 8080 -j DNAT --to-destination
192.168.XY.2:80

# NAT d'eixida de la xarxa interna
-A POSTROUTING -s 192.168.XY.0/24 -o enp0s3 -j MASQUERADE

COMMIT
```

> **Important:** no s'ha de crear una segona secció `*nat`. S'ha de modificar la que ja existeix.

Per exemple, per a la xarxa `192.168.12.0/24`:

```
*nat

:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]

-A PREROUTING -i enp0s3 -p tcp --dport 8080 -j DNAT --to-destination
192.168.12.2:80

-A POSTROUTING -s 192.168.12.0/24 -o enp0s3 -j MASQUERADE

COMMIT
```

---

8. Entendre la regla DNAT

La regla:

```
-A PREROUTING -i enp0s3 -p tcp --dport 8080 \
-j DNAT --to-destination 192.168.XY.2:80
```

es pot llegir de la següent manera:

```
Si arriba un paquet...

per la interfície enp0s3
```

```
utilitzant TCP

amb destinació al port 8080

canvia la seua destinació

i envia'l a:

192.168.XY.2:80
```

És a dir:

```
enp0s3:8080
      |
      | DNAT
      ▼
192.168.XY.2:80
```

---

9. Aplicar els canvis

Recarregar UFW:

```
sudo ufw reload
```

Si fora necessari reinicialitzar completament les regles:

```
sudo ufw disable
sudo ufw enable
```

---

10. Comprovar la regla NAT

Consultar les regles:

```
sudo iptables -t nat -L -n -v
```

S'hauria de poder localitzar una regla semblant a:

```
DNAT
tcp
dpt:8080
to:192.168.XY.2:80
```

També continuarà existint la regla:

```
MASQUERADE
```

que permet l'accés a Internet des de la xarxa interna.

---

11. Prova final

Des de **l'ordinador amfitrió**:

```
curl http://127.0.0.1:8080
```

També es pot utilitzar el navegador:

```
http://localhost:8080
```

Hauria d'aparéixer la pàgina allotjada en el servidor Apache.

El recorregut complet serà:

```
localhost:8080
      ↓
VirtualBox NAT
      ↓
Ubuntu Server:8080
      ↓
DNAT
      ↓
192.168.XY.2:80
      ↓
Apache
```

Per exemple, per a l'alumne de la filera 1 i ordinador 2:

```
localhost:8080
      ↓
VirtualBox NAT
      ↓
Ubuntu Server:8080
      ↓
DNAT
      ↓
192.168.12.2:80
```

---

12. Què s'ha aconseguit?

Al final de l'activitat s'han configurat dos mecanismes diferents:

NAT de VirtualBox

```
localhost:8080
      ↓
Ubuntu Server:8080
```

Permet que una connexió iniciada en l'amfitrió arribe fins a la màquina virtual.

DNAT en Ubuntu

```
Ubuntu Server:8080
      ↓
192.168.XY.2:80
```

Permet que el router envie la connexió fins a un servidor situat en la xarxa interna.

Per tant:

```
AMFITRIÓ
   ↓
VirtualBox NAT
   ↓
ROUTER UBUNTU
   ↓
DNAT
   ↓
SERVIDOR APACHE
```

---

13. Comparació amb el NAT d'eixida

En activitats anteriors es va configurar:

```
-A POSTROUTING -s 192.168.XY.0/24 -o enp0s3 \
-j MASQUERADE
```

Aquesta regla permet:

```
DINS → FORA
```

Ara s'ha afegit:

```
-A PREROUTING -i enp0s3 -p tcp --dport 8080 \
-j DNAT --to-destination 192.168.XY.2:80
```

que permet:

```
FORA → DINS
```

Es pot resumir així:

Mecanisme	Funció
`POSTROUTING + MASQUERADE`	Permetre que la xarxa interna isca cap a l'exterior
`PREROUTING + DNAT`	Publicar un servei situat en la xarxa interna

---

14. Diagnòstic d'errors

Si no funciona, s'ha de comprovar el recorregut en ordre.

Apache funciona?

En el servidor web:

```
curl http://localhost
```

El router arriba al servidor?

En el router:

```
curl http://192.168.XY.2
```

La màquina interna té el gateway correcte?

```
ip route
```

Ha d'utilitzar:

```
192.168.XY.1
```

Existeix el DNAT?

```
sudo iptables -t nat -L -n -v
```

Buscar:

```
dpt:8080
```

i:

```
to:192.168.XY.2:80
```

Existeix la regla de VirtualBox?

Comprovar:

```
VirtualBox
→ Configuració
→ Xarxa
→ NAT
→ Redirecció de ports
```

Ha d'existir:

```
127.0.0.1:8080 → VM:8080
```

Funciona el recorregut complet?

Des de l'amfitrió:

```
curl http://127.0.0.1:8080
```

---

15. Activitat final

Respon breument:

1. En quina màquina està instal·lat realment Apache?
2. En quin port escolta Apache?
3. Per què l'amfitrió no pot accedir directament a `192.168.XY.2`?
4. Quina funció realitza el Port Forwarding de VirtualBox?
5. Quina funció realitza el DNAT del router Ubuntu?
6. Per què s'utilitza `PREROUTING`?
7. Quina diferència hi ha entre `DNAT` i `MASQUERADE`?
8. Quina regla permet que la xarxa interna isca a Internet?
9. Quina regla permet publicar el servidor Apache?
10. Explica el recorregut complet d'una petició a:

```
http://localhost:8080
```

fins que arriba al servidor Apache.

Resultat esperat

Des de l'amfitrió:

```
curl http://localhost:8080
```

ha de mostrar la pàgina allotjada realment en:

```
192.168.XY.2:80
```

El recorregut complet és:

```
localhost:8080
      ↓
VirtualBox NAT
      ↓
Ubuntu Server:8080
      ↓
DNAT
      ↓
192.168.XY.2:80
      ↓
Apache
```