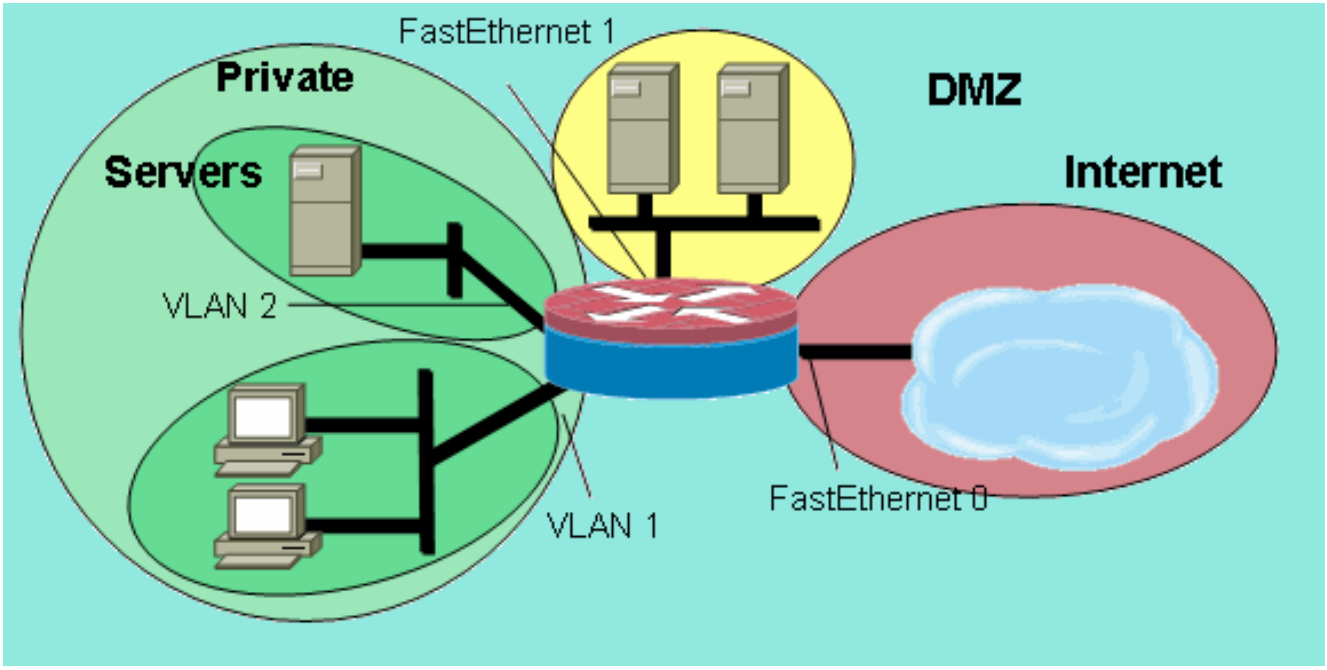
RDE. IES Haría
UT6-A9

Práctica

PAT con Linux



Práctica

Objetivo

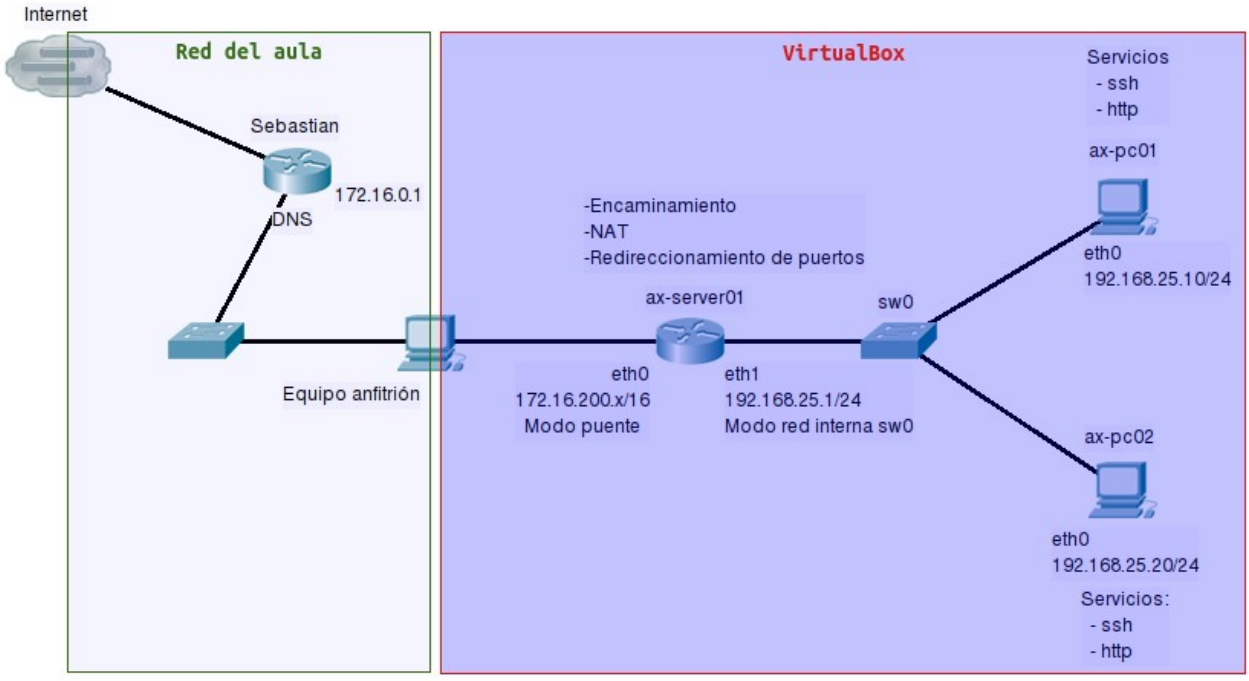
El objetivo es que utilizar la técnica de reenvío de puertos para acceder a servicios que están en una red privada.

Resumen

Para poder realizar la práctica se darán los siguientes pasos genéricos:

- Partiremos de la práctica UT5-A10 en la que creamos tres máquinas virtuales utilizando como base Ubuntu Server mini, sin entorno gráfica, con el software imprescindible.
- Configurar la red en todas las máquinas virtuales de la misma forma que en dicha práctica, de forma que en el equipo que hace de router tengamos habilitado el reenvío de paquetes y el NAT y configurado como puerta de enlace predeterminado el router de clase y las máquinas internas accederán a Internet a través de la máquina virtual que hace de router.
- En ambas máquinas internas instalaremos los servicios ssh y apache2 y en el equipo router configuraremos el reenvío de puertos (PAT) para poder acceder a los servicios de los equipos internos.

Esquema de red de la práctica



Pasos

1) Creación de las máquinas virtuales

Siguiendo los pasos descritos en UT5-A10 creamos las máquinas virtuales. Nos aseguramos de que:

- Reiniciar las direcciones MAC si hemos de crear máquina virtuales nuevas.
- La máquina virtual que hace de router tendrá dos tarjetas de red. Una en modo puente (conectará con la red de clase) y la en modo red interna con nombre **sw0**.
- Las máquinas virtuales de los Pcs tendrán una sóla tarjeta de red en modo red interna con nombre **sw0**. De esa forma los tres equipos quedarán interconectados

2) Configuración inicial de las máquinas virtuales.

Iniciamos las máquinas virtuales y nos aseguramos de que (**x** es tu número de equipo):

- Nombres de los equipos (ficheros **`/etc/hostname`** y **`/etc/hosts`**):
  - **`ax-server01`**: equipo que hace de router.
  - **`ax-pc01`** y **`ax-pc02`**: equipos Pcs internos.
- Configuración de la IP de las tarjetas de red de los equipos (almacenaremos la configuración en el fichero de configuración de la red **`/etc/network/interfaces`**)
  - **`ax-server01`**:
    - tarjeta red modo puente: `172.16.200.x/16`, puerta de enlace `172.16.0.1`
    - tarjeta de red modo red interna: `192.168.25.1/24`.
  - **`ax-pc01`** y **`ax-pc02`**: `192.168.25.10/24 y 192.168.25.20/24` respectivamente. Ambos tendrán como puerta de enlace `192.168.25.1`
- Servidor de DNS (editamos **`/etc/resolv.conf`**) : en todos los equipos pondremos

```
nameserver 172.16.0.1
```

No olvides **reiniciar** la configuración de red en todos los equipos para que se aplique la nueva configuración.

Al finalizar este paso el equipo que hace de router debería tener acceso a Internet y las máquinas internas deberían hacerse `ping` entre ellas y al equipo servidor en la IP `192.168.25.1`.

3) Configuración del acceso a Internet de las máquinas internas

- Activamos reenvío de paquetes en **`ax-server01`**, ejecutamos:

```
$ sudo su    ← para convertirnos en root
# echo "1" > /proc/sys/net/ipv4/ip_forward  ← activamos reenvío
```

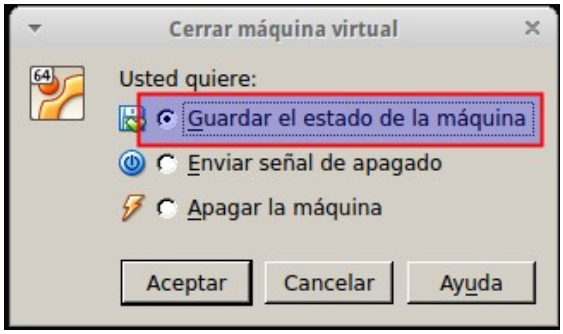
- Para que los equipos de las **redes internas** puedan acceder a Internet hemos de activar el enmascaramiento (NAT) para que salgan utilizando la IP “pública” de los equipos que hacen de router. En **`ax-server01`** ejecutamos (suponiendo que **`eth0`** es la interfaz externa):

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Al terminar este apartado desde todos los equipos deberíamos tener acceso a Internet también en los equipos de la red interna:

`$ ping rediris.es` ← en **ax-pc01** y **ax-pc02**

Los cambios hechos en este apartado se perderán si reiniciamos **ax-server01**, por lo que deberíamos volver a ejecutarlos en dicho caso. Una alternativa es guardar el estado de la máquina en VirtualBox en lugar de apagarla si hemos de continuar la práctica en otro momento.



4) Instalación de servicios en las máquinas internas

Para Instalar los servicios en las máquinas internas:

- **ax-pc01** y **ax-pc02**: ejecutamos

```
$ sudo apt-get update
$ sudo apt-get install ssh apache2
```

Comprobamos que los servicios se están ejecutando comprobando si sus puertos están a la escucha:

```
$ sudo netstat -lptn
```

5) Activamos el reenvío de puertos

Vamos a reenviar los puertos de **ax-server01** para poder acceder desde la red de clase a los servicios de la red interna virtual de acuerdo a la siguiente tabla:

Servicio	IP externa	Puerto externo	IP interna	Puerto interno
ssh	172.16.200.x	2200	192.168.25.10	22
http	172.16.200.x	8080	192.168.25.10	80
ssh	172.16.200.x	2201	192.168.25.20	22
http	172.16.200.x	8081	192.168.25.20	80

Para realizar el reenvío de puertos en el equipo **ax-server01**, ejecutamos:

```
$ sudo su

# iptables -A PREROUTING -t nat -i <ethx> -p tcp --dport <puerto_externo> -j DNAT
--to <IP_interna>:<puerto_interno>
```

Donde:

- **<ethx>** ← Interfaz de red externa del equipo, normalmente debería ser `eth0`.
- **<puerto_externo>** ← Puerto de **ax-server01** que se reenviará al servicio de la máquina interna.
- **<IP_interna>:<puerto_interno>** ← Dirección IP de la máquina interna y puerto por el que escucha el servicio de la máquina interna al que queremos dar acceso.

Ejemplo:

Para redireccionar el puerto `2200` de **ax-server01** para acceder al servicio ssh de `192.168.25.10` ejecutaríamos:

```
# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 2200 -j DNAT --to 192.168.25.10:22
```

Ejecuta en **ax-server01** los comando que permiten reenviar el resto de puertos.

Para comprobar que hemos hecho la redirección de puertos de manera correcta, podemos listar el contenido de la tabla NAT del Kernel ejecutando:

```
# iptables -L -t nat
```

Debería mostrarse la información de las cuatro redirecciones de puertos que hemos hecho.

6) Accediendo a los servicios desde la red de clase

Para acceder a los servicios internos desde cualquier equipo de la red de clase sólo tenemos que abrir el **cliente de dicho servicio** e introducir la **dirección adecuada**:

- Servidores web internos:
  - Abrimos navegador e introducimos: `http://172.16.200.x:8080` y `http://172.16.200.x:8081`
- Servidores ssh internos
  - Abrimos terminal y ejecutamos: `ssh usuario@172.16.200.x -p 2200` y `ssh usuario@172.16.200.x -p 2201`

7) Guardando los cambios para que se ejecuten al reiniciar el equipo

En el equipo router creamos un script con el nombre nat.sh:

```
$ nano nat.sh
```

E insertamos en el mismo los comandos que ejecutamos para activar el enrutamiento, activar el NAT y realizar la redirección de puertos:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 2200 -j DNAT --to 192.168.25.10:22
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 8080 -j DNAT --to 192.168.25.10:80
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 2201 -j DNAT --to 192.168.25.20:22
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 8081 -j DNAT --to 192.168.25.20:80
```

Guardamos el fichero y luego lo copiamos a la carpeta en la que se almacenan los scripts de inicio:

```
$ sudo mv nat.sh /etc/init.d
```

Le damos permiso de ejecución:

```
$ sudo chmod +x /etc/init.d/nat.sh
```

Hacemos que se ejecute al inicio del sistema enlazándolo en la carpeta del nivel de arranque por defecto:

```
$ sudo ln -s /etc/init.d/nat.sh /etc/rc2.d/S95masquradescript
```

Si ahora reiniciamos el equipo router se debería mantener el enrutamiento, el NAT y el redireccionamiento de puertos.

Cuando termines avisa al profesor para que revise la práctica