Configuración de una VPN entre un cliente MS Windows y servidor GNU/Linux

Sergio González González

Instituto Politécnico de Bragrança (http://www.ipb.pt/), Portugal

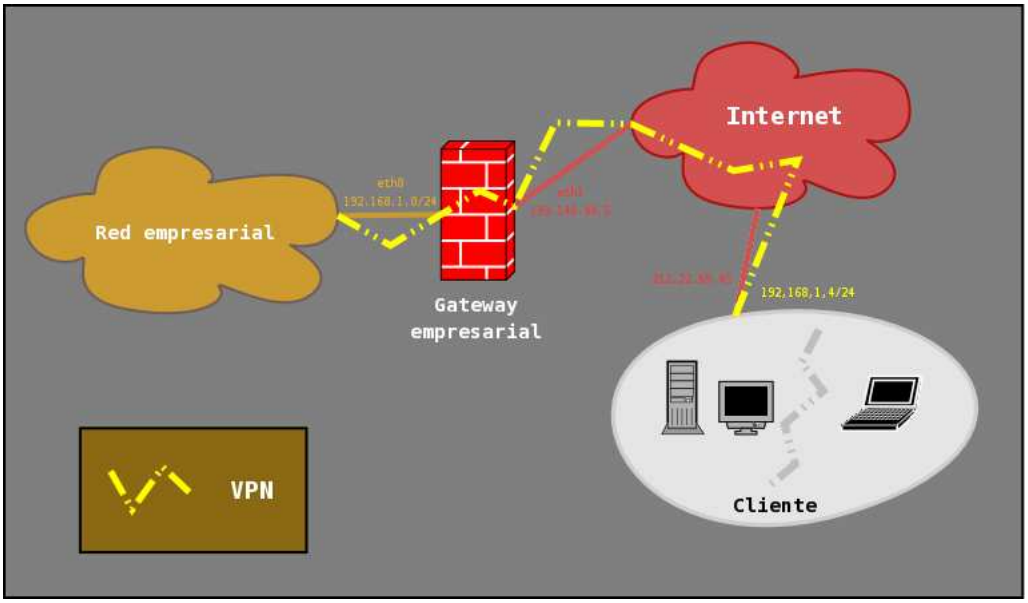
sergio.gonzalez@hispalinux.es

Documento explicativo sobre como configurar una red privada virtual entre una red empresarial, cuyo punto de salida hacia Internet es una máquina con GNU/Linux, y un sistema MS Windows XP (bien sea un ordenador portátil o un PC).

1. Introducción

A lo largo del presente documento explicaré la forma de configurar una máquina GNU/Linux para que actue como *gateway* de una empresa y permita la conexión de un cliente MS Windows XP (este puede ser un portátil o un PC) mediante una red privada virtual (VPN) a la red empresarial.

El esquema de red se muestra en la siguiente imagen[1]:



La tecnología elegida para la configuración de la red privada virtual es IPSec. La implementación elegida para dar soporte IPSec en GNU/Linux ha sido FreeS/WAN y los Parches X.509 para permitir una autentifiación segura. En MS Windows XP se utilizará la implementación IPSec del propio sistema operativo y la herramienta VPN de Marcus Müller.

> **Nota:** Para la realización de este documento se ha tomado como guia principal la entrada bibliográfica: "NateCarlson1"

2. Software necesario

Para poner en funcionamiento nuestra red privada virtual, necesitamos el siguiente software:

- FreeS/WAN
- Los Parches X.509 para FreeS/WAN
- Parches de encriptación para añadir múltiples algoritmos de encriptación (opcional).
- La herramienta VPN de Marcus Müller para Windows 2000/XP.
- OpenSSL

3. Instalación de FreeS/WAN y los parches X.509

Los parches X.509 son necesarios para permitir a FreeS/WAN trabajar con un cliente Windows 2000/XP nativo.

Antes de instalar el paquete FreeS/WAN, es necesario aplicar los parches X.509 al código fuente de FreeS/WAN. La forma de hacerlo se puede obtener de los propios paquetes de X.509 o de la entrada bibliográfica: AndreasSteffen1 (Puntos 1 a 4 de la 'Section 3: Installation').

De todas formas, en las siguientes secciones veremos la forma de instalar el software necesario a partir del código fuente de las apliaciones:

> **Nota:** Para el proceso de instalación de FreeS/WAN y de la aplicación de los Parches X.509 se han tomado como guias las entradas bibliográficas: DocFreeS/WAN y AndreasSteffen1, respectivamente.

3.1. Obtención del código fuente de las aplicaciones

Baje el código fuente de la página principal de FreeS/WAN y de los Parches X.509.

3.2. Comprobación de la firma y md5 de los programas

Una vez tenemos el software almacenado en nuestro ordenador, verificamos la procedencia del mismo y si se ha bajado correctamente, para ello es necesario obtener las claves públicas de los respectivos mantenedores de los paquetes. El archivo que contiene la clave pública de FreeS/WAN se denomina `freeswan-sigkey.asc` y el de los Parches X.509 `andreas_steffen.asc`.

Importamos dichas claves a nuestro anillo de claves:

```
$ gpg --import freeswan-sigkey.asc
gpg: clave 46EAFCE1: clave pública "Linux FreeS/WAN Software Team <build@freeswan.org>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1  (RSA: 1)
$ gpg --import andreas_steffen.asc
gpg: clave 40995359: clave pública "Andreas Steffen <andreas.steffen@strongsec.net>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1  (RSA: 1)
```

Antes de verificar la firma, comprobamos que el md5 está correcto:

```
$ md5sum -cv freeswan-2.04.tar.gz.md5
freeswan-2.04.tar.gz Correcto
$ md5sum -cv x509-1.4.8-freeswan-2.04.tar.gz.md5
x509-1.4.8-freeswan-2.04.tar.gz Correcto
```

Verificamos la firma del código fuente:

```
$ gpg --verify freeswan-2.04.k2.4.patch.gz.sig freeswan-2.04.k2.4.patch.gz
gpg: Firma creada el mar 11 nov 2003 21:40:35 WET usando clave RSA ID 46EAFCE1
gpg: Firma correcta de "Linux FreeS/WAN Software Team <build@freeswan.org>"
$ gpg --verify x509-1.4.8-freeswan-2.04.tar.gz.sign x509-1.4.8-freeswan-2.04.tar.gz
gpg: Firma creada el vie 14 nov 2003 21:40:35 WET usando clave RSA ID 40995359
gpg: Firma correcta de "Andreas Steffen <andreas.steffen@strongsec.net>"
```

3.3. Descompresión y desempaquetado del software

Descomprimimos y desempaquetamos el software en el lugar elegido, por ejemplo en `/usr/src`:

```
$ tar xzvf freeswan-2.04.tar.gz -C /usr/src
$ tar xzvf x509-1.4.8-freeswan-2.04.tar.gz -C /usr/src
```

3.4. Aplicando los parches X.509 a FreeS/WAN

Aplicamos los parches X.509 a FreeS/WAN:

```
$ cd /usr/src/freeswan-2.04/
$ cat ../x509-1.4.8-freeswan-2.04/freeswan.diff |patch -p1
```

En estos momentos, si todo ha ido bien, ya estamos en disposición de compilar e instalar el software.

3.5. Compilando e instalando FreeS/WAN

La forma elegida para añadir el soporte IPSec al núcleo Linux, es parcheando las fuentes de Linux y compilando un nuevo núcleo. Para ello, supondremos que las fuentes de Linux están en el directorio `/usr/src/linux`.

Antes de aplicar el parche FreeS/WAN, ha de configurar y compilar el nuevo núcleo. Una vez que ha finalizado, acceda al código fuente de FreeS/WAN y teclee:

```
$ cd /usr/src/freeswan-2.04/
$ make menugo
# make minstall
```

Al finalizar el proceso dispondremos tanto de las herramientas de espacio de usuario de FreeS/WAN como de los módulos necesarios para dar soporte IPSec al núcleo Linux. Ahora sólo le queda instalar el nuevo núcleo y reiniciar el sistema.

> **Nota:** La distribución Debian GNU/Linux ya provee las herramientas de espacio de usuario empaquetadas (con los Parches X.509 aplicados). Por lo que bastaría con ejecutar el siguiente comando para tenerlas completamente operativas:
>
> ```
> # apt-get install freeswan
> ```
>
> Debian también provee un parche para el núcleo debidamente preparado y parcheado, si quiere hacer uso del mismo, pruebe a instalar el paquete *kernel-patch-freeswan*

4. Creación de una entidad certificadora

Una de las partes más importantes de la configuración, es la creación de una entidad certificadora[2]. Para ello es necesario instalar OpenSSL (http://www.openssl.org/)[3] y una vez instalado, hacer nuestro certificado de autoridad. La forma de hacerlo se detalla en los siguientes pasos[4]:

i. Edite el archivo `/etc/ssl/openssl.cnf` y cambie la opción '*default_bits*' de 1024 a 2048 y la opción '*default_days*' a 365 (o similar)[5].

ii. Creamos un directorio para almacenar el nuevo certificado (algo similar a /var/tmp/sslca) y le cambiamos los permisos a *700*, para impedir que los usuarios tengan acceso al certificado.

iii. Edite el fichero `/usr/lib/ssl/misc/CA.sh` y cambie la línea '*DAYS="days 365"*' por un valor muy elevado[6]. Asegúrese de que este número es mayor que el establecido en el primer punto, o Windows no aceptará sus certificados.

iv. Ejecute el comando:

```
# /usr/lib/ssl/misc/CA.sh -newca
```

Y siga los pasos como se muestra a continuación. La letra en negrita es el texto que yo he tecleado:

Importante: No utilice caracteres especiales, como guiones, signos de suma, tildes, etc.; estos pueden confundir a la implementación IPSec de MS Windows.

```
# /usr/lib/ssl/misc/CA.sh -newca
CA certificate filename (or enter to create)

(enter)
Making CA certificate ...
Generating a 2048 bit RSA private key
.......+++
..................+++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:ca-password(enter)
Verifying - Enter PEM pass phrase:ca-password(enter)
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT(enter)
State or Province Name (full name) [Some-State]:Braganca(enter)
Locality Name (eg, city) []:Braganca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Instituto Politecnico de Braganca(enter)
Organizational Unit Name (eg, section) []:Comunicacoes(enter)
Common Name (eg, YOUR name) []:Sergio Gonzalez Gonzalez(enter)
Email Address []:sergio.gonzalez@hispalinux.es(enter)
```

Una vez finalizado el proceso de generación, ya disponemos de una entidad certificadora, con la cual podremos crear certificados.

5. Generación de los certificados

Lo primero que ha de hacer es genearar los certificados para su máquina *gateway*. Los pasos que se listan a continuación serán los mismos que deberá seguir si quiere generar certificados para otras máquinas.

i. Generamos el certificado en cuestión, como se muestra en la siguiente captura de pantalla:

```
# /usr/lib/ssl/misc/CA.sh -newreq
Generating a 2048 bit RSA private key
................................................+++
................................................+++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:req-password(enter)
Verifying - Enter PEM pass phrase:req-password(enter)
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Braganca
Locality Name (eg, city) []:Braganca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Instituto Politecnico de Braganca
Organizational Unit Name (eg, section) []:Comunicacoes
Common Name (eg, YOUR name) []:Sergio Gonzalez Gonzalez
Email Address []:sergio.gonzalez@hispalinux.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:(enter)
An optional company name []:(enter)
Request (and private key) is in newreq.pem
#
#
# /usr/lib/ssl/misc/CA.sh -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:ca-password(enter)
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Dec 12 16:25:34 2003 GMT
            Not After : Dec 11 16:25:34 2004 GMT
        Subject:
            countryName               = PT
            stateOrProvinceName       = Braganca
            localityName              = Braganca
            organizationName          = Instituto Politecnico de Braganca
            organizationalUnitName    = Comunicacoes
            commonName                = Sergio Gonzalez Gonzalez
            emailAddress              = sergio.gonzalez@hispalinux.es
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                43:A9:62:84:2D:90:F9:A9:5B:43:12:EC:3C:9E:40:13:09:25:57:6C
            X509v3 Authority Key Identifier:
                keyid:E7:9D:04:A6:98:8F:C5:AB:F8:E4:AA:A8:8D:69:AE:F6:82:0B:11:D5
                DirName:/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
                serial:00

Certificate is to be certified until Dec 11 16:25:34 2004 GMT (365 days)
Sign the certificate? [y/n]:y(enter)


1 out of 1 certificate requests certified, commit? [y/n]y(enter)
Write out database with 1 new entries
Data Base Updated
Certificate:
```

```
Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
    Validity
        Not Before: Dec 12 16:25:34 2003 GMT
        Not After : Dec 11 16:25:34 2004 GMT
    Subject: C=PT, ST=Braganca, L=Braganca, O=Instituto Politecnico de Braganca, OU=Comunicacoes,
             CN=Sergio Gonzalez Gonzalez/emailAddress=sergio.gonzalez@hispalinux.es
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:b1:ab:d1:e1:db:6f:0c:9b:a1:2c:eb:9a:58:5c:
                ad:9d:66:27:b6:47:84:50:d6:93:24:0d:92:32:a2:
                81:49:5b:8b:b4:86:f3:31:6d:9d:23:9c:e4:dd:99:
                35:26:d5:5a:f4:e7:2a:ad:51:69:0a:29:1d:a1:58:
                3c:3c:33:96:5f:91:ef:ee:4b:77:0d:2c:e2:df:d3:
                39:9c:fa:69:11:6f:64:41:c6:36:c1:2e:1f:1e:d9:
                2b:1d:2d:e0:6b:e7:a6:e7:4f:d3:eb:92:7f:a1:30:
                b3:61:1e:c8:2c:c9:e1:85:0b:ca:df:bf:a0:be:34:
                48:b5:4f:0d:6c:4f:3d:a2:21:9a:1a:d8:73:11:bb:
                a5:f3:ee:65:c3:5a:02:e4:a4:3c:8c:06:d3:4a:93:
                98:e4:1b:8a:e9:2f:bf:b4:32:e5:8f:26:bc:2a:93:
                2c:77:29:d3:98:c2:d2:88:f1:45:53:6b:84:7f:ee:
                c2:0a:ba:35:0a:8e:7a:1d:d8:ca:23:cc:25:4d:e9:
                cc:7b:ef:ea:46:d4:df:e6:8d:07:8d:8d:4c:ad:e5:
                72:35:92:6a:db:05:ca:60:a2:6e:9e:1d:81:41:d0:
                7b:32:0b:f1:ca:7c:96:34:e8:9c:d5:0d:b5:a7:ed:
                f1:35:c3:ef:c5:71:4c:1d:ab:e3:f2:10:28:d2:ff:
                dd:9b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            43:A9:62:84:2D:90:F9:A9:5B:43:12:EC:3C:9E:40:13:09:25:57:6C
        X509v3 Authority Key Identifier:
            keyid:E7:9D:04:A6:98:8F:C5:AB:F8:E4:AA:A8:8D:69:AE:F6:82:0B:11:D5
            DirName:/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
            serial:00

Signature Algorithm: md5WithRSAEncryption
    1a:d4:f2:72:ca:02:3a:7a:8d:ed:f5:c0:2a:03:56:14:d2:70:
    85:e1:c0:97:84:bb:29:5c:d1:38:f8:d9:56:95:44:e4:47:db:
    48:92:da:fd:9b:49:1e:e5:0c:15:15:a4:a9:f4:78:b2:80:31:
    81:7b:06:35:f3:86:81:e2:03:a0:37:25:ad:0b:70:17:6e:cd:
    80:3a:93:b8:b7:e3:15:0c:45:04:f4:c9:78:43:14:90:b9:3d:
    68:ca:2e:b0:9c:95:8c:2d:d3:d2:9a:ea:18:ca:52:24:d7:79:
    f6:3f:02:63:9c:09:f5:17:41:5b:f7:8d:d0:01:2b:66:59:5a:
    62:6b:e8:b7:6b:22:33:5a:a0:42:69:00:e1:83:30:5c:43:55:
    c7:aa:f8:f8:80:db:db:43:54:aa:6d:99:7a:fc:ea:40:48:af:
    65:56:e1:78:4b:b4:0d:c3:41:e5:b6:6e:18:c8:05:ab:db:dd:
    a0:45:f5:e9:77:69:a0:ab:b4:fa:8c:4e:32:89:eb:76:76:53:
```

```
        f5:13:b2:87:a4:45:4f:df:d0:9d:0e:fc:dd:a0:51:2e:0c:42:
        0c:22:d1:ec:7d:e4:ab:31:04:b1:ee:85:fb:a9:d7:83:28:dd:
        de:50:15:e9:22:22:73:0c:4a:8b:ad:35:66:bc:af:11:ee:2c:
        7c:0f:dd:66
-----BEGIN CERTIFICATE-----
MIIEUzCCAzugAwIBAgIBATANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMB4XDTAzMTIxMjE2MjUzNFoXDTA0MTIxMTE2MjUzNFowgccxCzAJBgNV
BAYTAlBUMREwDwYDVQQIEwhCcmFnYW5jYTERMA8GA1UEBxMIQnJhZ2FuY2ExKjAo
BgNVBAoTIUluc3RpdHV0byBQb2xpdGVjbmljbyBkZSBCcmFnYW5jYTEVMBMGA1UE
CxMMQ29tdW5pY2Fjb2VzMSEwHwYDVQQDExhTZXJnaW8gR29uemFsZXogR29uemFs
ZXoxLDAqBgkqhkiG9w0BCQEWHXNlcmdpby5nb256YWxlekBoaXNwYWxpbnV4LmVz
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsavR4dtvDJuhLOuaWFyt
nWYntkeEUNaTJA2SMqKBSVuLtIbzMW2dI5zk3Zk1JtVa9OcqrVFpCikdoVg8PDOW
X5Hv7kt3DSzi39M5nPppEW9kQcY2wS4fHtkrHS3ga+em50/T65J/oTCzYR7ILMnh
hQvK37+gvjRItU8NbE89oiGaGthzEbul8+5lw1oC5KQ8jAbTSpOY5BuK6S+/tDLl
jya8KpMsdynTmMLSiPFFU2uEf+7CCro1Co56HdjKI8wlTenMe+/qRtTf5o0HjY1M
reVyNZJq2wXKYKJunh2BQdB7MgvxynyWNOic1Q21p+3xNcPvxXFMHavj8hAo0v/d
mwIDAQABo4HKMIHHMAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wg
R2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBRDqWKELZD5qVtDEuw8nkAT
CSVXbDBtBgNVHSMEZjBkgBTnnQSmmI/Fq/jkqqiNaa72ggsR1aFJpEcwRTELMAkG
A1UEBhMCQVUxEzARBgNVBAgTClNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0
IFdpZGdpdHMgUHR5IEx0ZIIBADANBgkqhkiG9w0BAQQFAAOCAQEAGtTycsoCOnqN
7fXAKgNWFNJwheHAl4S7KVzROPjZVpVE5EfbSJLa/ZtJHuUMFRWkqfR4soAxgXsG
NfOGgeIDoDclrQtwF27NgDqTuLfjFQxFBPTJeEMUkLk9aMousJyVjC3T0prqGMpS
JNd59j8CY5wJ9RdBW/eN0AErZllaYmvot2siM1qgQmkA4YMwXENVx6r4+IDb20NU
qm2ZevzqQEivZVbheEu0DcNB5bZuGMgFq9vdoEX16XdpoKu0+oxOMonrdnZT9ROy
h6RFT9/QnQ783aBRLgxCDCLR7H3kqzEEse6F+6nXgyjd3lAV6SIicwxKi601Zryv
Ee4sfA/dZg==
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

ii. Renombramos ahora los archivos generados a algo más significativo:

```
# mv newcert.pem host.dominio.com.pem
# mv newreq.pem host.dominio.com.key
```

iii. Edite el archivo *.key* y borre todo el contenido existente entre la línea '-----BEGIN CERTIFICATE REQUEST-----' y '-----END CERTIFICATE REQUEST-----'. Una vez hecho esto, su archivo debería comenzar por '-----BEGIN RSA PRIVATE KEY-----' y terminar por '-----END RSA PRIVATE KEY-----'.

6. Instalación del certificado en el *gateway*

La instalación es muy sencilla, simplemente copie los archivos a sus ubicaciones[7]:

```
# cp /var/tmp/sslca/host.dominio.com.key /etc/ipsec.d/private
# cp /var/tmp/sslca/host.dominio.com.pem /etc/ipsec.d
# cp /var/tmp/sslca/demoCA/cacert.pem /etc/ipsec.d/cacerts
# openssl ca -gencrl -out /etc/ipsec.d/crls/crl.pem
```

7. Configuración de FreeS/WAN en la máquina *gateway*

Sigua los siguientes pasos para completar su configuración:

7.1. Configuración de `ipsec.secrets`

El archivo `/etc/ipsec.secrets` debe contener lo siguiente:

```
: RSA host.dominio.com.key "req-password"
```

La palabra *rep-password* ha de ser sustituida con la clave que introdujo a la hora de generar el certificado SSL, o con: *%prompt* si quiere que al arrancar IPSec pregunte por la clave.

> **Aviso**
>
> A lo largo de este documento estamos suponiendo el uso de una versión 1.96 o superior de FreeS/WAN.

7.2. Configuración de `ipsec.conf`

El archivo `/etc/ipsec.conf` ha de poseer un contenido similar a:

> **Importante:** Tenga en cuenta que la identación es importante, si no se respeta, FreeS/WAN fallará.

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file
# RCSID $Id: ipsec.conf.in,v 1.10.2.1 2003/06/13 23:27:25 sam Exp $

# This file:  /usr/share/doc/freeswan/ipsec.conf-sample
#
# Manual:     ipsec.conf.5
#
# Help:
# http://www.freeswan.org/freeswan_trees/freeswan-2.01/doc/quickstart.html
# http://www.freeswan.org/freeswan_trees/freeswan-2.01/doc/config.html
# http://www.freeswan.org/freeswan_trees/freeswan-2.01/doc/adv_config.html
#
# Policy groups are enabled by default. See:
# http://www.freeswan.org/freeswan_trees/freeswan-2.01/doc/policygroups.html
#
# Examples:
# http://www.freeswan.org/freeswan_trees/freeswan-2.01/doc/examples


version 2.0     # conforms to second version of ipsec.conf specification

config setup
    interfaces=%defaultroute
```

```
    klipsdebug=none
    plutodebug=none
    plutoload=%search
    plutostart=%search
    uniqueids=yes

conn %default
    keyingtries=1
    compress=yes
    disablearrivalcheck=no
    authby=rsasig
    leftrsasigkey=%cert
    rightrsasigkey=%cert

conn roadwarrior-net
    leftsubnet=192.168.1.0/24
    also=roadwarrior

conn roadwarrior
    right=%any
    left=%defaultroute
    leftcert=host.dominio.com.pem
    auto=add
    pfs=yes
```

Esta configuración permitirá a cualquier persona, con un certificado válido, conectarse a nuestro *host*. Hay dos perfiles de conexión: uno para las conexiones que se realizan directamente en el *gateway* y otro para los clientes que se conectan a la red que está detrás del *gateway*.

7.3. Arrancando IPSec

Ahora sólo falta arrancar el demonio IPSec tecleando:

```
# /etc/init.d/ipsec start
ipsec_setup: Starting FreeS/WAN IPsec 2.01...
ipsec_setup: Using /lib/modules/<uname -r>/kernel/net/ipsec/ipsec.o
```

Una vez que ipsec ha arrancado con normalidad, se habrá creado una nueva interfaz de red (ipsec0), el demonio pluto estará escuchando en el puerto UDP 500 y se habrán añadido algunas entradas en la tabla de rutas:

```
# /sbin/ifconfig
eth1      Link encap:Ethernet  HWaddr 00:00:00:00:00:01
          inet addr:193.146.99.5  Bcast:193.146.99.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:5 Base address:0x8f00

ipsec0    Link encap:Ethernet  HWaddr 00:00:00:00:00:02
          inet addr:192.168.1.254  Mask:255.255.255.0
          UP RUNNING NOARP  MTU:16260  Metric:1
```

```
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 0)

eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:02
          inet addr:192.168.1.254  Bcast:10.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xee80

# /sbin/route -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
193.146.99.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
193.146.99.0    0.0.0.0         255.255.255.0   U     0      0        0 ipsec0
0.0.0.0         193.146.99.254  128.0.0.0       UG    0      0        0 ipsec0
128.0.0.0       193.146.99.254  128.0.0.0       UG    0      0        0 ipsec0
0.0.0.0         193.146.99.254  0.0.0.0         UG    0      0        0 eth1
# /bin/netstat -putan | grep pluto
udp        0      0 10.0.1.4:500            0.0.0.0:*                           16428/pluto
```

8. Configuración de iptables en el *gateway*

Las reglas de iptables necesarias para que el *gateway* se comporte como debe son las siguientes:

```
#!/bin/bash
#

##
# Configuration
#

IPTABLES="/sbin/iptables"

#
# interfaces
#

INTERFACE_LO="lo"
INTERFACE_LAN="eth0"
```

```
INTERFACE_INTERNET="eth1"
INTERFACE_IPSEC="ipsec0"

#
# network
#

IP_LOCALHOST="127.0.0.1"

IP_LAN="192.168.1.254"
BCAST_LAN="192.168.1.255"

IP_INET="193.146.99.5"

IP_LAN_CLIENT_IPSEC="192.168.1.4"
IP_INET_CLIENT_IPSEC="212.22.69.45"

#
# ports
#

OPEN_TCP_PORTS="22"
OPEN_UDP_PORTS="500"
OPEN_ICMP_PORTS="0 3 5 8 11"

#
# IP NAT
#

IP_NAT="193.146.99.5"


##
# Reset iptables
#

${IPTABLES} -P INPUT ACCEPT
${IPTABLES} -P OUTPUT ACCEPT
${IPTABLES} -P FORWARD ACCEPT
${IPTABLES} -X
${IPTABLES} -F


##
# Policy
#

${IPTABLES} -P INPUT DROP
${IPTABLES} -P OUTPUT ACCEPT
${IPTABLES} -P FORWARD ACCEPT


##
# INPUT Chain
#

#
```

```
# open tcp ports
#

for x in ${TCP_PORTS}
do
        ${IPTABLES} -A INPUT -p TCP -i ${INERFACE_INET} --dport ${x} -j ACCEPT
done

#
# open udp ports
#

for x in ${UDP_PORTS}
do
        ${IPTABLES} -A INPUT -p UDP -i ${INERFACE_INET} --dport ${x} -j ACCEPT
done

#
# open icmp ports
#

for x in ${ICMP_PORTS}
do
        ${IPTABLES} -A INPUT -p ICMP -i ${INERFACE_INET} --icmp-type ${x} -j ACCEPT
done

#
# general input rules
#

${IPTABLES} -A INPUT -p ALL -i ${INTERFACE_LO}  -d ${IP_LOCALHOST} -j ACCEPT
${IPTABLES} -A INPUT -p ALL                     -d ${IP_LAN}       -j ACCEPT
${IPTABLES} -A INPUT -p ALL -i ${INTERFACE_LAN} -d ${BCAST_LAN}    -j ACCEPT
${IPTABLES} -A INPUT -m state --state ESTABLISHED,RELATED          -j ACCEPT


##
# OUTPUT Chain
#

${IPTABLES} -A OUTPUT -p ALL -s ${IP_LOCALHOST} -j ACCEPT
${IPTABLES} -A OUTPUT -p ALL -s ${IP_LAN}       -j ACCEPT

${IPTABLES} -A OUTPUT -p ALL -s ${IP_LAN} -o ${INTERFACE_IPSEC}    \
            -d ! ${IP_LAN_CLIENT_IPSEC} -j DROP
${IPTABLES} -A OUTPUT -p ALL -s ${IP_LAN} -o ${INTERFACE_INTERNET} \
            -d   ${IP_LAN_CLIENT_IPSEC} -j DROP

##
# NAT
#

${IPTABLES} -t nat -A POSTROUTING -o ${INTERFACE_INET} \
            -d ! ${IP_LAN_CLIENT_IPSEC} -j SNAT --to-source ${IP_NAT}
```

9. Configuración del cliente Windows XP

Importante: Si tiene instalado en su sistema la aplicación *SSH Sentinel*, y quiere utilizar la pila IPSec de MS Windows, ha de desinstalar (o desabilitar) *SSH Sentinel*, y habilitar el servicio '*ipsec*'.

Nota: En la siguiente dirección existen una serie de capturas de pantalla que muestran el proceso de importación de certificados en una máquina Windows:
http://support.real-time.com/open-source/ipsec/index.html
(http://support.real-time.com/open-source/ipsec/index.html)

Los pasos necesarios para configurar nuestro cliente MS Windows XP son los siguientes:

9.1. Crear el certificado para la máquina MS Windows

Cree el certificado para la máquina cliente, para ello siga los pasos detallados en la Sección 5. A partir de este momento, asumiremos que se ha denominado al certificado para Windows XP de la siguiente forma: *winhost.dominio.com*

9.2. Obtener el certificado en formato *.p12*

Desde el certificado generado para MS Windows, exporte un archivo *.p12* para la máquina MS Windows. La forma de hacerlo es la siguiente:

```
# openssl pkcs12 -export -in winhost.dominio.com.pem -inkey winhost.dominio.com.key \
-certfile demoCA/cacert.pem -out winhost.dominio.com.p12
Enter pass phrase for host.dominio.com.key:req-password(enter)
Enter Export Password:win-password(enter)
Verifying - Enter Export Password:win-password(enter)
```

Nota: Tenga en cuenta que puede necesitar añadir la opción '*-name friendly_name*', para que algunas versiones de MS Windows puedan leer el certificado.

Ejecute también el siguiente comando:

```
# openssl x509 -in demoCA/cacert.pem -noout -subject
```

Deberá apuntar el resultado obtenido, ya que lo necesitará para la configuración de su VPN. El resultado obtenido en mi caso ha sido:

```
subject= /C=PT/ST=Braganca/L=Braganca/O=Instituto Politecnico de Braganca
/OU=Comunicacoes/CN=Sergio Gonzalez Gonzalez/emailAddress=sergio.gonzalez@hispalinux.es
```

9.3. Copiar el certificado a MS Windows

Copie el archivo `winhost.dominio.com.p12` a su máquina MS Windows de forma segura.

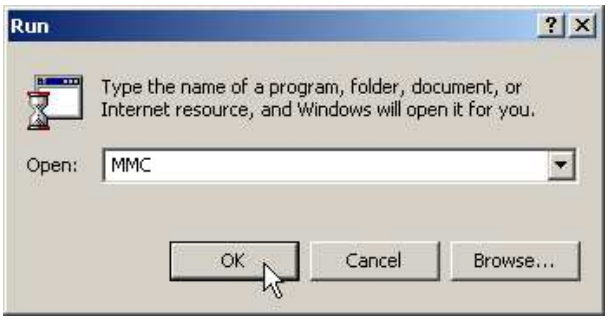
9.4. Aplicación ipsec.exe de Marcus Müller

Antes de instalar la aplicación VPN de Marcus Müller, ha de instalar el programa ipseeccmd. Para ello instale las *Win XP Support tools* que están en el CD de MS Windows XP en el directorio `\SUPPORT\TOOLS`. Ejecute el archivo `setup.exe` y seleccione la instalación completa.

Descomprima la aplicación ipsec.exe de Marcus Müller a un directorio de su máquina MS Windows, por ejemplo: `c:\ipsec`.

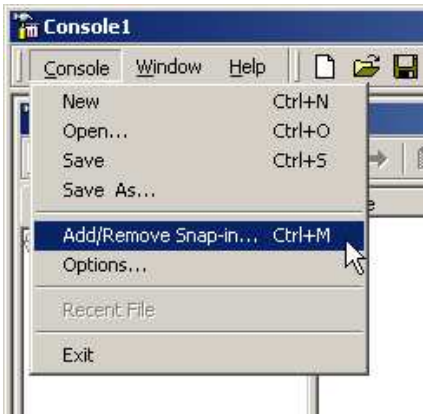
9.5. IPSec y certificados MMC

En esta sección se han empleado las capturas de pantalla y la información de esta página: RealTimeEnterprises1.

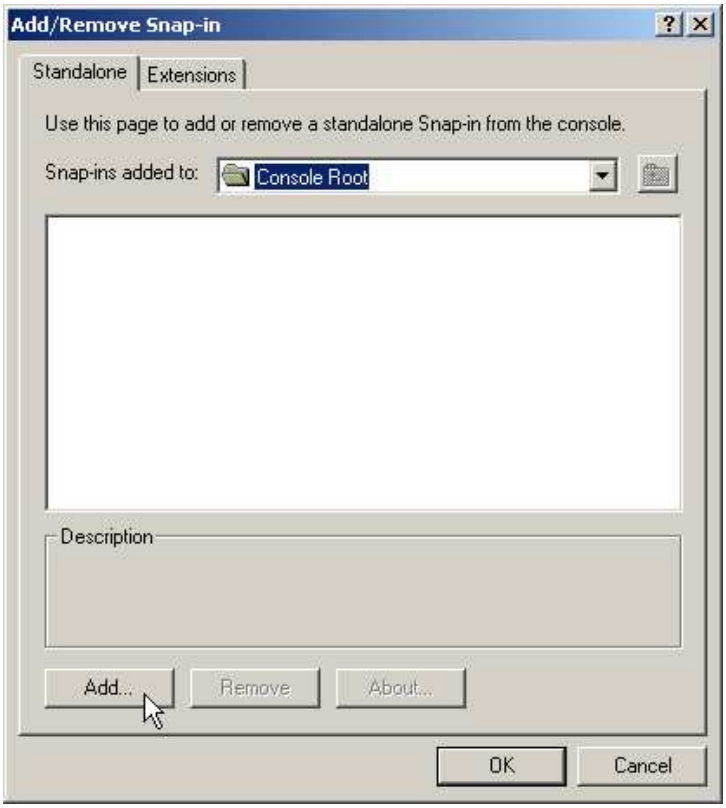


1. Haz click sobre el botón *inicio -> ejecutar*

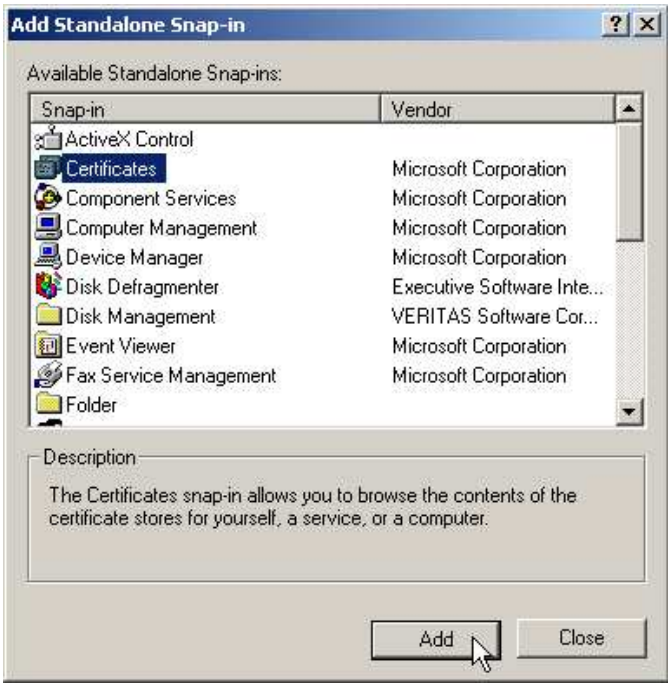
2. Teclee *MMC* y pulse *OK*



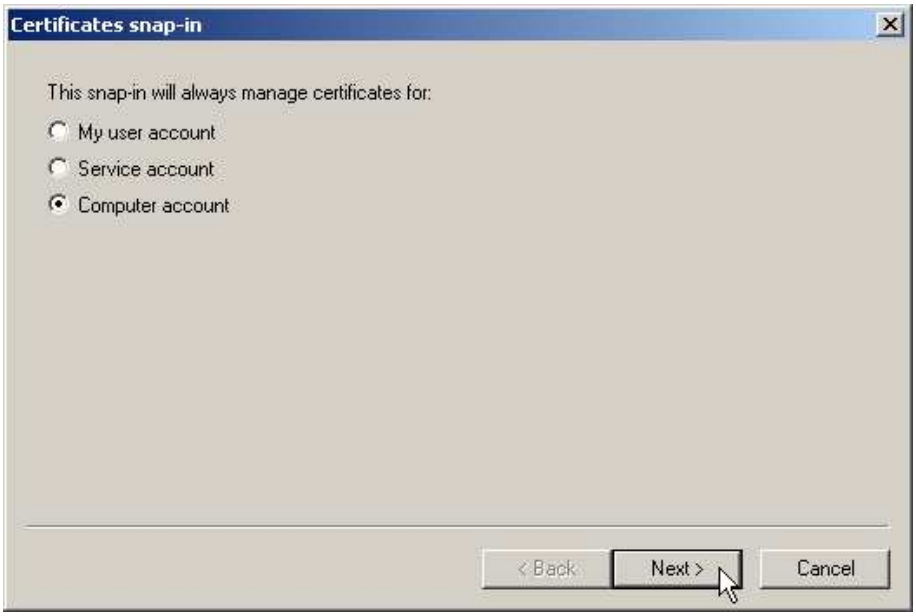
3. Pulse sobre el menú *Archivo* (o Console) y seleccione *Add/Remove Snap-in*



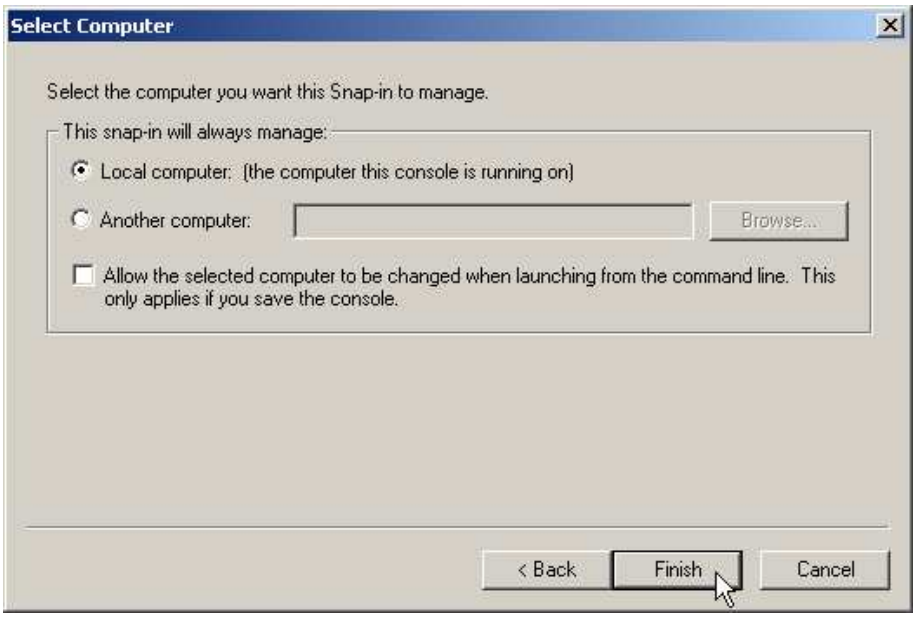
4. Pulse sobre *Añadir*



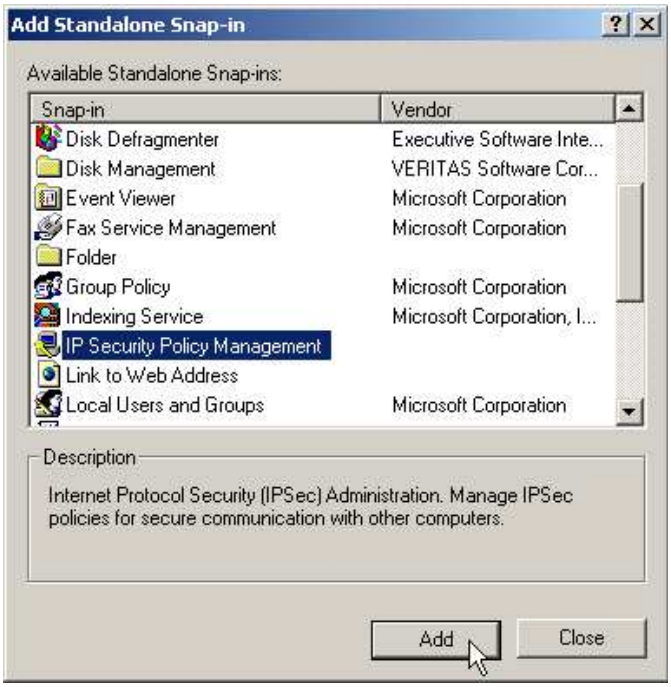
5. Pulse sobre *Certificados* y pulse sobre *Añadir*



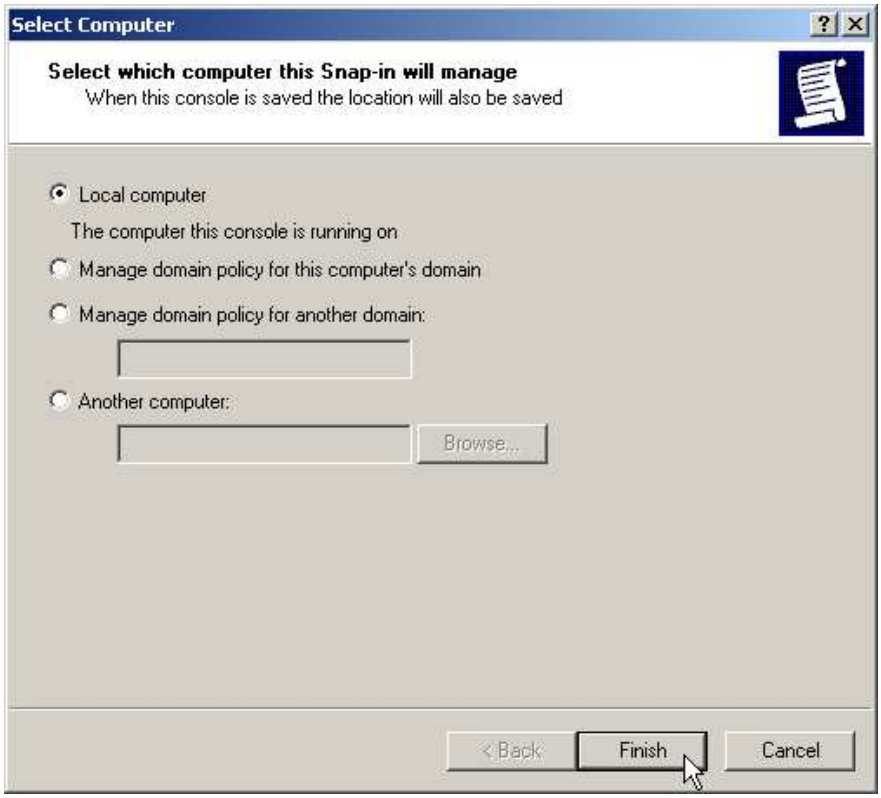
Seleccione *Cuenta de ordenador* y pulse sobre *Next*



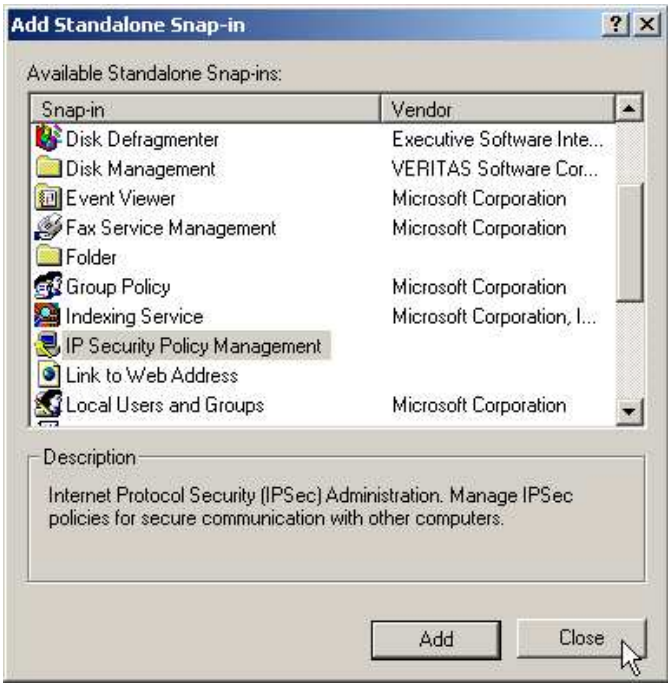
7. Seleccione *Ordenador local* y pulse sobre *Finalizar*



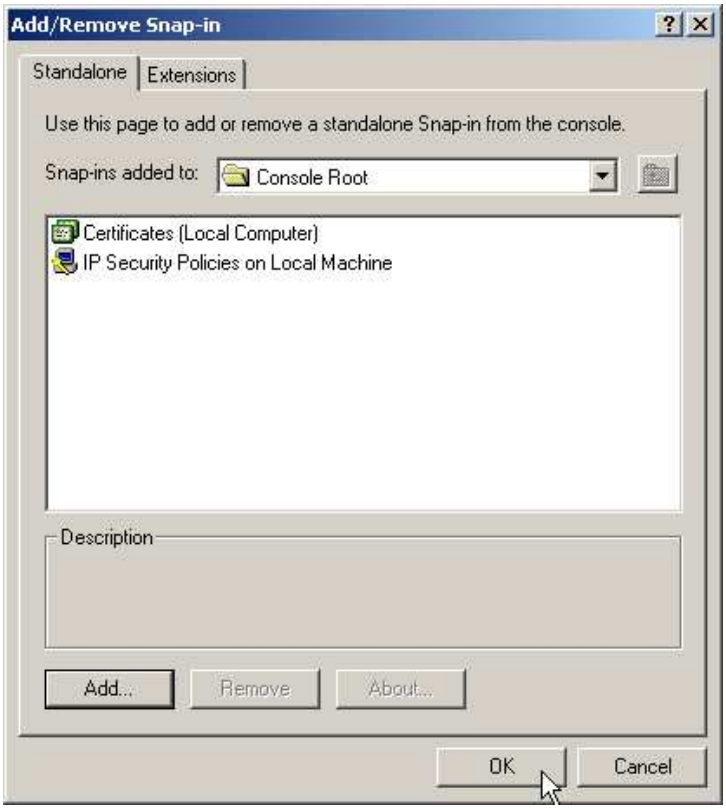
8. Busque y pulse la opción *Administración de las políticas de seguridad IP* y luego haga click sobre *Añadir*



9. Seleccione *Ordenador local* y pulse sobre *Finalizar*



10. Pulse sobre *Cerrar*

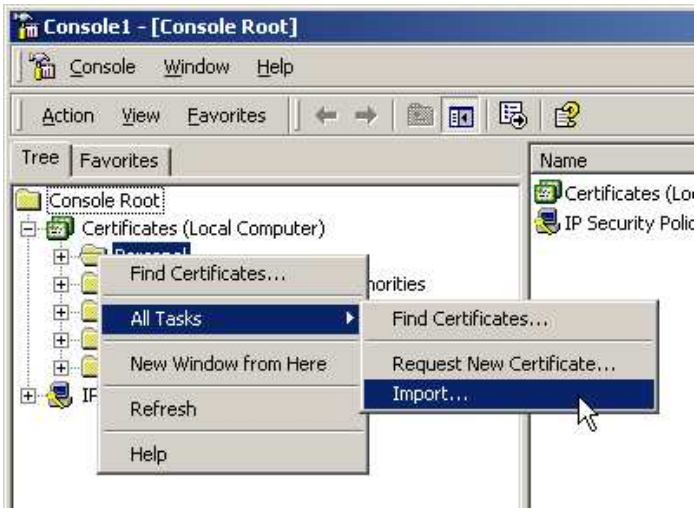


11. Pulse sobre *Aceptar*

9.6. Añadir el certificado

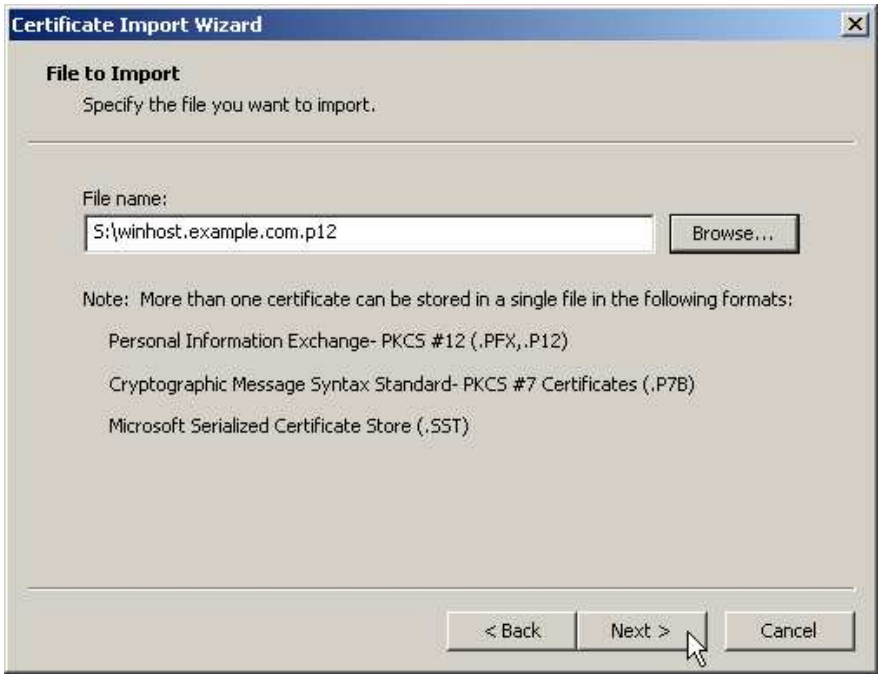
En esta sección se han empleado las capturas de pantalla y la información de esta página: RealTimeEnterprises1.

1. Pulse sobre el signo más de la opción *Certificados (ordenador local)*

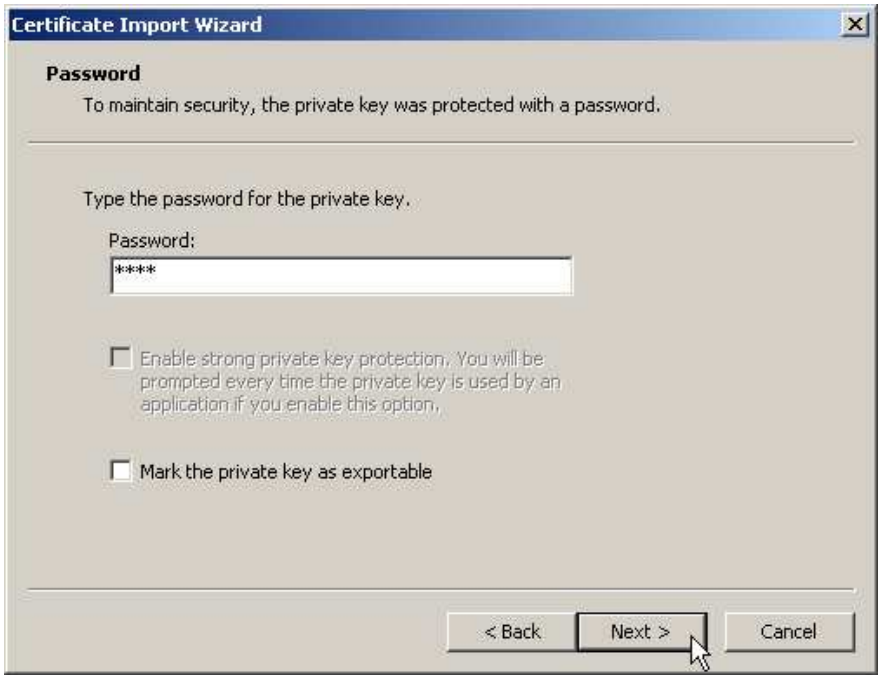


2. Pulse con el botón derecho sobre *Personal* y luego sobre *Todas las tareas* y más tarde sobre *Importar*

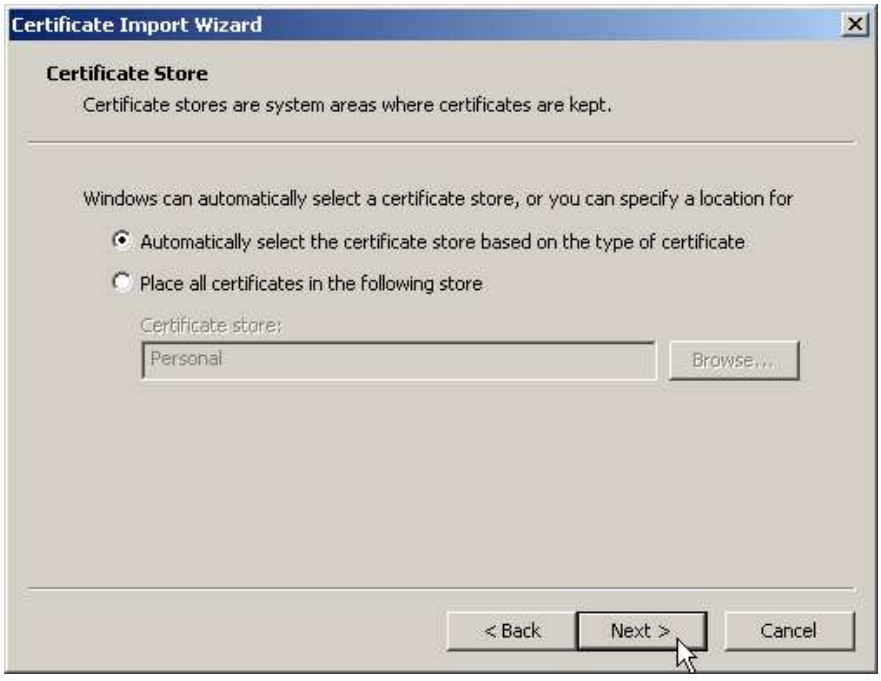
3. Pulse sobre *Siguiente*



4. Teclee la ruta al archivo *.p12* (o busque y seleccione el archivo), y pulse sobre *Siguiente*



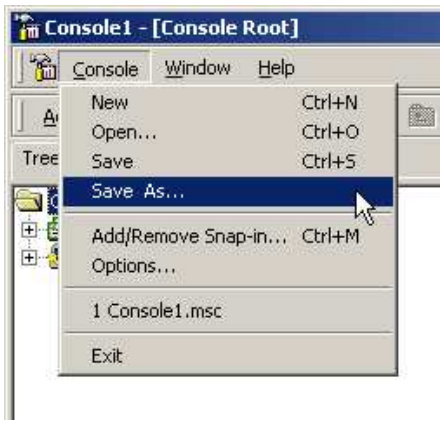
5. Teclee la clave del certificado y luego pulse *Siguiente*



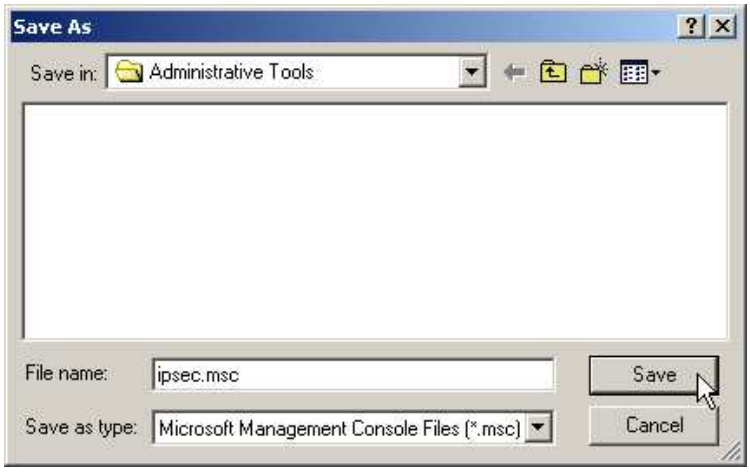
6. Seleccione la opción *Selección automática del almacenamiento del certificado basado en el tipo de certificado* y pusle sobre *Siguiente*

7. Pulse sobre *Finalizar*, y diga *Sí* a cualquier ventana de aviso que se muestre

8. Pulse sobre *Aceptar*



9. Guarde la configuración actual en un archivo, así no tendrá que añadir de nuevo el *Snap Ins* cada vez



10. Utilize el nombre por defecto, y pulse sobre *Guardar*

11. Salga de MMC

9.7. Configuración de la herramienta IPSec

Edite el archivo `ipsec.conf` (en la máquina MS Windows), reemplace la entrada "RightCA" con la salida obtenida al final de la Sección 9.2, tras ejecutar el comando:

```
# openssl x509 -in demoCA/cacert.pem -noout -subject
```

Nesecitará reformatear la salida como se muestra a continuación[8]:

```
conn roadwarrior
    left=%any
    right=193.146.99.5
    rightca="C=PT,S=Braganca,L=Braganca,O=Instituto Politecnico de Braganca,
             CN=Sergio Gonzalez Gonzalez,Email=sergio.gonzalez@hispalinux.es"
    network=auto
    auto=start
```

```
    pfs=yes

conn roadwarrior-net
    left=%any
    right=193.146.99.5
    rightsubnet=192.168.1.0/24
    rightca="C=PT,S=Braganca,L=Braganca,O=Instituto Politecnico de Braganca,
             CN=Sergio Gonzalez Gonzalez,Email=sergio.gonzalez@hispalinux.es"
    network=auto
    auto=start
    pfs=yes
```

9.8. Arrancando el enlace

Ejecute el comando ipsec.exe. A continuación se muestra un ejemplo de salida tras ejecutar dicho comando:

```
C:\ipsec>ipsec
IPSec Version 2.1.4 (c) 2001,2002 Marcus Mueller
Getting running Config ...
Microsoft's Windows XP identified
Host name is: (local_hostname)
No RAS connections found.
LAN IP address: 192.168.1.4
Setting up IPSec ...

Deactivating old policy...
Removing old policy...

Connection roadwarrior:
MyTunnel : 192.168.1.4
MyNet : 192.168.1.4/255.255.255.255
PartnerTunnel: 193.146.99.5
PartnerNet : 193.146.99.5/255.255.255.255
CA (ID) : C=PT,S=Braganca,L=Braganca,O=Instituto Politecnico de Braganca,...
PFS : y
Auto : start
Auth.Mode : MD5
Rekeying : 3600S/50000K
Activating policy...

Connection roadwarrior-net:
MyTunnel : 192.168.1.4
MyNet : 192.168.1.4/255.255.255.255
PartnerTunnel: 193.146.99.5
PartnerNet : 192.168.1.254/255.255.255.255
CA (ID) : C=PT,S=Braganca,L=Braganca,O=Instituto Politecnico de Braganca,...
PFS : y
Auto : start
Auth.Mode : MD5
Rekeying : 3600S/50000K
Activating policy...

C:\ipsec>
```

Una vez ha finalizado el arranque de IPSec, haga un ping a su *gateway*. Este debería decir '*Negotiating IP Security*' varias veces, y después dar respuestas al comando ping.

> **Nota:** Tenga en cuenta que el establecimiento del tunel puede llevar varios intentos; haciendo uso de una red T1 conectándose a un servidor detrás de un cable módem, el establecimiento toma unos 3-4 pings normalmente.

10. Licencia de este documento

Bibliografía

Documentación

[NateCarlson1] *Configuring an IPSec tunnel between FreeS/WAN and Windows 2000/XP (http://www.natecarlson.com/linux/ipsec-x509.php)* , Nate Carlson.

[JaccodeLeeuw1] *Using FreeS/WAN with Windows L2TP/IPsec (http://www.jacco2.dds.nl/networking/freeswan-l2tp.html)* , Jacco de Leeuw.

[AndreasSteffen1] *Installation and Configuration Guide (X.509 FreeS/WAN-version 1.4.8) (http://www.strongsec.com/freeswan/install.htm)* , Andreas Steffen.

[RealTimeEnterprises1] *IPSec, screenshots of the process of importing a certificate (http://support.real-time.com/open-source/ipsec/index.html)* , Real Time Enterprises, Inc..

[DocFreeS/WAN] *Documentación acompaña a FreeS/WAN* , Linux FreeS/WAN Software Team.

[Andreasson1] *Iptables Tutorial* , Oskar Andreasson, 2001-2002.

[Steffen1] *Virtual Private Networks Coping with Complexity (http://security.zhwin.ch/DFN_VPN.pdf)* , Andreas Steffen.

Software relacionado y utilizado

[FreeS/WAN] *FreeS/WAN (http://www.freeswan.org/)* .

[Parches X.509] *Parches X.509 (http://www.strongsec.com/freeswan/)* .

[MüllerVPN] *VPN (http://vpn.ebootis.de/)* , Marcus Müller.

[ParchesEncpt] *Parches de encriptación (http://www.irrigacion.gov.ar/juanjo/ipsec/)* .

[OpenSSL] *OpenSSL (http://www.openssl.org/)* .

[Dia] *Dia (http://www.lysator.liu.se/~alla/dia/)* .

[TheGimp] *The Gimp! (http://www.gimp.org/)* .

Sistemas Operativos empleados

[DebianGNULinux] *Debian GNU/Linux (http://www.debian.org/)* .

Núcleos implicados

[Linux] *Linux (http://www.kernel.org/)* .

Sin clasificar

[Windows] *MS Windows (http://www.microsoft.com/windows/)* .

Notas

1. Si desea el código fuente original de esta imagen, realizado con Dia, pulse aquí (./imagenes/esquema-de-red.dia)
2. CA: Certificate Authority
3. Si está utilizando un sistema Debian GNU/Linux, sólo tendrá que ejecutar:

   ```
   # apt-get install openssl
   ```

4. Vamos a suponer que estamos trabajando con un sistema Debian GNU/Linux para esta instalación.
5. Una recomendación sería establecer este número bastante elevado, algo similar a 3650, de esta forma, el certificado tiene una valided de 10 años.
6. Esto establece la valided de nuestra entidad certificadora
7. El proceso seguido aquí puede repetirse para todos aquellos equipos que quiera configurar y añadir a la red privada virtual.
8. Deberá cambiar los caracteres "/" por comas, y cambiar los nombres de algunos de los campos.