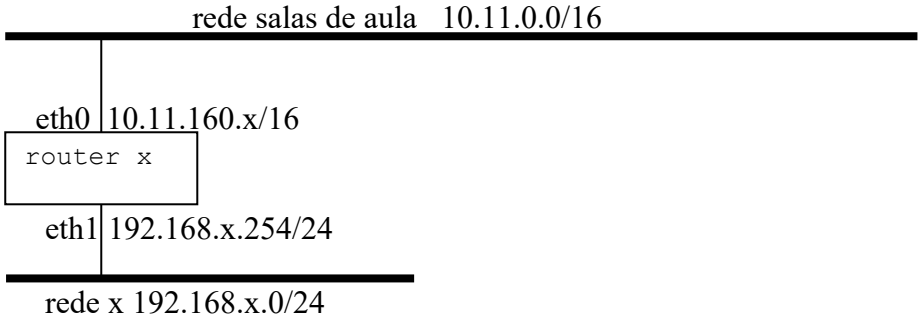
Numero: Nome: Data:

LAB05

Configuração de uma Firewall
Network Address Translation (NAT)

A. Filtragem do tráfego de saída (output)

Neste exercício vai-se configurar o programa `iptables` de forma a não autorizar o acesso à porta HTTP (80) e HTTPS (443) do servidor www.ualg.pt



1. Configura a placa de rede eth1 do router (a placa eth0 já está configurada)

```
#ifconfig eth1_____________________________________________________
```

2. Verifica a configuração das placas de rede eth0 e eth1 do router

```
#ifconfig
```

3. Verifica a configuração da tabela de routing do router

```
#route -n
```

_____
_____
_____

4. Verifica que NÃO existem das regras de filtragem activas no router

```
#iptables -L
```

_____
_____
_____

5. Verifica com o browser chromium (é o open source chrome) se podes aceder ao site `www.ualg.pt`.

```
#apt-get install chromium-browser
#ln -s /usr/bin/chromium-browser /usr/bin/chrome
#chrome --no-sandbox www.ualg.pt
```

Podes?_____ deves poder...

6. Escreve o comando:

```
#apt-get install dnsutils
#nslookup www.ualg.pt
#iptables -A OUTPUT -d ___.___.___.___/32  -p tcp --dport 80 -j
DROP
#iptables -A OUTPUT -d ___.___.___.___/32  -p tcp --dport 443 -j
DROP
```

7. Faz reload da página web (limpa o cache ou usa uma janela anónima). E agora ainda podes aceder? _____

8. Faz flush (apaga) estas regras:
```
#iptables -F
```

9. Escreve agora uma regra para impedir o acesso ao site web `fct.ualg.pt`

```
#nslookup fct.ualg.pt
#iptables _____________________________________________________
#iptables _____________________________________________________
```

Verifica com o browser que não consegues aceder). Podes? _____

10. Escreve agora um conjunto de regras que permitam APENAS dar acesso
    - ao servidor smtp.ualg.pt e a qualquer porta deste servidor.

```
#nslookup smtp.ualg.pt
#iptables -P OUTPUT _____________________________________________
#iptables -A OUTPUT _____________________________________________
#iptables -A OUTPUT _____________________________________________
```

11. Faz uma listagem das regras, e verifica (ping) que só consegues chegar a esta máquina e a mais nenhuma outra:_____

```
#iptables -L
#ping 193.136.224.139
```
Obtens resposta?_____ deves conseguir...
```
#ping 193.136.224.140
```
Obtens resposta?_____ deves conseguir...
```
#ping 193.136.224.33
```
Obtens resposta?_____ não deves conseguir...

B. Filtragem do tráfego de entrada (input)

Neste exercício vai-se configurar a firewall de forma a não permitir a entrada na porta ssh (porta 22) do router.

12. Verifica que o servidor se encontra activo (porta 22 está aberta)
```
#netstat -anp | grep sshd
```

13. Pede ao grupo do lado (router y) para fazer ssh para o teu router (router).

```
Router_y# ssh root@10.11.160.x
```

Consegues?_____ deves conseguir...

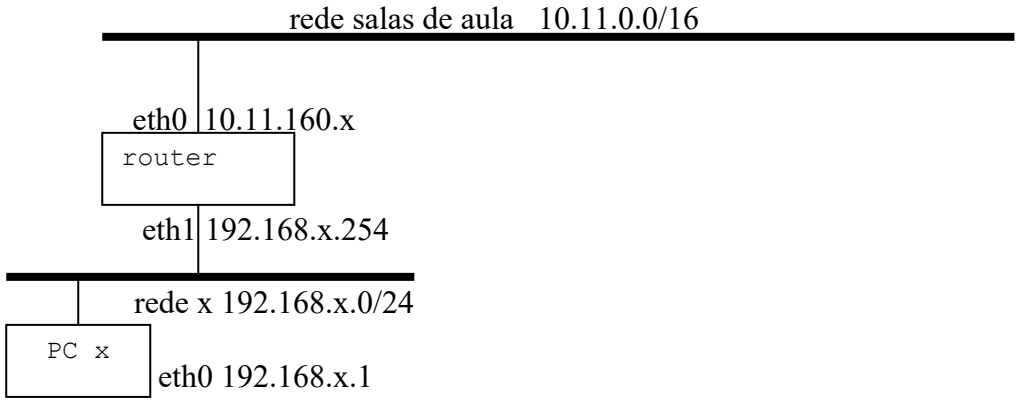
14. Instala as regras de filtragem que impedem o router do grupo do lado de aceder à porta ssh do teu router

```
#iptables –F
#iptables –P INPUT ACCEPT
#iptables –P OUTPUT ACCEPT
#iptables -A INPUT -s ________ -d _______ -p ___ --dport _____
-j_____
```

15. Pede novamente ao grupo do lado para fazer ssh para o teu router. Consegues? ____ não deves conseguir...

C. Filtragem do tráfego de passagem (forward)

Considera a seguinte rede:



16. Escreve um conjunto de regras que <u>apenas</u> deixem passar o tráfego proveniente da rede 192.168.x.0/24 com destino ao IP 10.11.160.1 porta tcp 80 (e obviamente também o tráfego de resposta!)

```
#iptables –P INPUT _______
#iptables –P OUTPUT _______
#iptables –P FORWARD _____
#iptables -A FORWARD -s ________ -d _______ -p ___ --dport ___ -j
_____
#iptables -A FORWARD -s ________ -d _______ -p ___ --sport ___ -j
_____
```

Numero: Nome: Data:

D. Network Address Translation (NAT)

A rede 192.16.8.x.0/24 é uma rede local, apenas conhecida pelo router e desconhecida dos outros routers. Como viste na LAB04 é necessário actualizar as tabelas de routing de todos os routers na rede 10.11.0.0/16 para eles saberem que a rede 192.168.x.0/24 existe e há um router que dá acesso para essa rede.

Se nada for feito na tabela de routing do router, um portátil na rede 192.16.8.x.0/24 quando envia tráfego para a rede 10.11.0.0/16 não recebe a resposta.

Também um portátil na rede 192.16.8.x.0/24 não consegue enviar tráfego para a Internet. A única alternativa quando se liga uma rede com endereços privados à Internet é Network Address Translation (NAT).

17. Utiliza o teu portátil. **Configura a interface de rede no portátil com**
    - **IP estático: `192.168.x.1/24`**
    - **gateway: `192.168.x.254`**
    - **servidor de DNS: `10.10.22.228`**

18. Verifica a configuração da placa de rede do teu portátil

```
[Windows]c:\>ipconfig /all
```

19. Verifica a configuração da tabela de routing do teu portátil

```
[Windows]c:\>route PRINT -4
```

_____

_____

20. Do teu portátil faz ping para qualquer router na sala (mas não o teu!). Por exemplo
    `[Windows]c:\> ping 10.11.160.15`
    Faz ping a um servidor web na Internet: Por exemplo
    `[Windows]c:\> ping www.google.pt`

Há resposta? _____. Porquê? _____

21. Configura agora o router (server x) para fazer NAT a todo o tráfego proveniente da rede local

```
#iptables -F
#iptables -P INPUT ACCEPT
#iptables -P FORWARD ACCEPT
#iptables -P OUTPUT ACCEPT
#iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
#iptables -L -t nat
```

22. Activa a função de router no kernel

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

23. Instala no router o programa de monitorização de tráfego `iptraf`

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

24. Numa shell arranca o programa iptraf e monitoriza o tráfego na placa eth0 e eth1 (**IP traffic monitor > all interfaces**)

```
#iptraf
```

25. A partir do teu portátil faz ping novamente para qualquer PC na sala 160 sala (mas não o teu!). Por exemplo

```
[Windows]c:\> ping 10.11.160.15
```

Sucesso? _____. Verifica com o programa `iptraf` que os pings estão a sair para a rede das salas de aula (placa eth0) **tendo como origem o IP do router**. Completa a tabela:

interface eth1:IP origem:_____Interface eth0:IP origem:_____
IP destino:_____ IP destino:_____

26. A partir do teu portatil faz uma sessão web com o browser (chrome, edge, firefox,...) para **www.google.pt**

Verifica com o programa `iptraf` que a ligação na rede interna (interface eth1) está a sair tendo como origem o IP do PC x, **mas a mesma ligação na rede da sala de aula (interface eth0) está a sair tendo com origem o IP do router.**

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

Completa a tabela:

interface eth1:IP origem:_____porta_____ interface eth0:IP origem:_____porta___
IP destino:_____porta_____ IP destino:_____ porta___

Termina aqui este laboratório. Faz “reboot” ao router