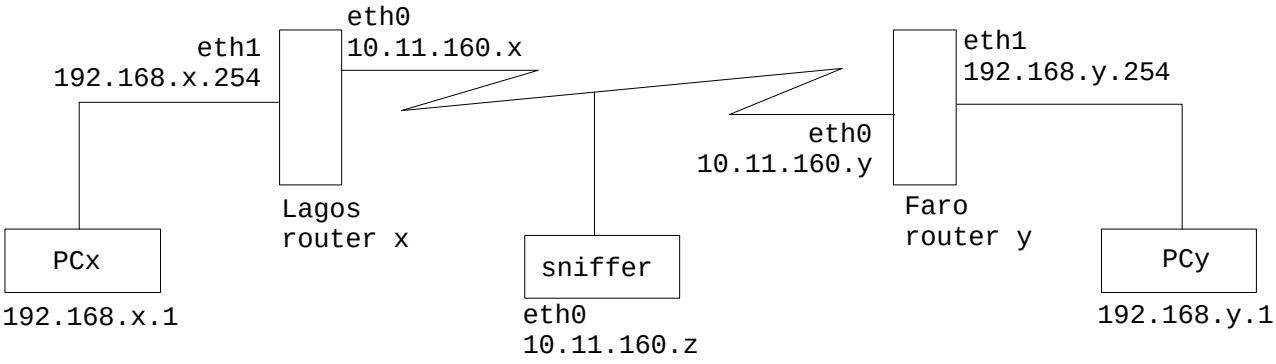
Numero: Nome: Data:

LAB012

Configuração de uma rede privada virtual (VPN) com a aplicação FreeSWAN

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

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 ethereal. 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:

10.11.160.y	10.11.160.x	192.168.y.1	192.168.x.1	TCP	dados

pacote IP original encriptado

Numero: Nome: Data:

A. Instalação de um novo kernel

1. Um kernel especialmente compilado para encriptar os pacotes IP encontra-se disponível no volume de rede /mnt. Repete estes comandos no Faro router e no Lagos router.

```
#cp -a /mnt/extras/FreeSwan/vmlinuz-2.2.18 /boot
#cp -a /mnt/extras/FreeSwan/System.map-2.2.18 /boot
#cp -a /mnt/extras/FreeSwan/ipsec.conf /etc
#cp -a /mnt/extras/FreeSwan/ipsec.secrets /etc
#cp -a /mnt/extras/FreeSwan/ipsec  /usr/local/sbin
#cp -a /mnt/extras/FreeSwan/ipsec.sh   /etc/init.d/ipsec


#cp -a /mnt/extras/FreeSwan/ipsec.tgz /usr/local/lib
#cd /usr/local/lib
#tar xzf ipsec.tgz

#apt-get install libgmp2
```

2. Re-inicia os computadores Faro router e Lagos router

B. 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.

3. no Lagos router

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

4. no Faro router

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

5. no PC x

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

6. no PC y

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

Numero: Nome: Data:

7. no PC x

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

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

8. no PC y

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

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

C. Configuração do PC "sniffer"

9. Instale o programa ethereal no PC "sniffer" e arranca o programa

```
sniffer#apt-get install ethereal
sniffer#ethereal
```

10. Captura apenas o trafego em que está envolvido o PC x e o PC y

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

11. No PC x faz uma sessão telnet para o PC y [1]

```
pcx#telnet 192.168.y.1
login as: user (substitui "user" por um utilizador válido no Pc y)
user@192.168.y.1's password: (a password do "user")
$uname -a
```

12. Verifica que o programa ethereal no PC "sniffer" interceptou a password e os dados:

Consegues ler a password e os dados?

_____

D. Configuração da rede VPN

Configura a aplicação FreeSWAN com os IPs que estás a utilizar para o Faro router e o Lagos router. O ficheiro `ipsec.conf` configura o túnel para os IP dos routers que estás a utilizar. O ficheiro `ipsec.secrets` contem a chave simétrica e a chave asimétrica (pública e privada).

(Opcional) Nota que podes fazer novas chaves utilizando os comandos

```
#ipsec rsasigkey 2048
#ipsec ranbits 256
```

[1] Nota: o PC y tem que ter um servidor telnet instalado!

13. no Faro router

```
faro#xedit /etc/ipsec.conf
faro#xedit /etc/ipsec.secrets
```

14. no Lagos router

```
lagos#xedit /etc/ipsec.conf
lagos#xedit /etc/ipsec.secrets
```

15. Em ambos os routers arranca o serviço NAT e o serviço VPN

```
lagos#ipchains -A forward -i eth0 -j MASQ
lagos#/etc/init.d/ipsec start
lagos#echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
lagos#echo 0 > /proc/sys/net/ipv4/conf/ipsec0/rp_filter

faro#ipchains -A forward -i eth0 -j MASQ
faro#/etc/init.d/ipsec start
faro#echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
faro#echo 0 > /proc/sys/net/ipv4/conf/ipsec0/rp_filter
```

E. Teste da rede encriptada

16. no PC x

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

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

17. no PC y

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

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

18. No PC x faz uma sessão telnet para o PC y

```
pcx#telnet 192.168.y.1
login as: user
```
(substitui "user" por um utilizador válido no Pc y)

```
user@192.168.y.1's password:
```
(a password do "user")

```
$uptime
```

19. Verifica que o programa ethereal no PC "sniffer" interceptou a ligação:

Capture > Start > Filter `host _____ and host _____`
Consegues ler o texto? _____

Termina aqui este laboratório. Devolve o cabo cruzado.

APÊNDICE A - IPSEC.CONF

```
$ cat ipsec.conf
# /etc/ipsec.conf - FreeS/WAN IPSEC configuration file

# More elaborate and more varied sample configurations can be found
# in FreeS/WAN's doc/examples file.



# basic configuration
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        interfaces="ipsec0=eth0"
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
        klipsdebug=none
        plutodebug=none
        # Use auto= parameters in conn descriptions to control startup actions.
        plutoload=lagos-faro
        plutostart=lagos-faro
        # Close down old connection when new one using same ID shows up.
        uniqueids=yes



# defaults for subsequent connection descriptions
conn %default
        # How persistent to be in (re)keying negotiations (0 means very).
        keyingtries=0
        # RSA authentication
        authby=rsasig



# sample connection
conn lagos-faro
        # Left security gateway, subnet behind it, next hop toward right.
        left=10.11.160.x
        leftsubnet=192.168.x.0/24
        leftfirewall=yes
        # RSA public key of lagos

leftrsasigkey=0x0103d55a8ddf51edab8f236759f70e11375ffcc9dbec2957e6ab0007bdcec659
3915d79c5181fd6a1fbccff24a3283490f1ea3afd6163edac3e2e40fbadeb8263d6a8d2d6eb473a6
bb8f22cf31a5fc113c5adfddbc96a945ce2160d0f600d138c209d0126b643645f59f51b55d957dd9
01ecdb9e1bee8200375ebcfe9de3e0963c42f7c745961d09c03fa10de82983a10e26a30577fdd4d8
e029b7f76873ab40925ca79b02a2b249da784e1bebe843b3855c452e3dc035d791f105cea026ea8d
0830ad1efd001f5e2d8bdc39a05889ab276606a7c885492315c2f8bc28db44b9e820b5cd3c66e3fa
c6c1459ba9f020cc9481a725175419da874d4ea70c947f86bed9
        # Right security gateway, subnet behind it, next hop toward left.
        right=10.11.160.y
        rightsubnet=192.168.y.0/24
        rightfirewall=yes
        # RSA public key of faro

rightrsasigkey=0x0103d55a8ddf51edab8f236759f70e11375ffcc9dbec2957e6ab0007bdcec65
93915d79c5181fd6a1fbccff24a3283490f1ea3afd6163edac3e2e40fbadeb8263d6a8d2d6eb473a
6bb8f22cf31a5fc113c5adfddbc96a945ce2160d0f600d138c209d0126b643645f59f51b55d957dd
901ecdb9e1bee8200375ebcfe9de3e0963c42f7c745961d09c03fa10de82983a10e26a30577fdd4d
```

```
8e029b7f76873ab40925ca79b02a2b249da784e1bebe843b3855c452e3dc035d791f105cea026ea8
d0830ad1efd001f5e2d8bdc39a05889ab276606a7c885492315c2f8bc28db44b9e820b5cd3c66e3f
ac6c1459ba9f020cc9481a725175419da874d4ea70c947f86bed9
        # To authorize this connection at startup,
        # uncomment this.
        auto=start
```

APÊNDICE B - IPSEC.SECRETS

```
$ cat ipsec.secrets
# This file holds shared secrets or RSA private keys for inter-Pluto
# authentication.  See ipsec_pluto(8) manpage, and HTML documentation.

# Shared secret (an arbitrary character string, which should be both long
# and hard to guess, enclosed in quotes) for a pair of negotiating hosts.
# Must be same on both; generate on one and copy to the other.
10.11.160.x 10.11.160.y : PSK "jxRU35Wk4nunU3n452nuTjTS1SRVuml5l4Uj3u3Rj3kml2u4
mTV4S2Suj1kWl2Tju54km3TWU"

# RSA private key for this host, authenticating it to any other host
# which knows the public part.  Put ONLY the "pubkey" part into connection
# descriptions on the other host(s); it need not be kept secret.
10.11.160.x 10.11.160.y : RSA   {
        # RSA 2048 bits   server06   Mon Nov 15 20:06:10 2004
        # for signatures only, UNSAFE FOR ENCRYPTION

#pubkey=0x0103d55a8ddf51edab8f236759f70e11375ffcc9dbec2957e6ab0007bdcec6593915d7
9c5181fd6a1fbccff24a3283490f1ea3afd6163edac3e2e40fbadeb8263d6a8d2d6eb473a6bb8f22
cf31a5fc113c5adfddbc96a945ce2160d0f600d138c209d0126b643645f59f51b55d957dd901ecdb
9e1bee8200375ebcfe9de3e0963c42f7c745961d09c03fa10de82983a10e26a30577fdd4d8e029b7
f76873ab40925ca79b02a2b249da784e1bebe843b3855c452e3dc035d791f105cea026ea8d0830ad
1efd001f5e2d8bdc39a05889ab276606a7c885492315c2f8bc28db44b9e820b5cd3c66e3fac6c145
9ba9f020cc9481a725175419da874d4ea70c947f86bed9
        #IN KEY 0x4200 4 1
AQPVWo3fUe2rjyNnWfcOETdf/Mnb7ClX5qsAB73Oxlk5FdecUYH9ah+8z/JKMoNJDx6jr9YWPtrD4uQP
ut64Jj1qjS1utHOmu48izzGl/BE8Wt/dvJapRc4hYND2ANE4wgnQEmtkNkX1n1G1XZV92QHs254b7oIA
N168/p3j4JY8QvfHRZYdCcA/oQ3oKYOhDiajBXf91NjgKbf3aHOrQJJcp5sCorJJ2nhOG+voQ7OFXEUu
PcA115HxBc6gJuqNCDCtHv0AH14ti9w5oFiJqydmBqfIhUkjFcL4vCjbRLnoILXNPGbj+sbBRZup8CDM
lIGnJRdUGdqHTU6nDJR/hr7Z
        # (0x4200 = auth-only host-level, 4 = IPSec, 1 = RSA)
        Modulus:
0xd55a8ddf51edab8f236759f70e11375ffcc9dbec2957e6ab0007bdcec6593915d79c5181fd6a1f
bccff24a3283490f1ea3afd6163edac3e2e40fbadeb8263d6a8d2d6eb473a6bb8f22cf31a5fc113c
5adfddbc96a945ce2160d0f600d138c209d0126b643645f59f51b55d957dd901ecdb9e1bee820037
5ebcfe9de3e0963c42f7c745961d09c03fa10de82983a10e26a30577fdd4d8e029b7f76873ab4092
5ca79b02a2b249da784e1bebe843b3855c452e3dc035d791f105cea026ea8d0830ad1efd001f5e2d
8bdc39a05889ab276606a7c885492315c2f8bc28db44b9e820b5cd3c66e3fac6c1459ba9f020cc94
81a725175419da874d4ea70c947f86bed9
        PublicExponent: 0x03
        # everything after this point is secret
        PrivateExponent:
0x8e3c5e94e1491d0a179a3bfa0960cf9553313d481b8fef1caaafd3df2ee6260e8fbd8babfe46bf
d3354c31770230b4bf17ca8eb97f3c829742b5273f256ed39c5e1e49cda26f27b4c1df766ea80b7d
91ea93d30f1b83dec0eb35f955e0d0815be00c4798242ea3bf8bce3e63a93b569de7bebd49ac0024
e9d354694295b97d80c2d576942fd9d32f2f15cd7f13d73b00cc353c6c1ced69a93478381d430cf3
df9d42be9e3488dcb601b76837a5e185b84314ada8c0456f1fe2e7911ee7c9abd19c68cfd021d24e
266f063020fa5c5bd5b9d8e5f64b2326196078a61efcf8f0c3b76b57712f9a7dfde8fd84b7ec9cd0
9d5ba8efa46901fac4d47cd9fa24e37a23
        Prime1:
0xeef5066603f16a535240b3dc128f12ac7289b1297ec586135da00ced8ad8baaf5882dfc816d6a3
b66a6652925f8de81f71e29303e317d1a60690cc5165769b88c8b5d2fd5c703f3c61d2b8187c7891
f5ae2c33e746573ab09d5cf42bb4eda46ef976b7895b022eafe263df3deeae226fd0f903d20dfdaf
a2a9722dbf4fea0b77
        Prime2:
0xe4920d51d1519925882c800ed34f22f8fe2bec322aaf3b988ba3075a3bd469dde33404ed4ca5eb
b0e1227d026b5354a86eaca63f3257999b2ae27a272967eaed79cbf24a90327915d3dda00e95a80b
```

```
afc1b63bac921721ec4aaa3b811456da8c293581b3c190db1485bb839e4f333925ccaeac0b6e59df
83667997ddf8477c2f
        Exponent1:
0x9f4e044402a0f18ce18077e80c5f61c84c5bcb70ff2e59623e6ab349073b271f90573fdab9e46d
2446eee1b6ea5e9abfa141b757ecba8bc40460883643a467b085ce8ca8e84ad4d2ebe1d01052fb0b
f91ec8229a2ee4d1cb13934d72789e6d9f50f9cfb0e756c9ca96ed3f7e9f1ec19fe0a6028c0953ca
6c70f6c92a3546b24f
        Exponent2:
0x98615e368b8bbb6e5ac8555f378a1750a9729d76c71f7d105d175a3c27e2f13e97780348ddc3f2
75eb6c5356f2378dc59f1dc42a218fbbbcc741a6c4c6454748fbdd4c31b576fb63e293c009b91ab2
752bced2730c0f6bf2dc717d00b839e7081b790122810b3cb85927ad1434ccd0c3ddc9c8079ee695
0244510fe9502fa81f
        Coefficient:
0x51302e630e6eb12f731eb03d3e219aa0edf53ccda675f00a900299493451898c45b64f7b894f1d
cc700164f694574f08f77663eda37061ccea8ce8c14286d8ec5a6b6c5024ee0bad8d10108462db8b
c7e1b05552ac9447d8f98d16f47bd6c34ffd347372f040f56d86188217196a075e385168fa5926c3
85b23b1fe93c02a56a
        }
# do not change the indenting of that "}"
```