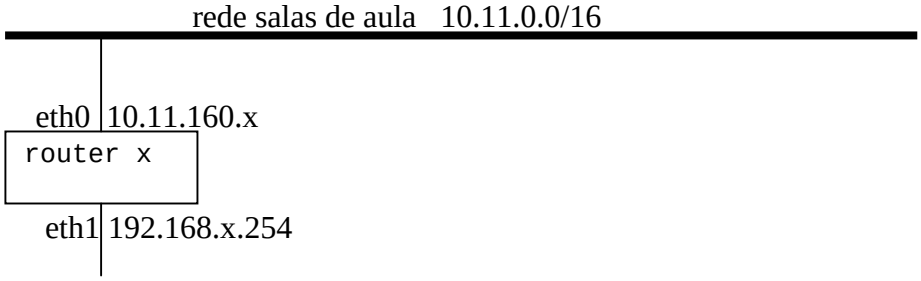
Numero: Nome: Data:

LAB05

Configuração de uma Firewall
Network Address Translation (NAT)

A. Filtragem do trafego de saída (output)

Neste exercício vai-se configurar o programa `iptables` de forma a <u>não autorizar</u> o acesso à porta 80 do servidor www.ualg.pt



1. Verifica a configuração das placas de rede do router x

```
#ifconfig
```

2. Verifica a configuração da tabela de routing do router x

```
#route –n
```

_____
_____

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

```
#iptables -L
```

_____
_____
_____

4. Verifica com o browser chromium (é o open source chrome) que 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?_____

5. Escreve o comando:

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

6. Faz reload da página web. E agora ainda podes aceder?_____

7. Faz flush (apaga) esta regra:

```
#iptables -F
```

8. Escreve agora uma regra para impedir o acesso à porta 80 do servidor www.fct.ualg.pt

```
#nslookup www.fct.ualg.pt
#iptables_____________________________________________________________
```

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

9. 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 _____________________________________________________
```

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

```
#iptables –L
#ping 193.136.224.7
```

Obtens resposta?_____

```
#ping 193.136.224.33
```

Obtens resposta?_____

B. Filtragem do trafego de entrada (input)

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

11. Verifica que o servidor se encontra activo (porta 22 está aberta)

```
#netstat -anp | more
```

12. Pede ao grupo do lado para fazer ssh para o teu router. Consegue?_____

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

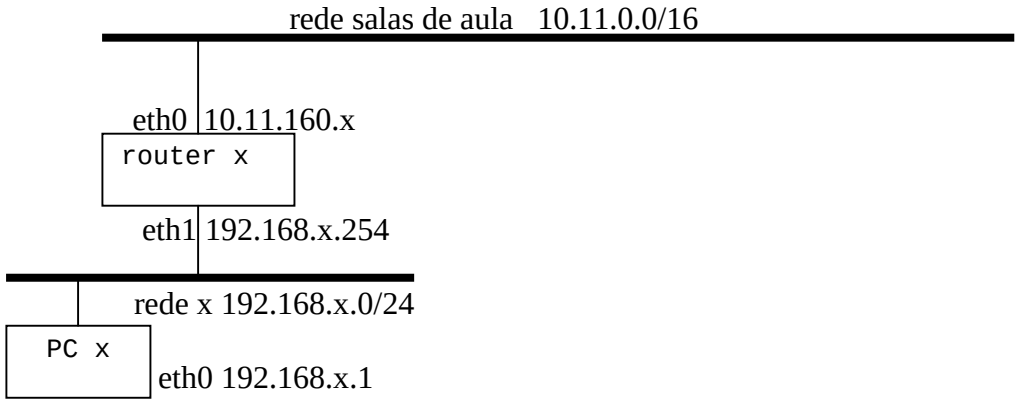
```
#iptables –F
#iptables –P INPUT ACCEPT
#iptables –P OUTPUT ACCEPT
#iptables -A INPUT -s __________ -d _______ -p ___ --dport ___
-j _____
```

14. Pede ao grupo do lado para fazer ssh para o teu router. Consegue?_____

Numero: Nome: Data:

C. Filtragem do trafego de passagem (forward)

Considera a seguinte rede:



15. Escreve um conjunto de regras que apenas 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
_______
```

D. Network Address Translation (NAT)

A rede 192.16.8.x.0/24 é uma rede local, apenas conhecida pelo router x 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 nas tabelas de routing dos routers na rede das salas de aula, um portatil na rede 192.16.8.x.0/24 quando envia tráfego para o exterior da rede não recebe a resposta.

Uma alternativa (a única quando se liga uma rede com endereços privados à Internet) é Network Address Translation (NAT).

16. Utiliza o teu portátil. Configura[1] a interface de rede no portatil com um IP estático 192.168.x.1/24, gateway 192.168.x.254, e servidor de DNS 10.10.22.228.

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

```
[Linux]#ifconfig
[Windows]c:\>ipconfig /all
```

[1] Em alternativa podes sempre activar o serviço DHCP no router com o comando:
`#/usr/sbin/dhcpd eth1`

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

```
[Linux]#route –n
[Windows]c:\>route PRINT -4
```

_____
_____

19. Do teu portatil faz ping para qualquer router na sala. Por exemplo

```
#ping 10.11.160.1
```

Há resposta? _____. Porquê? _____

20. Configura agora o router x (server x) para fazer NAT a todo o trafego 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
```

21. Activa a função de router no kernel

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

22. Instala no router x o programa de monitorização de trafego iptraf

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

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

```
#iptraf
```

24. A partir do teu portatil faz ping novamente para qualquer PC na sala 160. Por exemplo

```
#ping 10.11.160.1
```

25. 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 x

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

26. A partir do teu portatil faz uma sessão web com um browser para www.google.pt

27. Verifica com o programa iptraf que as ligações na rede interna (interface eth1) estão a sair tendo como origem o IP do PC x, <u>mas as mesmas ligações na rede das salas de aula (interface eth0) estão a sair tendo com origem o IP do router x</u>

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

Termina aqui este laboratório. Devolve o cabo cruzado. Desliga o router e o monitor