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 2ºparte (17694 lectures)

Per **sakroot**, ***sakroot*** (http://www.freeswan.org)

Creado el 25/07/2004 07:15 modificado el 25/07/2004 23:59

2ºPart 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 :)

NTEROPERABILIDAD ENTRE FREESWAN Y WINDOWS

2ªParte

Minihowto freeswan-windows
Licencia GPL
Autor: Diego de León Ojeda (sakroot)

Continuamos el minihowto, que dejamos a medias :)

- Es hora de mover los archivos de los certificados a sus
correspondientes sitios:

cp /etc/ssl/MYCA/linux.freeswan.key /etc/ipsec.d/private/
cp /etc/ssl/MYCA/linux.freeswan.pem /etc/ipsec.d/
cp /etc/ssl/MYCA/cacert.pem /etc/ipsec.d/cacerts
cp /etc/ssl/MYCA/crl.pem /etc/ipsec.d/crls/crl.pem

- Configuraremos nuestro servidor linux para que se entienda con win:

cat > /etc/ipsec.secrets #y pasteamos, en password pones el pass del certificado del server linux

: RSA linux.freeswan.key "password"

- editamos /etc/ipsec.conf

Supongamos que nuestro linux y su subred siempre van a ser "left"
y los equipos que se conecten a el (como los Windows) van a ser right.
Ok, os pongo comentarios de lo que hace cada linea en el archivo y su
configuración correcta:

vi /etc/ipsec.conf

```
config setup
#aquí ponemos la interfaz a la que va a afectar el túnel siempre
#con ipsecX=interfaz,siendo la X un 0,1,2,3, etc., podemos crear
#muchos interfaces ipsec.

interfaces="ipsec0=wlan0"


klipsdebug=none
plutodebug=none
plutoload=%search
plutostart=%search



conn %default
#use RSA based authentication with certificates
authby=rsasig
leftrsasigkey=%cert
rightrsasigkey=%cert
#freeswan security gateway
#left=192.168.1.1
#leftid="@C=ES, ST=SPAIN, L=Valladolid, O=SERVIDOR MEDUSA,
#OU=medusa.homeunix.net"

#el certificado de la maquina local hay que ponerlo siempre
leftcert=linux.freeswan.pem


conn windows
#ponemos any, por si tenemos ip dinamica
# y si tenemos ip fija puedes poner la ip fija,
#pero para probar nuestro primer tunel aconsejo
#dejarlo en any, luego ya experimentareis :)

right=%any

#en la versión 1.96 los certificados hay
#que meterlos en /etc/ipsec.d/.
#Apartir de la 2,x los certificados van en /etc/ipsec.d/certs/

#CERTIFICADO DE NUESTRA MAQUINA WINDOWS
rightcert=windows.freeswan.pem

#dirección del servidor linux
left=192.168.1.1

#con esta opción iran todos los datos a
#cualquier red detrás de nuestro servidor linux-freeswan
#encriptado

leftsubnet=0.0.0.0/0
auto=start
```

- Configuración de freeswan acabada.

nota: si tenemos iptables para filtrar las conexiones, (como es logico) agregaremos un par de politicas básicas, para que toda la gente que quiera entrar por el túnel, pueda hacer la autentificación satisfactoriamente.

iptables -I INPUT -i ipsec0 -j ACCEPT

nota2: por cierto si la interfaz que hicimos alias en nuestro ipsec.conf, en la seccion setup interfaces="ipsec0=wlan0", esta siendo utilizada por otro túnel del tipo openvpn,
paramos el tunel openvpn y despues ya lanzamos ipsec.

- Hora de lanzar nuestro freeswan:

/etc/init.d/ipsec start

- Vista de logs, tenemos varias opciones: D :

tail -n 200 /var/log/auth.log #aquí vemos las autentificaciones de ipsec
tail -n 200 /var/log/daemon.log

luego con la herramienta ipsec, nos dará un
buen diagnostico:

ipsec auto --status
ipsec auto --listpubkeys #listará los certificados
#cargados por ipsec

ipsec auto --listcacerts #para ver el certificado de nuestra
#ca.

ipsec barf #nos dará el log mas detallado

- No es preocupéis mucho de los avisos hasta que no configureis, vuestros clientes, de todos modos, os dejo unos logs orientativos,
desde que se lanza el daemon, hasta que se establece una ASOCIACION DE SEGURIDAD :D:

Jul 25 03:17:57 MeDuSa ipsec__plutorun: Starting Pluto subsystem...
Jul 25 03:17:57 MeDuSa Pluto[6970]: Starting Pluto (FreeS/WAN Version 1.96)
Jul 25 03:17:57 MeDuSa Pluto[6970]: including X.509 patch (Version 0.9.9)
Jul 25 03:17:57 MeDuSa Pluto[6970]: Changing to directory '/etc/ipsec.d/cacerts'
Jul 25 03:17:57 MeDuSa Pluto[6970]: loaded cacert file 'cacert.pem' (1464 bytes)

Jul 25 03:17:57 MeDuSa Pluto[6970]: Changing to directory '/etc/ipsec.d/crls'
Jul 25 03:17:57 MeDuSa Pluto[6970]: loaded crl file 'crl.pem' (609 bytes)
Jul 25 03:17:57 MeDuSa Pluto[6970]: loaded my X.509 cert file '/etc/x509cert.der' (1077 bytes)
Jul 25 03:17:58 MeDuSa Pluto[6970]: | from whack: got --esp=3des
Jul 25 03:17:58 MeDuSa Pluto[6970]: loaded host cert file '/etc/ipsec.d/otrocertificado.pem' (3
962 bytes)
Jul 25 03:17:58 MeDuSa Pluto[6970]: loaded host cert file '/etc/ipsec.d/certificado.pem' (395
4 bytes)
Jul 25 03:17:58 MeDuSa Pluto[6970]: added connection description "win2k-eth2"
Jul 25 03:17:59 MeDuSa Pluto[6970]: | from whack: got --esp=3des
Jul 25 03:17:59 MeDuSa Pluto[6970]: listening for IKE messages
Jul 25 03:17:59 MeDuSa Pluto[6970]: adding interface ipsec0/wlan0 192.168.1.1
Jul 25 03:17:59 MeDuSa Pluto[6970]: adding interface ipsec1/eth2 192.168.0.1
Jul 25 03:17:59 MeDuSa Pluto[6970]: loading secrets from "/etc/ipsec.secrets"
Jul 25 03:17:59 MeDuSa Pluto[6970]: loaded private key file '/etc/ipsec.d/private/clave-privada-server.key' (1720
bytes)
Jul 25 03:17:59 MeDuSa Pluto[6970]: "win2k-eth2": cannot route Road Warrior template
Jul 25 03:17:59 MeDuSa Pluto[6970]: "wifi-lerey": cannot route Road Warrior template
Jul 25 03:17:59 MeDuSa Pluto[6970]: "wifi-ibook": cannot route Road Warrior template
Jul 25 03:17:59 MeDuSa Pluto[6970]: "win2k-eth2": cannot initiate connection without knowing peer
IP address
Jul 25 03:17:59 MeDuSa Pluto[6970]: "wifi-lerey": cannot initiate connection without knowing peer
IP address
Jul 25 03:17:59 MeDuSa Pluto[6970]: "wifi-ibook": cannot initiate connection without knowing peer
IP address

ARRIBA VEMOS EL LOG, SIN CONECTAR CLIENTES A FREESWAN

Jul 25 03:34:23 MeDuSa Pluto[345]: "win2k-eth2" 192.168.0.10 #8: responding to Main Mode from unkn
own peer 192.168.0.10
Jul 25 03:34:27 MeDuSa Pluto[345]: "win2k-eth2" 192.168.0.10 #8: Peer ID is ID_DER_ASN1_DN: 'C=ES,
ST=loquesea, L=loquesea, O=loquesea, OU=loqueseat, CN=loquesea
ey, E=loquesea'
Jul 25 03:34:27 MeDuSa Pluto[345]: "win2k-eth2" 192.168.0.10 #8: sent MR3, ISAKMP SA established
Jul 25 03:34:27 MeDuSa Pluto[345]: "win2k-eth2" 192.168.0.10 #9: responding to Quick Mode
Jul 25 03:34:27 MeDuSa Pluto[345]: "win2k-eth2" 192.168.0.10 #9: loquesea

Arriba vemos que el host 192.168.0.10 ha solicitado comunicación, segura, y como lo tenemos autorizado en nuestro freeswan,
se establecerá la conexión--> IPsec SA established --< este mensaje, no sabéis la alegría que da, cuando lo ves por primera vez

---

CONFIGURACION DE WINDOWS XP, LA MAS DESEADA XDDD

- lo primero es llevar el certificado "/etc/ssl/MYCA/windows.freeswan.p12" al host windows, yo lo mande por samba jeje, cada cual que lo mande como quiera.

Una vez en nuestro escritorio el certificado, vamos a esta pagina
web y seguimos el procedimiento que pone:

http://support.real-time.com/open-source/ipsec/index.html
si este link esta anulado hacérmelo saber y os mando el enlace...

- Bien ahora crearemos nuestras políticas para establecer la comunicación con el freeswan.
1º Aseguramos que el servicio esta lanzado, en windows:

inicio->programas->herramientas administrativas->servicios
la directiva ipsec este automática,

2ºnos vamos al archivo en el que instalamos los utils,
c:\ipsec\ipsec.conf y lo editamos. Aquí me entro mucho dolor de
cabeza, porque lo tienes que poner a la perfección
Aun así falla, a veces.
Importante: Antes de editarlo, tener en cuenta que hay que
dejar los tabuladores en el archivo y ponerlo todo tal cual
os lo pongo en el ejemplo de abajo. Si tenéis el problema, que en el
certificado pusisteis un nombre con acentos, o ñ (cosa que no
recomiendo) en linux cuando en la consola pongáis este comando
"openssl x509 -in demoCA/cacert.pem -noout -subject" para
extraer los datos de la CA, os aparecerá caracteres raros, pero no
cometáis el fallo de ponerlo talcual os da la salida, ejemplo:

```
conn windows

#el any es nuestra dirección ip Windows, pero dejarlo así, por
#si os cambia
left=%any

#direccion ip del server linux,
right=192.168.1.

#ponemos el asterisco para poder conectar a todas las redes
#detrás del gateway
rightsubnet=*

#aquí ponemos lo que hemos abstraído del comando "openssl x509
#-in /etc/ssl/CA-LEREY/cacert.pem -noout -subject", en el
# servidor linux
#Si os dais cuenta, he puesto el acento en CN=Diego de León
#Ojeda, porque si lo ponéis así -> CN=Diego de le\xF3n Ojeda os
#volveréis locos porque no os funcionara el tunel.
rightca="C=ES, S=SPAIN, L=Valladolid, O=MONTAJES ELECTRICOS
LEREY, OU=medusa.lerey.net, CN=Diego de León Ojeda,
E=sakroot@medusa.homeunix.net"

#aquí puede ser lan o rsa, dejarlo en lan, o auto
network=lan

auto=start
pfs=yes

conn linux
left=%any
#nuestra dirección ip de la maquina Windows
```

```
right=192.168.0.10

#igual que arriba
rightca="C=ES, S=SPAIN, L=Valladolid, O=MONTAJES ELECTRICOS
LEREY, OU=medusa.lerey.net, CN=Diego de León Ojeda,
E=sakroot@medusa.homeunix.net"
network=lan
rekey=1800S/30000K
auto=start
pfs=yes
```

-Editado el archivo de arriba, lo guardamos con los cambios y lo dejamos sin comentarios ni nada, quedaría así:

```
conn windows
left=%any
right=192.168.1.1
rightsubnet=*
rightca="C=ES, S=SPAIN, L=Valladolid, O=MONTAJES ELECTRICOS i
LEREY, OU=medusa.lerey.net, CN=Diego de León Ojeda,
E=sakroot@medusa.homeunix.net"
network=lan
auto=start
pfs=yes

conn linux
left=%any
right=192.168.1.10
rightca="C=ES, S=SPAIN, L=Valladolid, O=MONTAJES ELECTRICOS
LEREY, OU=medusa.lerey.net, CN=Diego de León Ojeda,
E=sakroot@medusa.homeunix.net"
network=lan
rekey=1800S/30000K
auto=start
pfs=yes
```

Si os ha piíllado bien la configuración el xp (cosa rara, ya os diré porque), hacemos lo siguiente, para lanzar el túnel:

inicio-->cmd

cd c:\ipsec\

ejecutamos-> ipsec

veremos que carga las directivas. Posteriormente hacemos un ping (sino esta bloqueado con firewall) al server

freeswan, y debería de salir esto:

ping 192.168.1.1
Negotiating IP Security # y a los instantes nos devolverá el ping,
Respuesta desde 192.168.1.1: bytes=32 tiempo<10ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<10ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<10ms TTL=64

En caso que veamos 4 veces este mensaje, es que hay algo mal -->
Negotiating IP Security
Negotiating IP Security
Negotiating IP Security
Negotiating IP Security

También nos puede devolver el ping sin que aparezca "Negotiating IP Security" y puede estar el túnel hecho. Lo comprobamos en linux con

tcpdump -i wlan0

Una vez dentro del server, hacemos un ping al host Windows, y otro del host Windows al linux, nos tiene que salir algo parecido a esto:

05:54:52.553750 IP 192.168.1.1 > 192.168.0.10: ESP(spi=0x5567f46e,seq=0x2)
05:54:52.557218 IP 192.168.1.10 > 192.168.1.1: ESP(spi=0x7d4d1823,seq=0x4)
05:54:53.563757 IP 192.168.1.1 > 192.168.1.10: ESP(spi=0x5567f46e,seq=0x3)
05:54:53.566986 IP 192.168.1.5 > 192.168.1.1: ESP(spi=0x7d4d1823,seq=0x5)

fijaros arriba en ESP, si sale esp "Bieeeen¡¡¡¡

En caso de no ver ESP, puede ser que el winxp no halla cojido bien el certificado con la herramienta "c:\ipsec\ipsec.exe", entonces vamos exportarlo nosotros manualmente:

1- ejecuta inicio: y ponemos --> C:\ipsec\IPSec.msc, damos enter y nos aparece la consola mmc. De lo que vemos en pantalla, nos interesa la parte -->IP-nosequeenaleman, lo pinchamos y a la derecha veremos freeswan, nos aseguramos que ponga un sí en directiva asignada,de lo contraio, pulsamos sobre freeswan botón derecho y asignar. Sin cerrar la mmc, probamos el ping, si sigue mal la cosa, volvemos a la mmc y pinchamos Dos veces sobre freeswan; lo que vamos a hacer es remarcar los certificados en las cuatro reglas de seguridad
que nos aparecen como "host-window windows-host etc.", la ultima que pone, respuesta predeterminada ni la tocamos.Ahora vamos a hacer los mismos pasos en las cuatro reglas. "Importante" hacerlo bien en todas, aceptando y tal:

doble click en windows-host:

nos sale nueva pantalla-->pestaña-métodos de autentificación->doble clic "entidad emisora"-> examinar> seleccionamos nuestro certificado y aceptamos todo hasta volver a la ventana reglas de seguridad. Hacer esto con las otras 3 reglas exactamente igual.
Una vez seleccionado el mismo certificado en las cuatro reglas de seguridad, le damos aplicar, cerrar.
Volvemos a la mmc, damos botón derecho en freeswan>desasignar y otra vez botón derecho>asignar,

Con lo expuesto arriba, nos puede salvar la vida, probamos el ping y debería de ir todo bien, sino os va, mirar los logs en el servidor linux
Y con esto acabo el documento, espero que os valga de algo jejje.
Si tenéis algún problema, sakroot@medusa.homeunix.net o en el irc,
Servidor irc.debian.org #debian-es nick sakroot.

Agradeceria vuestros comentarios sobre el documento y vuestras experiencias :)

Un saludo a todos.

DOCUMENTO GPL

E-mail del autor: sakroot _ARROBA_ medusa.homeunix.net