ANEXO 4

CONFIGURACIÓN DE IPSEC

El presente anexo contiene la información correspondiente a la guía de configuración de IPsec en los enrutadores Cisco 2801 y en los hosts con OpenSwan sobre el sistema operativo Ubuntu en sus versiones 9.10 y 10.04, como se implementó para las pruebas desarrolladas en el trabajo de grado.

1. CONFIGURACIÓN DE ROUTER A ROUTER

1. Crear una Lista de Control de Acceso *crypto ACL*. El crypto ACL define cual tráfico deberá ser protegido y enviado a través del túnel IPsec.

```
Router1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

2. Configurar una política ISAKMP para determinar los parámetros ISAKMP que serán usados para establecer el túnel y la clave secreta.

```
Router1(config)#crypto isakmp policy 1
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# encr aes 256
Router1(config-isakmp)# hash md5
Router1(config-isakmp)# group 2
Router1(config-isakmp)# lifetime 3600

Router1(config)# crypto isakmp key 0 ipsec123 address 172.16.4.2
```

3. Definir el conjunto de transformación IPSec. La definición del conjunto de transformación define los parámetros que el túnel IPsec utilizará, y puede incluir los algoritmos de cifrado y integridad.

```
Router1(config)# crypto ipsec transform-set 1 ah-md5-hmac
```

4. Crear el ACL y crear el crypto-mapa. El crypto mapa agrupa los parámetros previamente configurados y define los dispositivos pares IPSec. El crypto mapa es aplicado a la interfaz saliente del router VPN.

   Se puede crear otro ACL específicamente para el siguiente crypto mapa, este definirá que trafico saliente será cifrado por esta conexión.

   ```
   Router1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
   0.0.0.255
   ```

Luego, se debe crear el crypto-map. En este caso se le ha dado el nombre de "ipsec"

```
Router1(config)# crypto map ipsec 10 ipsec-isakmp
Router1(config-crypto-map)# set peer 172.16.4.2
Router1(config-crypto-map)# set transform-set 1
Router1(config-crypto-map)# set pfs group2
Router1(config-crypto-map)# match address 100
Router1(config-crypto-map)# set security-association lifetime seconds 3600
```

5. Y por último, aplicar el crypto mapa a la interfaz correspondiente.

```
Router1(config)#interface fastEthernet 0/0
Router1(config-if)# crypto map ipsec
```

2. CONFIGURACION EZVPN

1. Habilitar Authentication, Authorization and Accounting (AAA):

```
Router1(config)#username ipsec password ipsec
Router1(config)#aaa new-model
Router1(config)#aaa authentication login default local none
```

2. Crear el pool de direcciones IP:

```
Router1(config)#ip local pool VPNCLIENTS 172.16.10.100 172.16.10.200
```

Y además crear la interfaz loopback dentro de este pool. Además, es esencial añadir esta red en la tabla de enrutamiento:

```
Router1(config)#interface loopback 0
Router1(config-if)#ip address 172.16.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
```

3. Configurar la Autorización de grupo:

```
Router1(config)#aaa authorization network IPSECAUTH local
```

4. Crear las políticas IKE

```
Router1(config)#crypto isakmp policy 1
Router1(config-isakmp)#encryption aes 256
Router1(config-isakmp)#hash md5
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#group 2
Router1(config-isakmp)#exit
```

Luego se debe configurar el grupo para asociar ISAKMP:

```
Router1(config)#crypto isakmp client configuration group ipsecgroup
Router1(config-isakmp-group)#key ipsec
Router1(config-isakmp-group)#pool VPNCLIENTS
Router1(config-isakmp-group)#acl 100
Router1(config-isakmp-group)#netmask 255.255.255.0
Router1(config-isakmp-group)#exit
```

Ahora, hay que crear la ACL, que en este caso es la número 100:

```
Router1(config)#access-list 100 permit ip 172.16.0.0 0.0.255.255 any
```

5. Configurar el conjunto de transformada IPsec:

```
Router1(config)#crypto ipsec transform-set 1 esp-3des esp-md5-hmac
Router1(cfg-crypto-trans)#mode tunnel
Router1(cfg-crypto-trans)#exit
```

6. Crear un Crypto Map dinámico:

```
Router1(config)#crypto dynamic-map ipsec 10
Router1(config-crypto-map)#set transform-set 1
Router1(config-crypto-map)#reverse-route
Router1(config-crypto-map)#exit
```

Luego se debe habilitar para que responda a solicitudes VPN:

```
Router1(config)#crypto map ipsec client configuration address respond
```

Luego asociar un grupo de autorización AAA con el mapa:

```
Router1(config)#crypto map ipsec isakmp authorization list IPSECAUTH
```

Después crear el crytpto map a partir del crytp map dinámico:

```
Router1(config)#crypto map ipsec 10 ipsec-isakmp dynamic ipsec
```

Y por último aplicar el crypto map a la interfaz que recibirá las solicitudes VPN:

```
Router1(config)#interface fastEthernet 0/1
Router1(config-if)#crypto map ipsec
Router1(config-if)#exit
```

7. Habilitar IKE DPD y XAUTH:

```
Router1(config)#crypto isakmp keepalive 30 5
Router1(config)#aaa authentication login VPNLOGIN local
Router1(config)#username ipsecuser password ipsecuser
Router1(config)#crypto isakmp xauth timeout 60
Router1(config)#crypto map ipsec client authentication list VPNLOGIN
```

3. CONFIGURACIÓN OPENSWAN

Se trabajó con la version 2.6.22 de OpenSwan en Ubuntu 9.10 y Ubuntu 10.04 sin el paquete openswan-modules-source. El kernel de Linux utilizado es el 2.6.32-21-generic según la salida del comando "uname -a":

> Linux isalaptop 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:09:38 UTC 2010 x86_64 GNU/Linux

Mediante el Gestor de Paquetes Synaptic se instalaron los siguientes paquetes, y sus dependencias:

> ipsec-tools (1:0.7.1-1.5ubuntu4)
> openswan (1:2.6.22+dfsg-1.1ubuntu1)

Se utilizaron los repositorios de Ubuntu 9.10 (universe), donde está la versión 2.6.22 de OpenSwan. A continuación se detalla el contenido del archivo /etc/apt/sources.list:

> deb http://archive.ubuntu.com/ubuntu karmic main restricted universe multiverse
> deb http://archive.ubuntu.com/ubuntu karmic-updates main restricted universe multiverse
> deb http://archive.ubuntu.com/ubuntu karmic-security main restricted universe multiverse
> deb http://archive.ubuntu.com/ubuntu karmic-proposed main restricted universe multiverse
> deb http://packages.medibuntu.org/ karmic free non-free
> deb http://archive.ubuntugames.org ubuntugames main

Los siguientes pasos se realizaron para la instalación y configuración de IPsec mediante OpenSwan:

FIGURA A4. 1 PASO 1: NO SE UTILIZÓ PKI

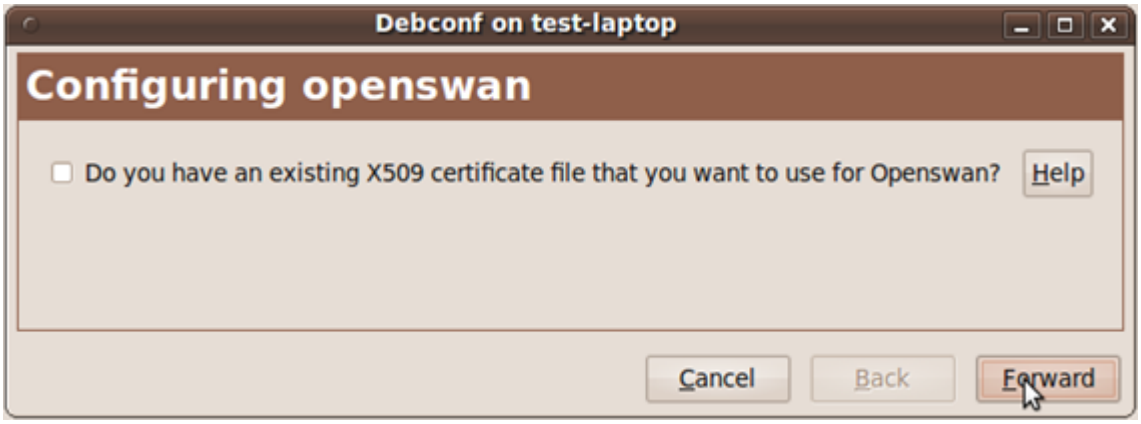

FIGURA A4. 2 NO HAY EXISTENCIA PREVIA DE CERTIFICADOS

FIGURA A4. 3 SE PERMITE CREAR Y AUTO-FIRMAR CERTIFADOS

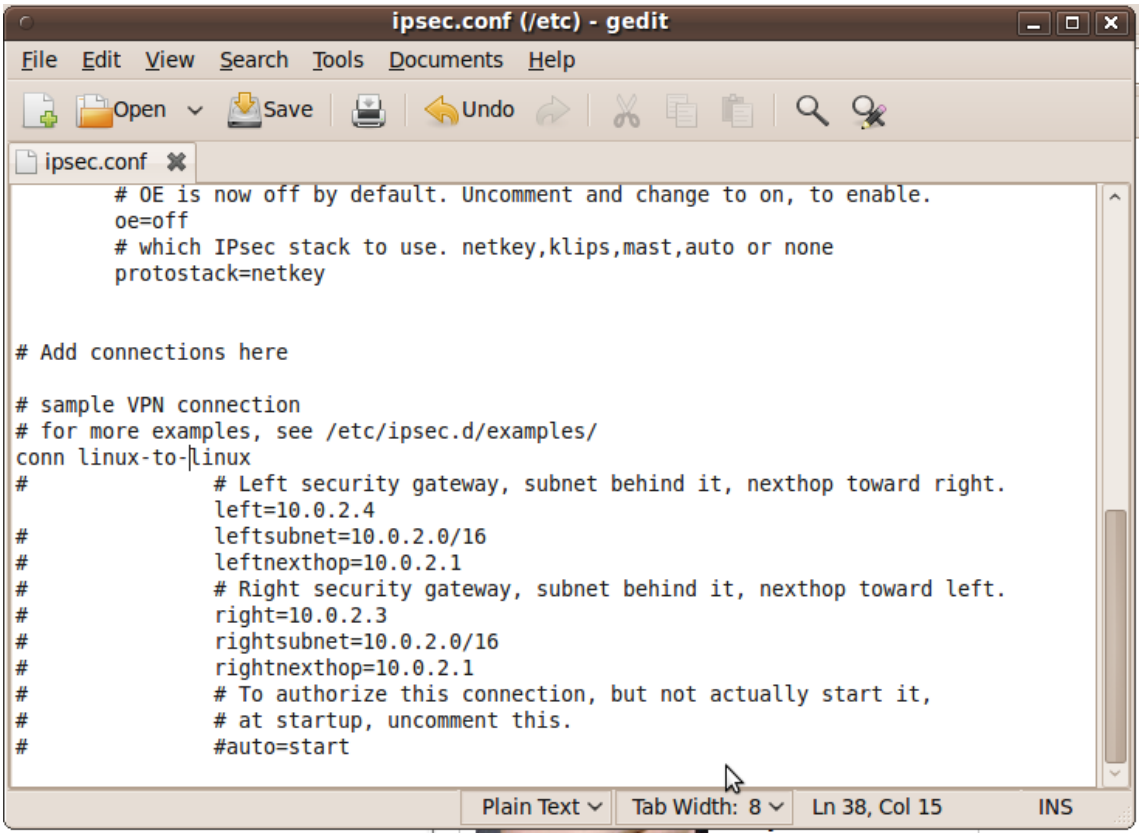

FIGURA A4. 4 CONTENIDO DEL ARCHIVO /ETC/IPSEC.CONF

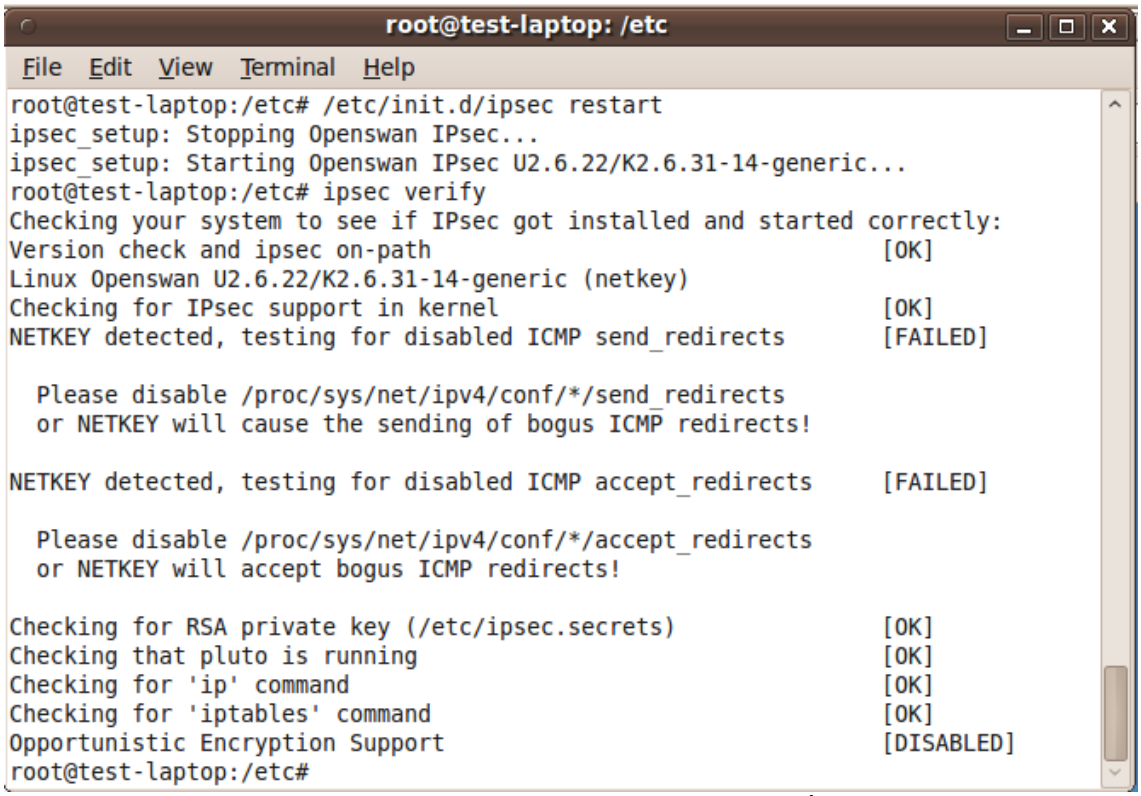

FIGURA A4. 5 VERIFICACION DE LA CORRECTA INSTALACIÓN DE OPENSWAN

Para la configuración se editó el archivo /etc/ipsec.conf, agregando la configuración de cada conexión al final, de la siguiente forma:

```
conn hhprueba1                  # Nombre de esta conexión: hhprueba1
        authby=secret           # Autenticación por clave pre-compartida
        left=192.168.1.2        # IP del extremo izquierdo de la conexión
        leftnexthop=192.168.1.1 # Gateway del extremo izquierdo
        right=192.168.3.2       # IP del extremo derecho de la conexión
        rightnexthop=192.168.3.1 # Gateway del extremo derecho
        keyexchange=ike         # Tipo de intercambio de claves
        ike=3des-sha1-modp1024  # Configuración de IKE según RFC4109
        pfs=yes                 # Habilitar Perfect Forward Secrecy
        aggrmode=yes            # Forzar Uso de Modo Agresivo
        keylife=60m             # Tiempo de vida de las SA en minutos
        rekey=yes               # Renovación automática de llaves
        ikelifetime=120m        # Tiempo de vida de las SA de IKE
        auto=add                # Agregar al iniciar OpenSwan, pero no iniciar la SA
        type=tunnel             # Modo de Operación (Túnel/Transporte)
        phase2=ah               # Protocolo a usar en la 2da fase
        phase2alg=sha2_256      # Algoritmo a utilizar en 2da fase.
```

Y en el archivo /etc/ipsec.secrets se deben agregar los datos de las direcciones IP y la clave pre-compartida entre los extremos de la conexión de la siguiente forma:

```
#Clave para la conexion de prueba host-host
192.168.1.2 192.168.3.2: "0x53f06ff6_78ecb58e_b586fafe_e66612f0"
```

4. INSTALACION DE VPNCLIENT EN LINUX

1. Descargar el VPN Client correspondiente a su arquitectura (32 o 64 bits) en este caso se utilizó: vpnclient-linux-x86_64-4.8.02.0030-k9.tar.gz.

2. Descargar el patch de: *http:///lamnk.com/download/vpnclient-linux-2.6.31-final.diff*

3. Descomprimir el VPN Client. Es recomendable copiar el archivo descomprimido a /usr/local.

4. Luego aplicar el patch con el comando:

```
patch < /home/juan/Escritorio/vpnclient-linux-2.6.31-final.diff
```

5. Instalar con la orden: *./vpn_install*

6. Y si sale error se utiliza el siguiente comando despues del paso 4:

```
sudo sed -i 's/const\ struct\ net_device_ops\ \*netdev_ops;/struct\ net_device_ops\
\*netdev_ops;/' `find /usr/src -name netdevice.h`
```

7. Si continúa saliendo error, se copia el archivo .diff dentro de la carpeta descomprimida y se reemplazar el comando 4 por: patch < ./vpnclient-linux-2.6.31-final.diff

8. Luego se da *Enter* cuando lo solicite, como se puede ver a continuación:

```
Cisco Systems VPN Client Version 4.8.02 (0030) Linux Installer
Copyright (C) 1998-2006 Cisco Systems, Inc. All Rights Reserved.

By installing this product you agree that you have read the
license.txt file (The VPN Client license) and will comply with
its terms.

Directory where binaries will be installed [/usr/local/bin] <enter>
Automatically start the VPN service at boot time [yes] <enter>

In order to build the VPN kernel module, you must have the
kernel headers for the version of the kernel you are running.

Directory containing linux kernel source code [/lib/modules/2.6.31-21-
generic/build] <enter>
* Binaries will be installed in "/usr/local/bin".
* Modules will be installed in "/lib/modules/2.6.31-21-generic/CiscoVPN".
* The VPN service will be started AUTOMATICALLY at boot time.
* Kernel source from "/lib/modules/2.6.31-21-generic/build" will be used to build
the module.

Is the above correct [y] <enter>
```

Si todo salió bien, se debe en obtener en consola algo como lo siguiente:

```
Making module
```

```
make -C /lib/modules/2.6.31-21-generic/build
SUBDIRS=/home/juan/Escritorio/vpnclient modules
make[1]: se ingresa al directorio `/usr/src/linux-headers-2.6.31-21-generic'
  CC [M]  /home/juan/Escritorio/vpnclient/linuxcniapi.o
  CC [M]  /home/juan/Escritorio/vpnclient/frag.o
  CC [M]  /home/juan/Escritorio/vpnclient/IPSecDrvOS_linux.o
  CC [M]  /home/juan/Escritorio/vpnclient/interceptor.o
/home/juan/Escritorio/vpnclient/interceptor.c: In function ‘interceptor_init’:
/home/juan/Escritorio/vpnclient/interceptor.c:140: warning: assignment discards
qualifiers from pointer target type
  CC [M]  /home/juan/Escritorio/vpnclient/linuxkernelapi.o
  LD [M]  /home/juan/Escritorio/vpnclient/cisco_ipsec.o
  Building modules, stage 2.
  MODPOST 1 modules
WARNING: could not find /home/juan/Escritorio/vpnclient/.libdriver.so.cmd for
/home/juan/Escritorio/vpnclient/libdriver.so
  CC      /home/juan/Escritorio/vpnclient/cisco_ipsec.mod.o
  LD [M]  /home/juan/Escritorio/vpnclient/cisco_ipsec.ko
make[1]: se sale del directorio `/usr/src/linux-headers-2.6.31-21-generic'
Copying module to directory "/lib/modules/2.6.31-21-generic/CiscoVPN".
Already have group 'bin'

Creating start/stop script "/etc/init.d/vpnclient_init".
   /etc/init.d/vpnclient_init
Enabling start/stop script for run level 3,4 and 5.
Creating global config /etc/opt/cisco-vpnclient

Installing license.txt (VPN Client license) in "/opt/cisco-vpnclient/":
   /opt/cisco-vpnclient/license.txt

Installing bundled user profiles in "/etc/opt/cisco-vpnclient/Profiles/":
* New Profiles     : sample

Copying binaries to directory "/opt/cisco-vpnclient/bin".
Adding symlinks to "/usr/local/bin".
   /opt/cisco-vpnclient/bin/vpnclient
   /opt/cisco-vpnclient/bin/cisco_cert_mgr
   /opt/cisco-vpnclient/bin/ipseclog
Copying setuid binaries to directory "/opt/cisco-vpnclient/bin".
   /opt/cisco-vpnclient/bin/cvpnd
Copying libraries to directory "/opt/cisco-vpnclient/lib".
   /opt/cisco-vpnclient/lib/libvpnapi.so
Copying header files to directory "/opt/cisco-vpnclient/include".
   /opt/cisco-vpnclient/include/vpnapi.h

Setting permissions.
   /opt/cisco-vpnclient/bin/cvpnd (setuid root)
   /opt/cisco-vpnclient (group bin readable)
   /etc/opt/cisco-vpnclient (group bin readable)
   /etc/opt/cisco-vpnclient/Profiles (group bin readable)
   /etc/opt/cisco-vpnclient/Certificates (group bin readable)
* You may wish to change these permissions to restrict access to root.
* You must run "/etc/init.d/vpnclient_init start" before using the client.
* This script will be run AUTOMATICALLY every time you reboot your computer.
```

4.1. CONFIGURACIÓN

Con la instalación se proporciona un ejemplo de configuración llamado sample.pcf que contiene lo siguiente:

```
[root@ubuntu]# gedit /etc/opt/cisco-vpnclient/Profiles/sample.pcf
[main]
Description=sample user profile
Host=10.212.20.52
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=chimchim
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=1
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Se guarda el contenido de este archivo con otro nombre, por ejemplo *ipsec.pcf*; y se modifica convenientemente de acuerdo a los parámetros de interés.

```
[root@ubuntu]# cp sample.pcf ipsec.pcf
```

A continuación se marcan los valores modificados en negrita.

```
[root@ubuntu]# gedit /etc/opt/cisco-vpnclient/Profiles/ ipsec.pcf
[main]
Description=Conexion VPN
Host= 192.168.1.1
AuthType=1
GroupName=groupipsec
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=ipsec
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=1
CertStore=0
CertName=
CertPath=
CertSubjectName=
```

```
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
UserPassword=
enc_UserPassword=
GroupPwd=
enc_GroupPwd=
ISPPhonebook=
NTDomain=
EnableMSLogon=1
MSLogonType=0
TunnelingMode=0
TcpTunnelingPort=10000
SendCertChain=0
PeerTimeout=90
EnableLocalLAN=0
```

Algunos datos se pueden proporcionar en el fichero o se solicitarán a la hora de realizar la conexión. Los datos privados, como son los passwords, se dejarán para introducir en cada sesión por razones de seguridad.

Una vez configurado el servicio, para que éste quede disponible para cuando se desee utilizarlo es necesario iniciar el "daemon" correspondiente, lo que se puede hacer de la forma habitual en Linux sabiendo que el proceso queda en /etc/init.d y su nombre es vpnclient_init.

Si no se quiere que el servicio quede disponible en el arranque del ordenador, para utilizarlo cada vez se deberá ejecutar el siguiente comando:

```
[root@ubuntu]# /etc/init.d/vpnclient_init start
```

4.2. UTILIZACIÓN

El comando *vpnclient* queda definido para arrancar el servicio en el PATH del sistema por lo que bastará con invocarlo con los parámetros adecuados para iniciar, parar o consultar el estado de la conexión VPN.

Con el argumento *connect* y el nombre del fichero de configuración que se ha creado se abre la conexión tras responder a las preguntas que se han dejado pendientes en la configuración, por ejemplo:

```
[root@ubuntu]# vpnclient connect ipsec
```

5. INSTALACIÓN DE IPSEC EN WINDOWS XP

El primer paso es dirigirse a Inicio -> Ejecutar, escribir *mmc* y dar click en Aceptar. Este comando abrirá una ventana de consola como aparece a continuación:

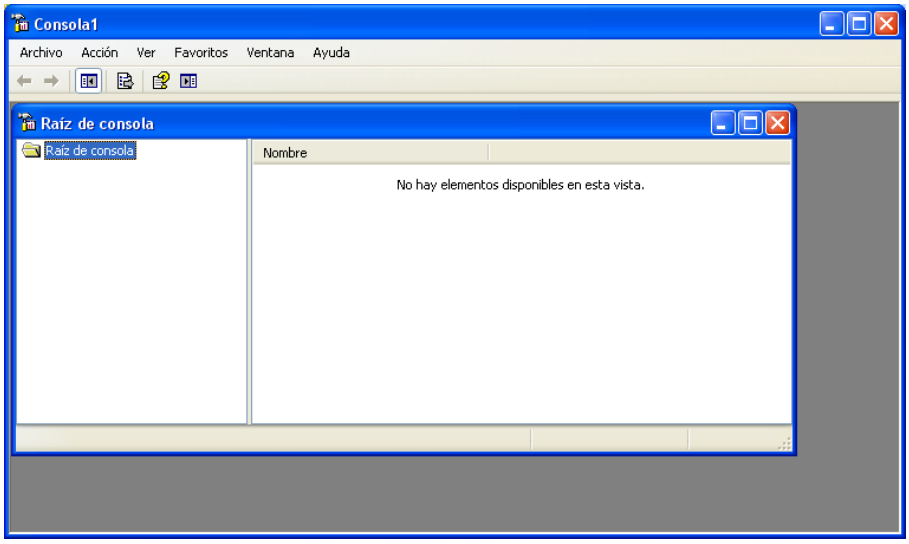

FIGURA A4. 6 MICROSOFT MANAGEMENT CONSOLE

Ahora se debe ir a Archivo -> Agregar o Quitar Complementos, que abrirá una nueva ventana y dentro de esta nueva ventana se escoge la opción de “Administrador de las directivas de seguridad de IP” y se pulsa el botón de -> Agregar.

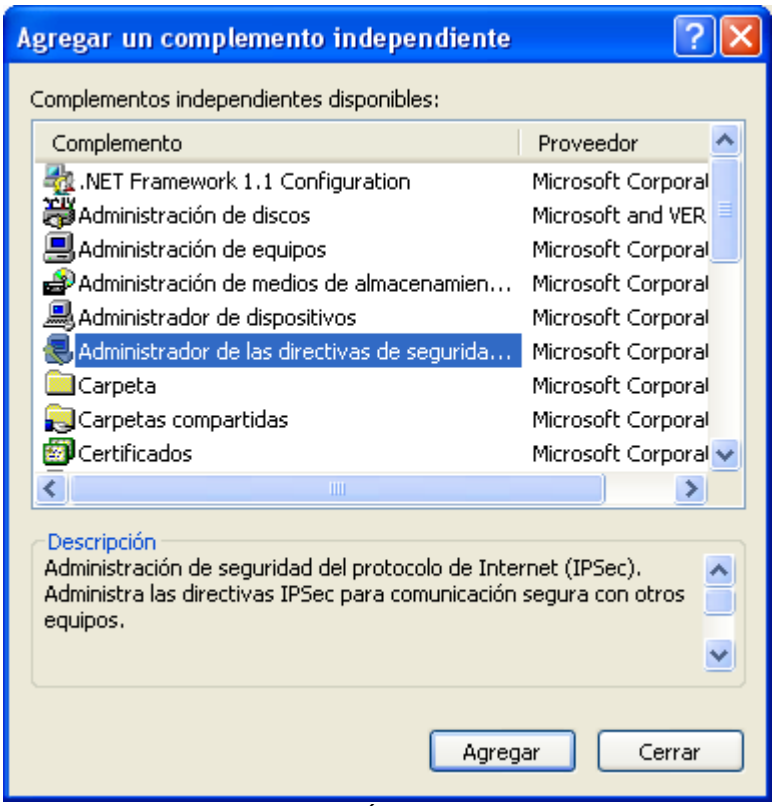

FIGURA A4. 7 ADICIÓN DE COMPLEMENTOS

Se configura según lo deseado, en este caso se escoge la opción equipo local.

Luego de este procedimiento se deberá tener en la pantalla de la consola algo como lo siguiente:

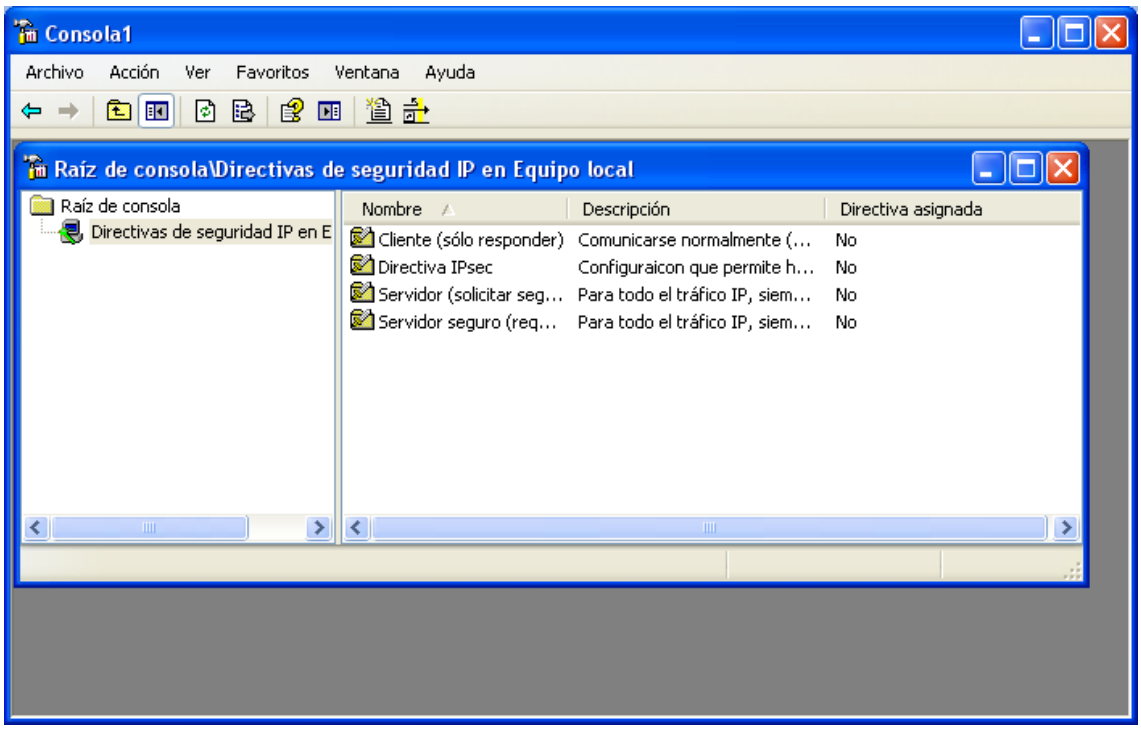

FIGURA A4. 8 MICROSOFT MANAGEMENT CONSOLE CON IPSEC CONFIGURADO

Posteriormente, se deberá empezar a configurar la Directiva IPsec según se desee, y luego de haberla configurado para activarla se realiza Click derecho sobre “Directiva IPsec” y se selecciona Asignar, cambiando el estado de No a Sí. Si se desea guardarla simplemente se va a Archivo -> Guardar.