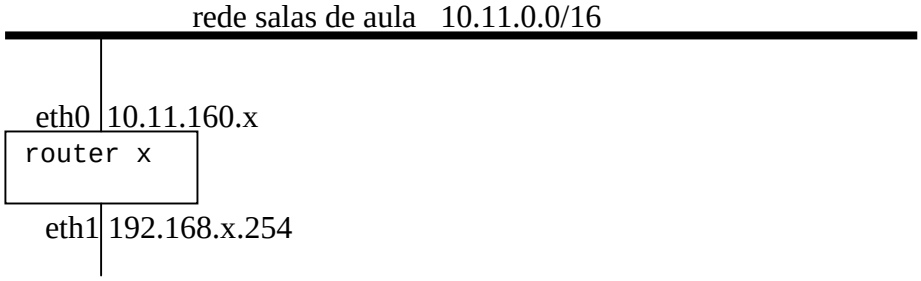
Numero: Nome: Data:

LAB05

Configuração de uma Firewall
Network Address Translation (NAT)

A. Filtragem do trafego de saída (output)

Neste exercício vai-se configurar o programa ipchains de forma a não autorizar 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

```
#ipchains -L
```

_____
_____
_____

4. Verifica com o browser opera que podes aceder ao site www.ualg.pt. Podes?_____

5. Escreve o comando:

```
#nslookup www.ualg.pt
#ipchains -A output -d ___.___.___.___/32 80 -p tcp -j DENY
```

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

7. Faz flush (apaga) esta regra:

```
#ipchains -F
```

8. Escreve agora a regra:

```
#ipchains -A output -d ___.___.___.___/32 80 –p tcp -j REJECT
```

Numero: Nome: Data:

9. Qual a diferença entre a acção DENY e REJECT? _____

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

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

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

11. 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
#ipchains -P output _____________________________________________
#ipchains -A output _____________________________________________
```

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

```
#ipchains –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 na porta telnet (porta 23) ou na porta ssh (porta 22).

13. Se ainda não estiver instalado, instala um servidor de telnet no router x

```
#apt-get install telnetd
```

14. Verifica que o servidor se encontra activo (porta 23 está aberta) e/ou (porta 22 está aberta)

```
#netstat -anp
```

15. Pede ao grupo do lado para fazer telnet ou ssh para o teu router. Consegue?_____

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

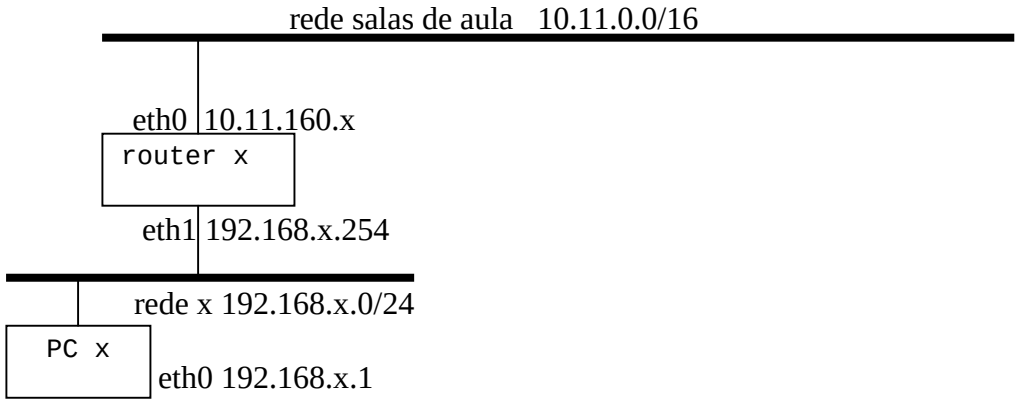
```
#ipchains –F
#ipchains –P input ACCEPT
#ipchains –P output ACCEPT
#ipchains –P forward ACCEPT
#ipchains -A input -s __________ -d _______ __ -p ___ -j _____
```

17. Pede ao grupo do lado para fazer telnet ou ssh para o teu router. Consegue?_____

Numero: Nome: Data:

C. Filtragem do trafego de passagem (forward)

Considera a seguinte rede:



18. 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!)

```
#ipchains –P input _______
#ipchains –P output ______
#ipchains –P forward _____
#ipchains -A forward -s __________ -d ______ -p ___ -j ______
#ipchains -A forward -s __________ -d ______ -p ___-j ______
```

19. Qual a opção que permite reduzir as duas últimas regras numa só?_____
    Escreve o comando ipchains correspondente às duas últimas regras numa só:

```
#ipchains -A forward ____________________________________________
```

D. Network Address Translation (NAT)

A rede 192.16.8.x.0/24 é uma rede local, desconhecida dos routers na rede das salas de aula. 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 há uma gateway para a rede 192.168.x.0/24.

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 a rede 10.11.0.0/16 não recebe a resposta. A resposta é enviada para o router de defeito (10.11.0.254) que desconhece a existência das redes privadas.

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

20. 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.

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

```
[Linux]#ifconfig
```

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

```
[Windows]#ipconfig /all
```

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

```
[Linux]#route –n
```

_____
_____

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

```
#ping 10.11.160.1
```

Há resposta? _____. Porquê? _____

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

```
#ipchains -F
#ipchains –P input ACCEPT
#ipchains -P forward ACCEPT
#ipchains -P output ACCEPT
#ipchains -A forward -s _____________ -d 0.0.0.0/0 -j MASQ
```

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

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

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

```
#iptraf
```

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

```
#ping 10.11.160.1
```

28. 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:_____

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

30. 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</u> na rede das salas de aula (interface eth0) estão a sair tendo com origem o IP do router x

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