



Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Freeswan (ipsec) como pasarela para clientes Windows 1ªparte ^(3755 lectures)

Per sakroot, [sakroot](http://www.freeswan.org) (<http://www.freeswan.org>)

Creat el 25/07/2004 07:09 modificat el 26/07/2004 00:08

1ªPart En este mini howto, describo como podemos conectar clientes windows a nuestro servidor Linux con freeswan 1.96, Hablo tanto de como configurar la maquina Linux, como tambien configurar el cliente windows (winxp/win2k) he dividido el documento en 2 partes, puesto que me ocupaba 14 hojas y en bulma no podia poner el minihowto tan grande :) Bueno espero que os sirva de ayuda.

INTEROPERABILIDAD ENTRE FREESWAN Y WINDOWS

1ªParte

Minihowto freeswan–windows

Licencia GPL

Autor: Diego de León Ojeda (sakroot)

Después de muchos dolores de cabeza, he conseguido conectar dos host windows a una pasarela linux con freeswan, para asegurar las conexiones.

El documento esta probado en win2k y windows XP home. En winxp profesional no lo he probado, pero no tiene porque haber problemas ;)

Comenzamos:

PREREQUISITOS E INSTALACION EN NUESTRA PASARELA LINUX FREESWAN:

– Freeswan 1.96 en nuestro servidor LINUX / UNIX

Podemos descargar los fuentes aqui: <http://www.freeswan.org/download.html>,

o bien, como yo hice me bajé la versión de woody, (versión 1.96):

freeswan, kernel–patch–freeswan

–para que podamos utilizar freeswan necesitamos parchear el kernel

en la versión 2.4.x. Si os sirve de referencia, y para que no tengáis ningún problema, esta versión funciona

perfectamente con el kernel 2.4.24, que es donde lo tengo yo instalado, ahh y el parche lo aplique al kernel oficial www.kernel.org. Para parchear el kernel ejecute lo siguiente:

```
cd /usr/src/linux
```

```
patch -p1 < /usr/src/kernel-patches/all/apply/freeswan
```

– después en el menuconfig seleccionáis:

```
Networking options ---->
```



y al final os aparecerá todo lo relacionado con ipsec.

seleccionamos todas la opciones de ipsec en el kernel, compilamos, reiniciamos y más adelante ya podemos lanzar nuestros túneles ipsec ;)

(Configurándolo claro esta :).

– Si lo que hemos hecho es bajarnos los fuentes de freeswan, tendremos que parchear el soporte X.509, tal parche lo podemos encontrar en

<http://www.strongsec.com/freeswan/> lo bajamos y a hacser un patch.

–soporte ssl OpenSSL 0.9.6b

instalar openssl

Y bien estos son los requisitos para configurar nuestro "linux freeswan"

WINDOWS 2000 PROFESIONAL

Prerrequisitos e instalación en Windows 2000:

* Windows 2000 Service Pack 2

Esto es para incluir el soporte de encriptación potente de 3DES que usa freeswan.

Puede ser encontrado ---> :

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/sp2lang.asp>

* la herramienta ipsecpol.exe Versión 1.22

esta herramienta la podemos encontrar en el propio cd en

/SUPPORT/TOOLS/SETUP, Pero ante la duda, la podemos descargar de aquí,

<http://agent.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp>
aconsejo instalar la versión en ingles

* descargamos ---> Windows 2000 VPN tool <http://vpn.ebootis.de/package.zip>

WINDOWS XP

Prerrequisitos e instalación para Windows XP:

– Herramienta VPN de ipsec para Windows

<http://vpn.ebootis.de/package.zip>

El autor de la utilidad, habla de que no ha sido testeada con "Windows XP home", pues bien yo ya lo he probado y da algun

inconveniente, pero bueno, al final funciona, ya lo veremos mas



adelante :)

– ipseccmd

Lo podemos obtener del CD original de Windows en esta ruta :
\\SUPPORT\TOOLS\setup.exe, seleccionamos la instalación completa.

– ahora nos creamos nuestro directorio, c:\ipsec y la utilidad
<http://vpn.ebootis.de/package.zip> la descomprimimos ahí.

– lo siguiente será importar nuestro certificado firmado por la
CERTIFICADORA AUTORIZADA, que en este caso la hemos creado nosotros
en nuestra maquina linux. Pasos a seguir:

EN DEBIAN

apt-get install openssl

cd /etc/ssl/

ln -sf /usr/lib/ssl/openssl.cnf /etc/ssl/openssl.cnf

editamos openssl.cnf, para decirle la ruta donde se creara nuestra CA
y sus archivos, certificados, listas de revocación etc...

Buscamos este parámetro --> dir = ./DemoCA
y lo he cambiad a esto --> dir = /etc/ssl/MYCA
Cada cual que ponga lo que quiera.

el siguiente paso es buscar -> days y poner mas días, en la duración
del certificado,Sino al año los certificados creados no valdrán, y
serán revocados automáticamente, para ello:

default_days = 3650 #así durará 10 años :)

bien, después de modificar el anterior archivo archivo, hacemos enlace
simbólico para que nos sea mas comodo crear nuestras CA, certificados
y firmas:

ln -sf /usr/lib/ssl/misc/CA.sh /usr/local/bin/CA

cd /etc/ssl/

Creamos la nueva CA:

CA -newca

le damos a enter, y nos preguntara, datos para crear el certificado,
lo único que es obligatorio de poner es el común name y la contraseña
que es muy importante, para firmar certificados y para crear o
modificar listas de revocados, lo demás lo podéis quedar por defecto.
yo la verdad, me cree una CA legal, pero allá cada uno :D.
Este es un ejemplo de lo que nos sale:

CA certificate filename (or enter to create)



```
(enter)
Making CA certificate ...
Using configuration from /usr/lib/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++
.....+++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:(enter password) This is the password you will need to create any other certificates.
Verifying password – Enter PEM pass phrase:(repeat password)
-----
```

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]:US(enter) Enter your country code here
```

```
State or Province Name (full name) [Some-State]:State(enter) Enter your state/province here
```

```
Locality Name (eg, city) []:City(enter) Enter your city here
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ExampleCo(enter) Enter your company name here (or leave blank)
```

```
Organizational Unit Name (eg, section) []:(enter) OU, if you like. I usually leave it blank.
```

```
OBLIGATORIO-----> :P -----> Common Name (eg, YOUR name) []:CA(enter) The name of your Certificate Authority
```

```
Email Address []:ca@example.com(enter) E-Mail Address
```

– El siguiente paso es crear un certificado para nuestro servidor y otro para nuestros clientes, con hacer uno, los demás son iguales, pero logicamente con los datos del nuevo certificado, claro ;):

En el password que os pide al principio ponerlo, pero el que os pide al final como---->A challenge password, dar a enter

```
CA -newreq
```

```
Using configuration from /usr/lib/ssl/openssl.cnf
Generating a 1024 bit RSA private key
.....+++
.....+++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:(enter password) Password to encrypt the new cert's private key with – you'll need this!
Verifying password – Enter PEM pass phrase:(repeat password)
-----
```

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]:US(enter)
State or Province Name (full name) [Some-State]:State(enter)
Locality Name (eg, city) []:City(enter)
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ExampleCo(enter)
Organizational Unit Name (eg, section) []:(enter)
Common Name (eg, YOUR name) []:host.example.com(enter) This can be a hostname, a real name, an e-mail address,
or whatever
Email Address []:user@example.com(enter) (optional)

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

Bien ahora lo que tenemos que hacer es firmar este certificado,
diciendo que pertenece a nuestra CA :D, nos pedirá un password,
ponemos el que pusimos para crear nuestra CA

CA -sign

```
/usr/lib/ssl/misc/CA.sh -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter PEM pass phrase:(password you entered when creating the ca)
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'State'
localityName :PRINTABLE:'City'
organizationName :PRINTABLE:'ExampleCo'
commonName :PRINTABLE:'host.example.com'
emailAddress :IA5STRING:'user@example.com'
Certificate is to be certified until Feb 13 16:28:40 2012 GMT (3650 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 snipped)
Signed certificate is in newcert.pem
```

- "Importante", se nos ha creado dos archivos:
newcert.pem y newreq.pem, los renombramos, para saber que pertenecen
a nuestra pasarela:



```
mv newcert.pem linux.freeswan.pem  
mv newreq.pem linux.freeswan.key
```

– Ahora, hacemos los dos pasos anteriores para crear otro certificado en nuestro cliente Windows, es decir:

```
CA –newreq y CA –sign y renombramos los archivos nuevos:  
mv newcert.pem windows.freeswan.pem mv newreq.pem windows.freeswan.key
```

Además de esto, para que los clientes win puedan entender nuestros certificados los tenemos que codificar al formato *.p12, así:

```
openssl pkcs12 –export –in windows.freeswan.pem –inkey  
windows.freeswan.key –certfile /etc/ssl/MYCA/cacert.pem –out  
windows.freeswan.p12
```

Se nos creara el archivo "windows.freeswan.p12", Que más adelante le utilizaremos :-D

– Lo siguiente será, crear nuestro archivo para poder agregar o quitar certificados revocados:

```
openssl ca –genctrl –out crl.pem
```

—BUENO VA BIEN LA COSA jeje...puff las 4:31 de la mañana,,, seguimos:
disculpado que no pueda acabar el mini howto, en un artículo, pero
bulma acepta 14kb :), hay otra parte,, para no quedaros a medias :)

ARTICULO PARTE 1
LICENCIA GPL

E-mail del autor: sakroot_ARROBA_medusa.homeunix.net

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=2065>