Proyecto de Sistemas Informáticos
Facultad de Informática
Universidad Complutense de Madrid
2010/2011

Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante OpenVPN

Autora:
Cristina Gil Álvaro
Profesor director:
Antonio Carlos Zaragoza Martín

Facultad de Informática
Universidad Complutense de Madrid

TITULO

Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante OpenVPN

AUTORA

Gil Alvaro, Cristina

PROFESOR DIRECTOR

Antonio Carlos Zaragoza Martín

CURSO ACADEMICO

2010/2011

ASIGNATURA

Sistemas Informáticos

Resumen

Esta memoria resume el trabajo realizado para el proyecto "*Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante VPN*", en el contexto de la asignatura Sistemas Informáticos de la Universidad Complutense de Madrid.

El objetivo ha sido elaborar una aplicación gráfica que proporcione un entorno amigable tanto para la máquina cliente como para la máquina servidor que permita de una manera clara y sencilla establecer una conexión VPN entre dos o más máquinas cliente situadas en cualquier lugar del mundo.

Con esta aplicación se ahorrará en tanto en costes como en infraestructuras al intentar establecer redes virtuales entre equipos muy distantes entre sí, manteniendo la seguridad y la rapidez que es necesaria en estos casos.

Se desarrollaran principalmente dos herramientas, la primera que se tratará es la herramienta servidor, encargada de realizar las principales configuraciones y de llevar a cabo la administración de los equipos conectados a la red. La segunda herramienta será el cliente, que permitirá de una manerá automatizada y transparente al usuario crear una red de usuarios o unirse a una existente mediante unas credenciales que le han sido proporcionadas.

Estas aplicaciónes haran uso de la aplicación gratuita OpenVPN que será finalmente la encargada de realizar las conexiones.

Palabras clave

Redes, VPN, OpenVPN, Servidor, Cliente, Túnel, Cifrado, IP, Interfaz, Conexión

Overview

This report summarizes the work done for the project "*Network tunnels for virtual private networking via VPN point to point*" in the context of the course Systems of the Universidad Complutense de Madrid.

The aim has been to develop a graphical application that provides a friendly environment for both the client machine to the server machine to allow a clear and simple way to establish a VPN connection between two or more client machines located anywhere in the world.

With this application we will save cost and infrastructure while trying to establish virtual networks between widely separated teams, maintaining the security and speed that is necessary in these cases.

Two main tools will be developed, the first is the tool server, for establishing the main settings and perform administration of the computers on the network. The second tool is the client, enabling an automated and transparent to the user to create a network of users or join an existing one using credentials that have been provided.

These applications will make use of the free utility OpenVPN which will finally be responsible for making connections.

Keywords

Networking, VPN, OpenVPN, Server, Client, Tunnel, Encryption, IP, Interface, Connection

Contenido

1. Enunciado del Proyecto

Titulo: Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante OpenVPN.

Resumen: Las redes privadas virtuales (VPN) permiten utilizar los medios de comunicación públicos como Internet para establecer comunicaciones entre redes locales ubicadas en lugares distintos, haciendo que se comporten como si fuesen la misma red local. Para ello se precisan técnicas de cifrado de la información y establecimiento de túneles sobre redes públicas, con objeto de mantener la seguridad de las comunicaciones. Habitualmente las VPN se montan mediante costosos productos hardware, routers o sistemas dedicados, aunque cada vez más van apareciendo nuevos productos para emular el establecimiento de túneles mediante software (Hamachi). OpenVPN es una herramienta libre y gratuíta que permite la configuración de túneles punto a punto y site to site, aunque su configuración suele ser bastante tediosa. Se trata de producir un producto software que permita la configuración automática de un servidor de túneles mediante OpenVPN a partir de especificaciones sencillas. Dicho servidor debe permitir el establecimiento de túneles punto a punto entre la red local donde se ubique el servidor de túneles y los equipos cliente que deseen formar parte de la misma, y que conozcan los patrones de autenticación.

El trabajo consiste en:

1) Automatizar la configuración de un servidor de túneles mediante OpenVPN a partir de una interfaz amigable que permita elegir la configuración de VPN deseada.

2) Automatizar la adhesión de clientes a la VPN mediante protocolos de autenticación adecuados, y eliminando la necesidad de conocimientos técnicos de los clientes.

3) Diseñar un producto software que permita un amigable establecimiento, configuración y mantenimiento de redes privadas virtuales punto a punto, entre el servidor y un número indeterminado de clientes, con interfaz Web. El sistema debe admitir el funcionamiento sobre conexiones a Internet con IP dinámica, tanto para el servidor como para los clientes.

4) Diseñar una interfaz de administración de servidores y clientes openVPN que permita monitorizar el comportamiento de la VPN: Equipos conectados, equipos desconectados, recursos disponibles, latencias, etc...

5) Diseñar una herramienta de conexión de clientes multiplataforma que permita, aparte del establecimiento de túneles, servicios como chat, exploración de recursos, ping y otros.

El servidor de túneles deberá funcionar sobre Windows XP, aunque deberá aceptar clientes VPN de distintas plataformas. Una vez establecidos los túneles, los equipos deben comportarse como miembros de la misma red local en la que esté el servidor, a todos los efectos.

2. Introducción a las redes VPN

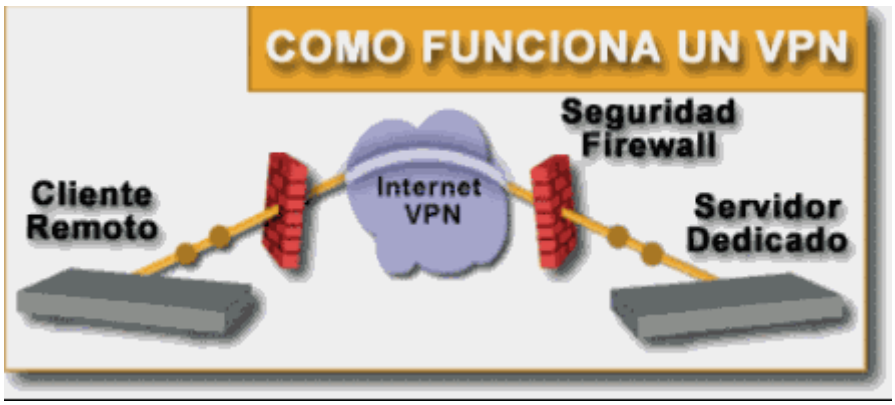
Descripción

Una red privada virtual, RPV en español, o VPN de las siglas en inglés Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

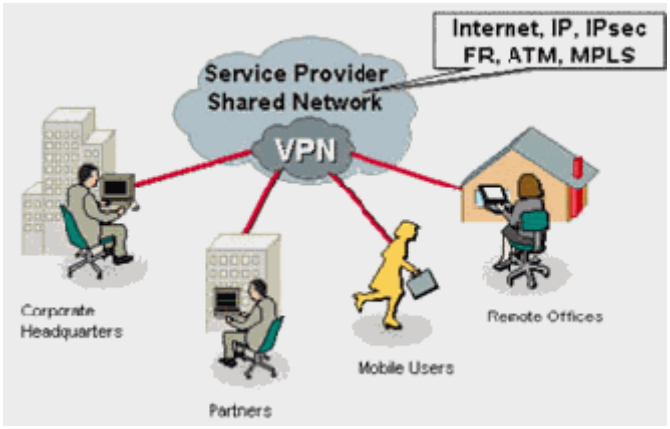
En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital. Por tanto dichas redes deben cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls.

Los datos que viajan a través de una VPN parten del servidor dedicado y llegan a un firewall que hace la función de una pared para engañar a los intrusos de la red, después los datos llegan a una nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad y ancho de banda garantizado lleguen a su vez al firewall remoto y terminen en el servidor remoto. Se muestra una imagen a continuación que ilustra el proceso:



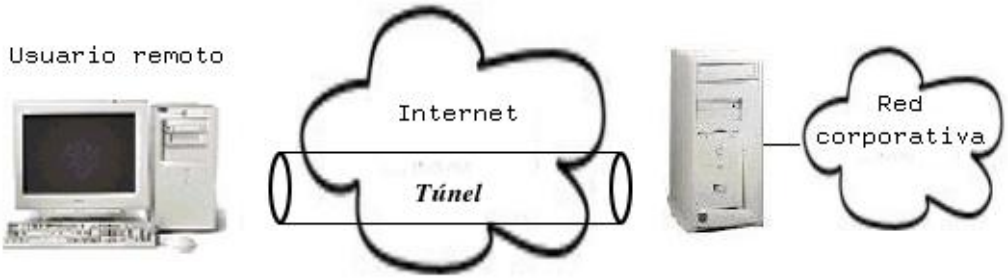
Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas, trabajadores desde casa, etc. mediante protocolos como internet, IP, IpSec, Frame Relay, ATM como muestra la imagen siguiente:



Arquitecturas de conexión VPN

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).



VPN punto a punto

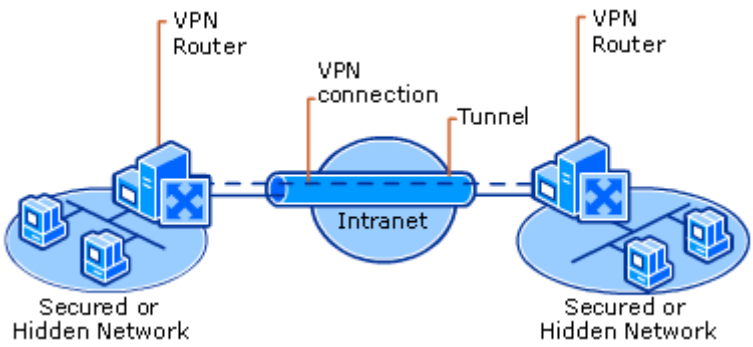
Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAcaddress, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN internas o externas.



Tipos Conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

Protocolos utilizados en una VPN

Las VPN trabajan con dos tipos comunes de protocolos: PPTP y L2TP.

El primero, cuyas siglas significan "Point to Point Tunneling Protocol", ha sido desarrollado por el consorcio PPTP Forum, integrado por Microsoft, US Robotics y 3com entre otras importantes empresas. En general PPTP es el más sencillo, aunque ofrece menor seguridad que L2TP, por este motivo se recomienda al usuario el reemplazo o actualización de las VPN montadas sobre este protocolo.

En cuanto al L2TP, cuyas siglas significan "Layer Two Tunneling Protocol", es un estándar creado por el IETF (Internet Engineering Task Force) para solventar y corregir los problemas del protocolo PPTP. El L2TP ofrece más seguridad que el PPTP, pero su implementación resulta más complicada para el usuario común.

Requerimientos para montar una VPN

Para montar correctamente una red VPN necesitaremos de:

-Tener conexión a internet.

-Servidor VPN.

-Al menos un cliente VPN.

-Asegurarse que la red sea capaz: encapsular y encriptar datos, autentificar usuarios y asignar IP´s de manera estática o dinámica.

Ventajas y Desventajas de OpenVPN

Ventajas de una VPN

Integridad, confidencialidad y seguridad de los datos.

Reducción de costos.

Sencilla de usar.

Sencilla instalación del cliente en cualquier plataforma o Sistema Operativo

Control de Acceso basado en políticas de la organización

Herramientas de diagnostico remoto.

Los algoritmos de compresión optimizan el tráfico del cliente.

Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

Desventajas de una VPN

El uso de redes VPN no tiene apenas desventajas, sin embargo cabe señalar que como toda la información se envía a través de Internet, es necesario tener una buena conexión. Con una conexión a Internet más básica, se pueden experimentar problemas y lentitud.

Formas de implementación

Una VPN se puede implantar por software o por hardware.

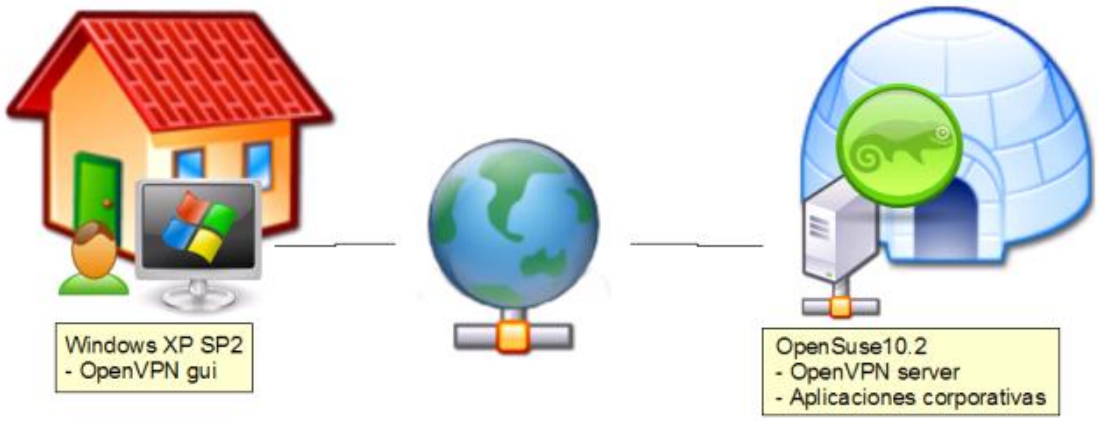
Las soluciones hardware ofrecen un mejor rendimiento y son más fáciles de configurar, pero tienen el problema de que a veces no son capaces de operar entre distintas plataformas y obligan a los usuarios de la VPN a estar en la misma plataforma, además son más caras.

Las soluciones software ofrecen más flexibilidad, pudiendo acceder a la VPN desde diferentes plataformas, pero son más difíciles de configurar. Son más baratas, e incluso se pueden encontrar versiones libres como OpenSSH y OpenVPN.

3. OpenVPN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre. OpenVPN, es un producto de software creado por James Yonan en el año 2001 y que ha estado mejorando desde entonces. Ninguna otra solución ofrece una mezcla semejante de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características.

Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.



OpenVPN es una excelente nueva solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria SSL/TLS para cifrar y combina todos las características mencionadas anteriormente en las otras soluciones VPN. Su principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. De todos modos no hay que preocuparse siempre que contemos con un Linux en el cual podremos implementarlo sin ningún problema mediante software.

Ventajas y Desventajas de OpenVPN

Ventajas de OpenVPN

Provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de IPsec.

Además ofrece ventajas que van más allá que cualquier otra solución como ser:

-Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).

-Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.

-Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.

-Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).

-Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.

-Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.

-Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.

-Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.

-Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.

-Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.

-Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son increíblemente simples.

-Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

Desventajas de OpenVPN

-No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.

-Falta de masa crítica.

-Todavía existe poca gente que conoce cómo usar OpenVPN.

-Al día de hoy sólo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

Si se busca alta seguridad e importa que la transferencia de datos sea segura, se debería usar OpenVPN. Si se desea una configuración fácil o poder usarlo en aparatos móviles, entonces es mejor PPTP. Hay otros protocolos disponibles, como L2P o IpSec, pero no son tan fáciles de usar ni tan rentables.

4. Componentes Gráficos OpenVPN

Para facilitar la manera de crear redes VPN, usando como base el software OpenVPN, se crean dos componentes gráficos. El primero que se detallará será la herramienta Servidor VPN, que permitirá crear, configurar y mantener redes VPN. A continuación se hablará del cliente gráfico OpenVPN que de la misma manera nos permitirá de una manera sencilla conectarnos a una red VPN previamente creada por otro usuario para compartir recursos con los otros miembros de la red.

La aplicación está basada en el intercambio de archivos entre clientes y el servidor mediante SSH. Cuando se crea un cliente, una red, un cliente se adhiere a una red, etc. se mandan archivos de los clientes al servidor. Cada cierto tiempo, tanto la aplicación cliente como la del servidor, necesitan actualizar el estado de las redes a las que pertenecen en el caso del cliente o el estado de todas las redes existentes en el caso del servidor. Para ello, los clientes recogen del servidor estos archivos actualizados por otros clientes.

Cuando se crea un cliente, se crea un archivo *NombreCliente.nom* en la carpeta redes dentro del directorio de instalación de OpenVPN, este archivo se le enviará al mismo directorio del servidor, con esto nos aseguramos que no vaya a haber dos clientes con el mismo nombre, ya que al crear un cliente se comprueba que este no exista en el directorio del servidor un archivo con este nombre.

Al crear un cliente, son necesarios algunos archivos creados en el servidor al crear las claves que también se traerán mediante SSH. Estos archivos son *ca.crt* y *ca.key*, también es necesario traer al cliente los datos introducidos para crear las claves del servidor, para usar los mismos al crear al cliente y las claves puedan ser creadas correctamente (archivo *Parametros.config*). Otros archivos que se traen del servidor y que son necesarios a la hora de crear las claves del cliente son *index.txt* y *serial*.

Cuando se crea una red, se generan dos archivos con el nombre de la red. El primero *NombreRed.eq*, contiene el listado de clientes que pertenecen a la red, en este caso solo aparecerá el cliente creador de la red; y el segundo *NombreRed.c* que contiene la clave para ingresar en la red. Estos archivos de depositan mediante SSH en el servidor, quedando esta red disponible para que otros clientes puedan conectarse.

Para conectarse a una red, la aplicación pide que se introduzca el nombre de la red y la contraseña, si estas coinciden con lo que existe en el servidor, se llevará hacia el cliente el archivo *NombreRed.eq*, este le editará y se incluirá en el listado, posteriormente se volverá a dejar el listado en el servidor para que otros clientes puedan disponer del listado actualizado y puedan agregarse de la misma manera.

Cuando un cliente se conecta por primera vez a la red VPN y se le asigna una IP, deposita en el servidor en la carpeta ccd un archivo *NombreCliente* con su IP, así el propio servidor y otros clientes tendrán disponibles las IP´s de los clientes de las redes a las que pertenecen para poder realizar las acciones implementadas (ping, chat, explorador…).

Tanto el servidor como los clientes disponen de estos archivos para poder actualizar estado de las redes cada cierto tiempo, del orden de los 30 segundos, accediendo a estos archivos y leyendo la información necesaria para mostrar la información actualizada y correcta.

Cuando desaparece un cliente, se borra de una red, etc. también se editan los archivos existentes en los clientes, y se vuelven a mandar al servidor, cuando los clientes se tengan que actualizar, recogerán los archivos modificados y mostrarán la información correctamente.

Resumen de archivos que intervienen en las aplicaciones.

-*NombreRed.eq*: contiene el listado de equipos que están conectados en a la red NombreRed, está en la carpeta tanto en los clientes como en el servidor %PATHINSTALACIONOPENVPN%redes

-*NombreRed.c*: contiene la clave para acceder a la red, está en el servidor en la carpeta %PATHINSTALACIONOPENVPN%redes

-*NombreEquipo.nom*: se crea cuando se da de alta un cliente y se elimina cuando desaparece en el servidor, está en %PATHINSTALACIONOPENVPN%redes

-*NombreEquipo*: contiene la IP del Equipo y está en la carpeta %PATHINSTALACIONOPENVPN%ccd al existir en esa carpeta, mediante un parámetro de configuración en el servidor, se consigue que a los equipos se les asigne siempre la misma IP.

-*Parámetros.config*: contiene la información introducida por el Administrador para generar las claves del servidor. Al crearse un cliente, viaja al cliente para usar esos mismos datos para poder generar la clave simétrica.

- *ca.crt*, *ca.key*, *index.txt* y *serial*: archivos que son traídos desde el servidor a la hora de dar de alta un nuevo cliente para poder crear las claves, son depositados en %PATHINSTALACIONOPENVPN%easy-rsa/keys.

-*Servidor.ovpn* y *Cliente.ovpn* (.conf en el caso de Linux): contienen los parámetros de configuración. Están en %PATHINSTALACIONOPENVPN%config.

5. Servidor OpenVPN

Es una aplicación gráfica, que permite crear el nodo de la red principal para poder establecer una red VPN. A continuación se explicaran detalles técnicos sobre la implementación, así como un manual de instalación, configuración y uso de la herramienta.

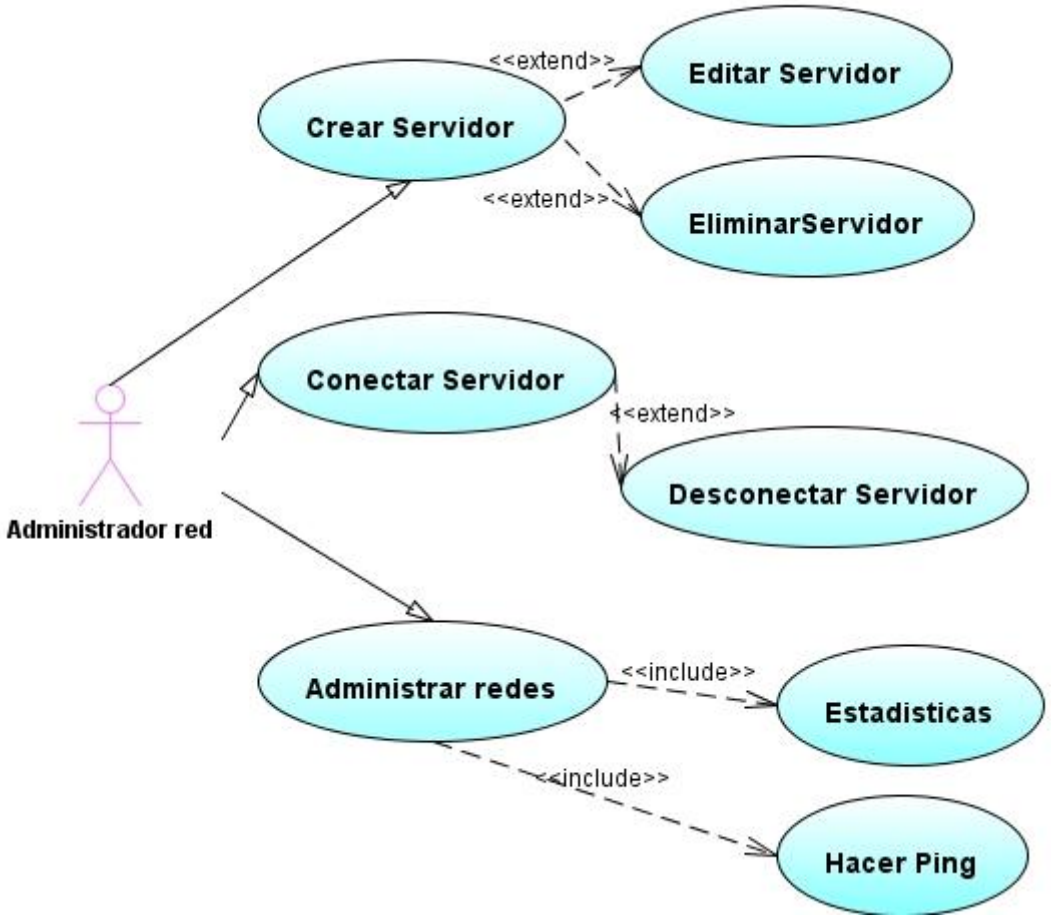
Detalles de implementación

La herramienta ha sido desarrollada mediante Java, usando la Máquina Virtual jre1.6.0_07 y usando el IDE NetBeans 7.0.

Se compone de una serie de clases de las cuales la mayoría son interfaces gráficas de Usuario para poder realizar las acciones que se han implementado (crear servidor, editarlo, conectar, etc.)

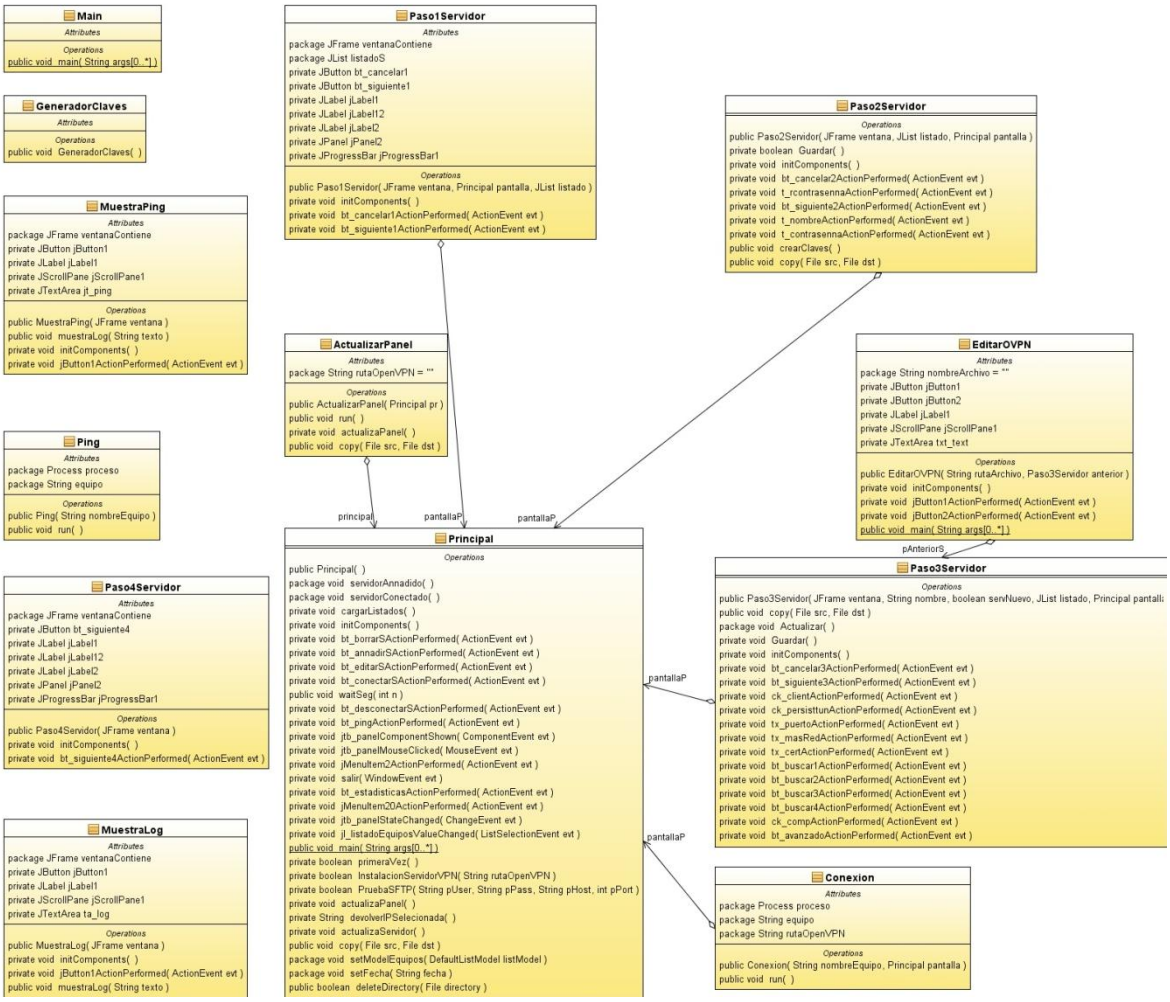
A continuación se detalla la documentación técnica del proyecto

El diagrama de casos de uso para el Servidor Gráfico OpenVPN es como se detalla a continuación:



El usuario del sistema, será a su vez el administrador de la red VPN, por lo que deberá de tener conocimientos sobre redes OpenVPN y de la configuración de estas. Este usuario podrá llevar a cabo distintas funciones como pueden ser, crear, editar o borrar una configuración de servidor, conectar o desconectar el servidor y por lo tanto crear o desmantelar la red. Además podrá visualizar el estado de redes y las estadísticas de los equipos de la red, como los últimos ping realizados, última conexión, etc. Podrá además realizar pings a otros equipos de la red para comprobar el estado de las comunicaciones.

El siguiente diagrama de clases muestra como se interrelacionan las distintas clases del proyecto (se ocultan los atributos de las clases para facilitar el poder incluir la imagen en este documento):



La clase *Principal.java*, como su nombre indica es la clase más importante de la aplicación. Es el formulario principal de la aplicación, en el que se puede crear, configurar, borrar y conectar un servidor. Además permite la visualización del estado de los clientes y redes existentes, así como estadísticas y pings de los equipos conectados.

Las clases *PasoXServidor.java*, suponen los distintos pasos para crear un servidor ofreciendo una guía sencilla para crear el archivo de configuración del servidor y los archivos de claves para la comunicación. Será transparente al usuario el crear los archivos de claves para el servidor y el archivo de configuración. Al final de este paso, tendremos creados junto con el archivo *Servidor.ovpn* de configuración del servidor*:*

Nombre del Archivo	Es necesario para	¿Qué es?	¿Debe ser secreto?
Ca.crt	Servidor y todos los clientes	Certificado para el CA	NO
Ca.key	Solo el ordenador con llave para firmar	Llave para el CA	SI
Dh2048.pem	Servidor	Parámetros Diffie Hellman	NO
Servidor.crt	Solo servidor	Certificado para el servidor	NO
Servidor.key	Solo servidor	Llave privada para servidor	SI

Las clases *EditarOVPN.java*, *MuestraLog.java*, *MuestraPing.java* son paneles gráficos que realizan distintas funcionalidades como sus nombres indican.

El resto de clases proporcionan otras funcionalidades al proyecto como son lanzar el ejecutable de OpenVPN para realizar la conexión, hacer ping a los clientes en diferentes hilos, etc.

Instalación y configuración

Antes de Ejecutar el Servidor Gráfico OpenVPN es necesario reunir las siguientes características técnicas y seguir una serie de pasos. Posteriormente se ejecutará la aplicación ServidorVPN.exe del paquete InstaladorServidor proporcionado.

Requerimientos mínimos de hardware y software

Windows XP

Conexión a Internet

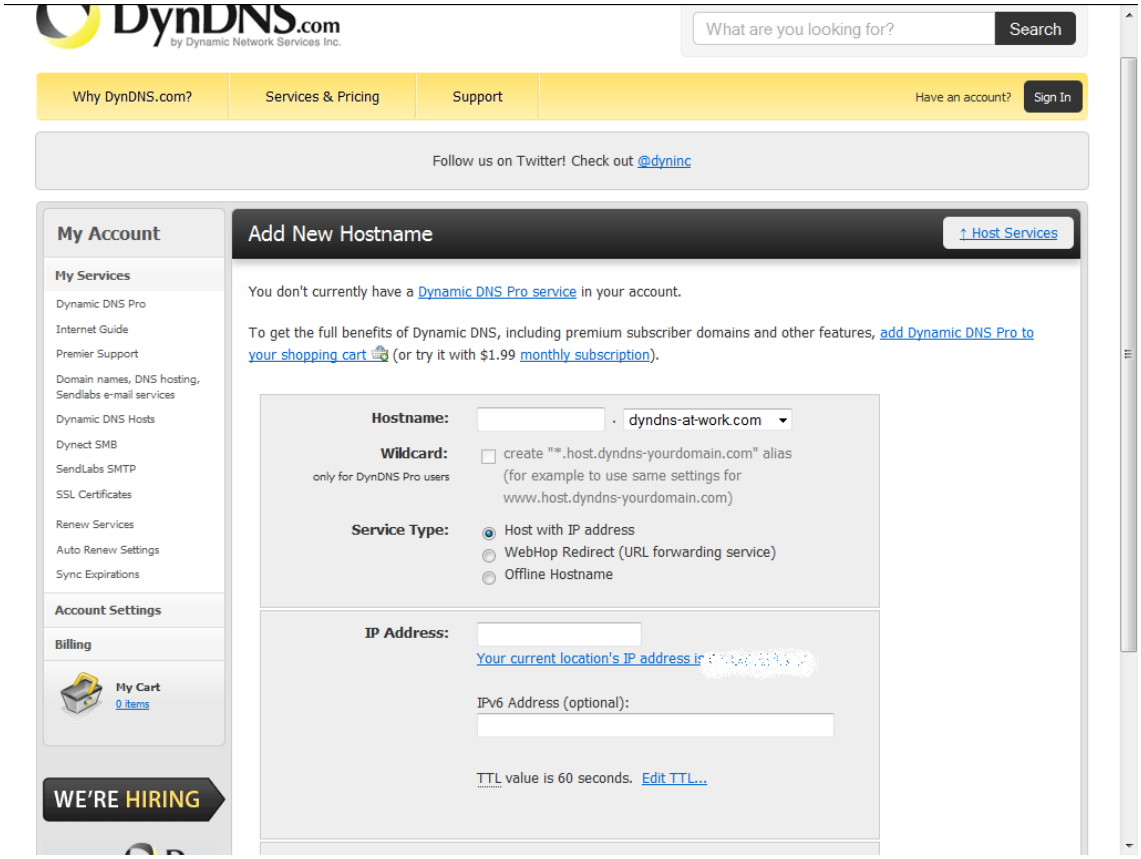
Pasos de instalación

1 Crear cuenta DynDNS (este paso se podrá saltar si el equipo tiene salida directa a internet y no pertenece a una red local).

El equipo accede a internet a través de un router, este será entonces el que reciba los mensajes de la red VPN y deberá redirigirlos al equipo que tenga instalado el software del servidor. Algunos ISP no proveen IP´s fijas a los routers por lo que habrá que asignar un nombre al servidor que mediante DynDNS asegurará que los clientes estarán siempre accediendo al mismo servidor aunque este cambie de IP, o de lugar.

En la web http://www.dyndns.com/ podremos crear una cuenta DynDNS con el nombre que queramos que aun no exista y asignárselo a nuestra IP de salida actual.

Si nuestra IP cambia DynDNS se encargará automáticamente de redirigir la información hacia nuestra nueva IP.

6. 

2. Configuración router (este paso se podrá saltar si el equipo tiene salida directa a internet y no pertenece a una red local).

   Algunos routers precisan que se les indique datos sobre la cuenta DNS que se ha creado para, esta opción suele aparecer como “DDNS (Dynamic DNS) Settings” dentro de la página de configuración del servidor (consultar el manual del router para más información)

   El siguiente paso es redirigir los puertos necesario al equipo de la red local donde está instalado el servidor. Hay que redirigir el puerto UDP 1194 (puerto por defecto de OpenVPN) hacia el equipo servidor, en el siguiente ejemplo el PC servidor tiene la IP de la red local 192.168.2.102.

   También hay que redirigir el puerto TCP y UDP 22 usado para las conexiones SSH de las que posteriormente se hablarán al equipo servidor (en nuestro ejemplo el 192.168.2.102)

   Guardar los cambios en el router y reiniciarlo si es necesario

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable
1	192.168.2.102	UDP	1194	1194	☑
2	192.168.2.102	TCP&UDP	22	22	☑

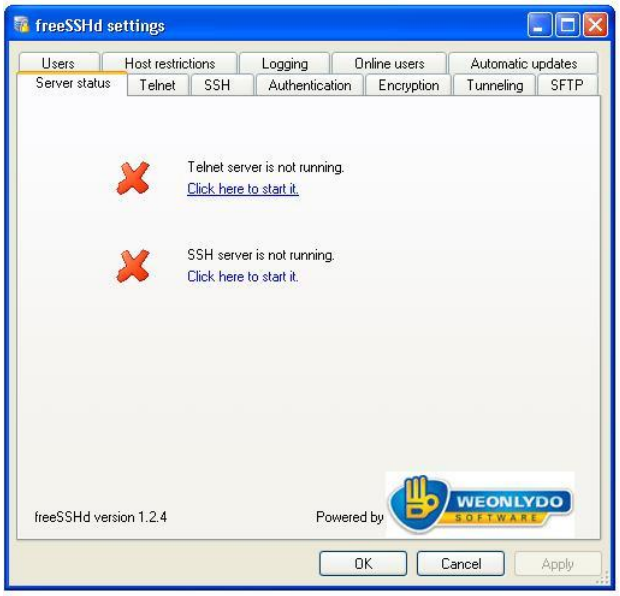
3. Editar la variable del registro

   Abrir el editor de registro de Windows Regedt32.exe en Inicio->Ejecutar y editar la siguiente variable IPEnableRouter con valor 1 localizada en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

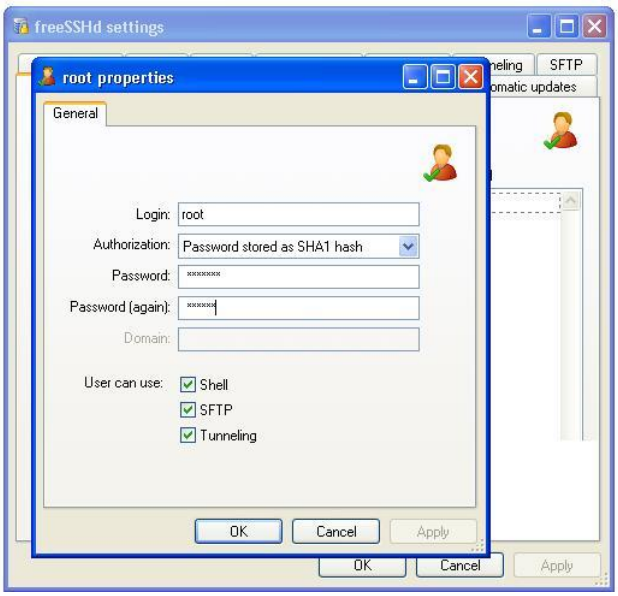
   Con esto conseguiremos que el equipo sea configurado como un Gateway de la red VPN.

4. Instalar servidor SSH. FreeSSHd.
   Para el intercambio de archivos entre cliente y servidor que se ha hablado en el punto anterior, para informar acerca de redes, IPs de los nodos de la red, equipos que pertenecen a una red, creación de claves, etc. hace falta montar un servidor SSH para que el servidor pueda recibir estos archivos de los cliente y que ellos puedan obtenerlos mediante una simple conexión. Para ello se instala la aplicación FreeSSHd que montará sencillamente un servidor SSH. Se deberá descargar de la página http://www.freesshd.com/?ctt=download.
   Tras instalar la aplicación, se deberá hacer click el icono creado en el escritorio

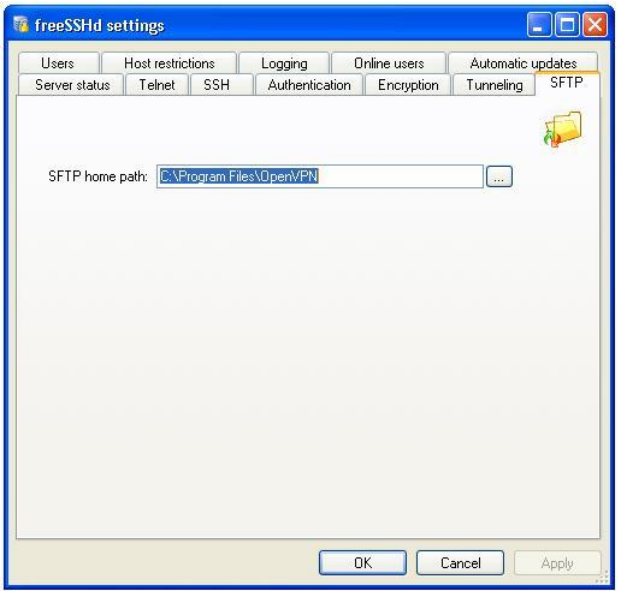
   , se lanzará la aplicación y habrá que realizar tres acciones:



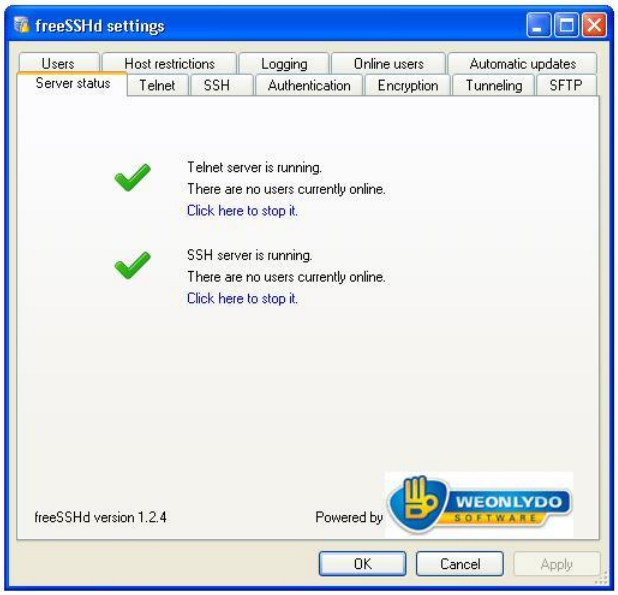
   -Crear usuario: se pulsa sobre la pestaña Users y se pulsa el botón Add… Se rellenan los campos como sigue



-Configurar directorio de entrada: en la pestaña SFTP se indica cual va a ser el directorio donde los clientes se van a conectar cuando introduzcan el nombre de usuario y clave, será entonces el directorio de instalación de OpenVPN. Este paso se podría dejar para cuando se haya instalado OpenVPN, o dejarlo ya configurado.



-Levantar servicios: por último en la pestaña Server Status, se deben levantar los servicios de Telnet y SSH.



5. Instalar Servidor Gráfico

   El último paso antes de poder usar el servidor gráfico es la instalación de la aplicación gráfica del servidor, que está a su vez realizará la instalación desatendida de OpenVPN. Al hacer doble click en el ejecutable ServidorOpenVPN.exe proporcionado en el pack de instalación InstaladorServidor, se mostrará un mensaje como sigue

   Al pulsar el botón aceptar, tras unos segundos aparecerá una mensaje preguntando sobre si se desea instalar un Adaptador de Red Virtual

Se deberá pulsar continuar ya que de no ser así el servidor no funcionará correctamente. Tras unos segundos se volverá a mostrar un mensaje informando acerca del resultado de la instalación

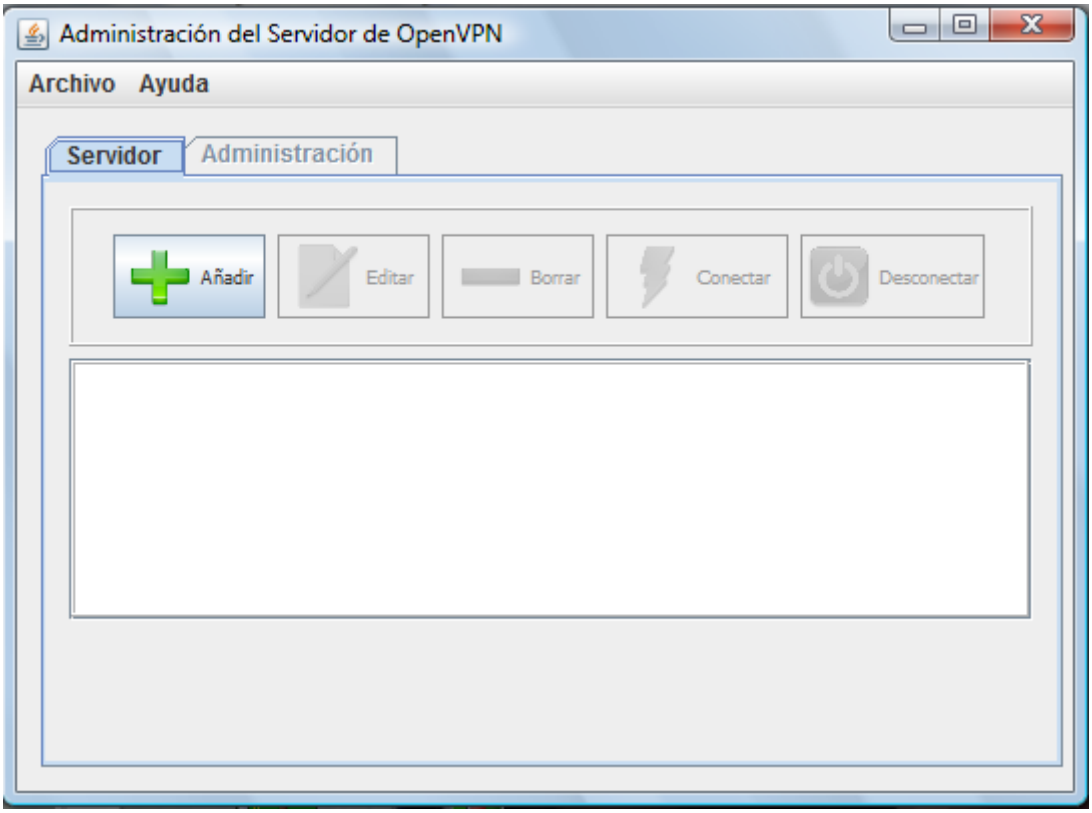
Si por el contrario ha existido algún problema durante la instalación se le informará al usuario con un mensaje similar indicando lo ocurrido.

También puede ocurrir que el usuario lance el instalador teniendo previamente instalada la aplicación OpenVPN, en tal caso el programa saltará el paso de la instalación de esta aplicación.

En este punto ya se puede hacer uso de la aplicación gráfica para el servidor OpenVPN según se ilustra en el siguiente manual

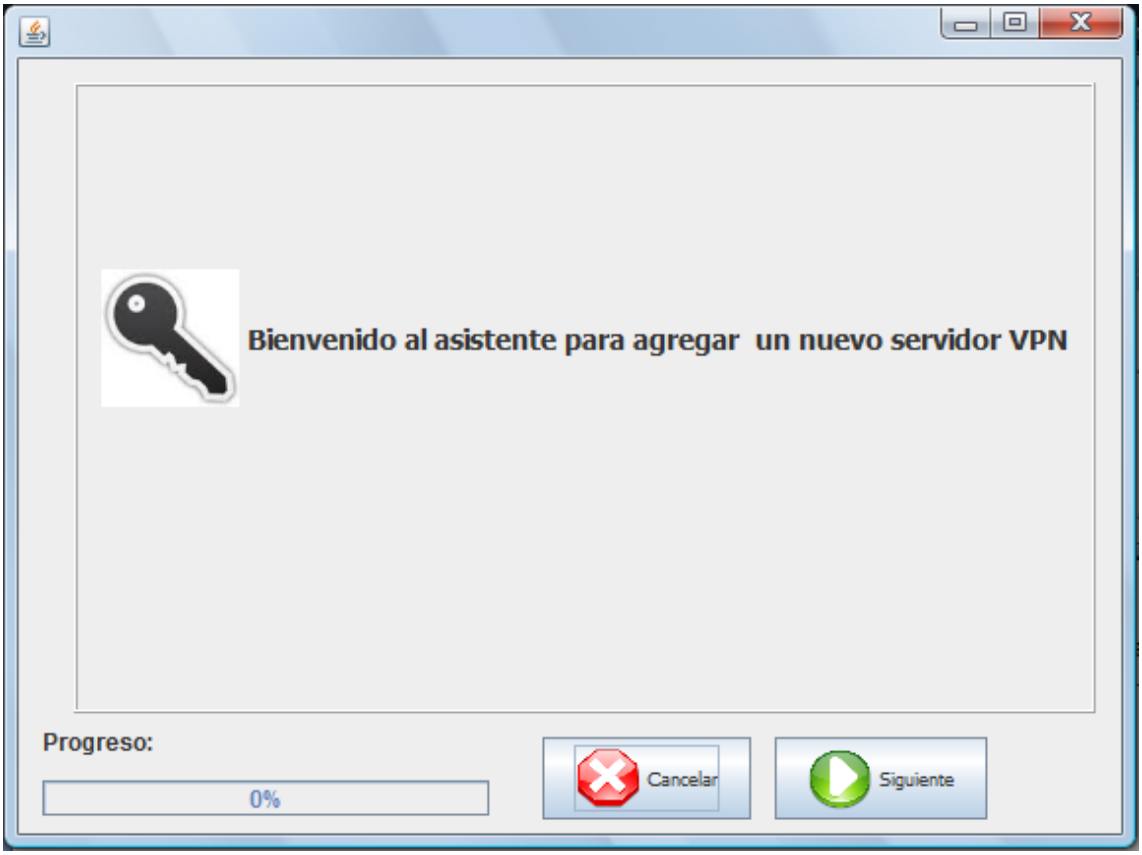
Manual de USO

Tras finalizar la instalación se abrirá una pantalla como la siguiente, el primer paso entonces será crear un Servidor

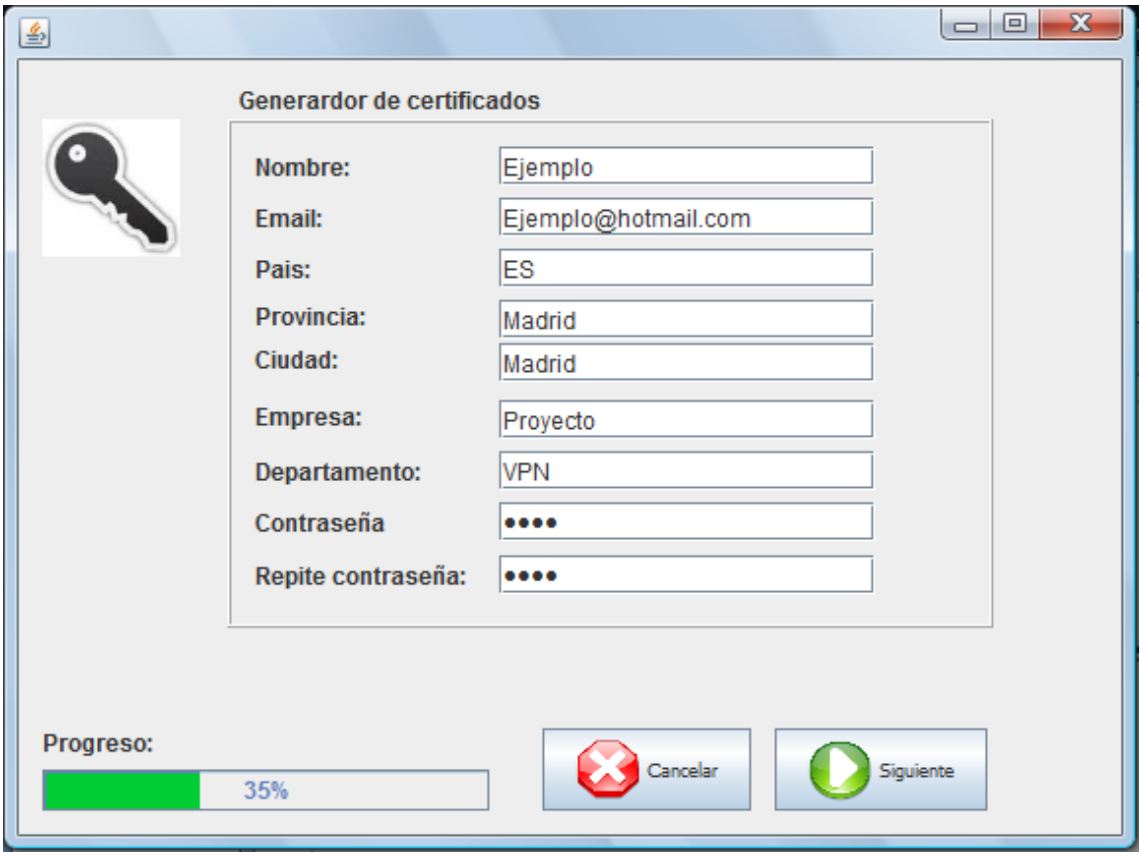


Crear un servidor

Si se pulsa sobre el botón añadir, se iniciará un proceso guiado que llevará a crear un servidor OpenVPN. Solo se podrá crear un servidor en un equipo, por lo que cuando finalice el proceso de crear un servidor, será necesario eliminar este para crear otro



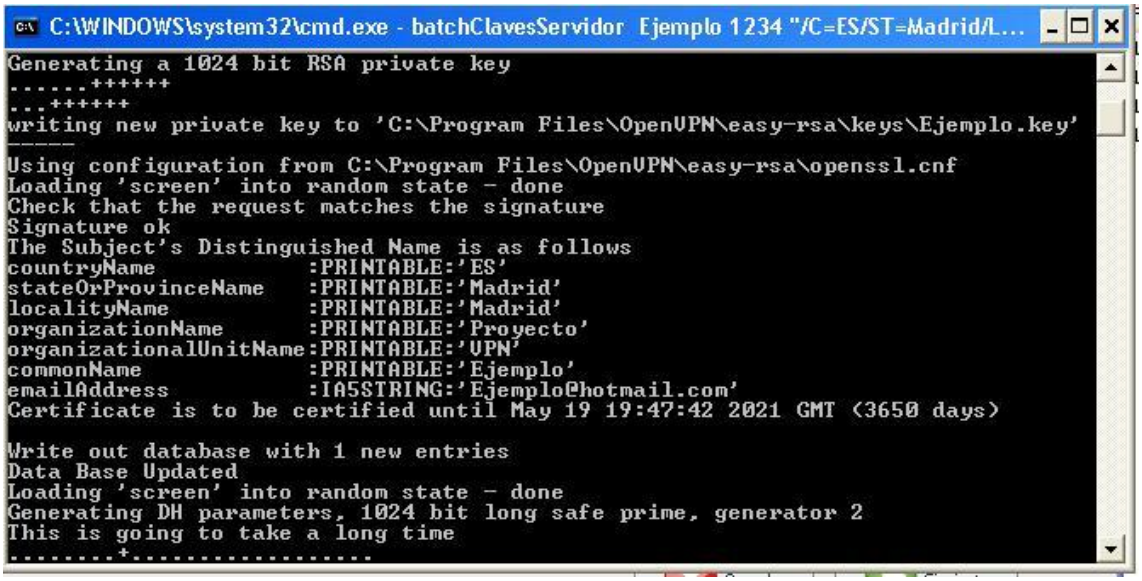
Tras pulsar el botón siguiente, se abrirá otro panel para rellenar los datos necesarios para generar las claves del servidor.



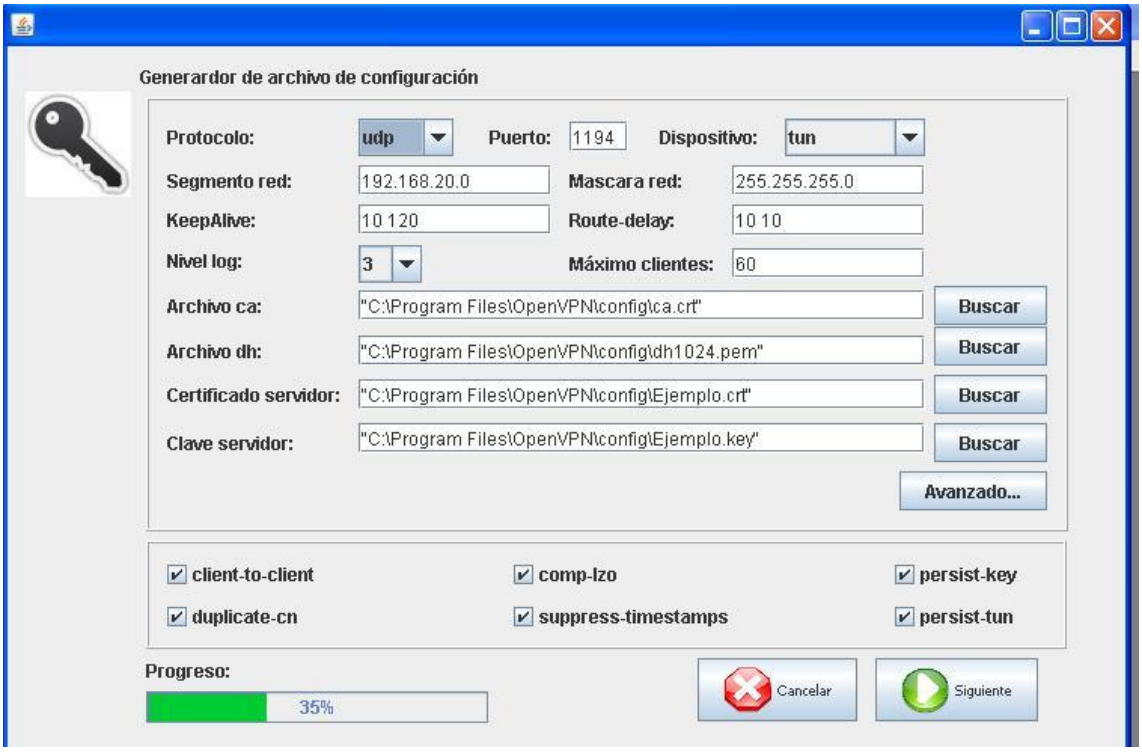
Cuando se hayan rellenado todos los campos, tras pulsar el botón siguiente, ocurrirán dos eventos, el primero abrirá una Shell MS-Dos que ejecutará un .bat para generar las claves del servidor. También se mostrará un panel que editará el archivo .ovpn del servidor creado por defecto, este archivo contiene toda la información necesaria para realizar la conexión según las necesidades del administrador. Al finalizar este paso habremos creado, los archivos *NombreServidor.ovpn* de configuración del servidor y los archivos *ca.crt*, *ca.key*, *dh1024.pem*, *NombreServidor.key*, *NombreServidor.crt* y *NombreServidor.csr.*

Nombre del Archivo	Es necesario para	¿Qué es?	¿Debe ser secreto?
Ca.crt	Servidor y todos los clientes	Certificado para el CA	NO
Ca.key	Solo el ordenador con llave para firmar	Llave para el CA	SI
Dh2048.pem	Servidor	Parámetros Diffie Hellman	NO
Servidor.crt	Solo servidor	Certificado para el servidor	NO
Servidor.key	Solo servidor	Llave privada para servidor	SI

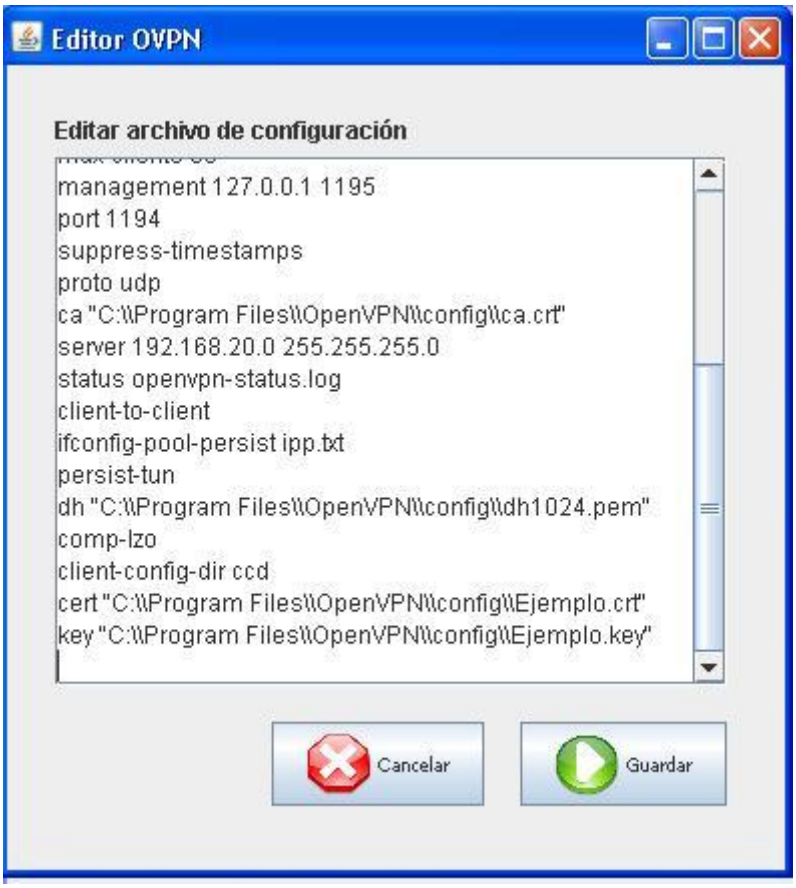
Este proceso aleatoriamente podrá durar desde unos segundos, a unos minutos.



Pantalla de edición del ovpn



Esta pantalla contiene lo valores para crear un servidor VPN por defecto, el administrador de la red, podrá editar esta configuración. Pulsando sobre el botón avanzado, se podrán añadir más opciones de configuración que no aparecen reflejadas en el panel mediante campos de texto, menús o checks. Para facilitar la configuración, se incluye un Apéndice A en esta documentación con más opciones posibles de configuración de un servidor OpenVPN.

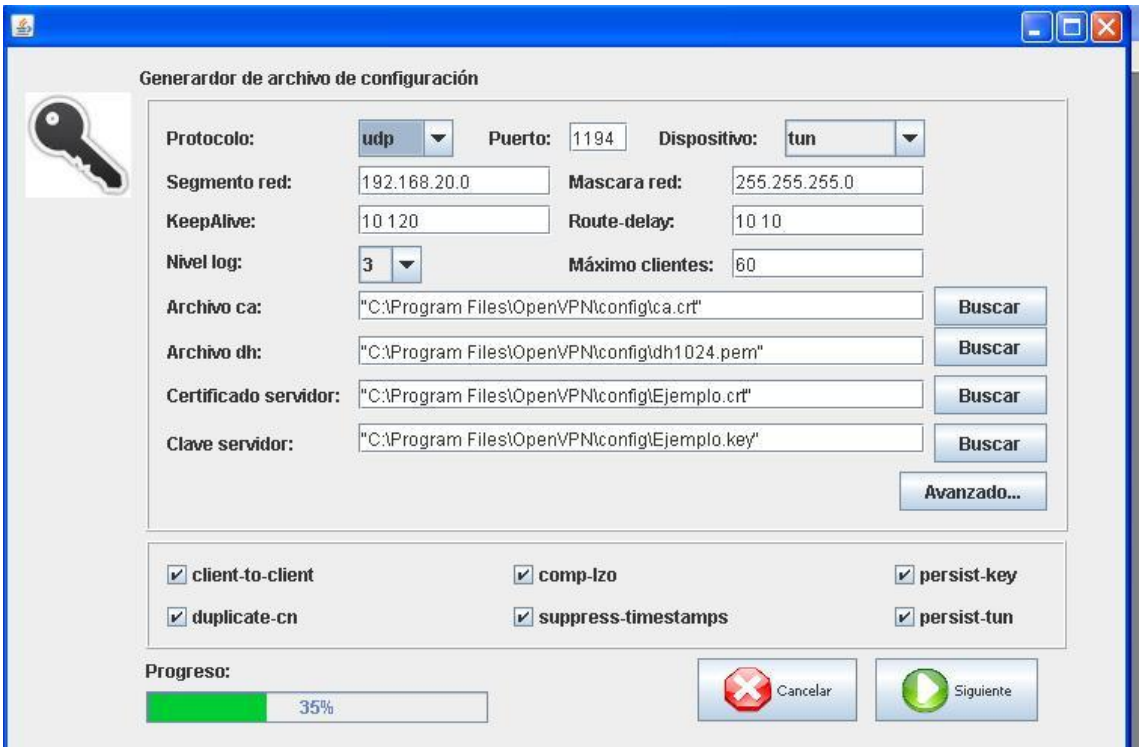


Tras pulsar en el botón siguiente de la pantalla de edición de la configuración del Servidor, se mostrará una ventana indicando el resultado de la operación.

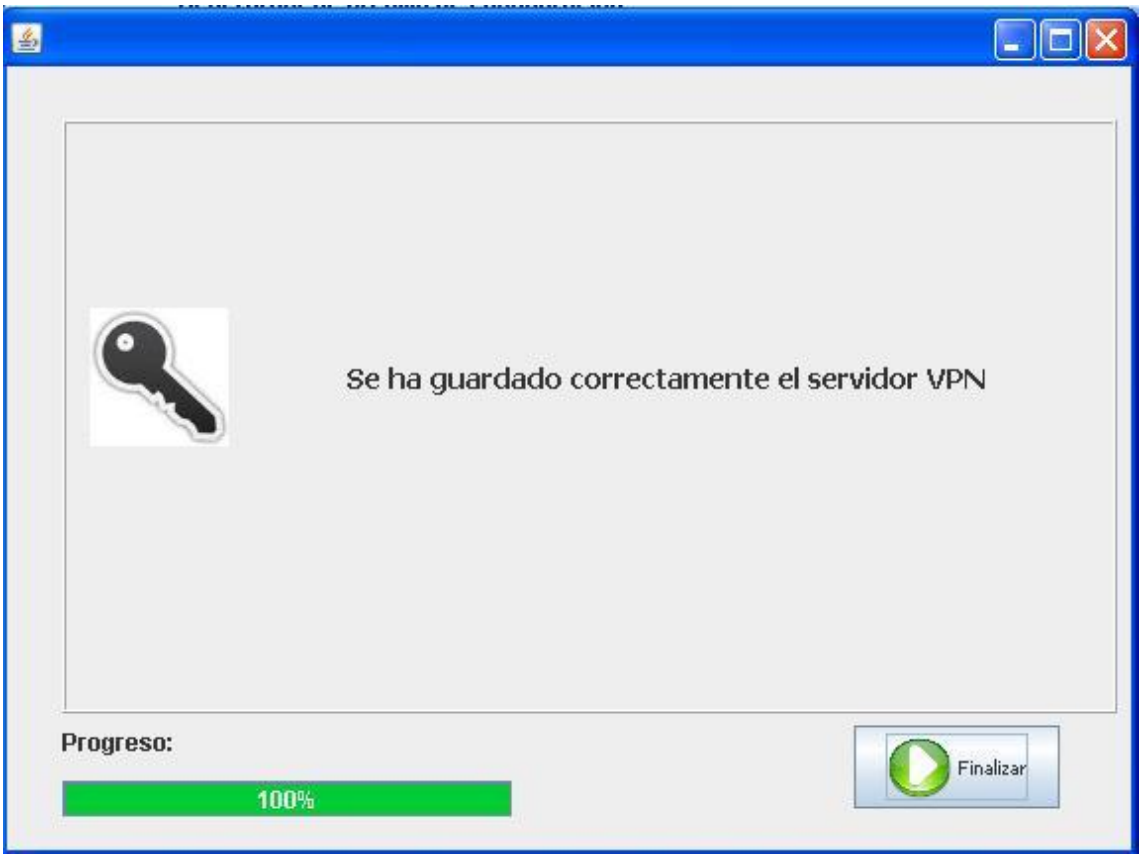
Ya tenemos configurado un servidor para poder crear una red VPN.

Editar un Servidor

Una vez creado un servidor, el botón de edición se activa. Al pulsar sobre él, se mostrará una ventana similar de edición a la mostrada en la creación del servidor. De nuevo se pueden ampliar las opciones de configuración de OpenVPN pulsando en el botón Avanzado… como se muestra en las siguientes figuras. Consultar el Apéndice A para ampliar la información de las opciones de configuración posibles para OpenVPN.



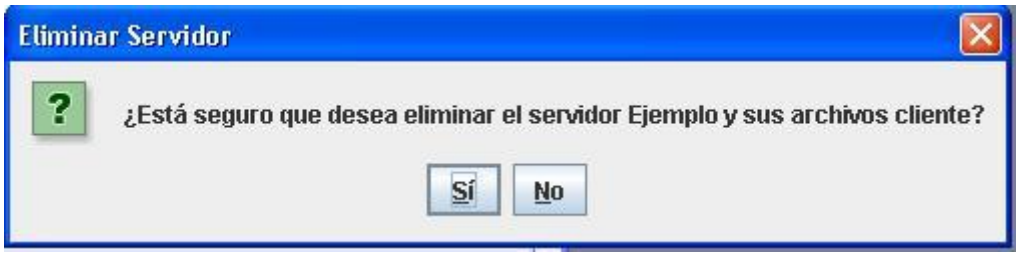
Pulsando el botón siguiente se volverá a mostrar un panel de confirmación y se almacenarán los datos en el archivo Servidor.ovpn



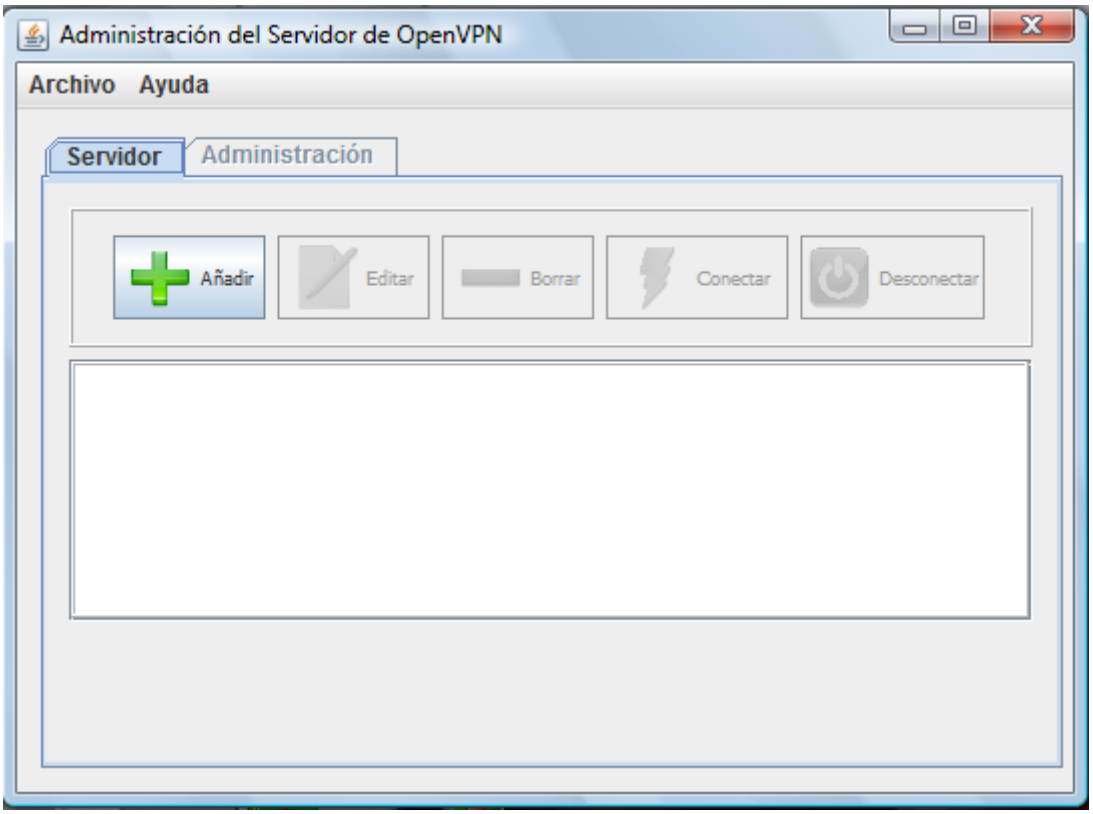
Eliminar un Servidor

Si se desea eliminar un servidor, basta con pulsar el botón Borrar y confirmar la operación.

Se eliminaran todos los archivos relacionados con el servidor.



Tras pulsar Sí, se volverá a la pantalla inicial del Servidor VPN

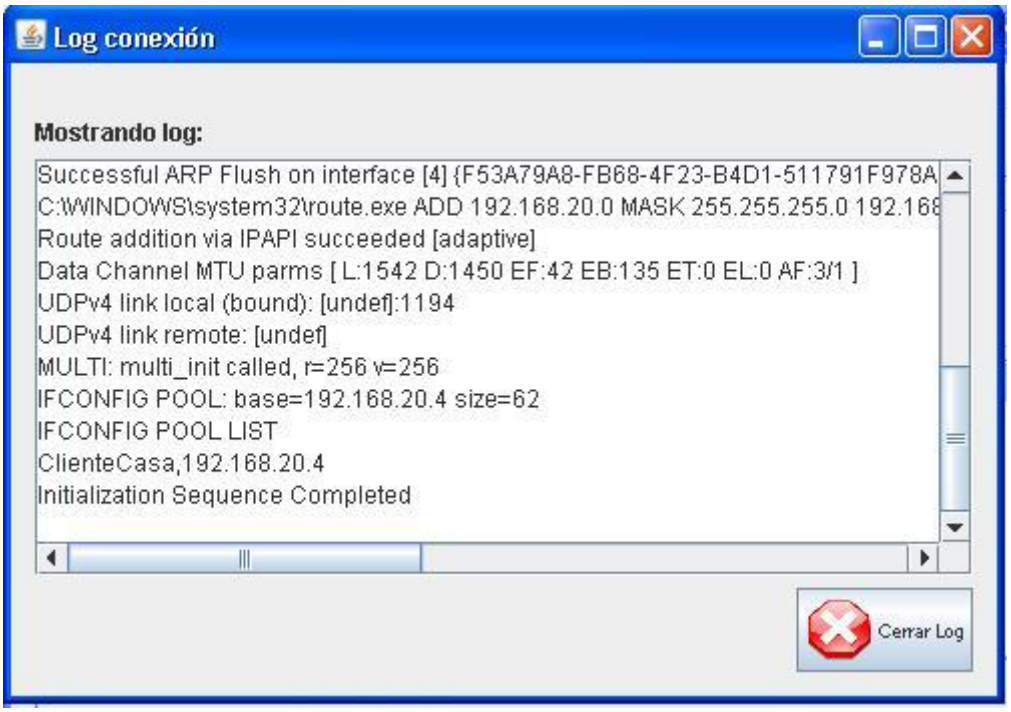


Si se pulsa No, no se eliminará ningún archivo ni cambiará el estado del servidor.

Conectar y desconectar

Si existe un servidor creado, tras pulsar el botón Conectar, se abrirá una ventana con el log arrojado por OpenVPN. Este log mostrará si la conexión se ha realizado con éxito terminando en “Initialization Sequence Completed” o si por el contrario ha habido algún error, indicará el motivo.

Se puede cerrar la ventana de log sin que esto influya en la conexión.

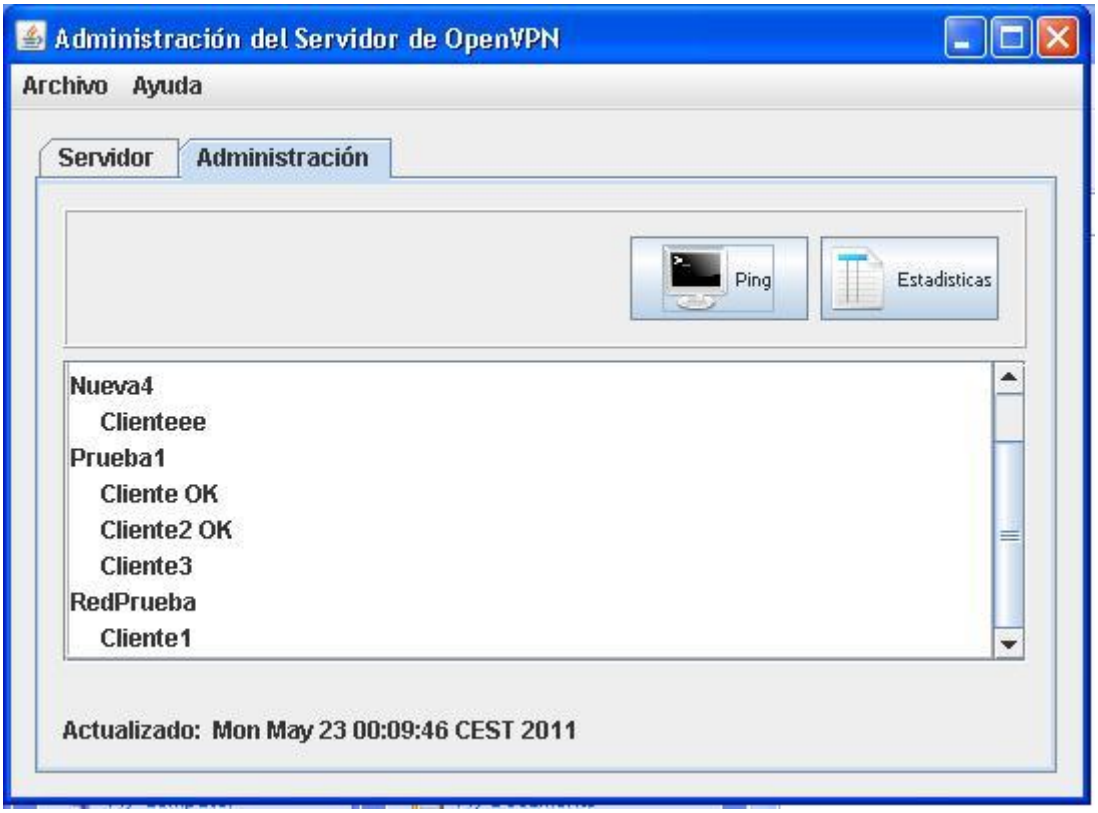


Tras finalizar la conexión, solo aparecerá el botón desconectar activado, por lo que en estos momentos y mientras siga conectado no se puede editar ni borrar el servidor

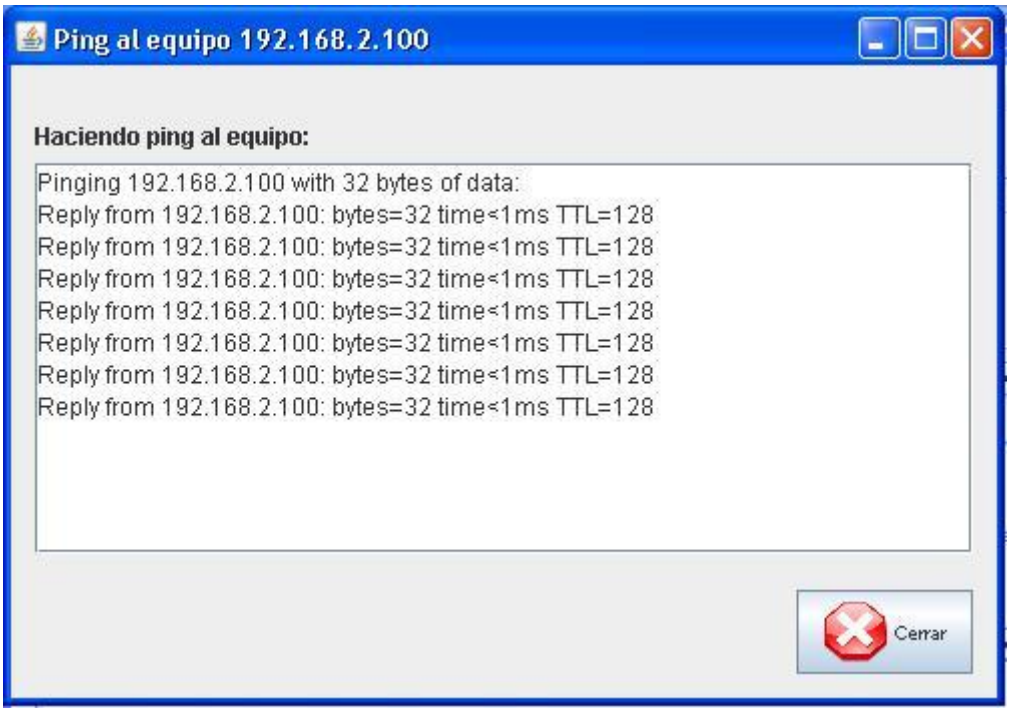
Si se desea desconectar el servidor, cuando se pulse el botón desconectar, se mostrará un mensaje indicando que se ha desconectado la red de área local. El número de conexión podrá variar dependiendo del número de adaptadores que tenga el equipo instalado, en nuestro ejemplo es el 4.

Administrar equipos

Pulsando sobre la pestaña Administración, se mostrará el estado de los clientes y de las redes a las que pertenecen. Si tras el nombre del equipo existe la palabra OK, querrá decir que el equipo se haya conectado en estos momentos.

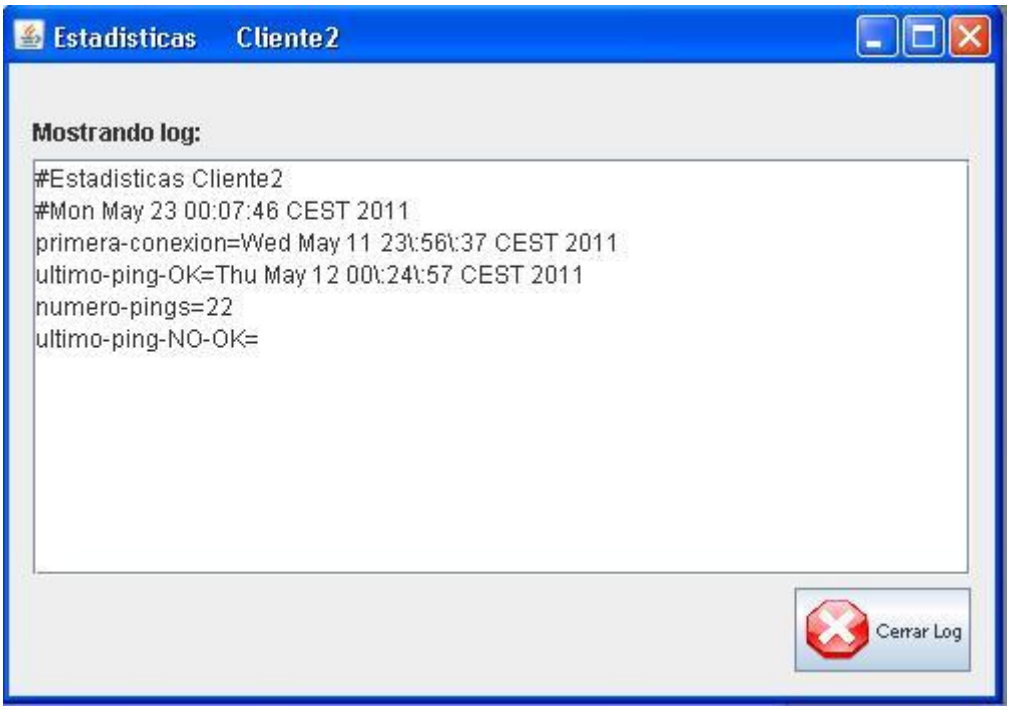


Se pueden realizar dos acciones con cada equipo cliente. Se les puede hacer ping o ver sus últimas estadísticas. Si seleccionamos un equipo y pulsamos sobre el botón Ping, se mostrará un panel en el que se le realizará ping al equipo pudiéndose visualizar su IP



Si por el contrario el equipo se encuentra desconectado, al intentar hacerle ping, se mostrará un mensaje de error

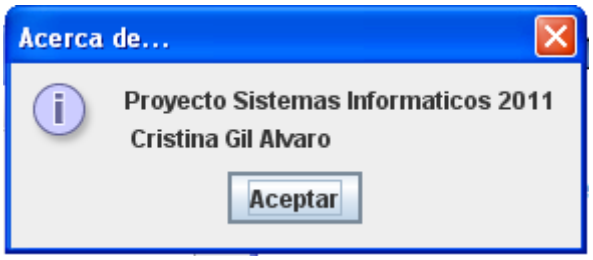
Para visualizar las últimas estadísticas, se debe seleccionar nuevamente un equipo y hacer click sobre el botón Estadísticas. Se mostrará un panel con información sobre los últimos IPs realizados, la fecha de la primera conexión, etc.



En la esquina inferior de la pestaña de Administración se muestra la fecha de la última actualización del estado de los equipos.

Ayuda

Pulsando en el menú ayuda se muestra la opción Acerca de…, que se encarga de proporcionar información sobre el proyecto y el desarrollador



Desinstalar el Servidor Gráfico OpenVPN

Si se desea hacer desaparecer del equipo el componente gráfico OpenVPN, se puede realizar haciendo doble click sobre el ejecutable Uninstall.exe proporcionado en el paquete de instalación, está aplicación llamará al desinstalador de OpenVPN y eliminará todos los archivos creados por la aplicación.

Opcionalmente se puede decidir por desinstalar también el servidor gráfico FreeSSHd, desde Panel de Control->Programas.

Si ha sido necesaria la configuración del router (equipos sin acceso directo a internet) se debería dejar tal cual estaba antes de instalar la herramienta (dejar de redirigir puertos 22 y 1194) y desvincular la cuenta de DynDNS creada al inicio de la instalación.

Por último se debería de volver a editar la variable del registro de Windows IPEnableRouter con valor a 0 localizada en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

Como paso opcional de eliminaría la carpeta InstaladorServidor, con este paso nos aseguramos que no queda rastro de la aplicación en el equipo.

Es necesario reiniciar el equipo para que los cambios surjan efecto correctamente.

6. Cliente OpenVPN

Es una aplicación gráfica, que permite de una manera sencilla e intuitiva crear un cliente para después agregarse a una o más redes VPN. A continuación se explicaran detalles técnicos sobre la implementación, así como un manual de instalación, configuración y uso de la herramienta.

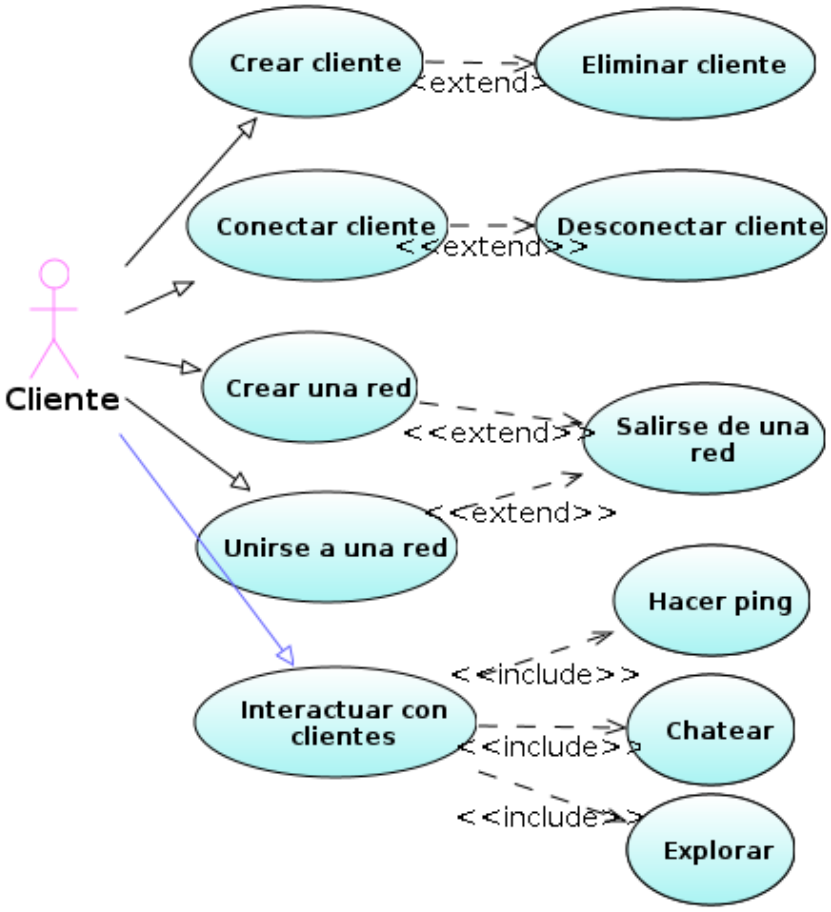
Detalles de implementación

La herramienta ha sido desarrollada mediante Java, usando la Máquina Virtual jre1.6.0_07 y usando el IDE NetBeans 7.0.

Se compone de una serie de clases de las cuales la mayoría son interfaces gráficas de Usuario para poder realizar las acciones que se han implementado (crear cliente, crear una red, unirse a una red, charlar con otros clientes, etc.)

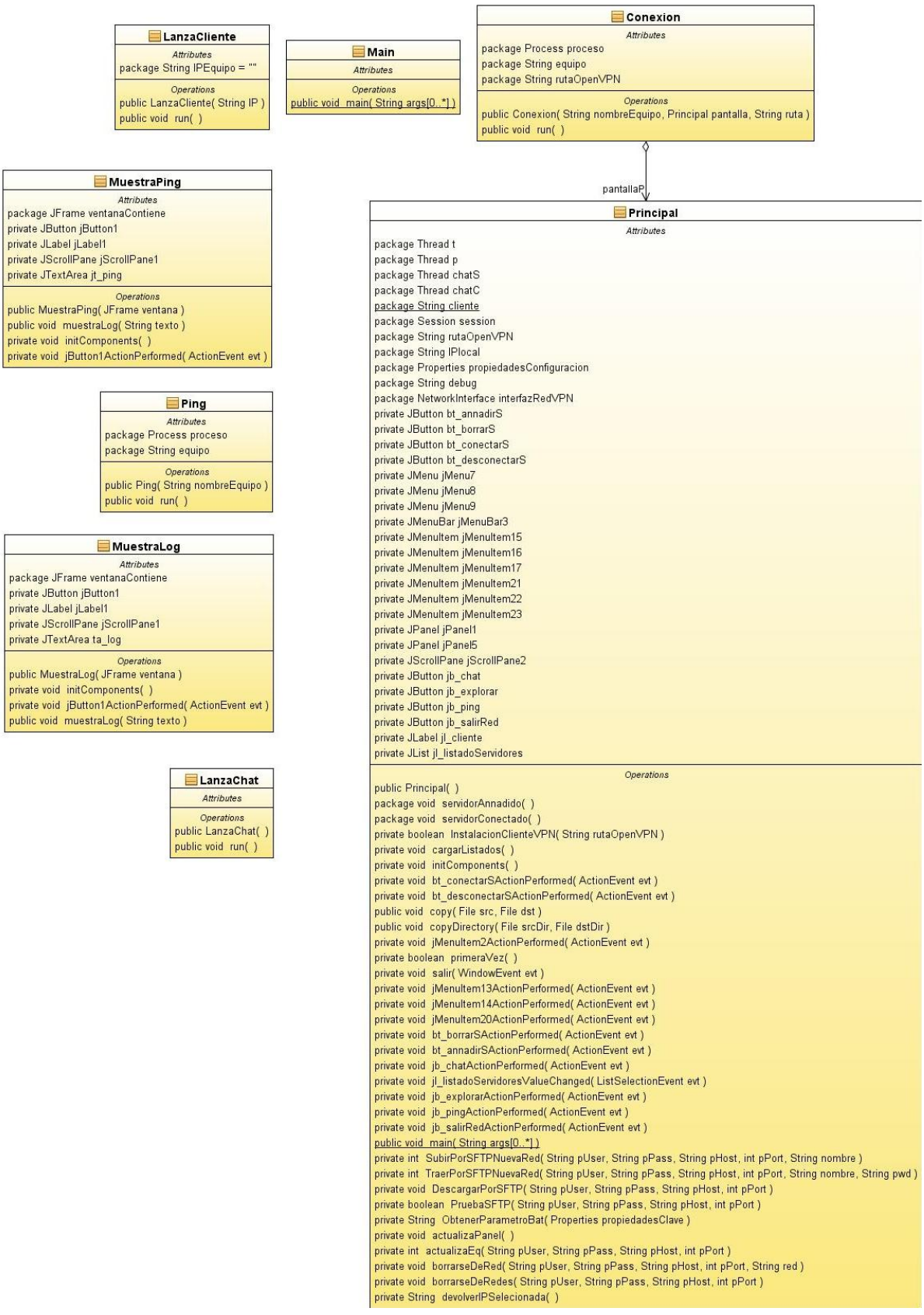
A continuación se detalla la documentación técnica del proyecto.

El diagrama de casos de uso para el Cliente Gráfico OpenVPN es como se detalla a continuación:



El usuario del sistema tiene como función principal unirse a una red VPN, pero no tiene porqué tener conocimientos sobre redes OpenVPN y de la configuración de estas. Este usuario podrá llevar a cabo distintas funciones como pueden ser crear un cliente con un determinado nombre, eliminarlo, conectarlo o desconectarlo, crear o unirse a una red, salirse de una red, hacer ping, mantener una charla o explorar los recursos de otros clientes que pertenezcan a alguna red en común y que se encuentren conectados.

El siguiente diagrama de clases muestra como se interrelacionan las distintas clases del proyecto:


LanzaCliente
Attributes
package String IPEquipo = ""
Operations
public LanzaCliente(String IP)
public void run( )
Main
Attributes
Operations
public void main(String args[0..*])
Conexion
Attributes
package Process proceso
package String equipo
package String rutaOpenVPN
Operations
public Conexion(String nombreEquipo, Principal pantalla, String ruta)
public void run( )
pantallaP
MuestraPing
Attributes
package JFrame ventanaContiene
private JButton jButton1
private JLabel jLabel1
private JScrollPane jScrollPane1
private JTextArea jt_ping
Operations
public MuestraPing(JFrame ventana)
public void muestraLog(String texto)
private void initComponents( )
private void jButton1ActionPerformed(ActionEvent evt)
Ping
Attributes
package Process proceso
package String equipo
Operations
public Ping(String nombreEquipo)
public void run( )
MuestraLog
Attributes
package JFrame ventanaContiene
private JButton jButton1
private JLabel jLabel1
private JScrollPane jScrollPane1
private JTextArea ta_log
Operations
public MuestraLog(JFrame ventana)
private void initComponents( )
private void jButton1ActionPerformed(ActionEvent evt)
public void muestraLog(String texto)
LanzaChat
Attributes
Operations
public LanzaChat( )
public void run( )
Principal
Attributes
package Thread t
package Thread p
package Thread chatS
package Thread chatC
package String cliente
package Session session
package String rutaOpenVPN
package String IPlocal
package Properties propiedadesConfiguracion
package String debug
package NetworkInterface interfazRedVPN
private JButton bt_annadirS
private JButton bt_borrarS
private JButton bt_conectarS
private JButton bt_desconectarS
private JMenu jMenu7
private JMenu jMenu8
private JMenu jMenu9
private JMenuBar jMenuBar3
private JMenuItem jMenuItem15
private JMenuItem jMenuItem16
private JMenuItem jMenuItem17
private JMenuItem jMenuItem21
private JMenuItem jMenuItem22
private JMenuItem jMenuItem23
private JPanel jPanel1
private JPanel jPanel5
private JScrollPane jScrollPane2
private JButton jb_chat
private JButton jb_explorar
private JButton jb_ping
private JButton jb_salirRed
private JLabel jl_cliente
private JList jl_listadoServidores
Operations
public Principal( )
package void servidorAnnadido( )
package void servidorConectado( )
private boolean InstalacionClienteVPN(String rutaOpenVPN)
private void cargarListados( )
private void initComponents( )
private void bt_conectarSActionPerformed(ActionEvent evt)
private void bt_desconectarSActionPerformed(ActionEvent evt)
public void copy(File src, File dst)
public void copyDirectory(File srcDir, File dstDir)
private void jMenuItem2ActionPerformed(ActionEvent evt)
private boolean primeraVez( )
private void salir(WindowEvent evt)
private void jMenuItem13ActionPerformed(ActionEvent evt)
private void jMenuItem14ActionPerformed(ActionEvent evt)
private void jMenuItem20ActionPerformed(ActionEvent evt)
private void bt_borrarSActionPerformed(ActionEvent evt)
private void bt_annadirSActionPerformed(ActionEvent evt)
private void jb_chatActionPerformed(ActionEvent evt)
private void jl_listadoServidoresValueChanged(ListSelectionEvent evt)
private void jb_explorarActionPerformed(ActionEvent evt)
private void jb_pingActionPerformed(ActionEvent evt)
private void jb_salirRedActionPerformed(ActionEvent evt)
public void main(String args[0..*])
private int SubirPorSFTPNuevaRed(String pUser, String pPass, String pHost, int pPort, String nombre)
private int TraerPorSFTPNuevaRed(String pUser, String pPass, String pHost, int pPort, String nombre, String pwd)
private void DescargarPorSFTP(String pUser, String pPass, String pHost, int pPort)
private boolean PruebaSFTP(String pUser, String pPass, String pHost, int pPort)
private String ObtenerParametroBat(Properties propiedadesClave)
private void actualizaPanel( )
private int actualizaEq(String pUser, String pPass, String pHost, int pPort)
private void borrarseDeRed(String pUser, String pPass, String pHost, int pPort, String red)
private void borrarseDeRedes(String pUser, String pPass, String pHost, int pPort)
private String devolverIPSelecionada( )

La clase *Principal.java*, como su nombre indica es la clase más importante de la aplicación. Es el formulario principal de la aplicación, en el que se puede crear, conectar y desconectar a un cliente. Además permite crear o unirse a redes, así como distintas acciones con otros clientes que pertenezcan a la red (chat, ping y explorar)

MuestraLog.java, *MuestraPing.java* son paneles gráficos que realizan distintas funcionalidades como sus nombres indican.

El resto de clases proporcionan otras funcionalidades al proyecto como son lanzar el ejecutable de OpenVPN para realizar la conexión, hacer ping a los clientes en diferentes hilos, etc.

El paquete chat proporciona dos clases *Cliente.java* y *Servidor.java* que permitirán que el cliente pueda comunicarse con otros clientes de una de sus redes, tomando la iniciativa (será el cliente de la conversación) o esperando que alguien la tome (en este caso será el servidor).

Instalación y configuración

Requerimientos mínimos de hardware y software

Windows XP o Linux Suse 11

Conexión a Internet

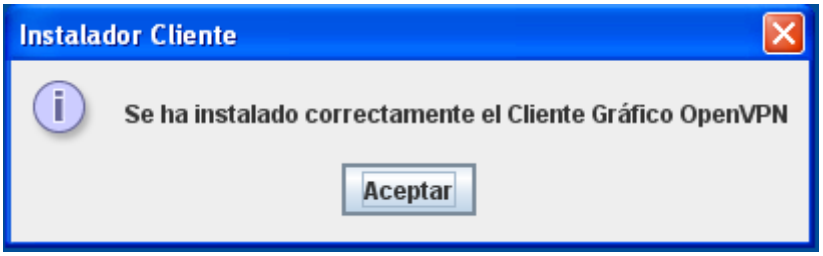
Pasos de instalación

Para poder usar el cliente gráfico de OpenVPN hay que instalar la aplicación gráfica del cliente, que ésta a su vez realizará la instalación desatendida de OpenVPN.

Al hacer doble click en el ejecutable ClienteOpenVPN.exe proporcionado en el pack de instalación InstaladorCliente, se mostrará un mensaje como sigue

Al pulsar el botón aceptar, tras unos segundos aparecerá una mensaje preguntando sobre si se desea instalar un Adaptador de Red Virtual

Se deberá pulsar continuar ya que de no ser así el cliente no funcionará correctamente. Tras unos segundos se volverá a mostrar un mensaje informando acerca del resultado de la instalación.



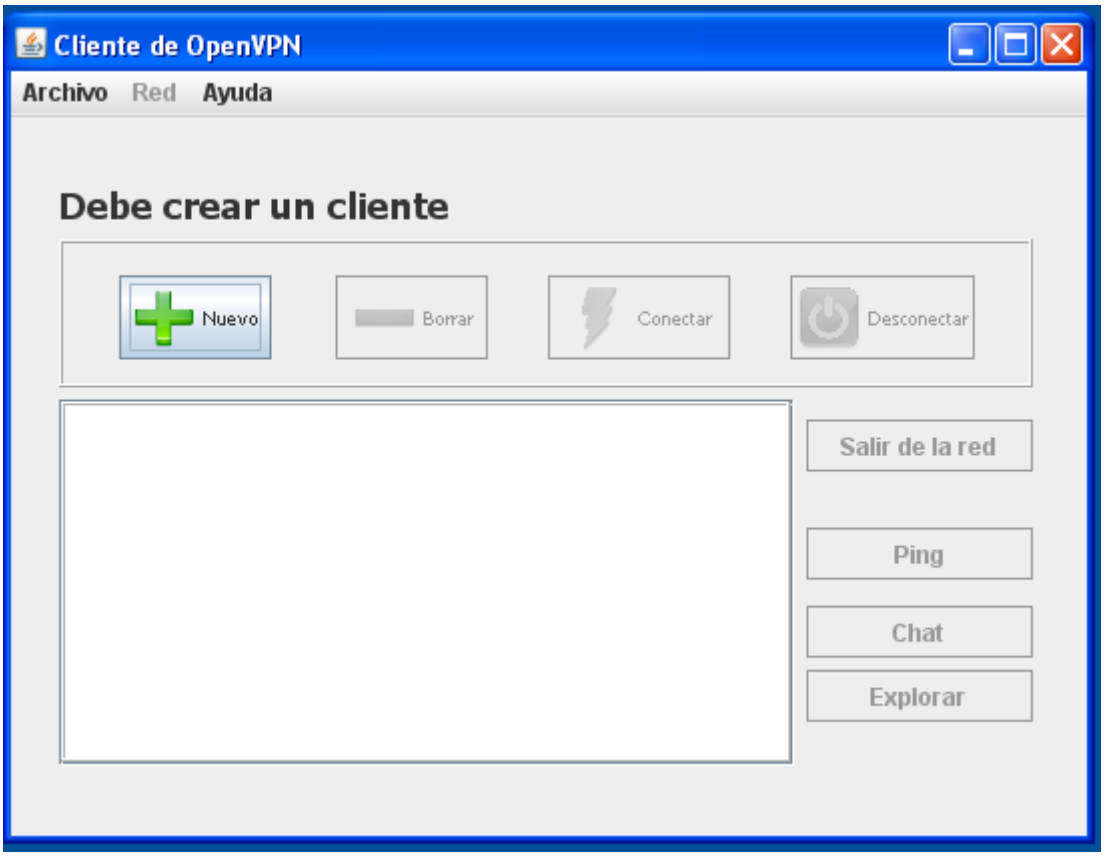
Si por el contrario ha existido algún problema durante la instalación se le informará al usuario con un mensaje similar indicando lo ocurrido.

También puede ocurrir que el usuario lance el instalador teniendo previamente instalada la aplicación OpenVPN, en tal caso el programa saltará el paso de la instalación de esta aplicación.

En este punto ya se puede hacer uso de la aplicación gráfica para el cliente OpenVPN según se ilustra en el siguiente manual

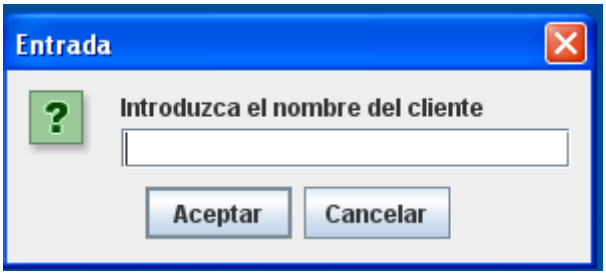
Manual de USO

Tras finalizar la instalación se abrirá una pantalla como la siguiente, el primer paso entonces será crear un Cliente



Crear un cliente

Si se pulsa sobre el botón añadir, se iniciará un proceso automático que llevará a crear un cliente OpenVPN. Solo se podrá crear un cliente en un equipo, por lo que cuando finalice el proceso de crear un cliente, será necesario eliminar este para crear otro

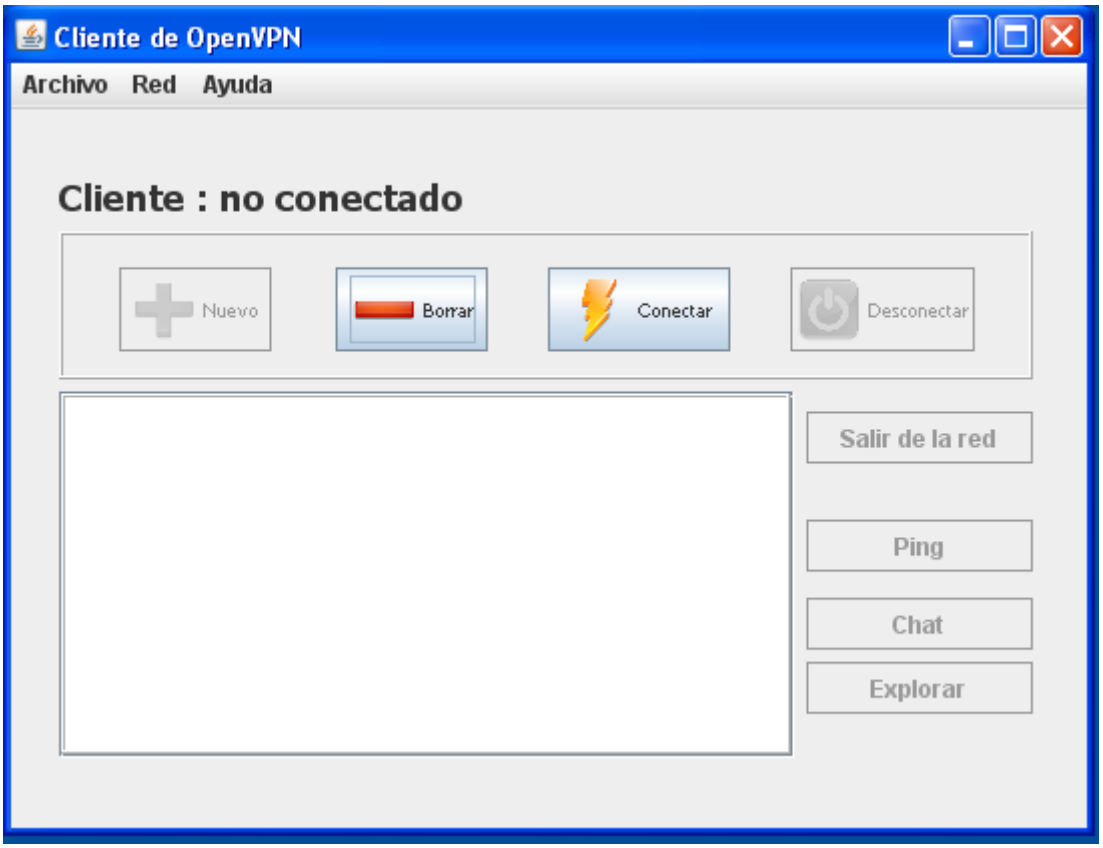


Tras introducir un nombre válido, se hará una comprobación de que este no exista ya en el servidor, para evitar clientes duplicados. Este proceso podrá durar unos segundos. Al finalizar habremos creado, los archivos *NombreCliente.ovpn(o NombreCliente.conf* en el caso de Linux) de configuración del cliente y los archivos *Cliente.crt*, *Cliente.key*.

Cliente1.crt	Solo cliente	Certificado para el cliente1	NO
Cliente1.key	Solo cliente	Llave para el cliente2	SI

El archivo *NombreCliente.ovpn(o NombreCliente.conf)* ubicado en la carpeta config del directorio de instalación de OpenVPN contiene lo valores para crear un cliente VPN por defecto. Si se trata de un usuario avanzado, podrá editar esta configuración. Para ello se incluye un Apéndice A en esta documentación con más opciones posibles de configuración de un cliente OpenVPN. Si no se dispone de conocimiento en el área de las redes VPN, se recomienda dejar el archivo como está ya que contiene la configuración necesaria para poder conectarse a la red correctamente.

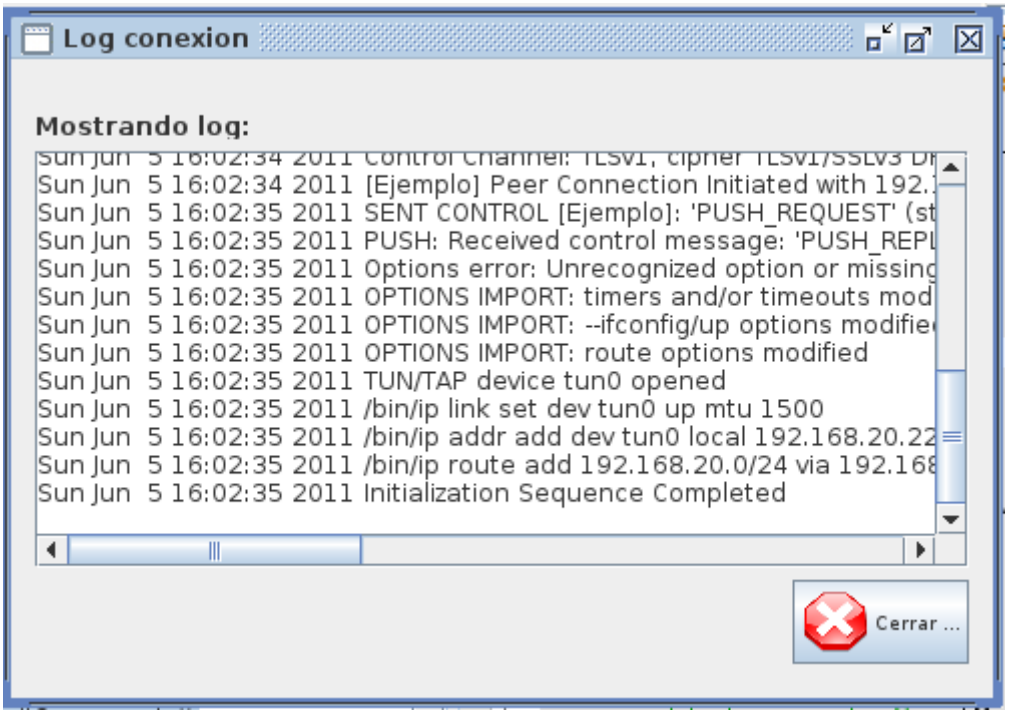
Ya está configurado un cliente para poder realizar distintas acciones que se detallaran a continuación



Conectar y desconectar

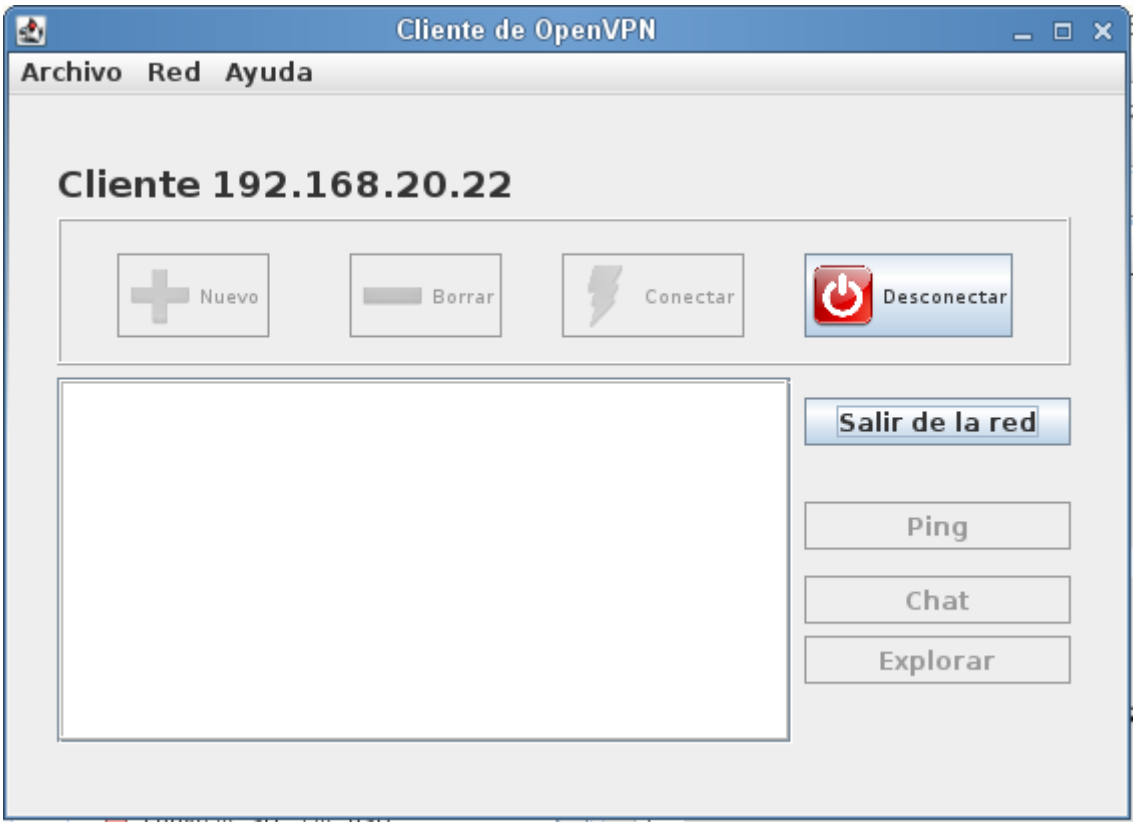
Si existe un cliente creado, tras pulsar el botón Conectar, se abrirá una ventana con el log arrojado por OpenVPN. Este log mostrará si la conexión se ha realizado con éxito o si por el contrario ha habido algún error, indicará el motivo.

Se puede cerrar la ventana de log sin que esto influya en la conexión.



Tras finalizar la conexión, solo aparecerá el botón desconectar activado, por lo que en estos momentos y mientras siga el cliente conectado no se puede borrar el cliente

En la parte superior del panel aparece el nombre del cliente y la IP que ha sido asignada por el servidor.

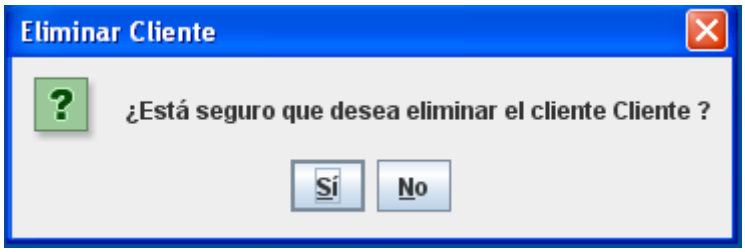


Si se desea desconectar el cliente, cuando se pulse el botón desconectar, se mostrará un mensaje indicando que se ha desconectado la red de área local. El número de conexión podrá variar dependiendo del número de adaptadores que tenga el equipo instalado, en nuestro ejemplo es el 4.

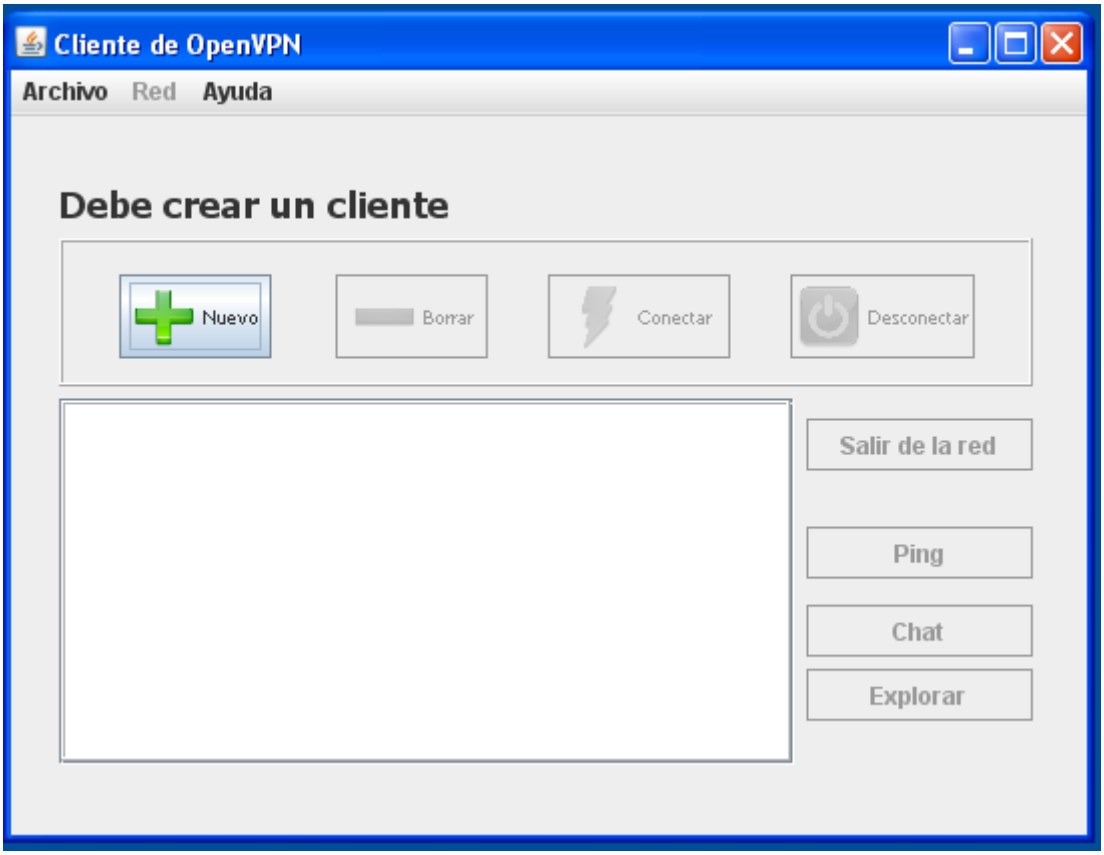
Eliminar un Cliente

Si se desea eliminar un cliente, basta con pulsar el botón Borrar y confirmar la operación.

Se eliminaran todos los archivos relacionados con el cliente.



Tras pulsar Sí, se volverá a la pantalla inicial del Cliente OpenVPN

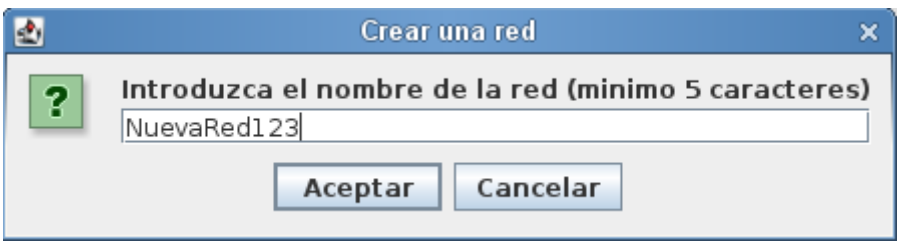


Si se pulsa No, no se eliminará ningún archivo ni cambiará el estado del cliente.

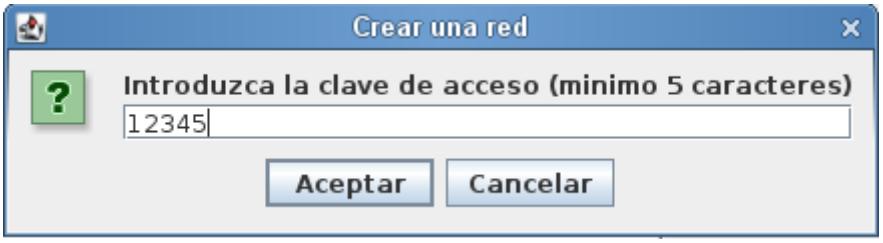
Crear una red

Un usuario puede crear una red con un determinado nombre y asignarle una contraseña que solo proporcionará a los clientes con los que quiera compartir la red.

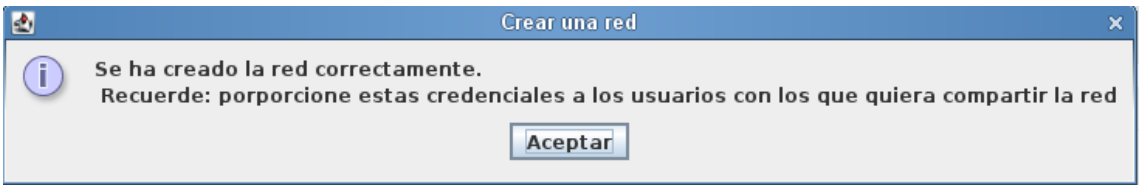
Para ello deberá de pulsar sobre el menú Red y seleccionar la opción Crear una red…



Tras introducir un nombre de red que sea válido y que aún no exista, se pedirá que introduzca una contraseña de al menos 5 caracteres.

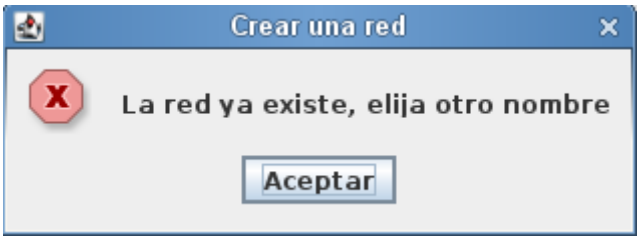


Si todo ha ido bien se mostrará el mensaje:



Se creará una red con ese nombre y se mostrará en el panel inferior que ya pertenecemos a esta red.

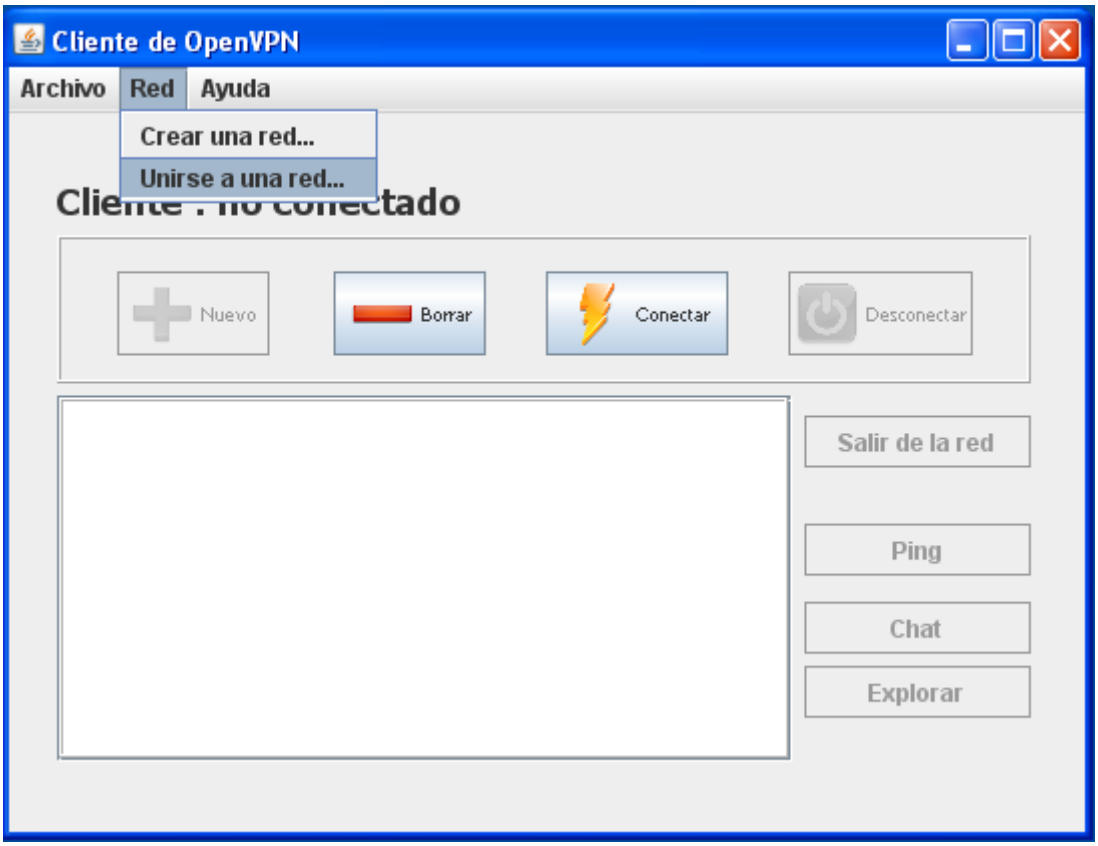
En otro caso se mostrará el mensaje de error que corresponda



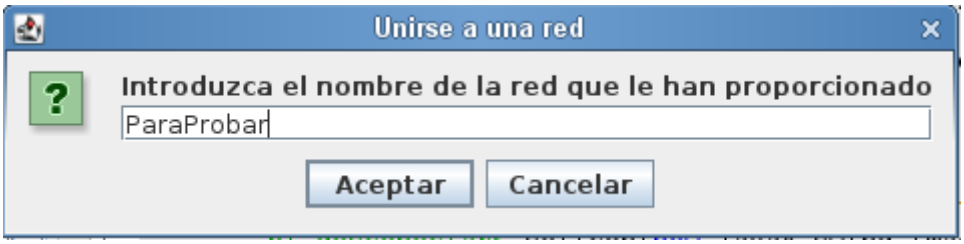
Si queremos que otros clientes formen parte de nuestra red, debemos proporcionales estos datos para que puedan unirse a nuestra red de la manera que se explica en el siguiente punto.

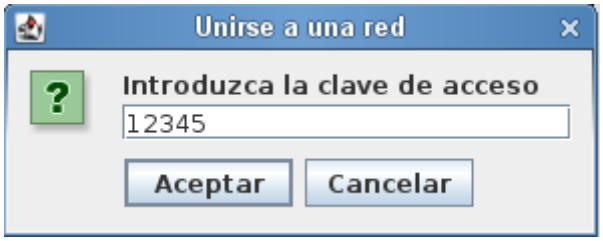
Unirse a una red

Si disponemos de unas credenciales válidas para acceder a una red VPN creada previamente por otro usuario, podremos unirnos a la red. Para ello se pulsará en el menú Red y después en la opción Unirse a una Red

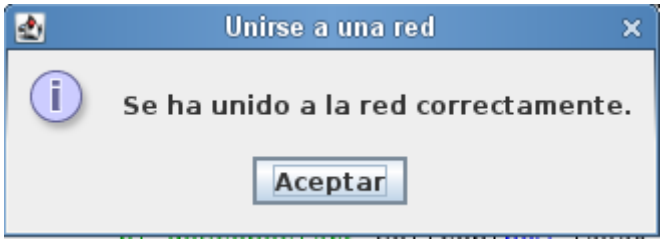


Se nos pedirá en primer lugar el nombre de la red a la que queremos conectarnos y en segundo lugar la contraseña que nos han proporcionado

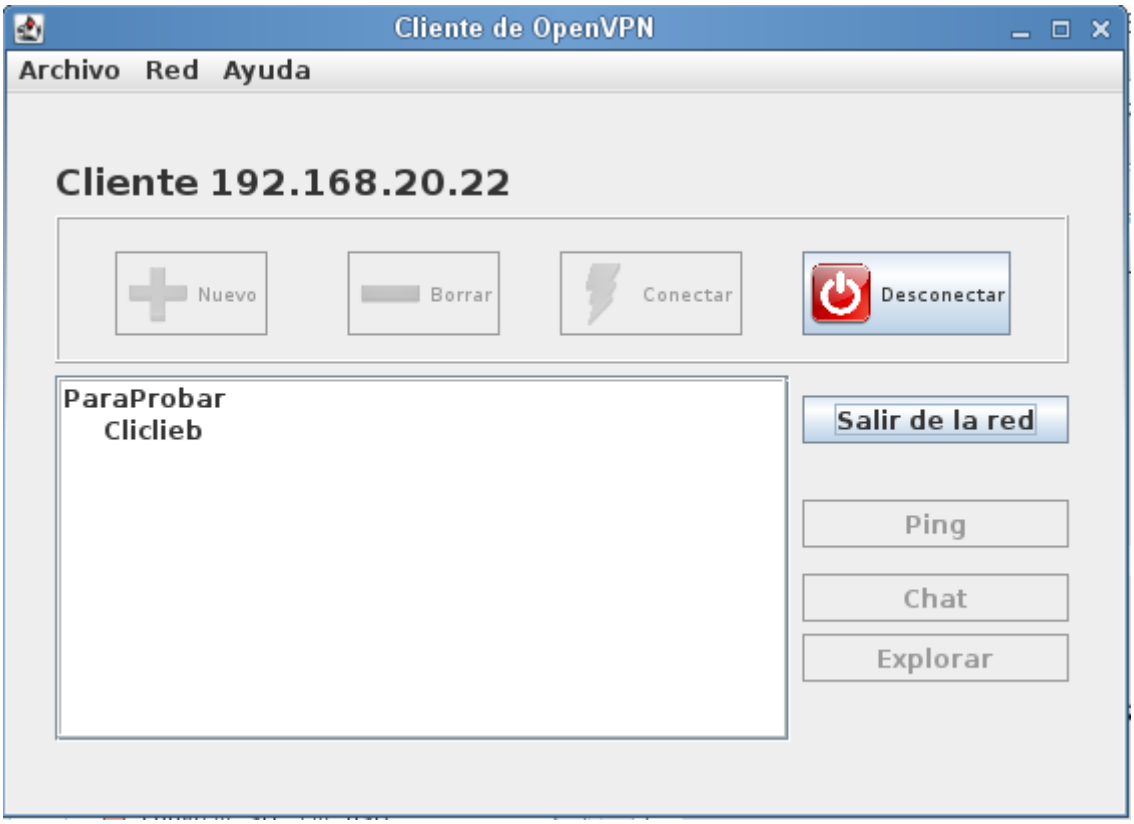




Si los datos introducidos son correctos, se mostrará un mensaje indicando que nos hemos unido correctamente a la red.



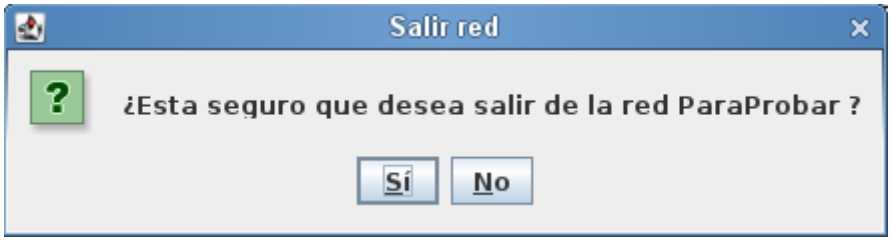
Se mostrará en el panel inferior que ya pertenecemos a la red, junto con un listado de los usuarios que ya pertenece a ella, mostrando al final de cada nombre OK, si en estos momentos se encuentran conectados.



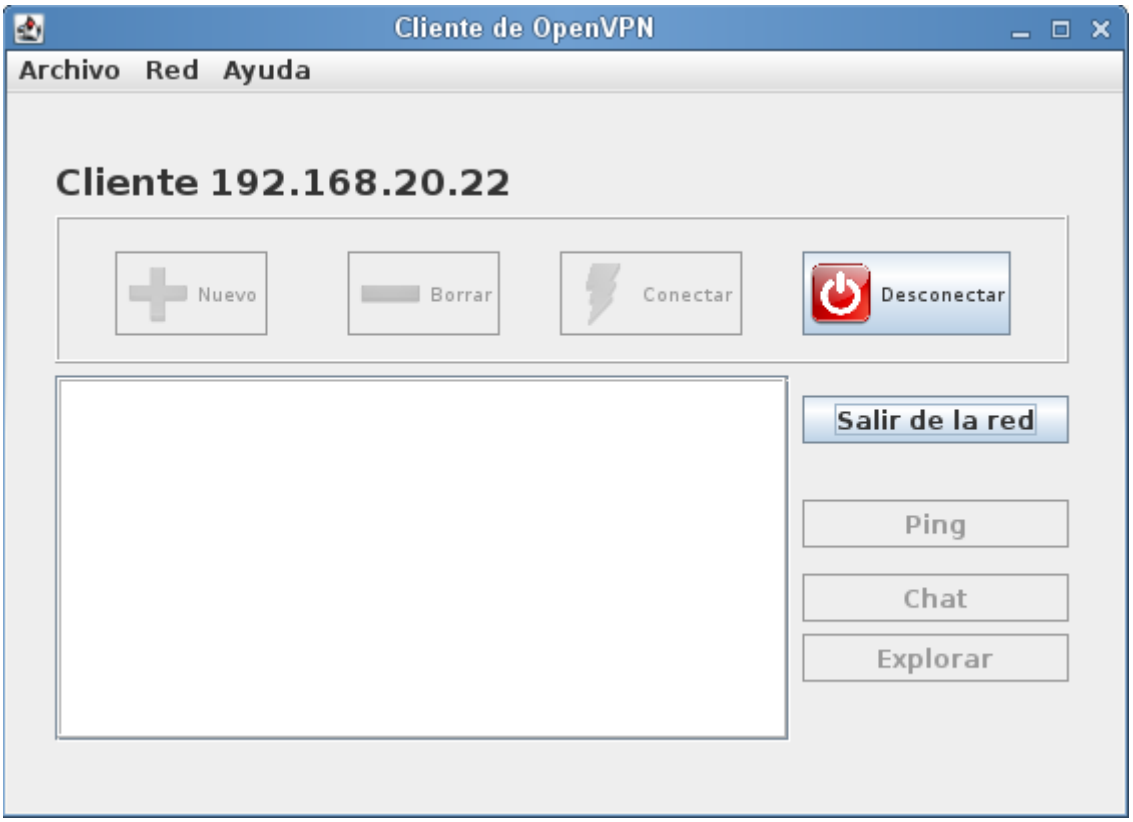
Se mostrará un mensaje de error en caso contrario

Salirse de una red

Si se desea dejar de pertenecer a una red de usuarios, solo habrá que seleccionarla y pulsar el botón situado a la derecha Salir de la Red



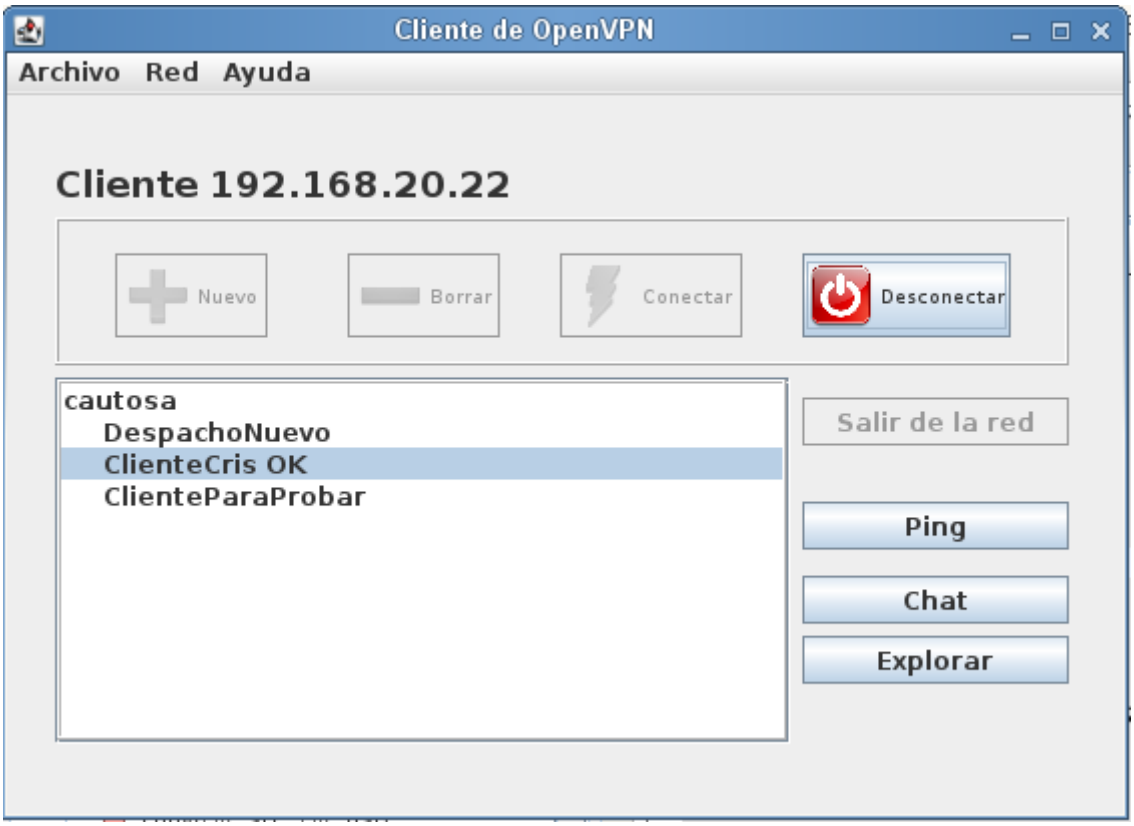
Tras la confirmación desaparecerá el nombre de la red de nuestro panel de redes, junto con los usuarios que pertenecían a la red.



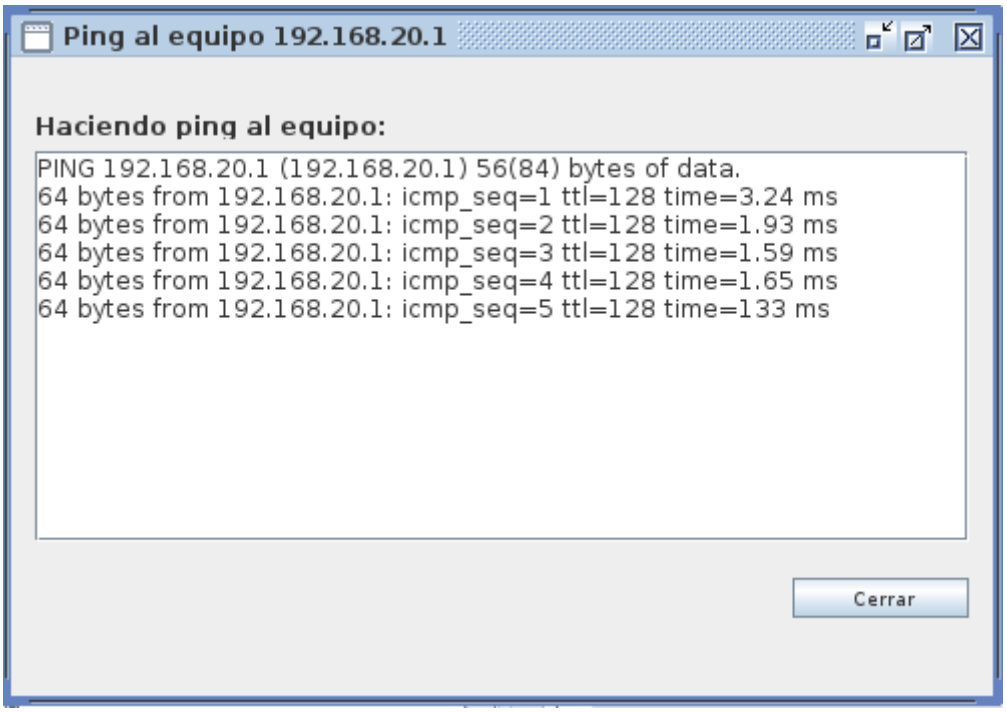
Si deseamos volver a conectarnos a la misma red, habría que hacerlo como se especifica en el punto Unirse a una Red volviendo a proporcionar las credenciales.

Hacer Ping a un cliente de nuestra red

Cuando un cliente se encuentra conectado se puede interactuar con otros clientes que pertenezcan a alguna de las redes a las que estamos conectados. Para hacer ping a un cliente que esté conectado a la red en este momento (aparece la palabra OK al final de su nombre) se debe seleccionar el cliente del panel, y pulsar el botón Ping

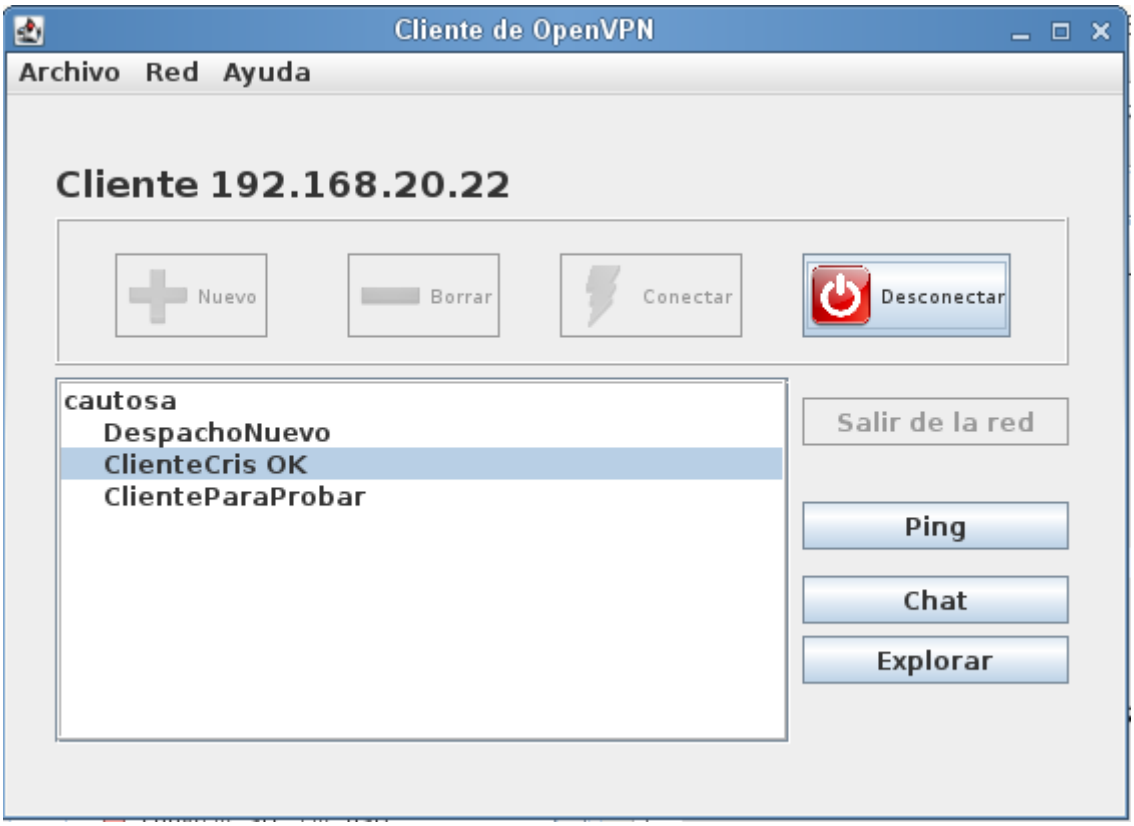


En unos segundos aparecerá una ventana en la que se mostrará su IP y el resultado del ping, paquetes recibidos, enviados, tiempo, etc. El comando usado es ping –t que nos permite hacer ping indefinidamente a un equipo hasta que se cierre la ventana.

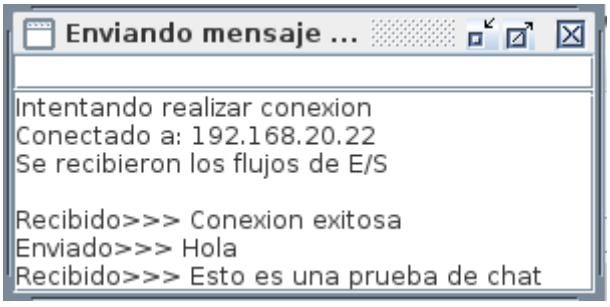


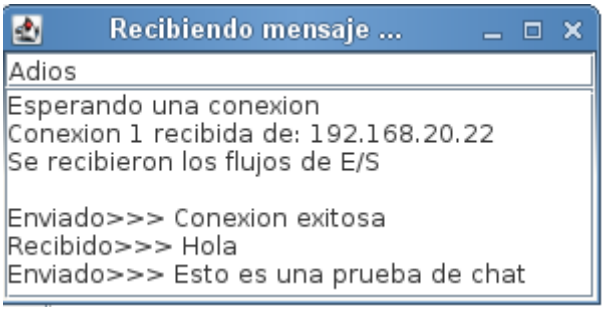
Chatear con un cliente de nuestra red

Cuando un cliente se encuentra conectado se puede interactuar con otros clientes que pertenezcan a alguna de las redes a las que estamos conectados. Para chatear con un cliente que esté conectado a la red en este momento (aparece la palabra OK al final de su nombre) se debe seleccionar el cliente del panel, y pulsar el botón Chat

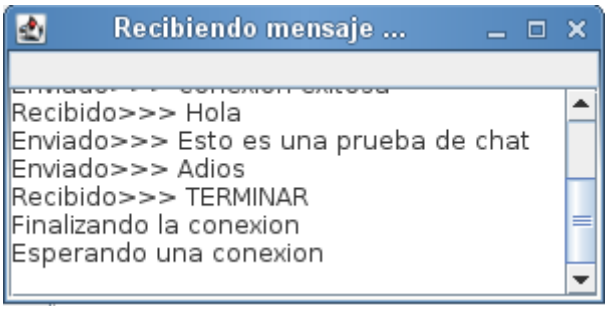


En estos momentos se abrirá un panel en los dos clientes que van a intervenir en la conversación que permitirá intercambiar mensajes.





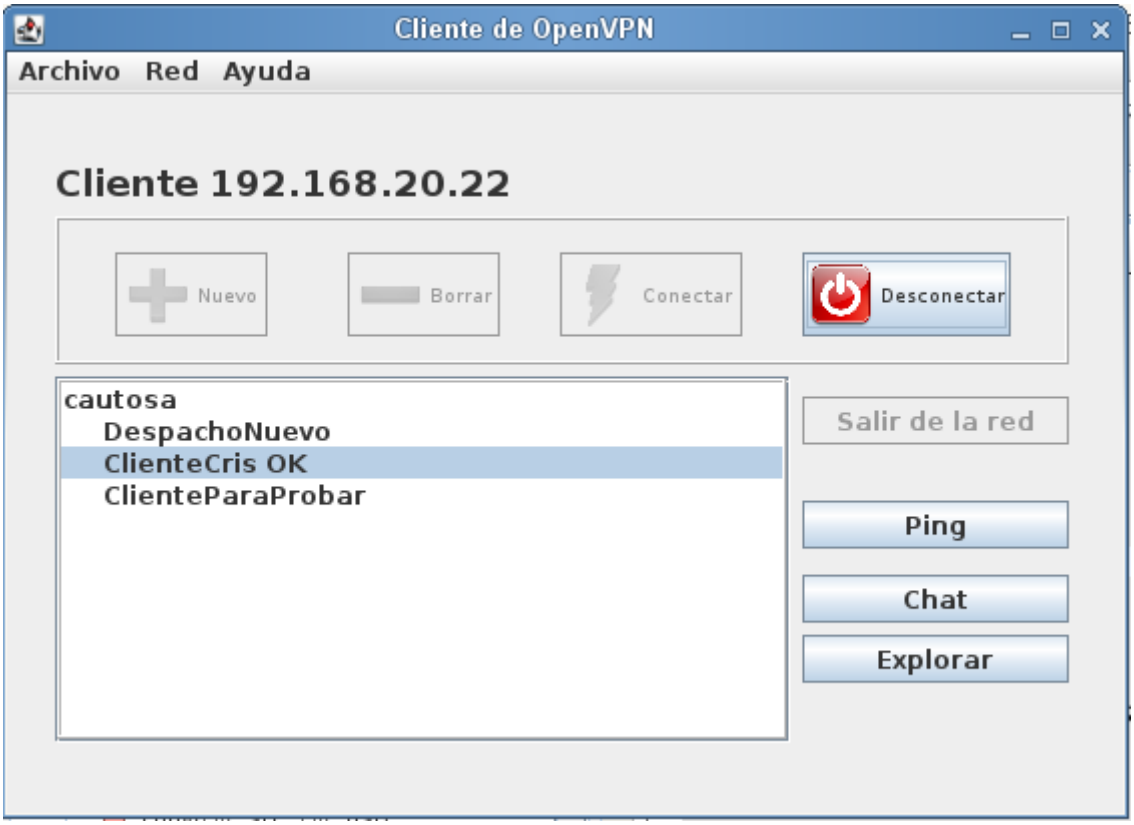
Cuando uno de los dos clientes decida terminar la conversación y cierre el panel de chat, al otro el panel se le desactivará y se le mostrará el mensaje TERMINAR.



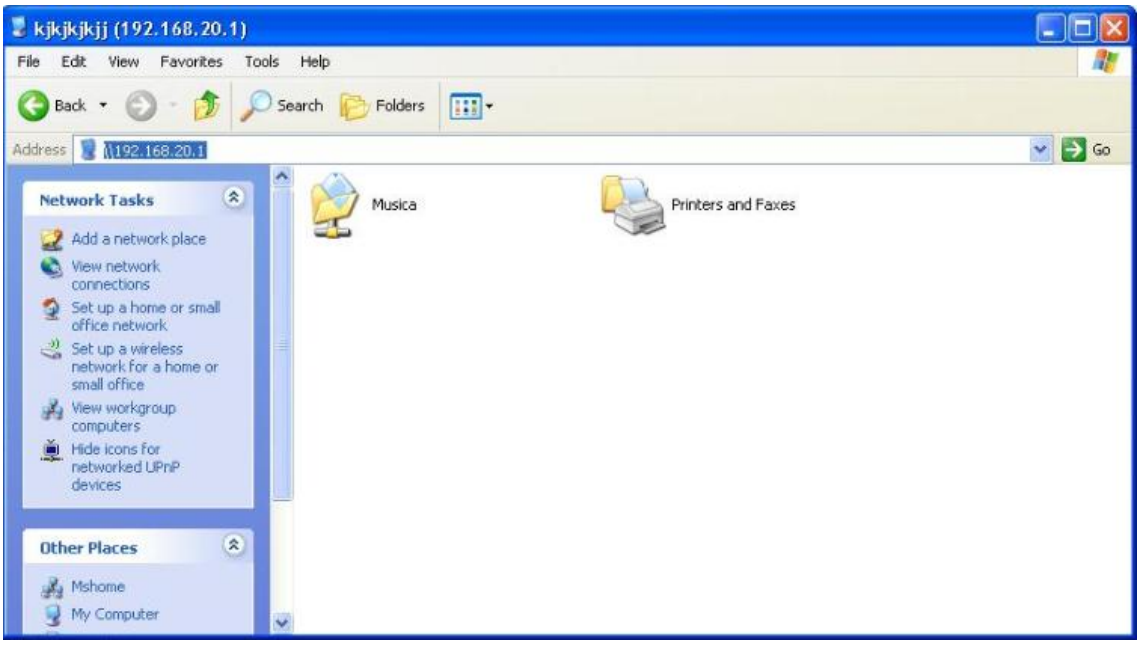
Si se desea volver a conversar con el mismo cliente se tendrá que volver a seleccionar en el panel de la aplicación y volver a pulsar el botón de Chat

Explorar recursos de un cliente de nuestra red

Cuando un cliente se encuentra conectado se puede interactuar con otros clientes que pertenezcan a alguna de las redes a las que estamos conectados. Para explorar los recursos compartidos de un cliente que esté conectado a la red en este momento (aparece la palabra OK al final de su nombre) se debe seleccionar el cliente del panel, y pulsar el botón Explorar



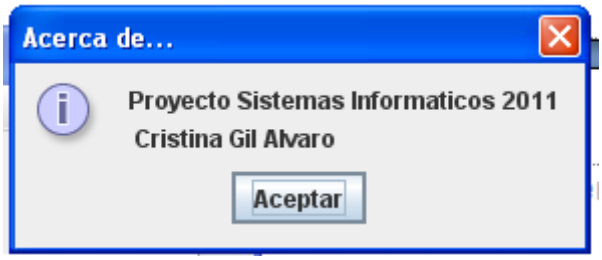
Se abrirá una ventana en la que se mostrarán sus recursos compartidos



Podremos navegar, editar, borrar, copiar archivos, etc. Siempre y cuando el cliente nos haya asignado permisos para realizar estas acciones.

Ayuda

Pulsando en el menú ayuda se muestra la opción Acerca de…, que se encarga de proporcionar información sobre el proyecto y el desarrollador



Desinstalar el Cliente Gráfico OpenVPN

Si se desea hacer desaparecer del equipo el componente gráfico OpenVPN, se puede realizar haciendo doble click sobre el ejecutable Uninstall.exe proporcionado en el paquete de instalación, está aplicación llamará al desinstalador de OpenVPN y eliminará todos los archivos creados por la aplicación

Como paso opcional de eliminaría la carpeta InstaladorCliente, con este paso nos aseguramos que no queda rastro de la aplicación en el equipo.

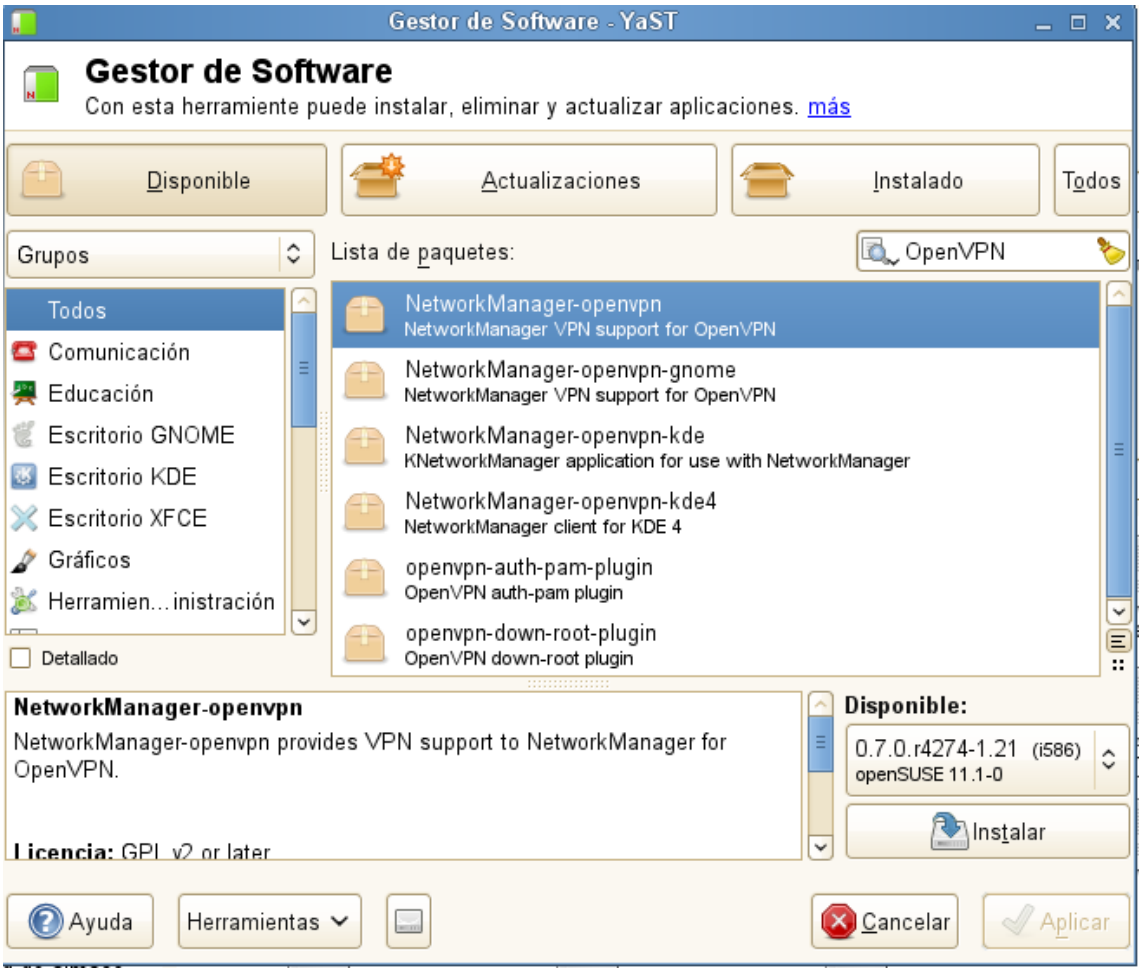
Es necesario reiniciar el equipo para que los cambios surjan efecto correctamente

Notas para clientes Linux

Para poder lanzar la aplicación en el sistema operativo Linux Suse 11, hay que realizar unos pasos previos que requieren la intervención del usuario administrador del sistema:

1. Instalar la aplicación OpenVPN

Debido a que para instalar OpenVPN es necesario instalar otros paquetes previos, se usará la herramienta para instalar software que proporciona Suse 11 que instalará en un paso todo lo necesario para poder usar OpenVPN. Se deberá pulsar el botón Equipo y seleccionar la opción Instalar Software, tras introducir la contraseña de administrador, se abrirá una pantalla como la que sigue.



Se deberá de escribir en el campo buscar OpenVPN y automáticamente nos mostrará las opciones disponibles. Si seleccionamos la primera, se habilitará el botón Instalar, que llevará a cabo la instalación completa del software.

2. Asignar permisos en carpetas

La aplicación puede ser lanzada por un usuario distinto al administrador, como se realizaran intercambio de archivos entre cliente y servidor el usuario deberá tener permisos en las carpetas de instalación de OpenVPN. Habrá que asignar permisos totales a varias carpetas. Abriendo un terminal de consola, con el comando "chmod –R 777" se asignaran permisos a las carpetas y a los archivos que estas contienen de lectura, escritura y ejecución:

- usr/share/openvpn
- usr/sbin/openvpn

Por último habría que editar el archivo /etc/sudoers para no sea necesario que se solicite contraseña a la hora de lanzar la aplicación OpenVPN, ya que un usuario común no tiene permisos para montar la interfaz de red tun.

Habrá que buscar la línea que se refiere a los privilegios del usuario administrador y sustituirla por

```
root    ALL=(ALL) NOPASSWD: ALL
```

3. Configuración del cortafuegos de Linux

Cuando usamos una VPN se recomienda configurar nuestro firewall. Se pueden usar las reglas de iptables o hacerlo gráficamente mediante la aplicación a la que se llega pulsando el botón Equipo, seleccionando la aplicación YaST2; tras introducir la contraseña seleccionar en Seguridad y Usuarios la opción cortafuegos. Para configurar el cortafuegos mediante reglas iptables, se deberá abrir un terminal y escribir las siguientes reglas:

[root@test ~]# iptables -A INPUT -i ppp0 -p udp --dport 1194 -j ACCEPT

[root@test ~]# iptables -A OUTPUT -0 ppp0 -p udp --sport 1194 -j ACCEPT

En este caso la interfaz de escucha del servicio es ppp0 pero también puede ser eth0. Permitimos la conexión desde cualquier equipo por la interfaz tun.

[root@test ~]# iptables -A INPUT -i tun+ -j ACCEPT

[root@test ~]# iptables -A OUTPUT -o tun+ -j ACCEPT

Permitimos que los equipos de las otras redes accedan a nuestra red.

[root@test ~]# iptables -A FORWARD -i tun+ -j ACCEPT

[root@test ~]# iptables -A FORWARD -o tun+ -j ACCEPT

Generamos el archivo de reglas del firewall.

[root@test ~]# iptables-save > iptables

Movemos el archivo generado a /etc/sysconfig

[root@test ~]# mv iptables /etc/sysconfig

Reiniciamos el servicio de firewall.

[root@test sysconfig]# /etc/init.d/iptables restart

Expurgar reglas del cortafuegos: [OK]

Configuración de cadenas a la política ACCEPT: filter [OK]

Descargando módulos iptables: [OK]

Aplicando reglas del cortafuegos iptables: [OK]

Cargando módulos iptables adicionales:ip_conntrack_netbios_[OK]

[root@test sysconfig]#

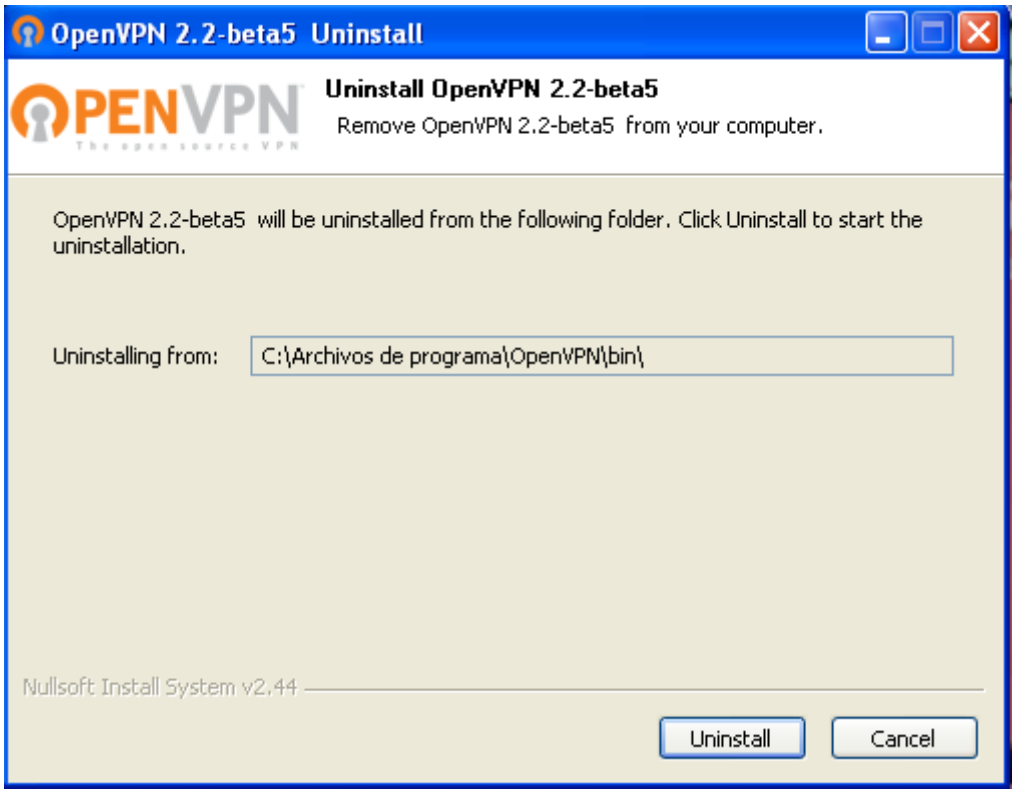
Si se han seguido estos pasos correctamente, ya se podría lanzar el cliente gráfico de Linux para poder realizar una conexión correctamente.

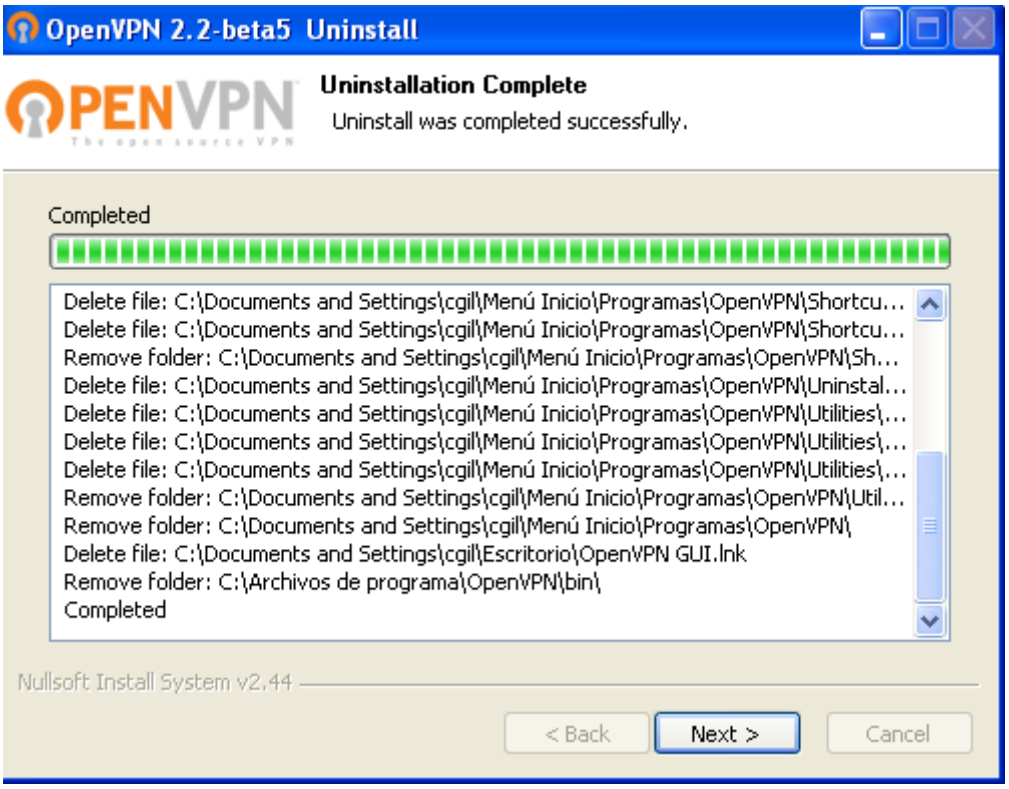
7. Desinstalador OpenVPN

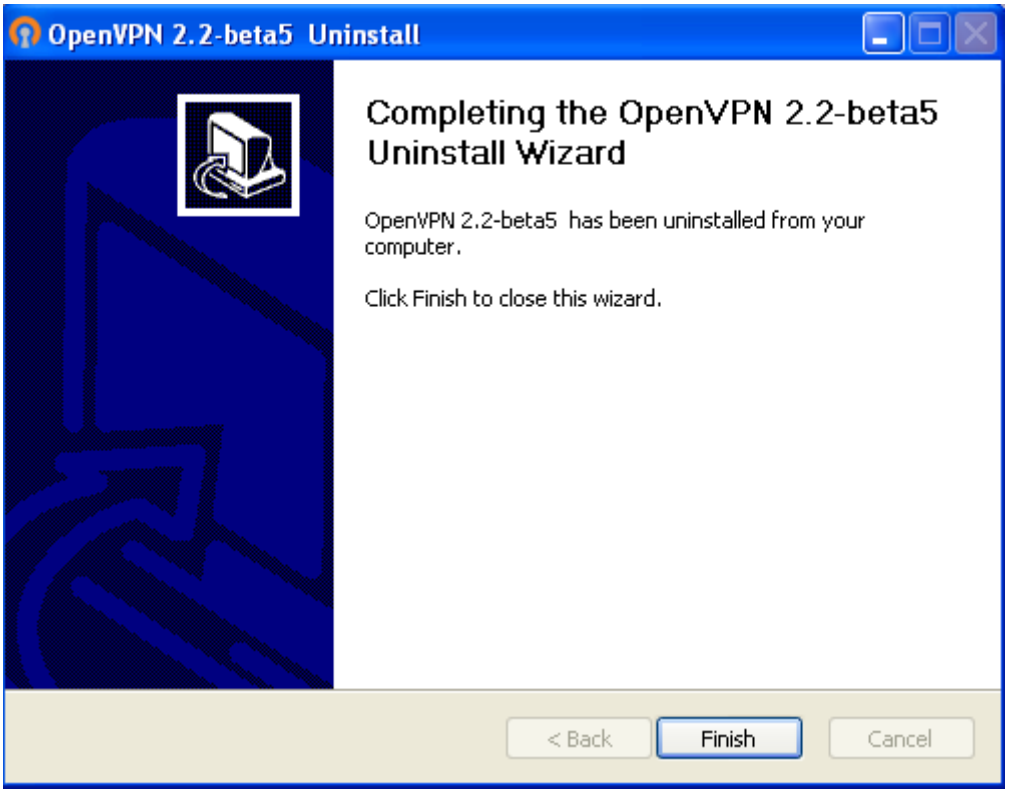
Se proporciona en los paquetes de instalación del cliente y servidor un desinstalador desarrollado también en java encargado de llamar al ejecutable uninstall de OpenVPN.

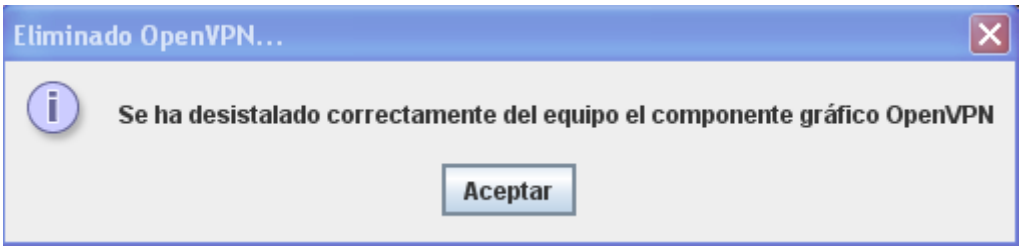
Cuando ha finalizado la desinstalación se encarga de eliminar todos los archivos de creados por los usuarios, para que no quede rastro de la aplicación gráfica de OpenVPN en el sistema.

Se muestran a continuación una serie de imágenes que ilustran las desinstalación de OpenVPN y del componente gráfico.




OpenVPN 2.2-beta5 Uninstall
OPENVPN
Uninstallation Complete
Uninstall was completed successfully.
Completed
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Shortcu...
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Shortcu...
Remove folder: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Sh...
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Uninstal...
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Utilities\...
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Utilities\...
Delete file: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Utilities\...
Remove folder: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\Util...
Remove folder: C:\Documents and Settings\cgil\Menú Inicio\Programas\OpenVPN\
Delete file: C:\Documents and Settings\cgil\Escritorio\OpenVPN GUI.lnk
Remove folder: C:\Archivos de programa\OpenVPN\bin\
Completed
Nullsoft Install System v2.44
< Back
Next >
Cancel


OpenVPN 2.2-beta5 Uninstall
Completing the OpenVPN 2.2-beta5 Uninstall Wizard
OpenVPN 2.2-beta5 has been uninstalled from your computer.
Click Finish to close this wizard.
< Back
Finish
Cancel


Eliminado OpenVPN...
Se ha desistalado correctamente del equipo el componente gráfico OpenVPN
Aceptar

Apéndice A

Se indican a continuación todos los posibles comandos de configuración para OpenVPN que se pueden incluir en los archivos de configuración ovpn (o .conf para equipos Linux). Si se desea ampliar la información de cada uno de ellos bien visitar el enlace: http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html#lbAH o escribir en un terminal **OpenVPN** [**--help**]

Comandos OpenVPN:

openvpn [**--help**]

openvpn [**--config** *file*]

openvpn [**--genkey**] [**--secret** *file*]

openvpn [**--mktun**] [**--rmtun**] [**--dev** *tunX* | *tapX*] [**--dev-type** *device-type*] [**--dev-node** *node*]

openvpn [**--test-crypto**] [**--secret** *file*] [**--auth** *alg*] [**--cipher** *alg*] [**--engine**] [**--keysize** *n*] [**--no-replay**] [**--no-iv**]

openvpn [**--askpass** *[file]*] [**--auth-nocache**] [**--auth-retry** *type*] [**--auth-user-pass-verify** *script*] [**--auth-user-pass** *up*] [**--auth** *alg*] [**--bcast-buffers** *n*] [**--ca** *file*] [**--ccd-exclusive**] [**--cd** *dir*] [**--cert** *file*] [**--chroot** *dir*] [**--cipher** *alg*] [**--client-cert-not-required**] [**--client-config-dir** *dir*] [**--client-connect** *script*] [**--client-disconnect**] [**--client-to-client**] [**--client**] [**--comp-lzo**] [**--comp-noadapt**] [**--config** *file*] [**--connect-freq** *n sec*] [**--connect-retry** *n*] [**--crl-verify** *crl*] [**--cryptoapicert** *select-string*] [**--daemon** *[progname]*] [**--dev-node** *node*] [**--dev-type** *device-type*] [**--dev** *tunX* | *tapX* | *null*] [**--dev** *tunX* | *tapX*] [**--dh** *file*] [**--dhcp-option** *type [parm]*] [**--dhcp-release**] [**--dhcp-renew**] [**--disable-occ**] [**--disable**] [**--down-pre**] [**--down** *cmd*] [**--duplicate-cn**] [**--echo** *[parms...]*] [**--engine** *[engine-name]*] [**--explicit-exit-notify** *[n]*] [**--fast-io**] [**--float**] [**--fragment** *max*] [**--genkey**] [**--group** *group*] [**--hand-window** *n*] [**--hash-size** *r v*] [**--help**] [**--http-proxy-option** *type [parm]*] [**--http-proxy-retry**] [**--http-proxy-timeout** *n*] [**--http-proxy** *server port [authfile] [auth-method]*] [**--ifconfig-noexec**] [**--ifconfig-nowarn**] [**--ifconfig-pool-linear**] [**--ifconfig-pool-persist** *file [seconds]*] [**--ifconfig-pool** *start-IP end-IP [netmask]*] [**--ifconfig-push** *local remote-netmask*] [**--ifconfig** *l rn*] [**--inactive** *n*] [**--inetd** *[wait|nowait] [progname]*] [**--ip-win32** *method*] [**--ipchange** *cmd*] [**--iroute** *network [netmask]*] [**--keepalive** *n m*] [**--key-method** *m*] [**--key** *file*] [**--keysize** *n*] [**--learn-address** *cmd*] [**--link-mtu** *n*] [**--local** *host*] [**--log-append** *file*] [**--log** *file*] [**--suppress-timestamps**] [**--lport** *port*] [**--management-hold**] [**--management-log-cache** *n*] [**--management-query-passwords**] [**--management** *IP port [pw-file]*] [**--max-clients** *n*] [**--max-routes-per-client** *n*] [**--mktun**] [**--mlock**] [**--mode** *m*] [**--mssfix** *max*] [**--mtu-disc** *type*] [**--mtu-test**] [**--mute-replay-warnings**] [**--mute** *n*] [**--nice** *n*] [**--no-iv**] [**--no-replay**] [**--nobind**] [**--ns-cert-type** *client|server*] [**--passtos**] [**--pause-exit**] [**--persist-key**] [**--persist-local-ip**] [**--persist-remote-ip**] [**--persist-tun**] [**--ping-exit** *n*] [**--ping-restart** *n*] [**--ping-timer-rem**] [**--ping** *n*] [**--pkcs12** *file*] [**--plugin** *module-pathname init-string*] [**--port** *port*] [**--proto** *p*] [**--pull**] [**--push-reset**] [**--push** *"option"*] [**--rcvbuf** *size*] [**--redirect-**

gateway *["local"] ["def1"]*] [**--remap-usr1** *signal*] [**--remote-random**] [**--remote** *host [port]*] [**--reneg-bytes** *n*] [**--reneg-pkts** *n*] [**--reneg-sec** *n*] [**--replay-persist** *file*] [**--replay-window** *n [t]*] [**--resolv-retry** *n*] [**--rmtun**] [**--route-delay** *[n] [w]*] [**--route-gateway** *gw*] [**--route-method** *m*] [**--route-noexec**] [**--route-up** *cmd*] [**--route** *network [netmask] [gateway] [metric]*] [**--rport** *port*] [**--secret** *file [direction]*] [**--secret** *file*] [**--server-bridge** *gateway netmask pool-start-IP pool-end-IP*] [**--server** *network netmask*] [**--service** *exit-event [0|1]*] [**--setenv** *name value*] [**--shaper** *n*] [**--show-adapters**] [**--show-ciphers**] [**--show-digests**] [**--show-engines**] [**--show-net-up**] [**--show-net**] [**--show-tls**] [**--show-valid-subnets**] [**--single-session**] [**--sndbuf** *size*] [**--socks-proxy-retry**] [**--socks-proxy** *server [port]*] [**--status** *file [n]*] [**--status-version** *n*] [**--syslog** *[progname]*] [**--tap-sleep** *n*] [**--tcp-queue-limit** *n*] [**--test-crypto**] [**--tls-auth** *file [direction]*] [**--tls-cipher** *l*] [**--tls-client**] [**--tls-exit**] [**--tls-remote** *x509name*] [**--tls-server**] [**--tls-timeout** *n*] [**--tls-verify** *cmd*] [**--tmp-dir** *dir*] [**--tran-window** *n*] [**--tun-ipv6**] [**--tun-mtu-extra** *n*] [**--tun-mtu** *n*] [**--txqueuelen** *n*] [**--up-delay**] [**--up-restart**] [**--up** *cmd*] [**--user** *user*] [**--username-as-common-name**] [**--verb** *n*] [**--writepid** *file*]

Bibliografía

http://es.wikipedia.org/wiki/Red_privada_virtual

http://www.monografias.com/trabajos11/repri/repri.shtml

http://www.slideshare.net/elplatin/exposicion-redes-vpn

http://www.ekontsulta.net/test/wiki/index.php/VPN

http://openvpn.net/

http://es.wikipedia.org/wiki/OpenVPN

http://blog.tuvpn.com/2010/06/%C2%BFopenvpn-o-pptp/?lang=es

www.freesshd.com/

http://www.ecualug.org/2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn

http://www.ubuntu-es.org/node/5290

http://sololinex.wordpress.com/2009/01/02/como-configurar-servidor-punto-multipunto-con-openvpn-y-cliente-en-windows-o-linux/

http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html#lbAH

La alumna Cristina Gil Álvaro como autora del proyecto autoriza a la Universidad Complutense a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a sus autores, tanto la propia memoria, como el código, la documentación y/o el prototipo desarrollado

Cristina Gil Álvaro