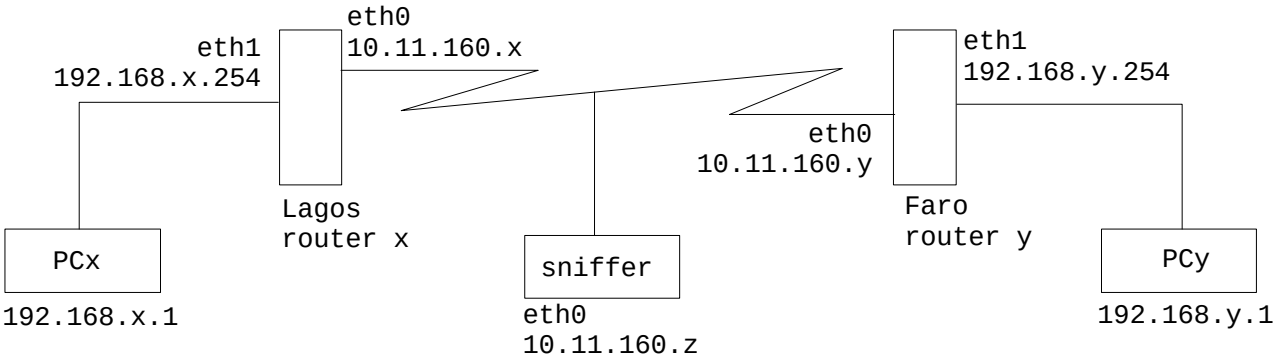
Numero: Nome: Data:

LAB012

Configuração de uma rede privada virtual (VPN) com a aplicação IPsec[1]

Neste laboratório vamos implementar uma ligação segura (túnel encriptado) entre dois escritórios da mesma empresa: a filial de Lagos e a filial de Faro

A configuração da rede é a seguinte:



A rede da sala de aula 10.11.0.0/16 funciona como rede pública, onde é realizado o túnel encriptado entre o Lagos router ("router_x") e o Faro router ("router_y").

A rede 192.168.x.0/24 é a rede privada da filial de Lagos. A rede 192.168.y.0/24 é a rede privada da filial de Faro.

O PC com o IP 10.11.160.z é um outro qualquer PC na rede da sala de aula que funciona como "sniffer" correndo o programa wireshark (ou tcpdump). Funciona como prova que a comunicação entre a filial de Faro e a filial de Lagos está encriptada.

O laboratório é realizado por dois grupos que trabalham em conjunto. Um grupo administra a rede privada da filial de Faro; o outro grupo administra a rede privada da filial de Lagos.

Como funciona

Quer o Faro router quer o Lagos router encriptam o datagrama IP original:

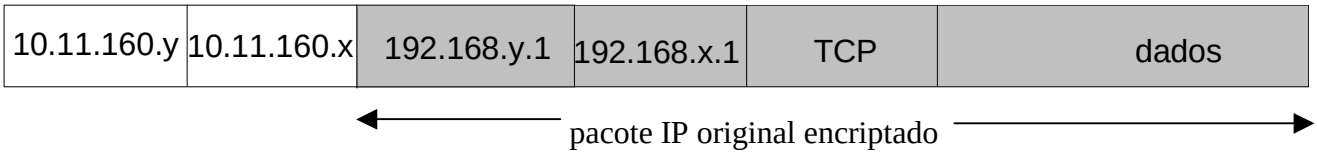
Pacote IP original (dentro da rede privada):

192.168.y.1	192.168.x.1	TCP	dados

Pacote IP na Internet:

[1] https://wiki.debian.org/IPsec

Numero: Nome: Data:



A. Teste da rede não encriptada

É importante verificar o funcionamento correcto da rede antes de se realizar o túnel. Realizam-se aqui os passos necessários para realizar os testes[2].

1. no Lagos router

```
router_x# ifconfig eth0 _____________ netmask _____________
router_x# ifconfig eth1 _____________ netmask _____________
router_x# route add -net 192.168.y.0 netmask 255.255.255.0 gw _____________
router_x# echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. no Faro router

```
router_y# ifconfig eth0 _____________ netmask _____________
router_y# ifconfig eth1 _____________ netmask _____________
router_y# route add -net 192.168.x.0 netmask 255.255.255.0 gw _____________
router_y# echo 1 > /proc/sys/net/ipv4/ip_forward
```

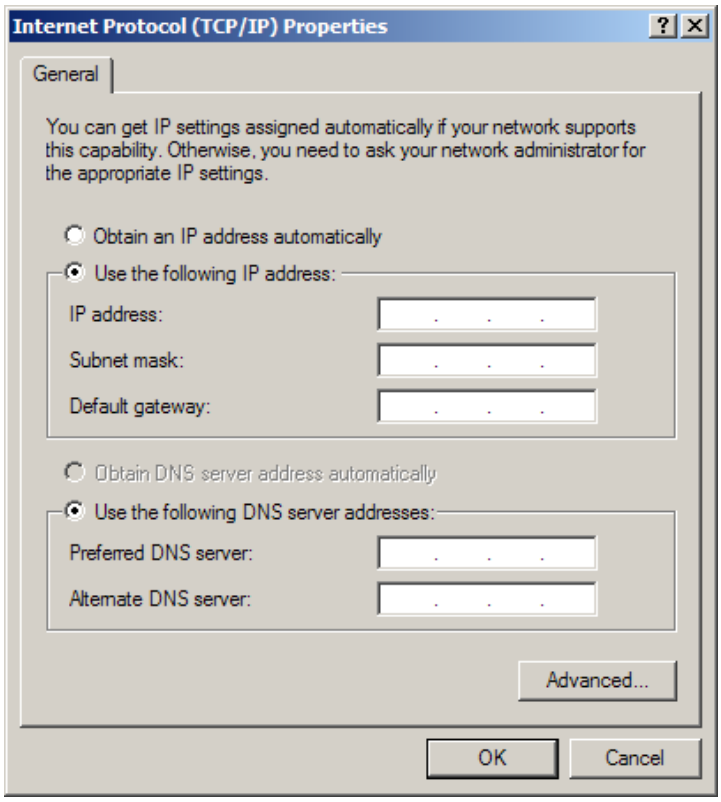
3. no portatil x

[Windows]

Em Windows deves utilizar a janela correspondente à tua versão do sistema operativo para configurares a interface com um **IP estático**.

[2] Em caso de dúvida consultar o Lab04 em http://intranet.deei.fct.ualg.pt/GRS/lab04.pdf

Numero: Nome: Data:



[Linux]

Utiliza a janela correspondente à tua versão do Linux. Em alternativa, desliga o serviço Network Manager e configura a placa de rede manualmente:

```
pcx# service network-manager stop

pcx# ifconfig eth0 _____________ netmask _____________
pcx# route add default gw _________________
```

4. no portatil y a configuração é idêntica

[Linux]

```
pcy# ifconfig eth0 _____________ netmask _____________
pcy# route add default gw _________________
```

5. no portatil x

```
pcx# ping 192.168.y.1
```

Recebes o echo? _____ Realiza as correcções necessárias nas configurações da rede até obteres sucesso.

6. no portatil y

```
pcy# ping 192.168.x.1
```

Numero: Nome: Data:

Recebes o echo? _____ Realiza as correcções necessárias nas configurações da rede até obteres sucesso.

Nota: Desliga a firewall no windows e a rede wireless. Não é preciso o ping funcionar de ambos os lados para testar a ligação, basta o ping funcionar de um lado...

B. Configuração do PC "sniffer"

7. Instale o programa wireshark no PC "sniffer" e arranca o programa

```
router_z# apt-get install wireshark
router_z# wireshark
```

8. Captura apenas o trafego em que está envolvido o portatil x e o portatil y

Capture > Start > Filter `host _____ and host _____`

9. No portatil x com o teu browser preferido faz uma sessão web (HTTP) para o portatil y [3]

```
pcx# chrome 192.168.y.1
```

10. Verifica que o programa wireshark no PC "sniffer" interceptou a comunicação entre o browser e o servidor web:

Consegues ler os dados? _____

C. Configuração da rede VPN

Instala e configura os pacotes `racoon ipsec-tools` em ambos os routers.

```
router_x# apt-get install racoon ipsec-tools
router_y# apt-get install racoon ipsec-tools
```

Nota: cada grupo é apenas responsável pela configuração do seu router!

11. Configura o tunel visto do router_x (substitui "`10.11.160.x`" e "`10.11.160.y`" pelos Ips dos routers envolvidos). Nota: cada grupo é apenas responsável pela configuração do seu router!

Segue as instruções no APÊNDICE A1

12. Configura o tunel visto do router_y (substitui "`10.11.160.x`" e "`10.11.160.y`" pelos Ips dos routers envolvidos). Nota: cada grupo é apenas responsável pela configuração do seu router!

[3] Nota: o portatil y tem que ter um servidor servidor web (porta 80). Em Linux utiliza o gestor de pacotes da tua distribuição. Em Windows sugere-se fazer o download de http://tinyserver.sourceforge.net/

Numero: Nome: Data:

Segue as instruções no APÊNDICE B1

13. Configura a chave simétrica partilhada por ambos os routers. Nota: cada grupo é apenas responsável pela configuração do seu router!

```
router_x#  nano /etc/racoon/psk.txt

10.11.160.y  a9993e364706816aba3e

router_y#  nano /etc/racoon/psk.txt

10.11.160.x  a9993e364706816aba3e
```

14. Configura a política de segurança no "lagos router". Nota: cada grupo é apenas responsável pela configuração do seu router!

Segue as instruções no APÊNDICE A2

15. Configura a política de segurança no "faro router". Nota: cada grupo é apenas responsável pela configuração do seu router!

Segue as instruções no APÊNDICE B2

16. Arranca o túnel nos dois routers

```
router_x#  /etc/init.d/setkey restart
router_x#  /etc/init.d/racoon restart

router_y#  /etc/init.d/setkey restart
router_y#  /etc/init.d/racoon restart
```

D. Teste da rede encriptada

17. no portatil x

```
pcx# ping  192.168.y.1
```

Recebes o echo? _____ Realiza as correcções necessárias nas configurações da rede até obteres sucesso.

18. no portatil y

```
pcy# ping  192.168.x.1
```

Recebes o echo? _____ Realiza as correcções necessárias nas configurações da rede até obteres sucesso.

Nota: Não é preciso o ping funcionar de ambos os lados para testar a ligação, basta o ping funcionar de um lado...

Numero: Nome: Data:

19. No portatil x com o teu browser preferido faz uma sessão web (HTTP) para o portatil y

```
pcx# chrome 192.168.y.1
```

20. Configura o programa wireshark no `router_z` para interceptar a ligação:

Capture > Start > Filter `host _____ and host _____`

Consegues ler os dados? _____
Qual é o protocolo de encriptação detectado? _____

Termina aqui este laboratório. Devolve o cabo cruzado.

APÊNDICE A1 - Configuração do tunel no router_x

```
router_x# cp -a /etc/racoon/racoon.conf /etc/racoon/racoon.conf.dpkg-dist
router_x# nano /etc/racoon/racoon.conf

path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

remote 10.11.160.y {
        exchange_mode main,aggressive;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2;
        }
#        generate_policy off;
}
#
sainfo address 192.168.x.0/24 any address 192.168.y.0/24 any {
        pfs_group 2;
        encryption_algorithm 3des, blowfish 448, rijndael;
        authentication_algorithm hmac_sha1, hmac_md5;
        compression_algorithm deflate;
}
```

APÊNDICE A2 - Configuração da política de segurança no router_x

```
router_x#  cp -a /etc/ipsec-tools.conf /etc/ipsec-tools.conf.dpkg-dist
router_x#  nano /etc/ipsec-tools.conf

#!/usr/sbin/setkey -f
# NOTE: Do not use this file if you use racoon with racoon-tool
# utility. racoon-tool will setup SAs and SPDs automatically using
# /etc/racoon/racoon-tool.conf configuration.
#

## Flush the SAD and SPD
#
flush;
spdflush;

## Some sample SPDs for use racoon
#
spdadd 192.168.y.0/24 192.168.x.0/24 any -P in ipsec
    esp/tunnel/10.11.160.y-10.11.160.x/require;
#
spdadd 192.168.x.0/24 192.168.y.0/24 any -P out ipsec
    esp/tunnel/10.11.160.x-10.11.160.y/require;
#
```

APÊNDICE B1 - Configuração do tunel no router_y

```
router_y# cp -a /etc/racoon/racoon.conf /etc/racoon/racoon.conf.dpkg-dist
router_y# nano /etc/racoon/racoon.conf
```

```
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";


remote 10.11.160.x {
        exchange_mode main,aggressive;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group 2;
        }
#        generate_policy off;
}
#
sainfo address 192.168.y.0/24 any address 192.168.x.0/24 any {
        pfs_group 2;
        encryption_algorithm 3des, blowfish 448, rijndael;
        authentication_algorithm hmac_sha1, hmac_md5;
        compression_algorithm deflate;
}
```

APÊNDICE B2 - Configuração da política de segurança no router_y

```
router_y#  cp -a /etc/ipsec-tools.conf /etc/ipsec-tools.conf.dpkg-dist
router_y#  nano /etc/ipsec-tools.conf
#!/usr/sbin/setkey -f

# NOTE: Do not use this file if you use racoon with racoon-tool
# utility. racoon-tool will setup SAs and SPDs automatically using
# /etc/racoon/racoon-tool.conf configuration.
#

## Flush the SAD and SPD
#
flush;
spdflush;

## Some sample SPDs for use racoon
#
spdadd 192.168.x.0/24 192.168.y.0/24 any -P in ipsec
    esp/tunnel/10.11.160.x-10.11.160.y/require;
#
spdadd 192.168.y.0/24 192.168.x.0/24 any -P out ipsec
    esp/tunnel/10.11.160.y-10.11.160.x/require;
#
```