Numero: Nome: Data:

LAB05a

Configuração de um router com IP port forwarding

INTRODUÇÃO

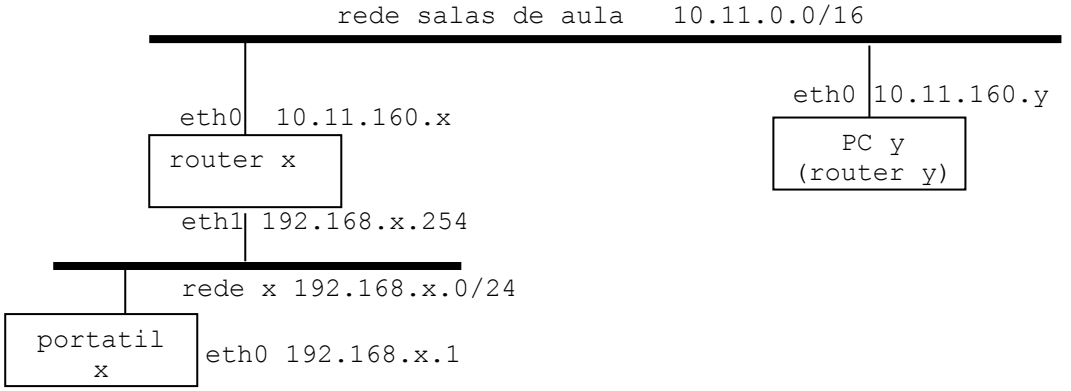
É necessário instalar no portátil um "serviço" web (ou ssh).

- Em Linux utiliza o gestor de pacotes da tua distribuição.
- Em Windows sugere-se
  - serviço ssh (porta 22): fazer o download de http://www.freesshd.com/
  - serviço web (porta 80): fazer o download de http://tinyserver.sourceforge.net/

A. IP port forwarding

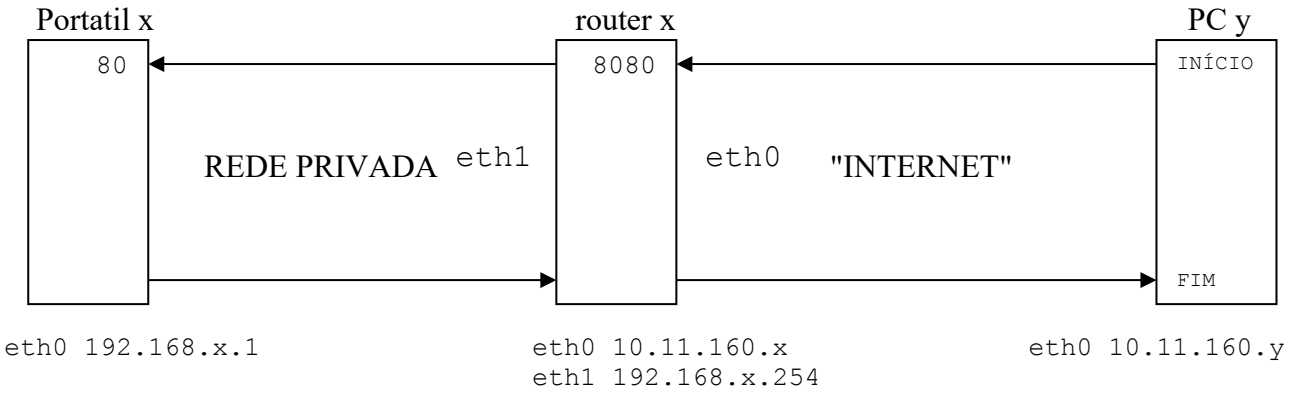
Pretende-se neste laboratório permitir o acesso a partir da "Internet" a um serviço oferecido por um servidor numa rede privada.

Considere a seguinte rede:



Como exemplo vai-se usar o serviço HTTP (porta 80) oferecido pelo teu "portátil" na rede privada "192.168.x.0/24 -rede x". Outra alternativa é o serviço ssh (porta 22). A "Internet" é representada pela rede das salas de aula.

Para atingir o objectivo vai-se abrir uma porta no router x com o número 8080, ou 2222, **e redireccionar todo o tráfego que dê entrada nessa porta** para a porta 80 (HTTP), ou para a porta 22 (ssh) do portátil x na rede privada, como se mostra na figura:



Numero: Nome: Data:

O PC y representa qualquer outro router na rede da sala (que assume aqui o papel de um PC na Internet). Pede a colaboração do grupo do lado durante os testes finais.

1. Configura a placa de rede eth1 do router

```
router# ifconfig eth1
```

_____

2. Verifica a configuração da tabela de routing do router

```
router# route -n
```

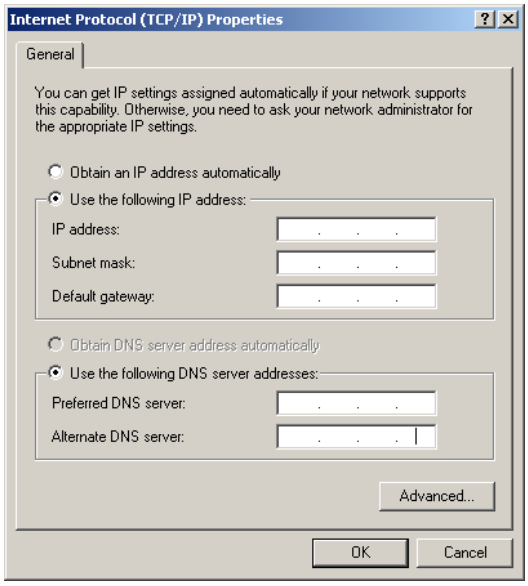
_____

3. Verifica que NÃO existem regras de filtragem activas no router

```
router# iptables -L
```

4. Configura o portátil com um IP estático (192.168.x.1/255.255.255.0 e gateway 192.168.x.254) e verifica a configuração da placa de rede e da tabela de routing

- Em Linux, utiliza a interface gráfica do serviço "Network Manager"[1]
- Em Windows utiliza a "janela" correspondente à tua versão do sistema operativo para configurar a placa de rede
    - Carrega simultâneamente nas teclas Windows+R
    - Na janela "Run" que aparece escreve "ncpa.cpl"
    - Clica com o botão direito do rato em "Local Area Connection"



[1] Ou, em alternativa, pára o serviço "Network Manager" e configura manualmente:

```
[Linux]portatil# service network-manager stop

[Linux]portatil# ifconfig eth0 ____________________________________

[Linux]portatil# route add default gw ____________________________
```

5. Verifica o funcionamento da rede local no portátil "pingando" a gateway:

```
[Linux] portatil# ifconfig
[Linux] portatil# ping 192.168.x.254

[Windows] c:\> ipconfig /all
[Windows] c:\> route PRINT -4
[Windows] c:\> ping 192.168.x.254
```

6. Activa no router a funcionalidade de "router"

```
router# echo 1 > /proc/sys/net/ipv4/ip_forward
```

7. Configura o router para fazer **port forward** do tráfego que chega ao router na porta 8080 para a porta 80 do portátil

```
router# iptables -t nat -A PREROUTING -i eth0 -p tcp -d ___.___.___.__
--dport 8080 -j DNAT --to-destination ___.___.___._:__
```

E/OU configura o router para fazer **port forward** do tráfego que chega ao router na porta 2222 para a porta 22 do portátil

```
router# iptables -t nat -A PREROUTING -i eth0 -p tcp -d __.____.___.__
--dport 2222 -j DNAT --to-destination ___.___.___._:__
```

Configura o router para fazer NAT do tráfego proveniente da rede interna

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

Verifica que as regras de port forward e NAT estão correctas:

```
router# iptables -L -t nat -n
```

8. Verifica que existe um servidor web (porta 80) activo no portátil. Usa o teu browser preferido. Por exemplo, em Linux,

```
[Linux]portatilx# chrome http://127.0.0.1:80
[Windows] c:\> chrome http://127.0.0.1:80
```

NOTA: em alternativa podes instalar o serviço ssh (porta 22) no portátil. Neste caso não te esqueças de fazer as alterações correspondentes nos pontos 6. e 7 e utiliza o PuTTY para verificares que o teu portátil (IP 127.0.0.1) tem aberta a porta 22

9. Instala no router o programa de monitorização de trafego iptraf

```
router# apt-get install iptraf
```

Numero: Nome: Data:

10. Numa shell do router x arranca o programa **iptraf** e monitoriza o tráfego na placa eth0 e na placa eth1 (**`IP traffic monitor > all`**)

```
router# iptraf
```

11. A partir do portátil y ou do router[2] y (pede a colaboração do grupo y ao lado) faz uma sessão web especificando a porta 8080 para o teu router (IP 10.11.160.x)

```
[Windows portatil_y] c:\> chrome http://10.11.160.x:8080
[Linux]router_y# chromium-browser http://10.11.160.x:8080
```

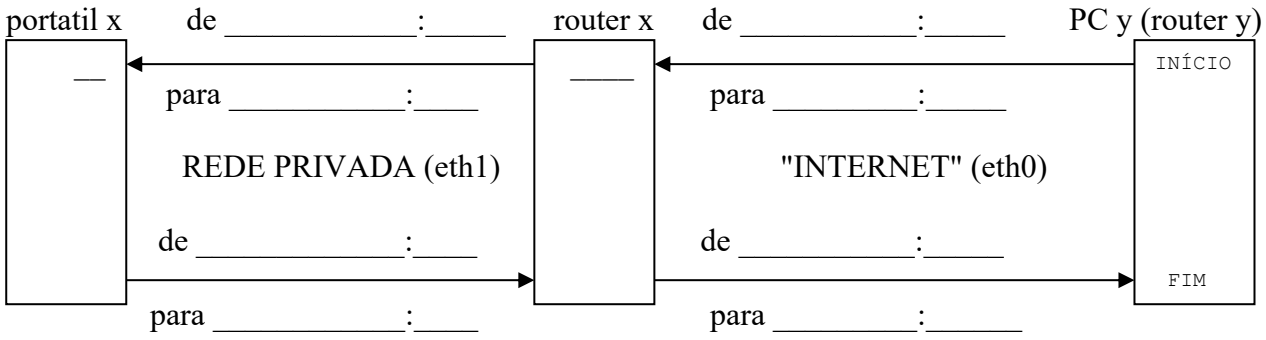
ou em alternativa faz uma sessão ssh especificando a porta 2222

```
[Linux]router_y# ssh root@10.11.160.x -p 2222
[Windows portatil_y] c:\> PuTTY
```

12. Confirma que os pedidos de ligação estão a ser redireccionados pelo router e a chegar ao serviço correspondente no portatil x na rede interna.

Completa o esquema com os dados que obtiveste com o programa iptraf (os campos do esquema devem ser completados do "INÍCIO" para o "FIM", isto é, da direita para a esquerda na figura...).

NOTA: o iptraf está a registar muito tráfego? Podes sempre "congelar" o display com CTRL-S e "descongelar" o display com CTRL-Q...



13. Termina aqui este laboratório. Faz reboot ao router.

[2] poderá ser necessário instalar um browser (por exemplo o chromium) no router:

```
router_y# apt-get install chromium-browser
```

Numero: Nome: Data:

14. (OPCIONAL) Configura o router x para encaminhar **exclusivamente o tráfego que tem origem na rede exterior** e tem por destino a porta 80 do portatil

```
router# iptables -P FORWARD DROP
router#iptables -A FORWARD -i eth0 -o eth1 -p tcp --syn -d __.__.___.__     -
-dport 80 -m conntrack --ctstate NEW -j ACCEPT
router# iptables -A FORWARD -i eth0 -o eth1 -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
router# iptables -A FORWARD -i eth1 -o eth0 -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
```

15. Para que serve a primeira regra? E a segunda? E a terceira? E a quarta?
