Configuración de un cliente OpenVPN en Windows, Linux, Mac OS X y Windows Mobile para Pocket PC

El propósito de este breve documento es guiar a configurar el cliente para obtener acceso a su red local a través de OpenVPN. Vamos a considerar la interfaz de usuario principal de OpenVPN para Windows, Linux, Mac OS X, Windows Mobile para Pocket PC y poner fin al uso de OpenVPN desde la línea de comandos sin interfaz gráfica de usuario. Esta última posibilidad es útil porque el comando *OpenVPN*, Convocada por sistema (ya sea un comando de shell de Unix del sistema de Windows), acepta los mismos parámetros y se comporta de la misma manera, independientemente de la plataforma. Por otra parte, el comando *OpenVPN* se puede utilizar en scripts para automatizar el inicio automático de la VPN.
Nuestro objetivo es tener acceso a un servidor VPN con Zeroshell construido y configurado con los parámetros por defecto. Para lograr este servidor será suficiente, por lo tanto, una vez en una red de servidores Zeroshell, simplemente habilitar el servicio OpenVPN activar la casilla de *Habilitado* en el [VPN] -> [l] Zeroshell interfaz Web. Por defecto, el servicio de nuestro servidor OpenVPN escuchara en el puerto 1194/TCP con encriptación TLS / SSL y compresión lzo habilitado. La autenticación de usuarios se hará con nombre de usuario y contraseña, pero también la varieremos de su configuración para poner la autenticación con certificados digitales X.509.
Para más detalles sobre la configuración de un servidor OpenVPN, que están fuera del alcance de este documento, puede consultar la guía "Un servidor con OpenVPN Zeroshell.

Éstas son las secciones que conforman el resto de esta guía. Tenga en cuenta que la primera de ellas, “archivo de configuración de OpenVPN” es común a otras secciones y es independiente de la interfaz gráfica de usuario o el sistema operativo que utilice.

- El archivo de configuración de OpenVPN
- OpenVPN GUI para Windows
- Tunnelblick para Mac OS X
- Kvpnc Linux
- OpenVPN para Windows Mobile Pocket PC
- La línea de mando de OpenVPN
- Compilación e instalación de OpenVPN

El archivo de configuración de OpenVPN

Gracias a los muchos parámetros que pueden ser incluidos en el archivo de configuración o especificados en la línea de comandos, la configurabilidad OpenVPN es realmente impresionante. Sin embargo, con el fin de conectarse a un servidor construido con OpenVPN Zeroshell es suficiente conocer algunos de ellos. Para simplificar aún más el procedimiento, usted puede descargar un archivo de configuración predeterminados, haga clic en el vínculo Archivo de configuración de clientes OpenVPN. “ver siguiente pagina”.

```
#============================================== ==========================#
# Especifica el nombre de host o dirección IP, número de puerto y el #
# Protocolo con el que llega a el servidor OpenVPN #
# El nombre de host también puede ser dinámico "(es decir, DynDNS). #
#============================================== ==========================#

zeroshell.example.com remoto 1194
proto tcp


#============================================== ==========================#
# Deja que la siguiente entrada es necesaria si desea nombre de usuario y
contraseña. #
# Comentario si desea utilizar la autenticación con certificados X.509. #
#============================================== ==========================#

-auth user-pass


#============================================== ==========================#
# No importa el tipo de autenticación, siempre debe especificar un #
# Archivo en formato PEM, que contiene el certificado de la Certificación #
# Autoridad que firmó el certificado del servidor OpenVPN. #
# Se puede obtener este certificado, haga clic en el enlace en la página # CA
# Nombre de ZeroShell. #
#============================================== ==========================#

ca CA.pem


#============================================== ==========================#
# Si desea utilizar la autenticación X.509, debe especificar el archivo #
# Contiene el certificado y su clave privada en formato PEM. #
# Usted puede unirse al certificado y la clave privada en el mismo archivo. #
#============================================== ==========================#

, Client.pem cert
; Client.pem clave


#============================================== ==========================#
# No debería ser necesario configurar los siguientes parámetros #
#============================================== ==========================#

comp-lzo
verb 3
silenciar 20
resolv-retry infinito
nobind
cliente
dev tap
persisten-clave
persisten-tun
```

Para cada parámetro que podría ser de interés para el usuario, el archivo de configuración contiene un comentario. Sin embargo, sólo hay dos parámetros que usted necesita definitivamente cambiar para poder conectarse a un servidor construido con OpenVPN Zeroshell:

- *zeroshell.example.com remoto 1194*

  Debe reemplazar zeroshell.example.com, con el nombre de host o dirección IP del servidor OpenVPN. La configuración por defecto proporciona la escucha de Zeroshell OpenVPN en el puerto 1194/TCP y por lo tanto el segundo parámetro (1194) pueden permanecer sin cambios.

ca CA.pem

Parámetro *ca* indica un archivo en formato PEM que contiene el certificado X.509 de la Autoridad de Certificación que firmó el certificado del servicio del servidor OpenVPN. Para obtener este certificado, simplemente, haga clic en el enlace en la página de acceso CA Zeroshell (véase el Figura).

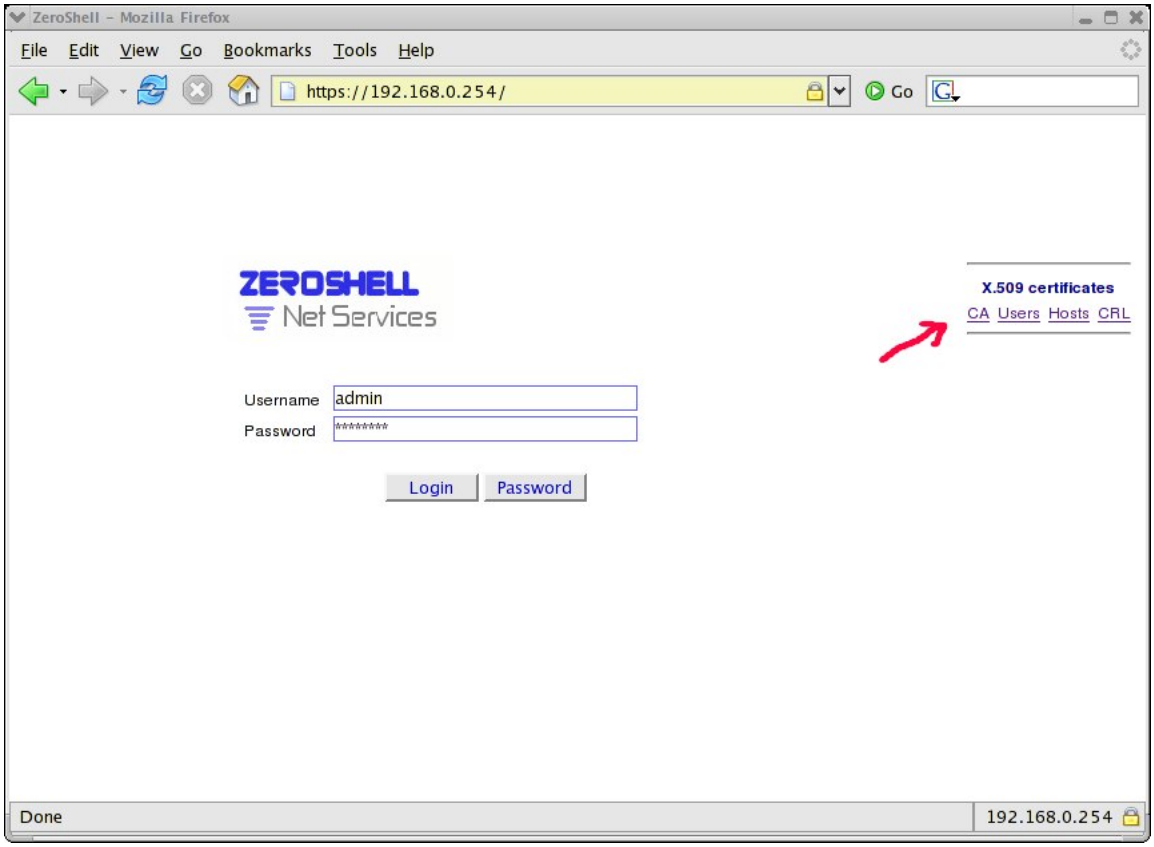

Figura.

- Si guarda el certificado en el mismo directorio que el archivo de configuración y lo llama CA.pem, puede dejar este parámetro sin cambios. De lo contrario, es necesario indicar la ruta absoluta.
  Tenga en cuenta que el certificado de Autoridad de Certificación es necesario incluso si usted no utiliza la autenticación X.509 del cliente y luego optar por la autenticación de *"Sólo Password"* (Por defecto en Zeroshell).

Observe que los OpenVPN GUI no dará ningún apoyo a la creación o modificación de archivos de configuración. Sólo permite la conexión, desconexión y requiere nombre de usuario y contraseña cuando sea necesario. Este archivo debe ser editado manualmente.

OpenVPN GUI para Windows

Para instalar OpenVPN GUI para Microsoft Windows XP 32-o 64 bits, haga lo siguiente:

- Descargar el paquete de instalación de la URL http://openvpn.se/download.html.
- Elija la versión que contiene, además de software la interfaz gráfica de usuario OpenVPN
- Iniciar la instalación. Elija las opciones por defecto y confirme su intención de continuar con la instalación de la *TAP-Win32 Adapter V8* (Interfaz virtual es usado por OpenVPN).
  Después del proceso de instalación, aparece un icono en la barra de tareas con dos terminales y un globo rojo. Estos terminales se ponen amarillos cuando se intenta una conexión y, finalmente, de color verde cuando se establece la conexión VPN con la red LAN remota;
- Desde el menú Inicio de Windows, haga clic en [Inicio] -> [Programas] -> [l] -> [l directorio de archivos de configuración]. Esto abrirá la carpeta:

  C: \ Archivos de programa \ OpenVPN \ config

  cuando tenemos que copiar un archivo dentro de la *zeroshell.ovpn* que contiene la configuración y la *CA.pem* que contiene el certificado X.509 de la Autoridad de Certificación. Consulte sección anterior Si no estás seguro de cómo conseguir los dos archivos;

- Editar el archivo *zeroshell.ovpn* y sustituir *zeroshell.example.com* con el nombre de host o dirección IP del servidor OpenVPN;
- En este punto, haciendo doble clic en el icono OpenVPN en la barra de la bandeja, se inicia el procedimiento de conexión. Un pop-up de diálogo aparece y en el hay que insertar un nombre de usuario y contraseña (ver Nota *). Si la autenticación es satisfactoria, la conexión VPN se establecerá y las dos terminales de OpenVPN mostraran un icono verde.

Al hacer clic en el botón derecho del ratón sobre el icono de la barra de tareas de OpenVPN aparece un menú con varias opciones útiles que se enumeran a continuación y hablan por sí solas: *Conectar*, *Desconectar*, *Mostrar el estado*, *Ver Log*, *Editar, Configurar*, *Configuración de proxy*. En particular, si usted experimenta problemas de conexión y útil la opcion *Ver Log* para determinar la causa del fallo.

Pero si se realiza la conexión, entonces la terminal 2 del icono es verde, pera llegar a la red LAN remota o Internet, puede que quiera usar el comando ***ipconfig / all***
He aquí un ejemplo:

```
Adaptador Ethernet Conexión de área local (LAN) 7:

        De conexión específica sufijo DNS:
        Descripción. . . . . . . . . . . . . : TAP-Win32 Adapter V8
        Dirección física. . . . . . . . . . . : 00-FF-AD-63-83-3D
        DHCP habilitado. . . . . . . . . . . . Sí
        Configuración automática habilitada. Sí
        Dirección IP. . . . . . . . . . . . . : 192.168.250.51
        Máscara de subred. . . . . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada. . . . . . . . . : 192168250254
        Servidor DHCP. . . . . . . . . . . . . : 192.168.0.0
        Servidor DNS. . . . . . . . . . . . . : 192168250254
        Obtención de la concesión. . . . . . . . . . . . : Jueves, septiembre
20, 2007 19:51:37
        Vence el contrato. . . . . . . . . . . .: Viernes, septiembre 19, 2008
19:51:37
```

Usted debe comprobar que la VPN se completo correctamente, que la ruta se lleva a cabo correctamente y, a continuación la dirección IP y puerta de enlace predeterminada pertenecen a la subred LAN remota a la que se registran en Red Privada Virtual. Como garantía adicional de que el tráfico es realmente enrutado a través de la VPN, escriba el comando: ***tracert / d <dirección IP ordenador>***. Si el primer router que se encuentra en la LAN remota a la que ha conectado, entonces hay que ver el flujo de tráfico en VPN encriptado como se esperaba.

Tunnelblick para Mac OS X

Una interfaz gráfica de usuario para OpenVPN en Mac OS X *Tunnelblick*. Para instalar la interfaz gráfica de usuario que utiliza los pasos siguientes:

- Descargar el paquete de instalación de la URL http://www.tunnelblick.net. Este es un archivo comprimido. Zip que tambien contiene la GUI de OpenVPN;
- Haga doble clic en el archivo zip (supongamos que está en el escritorio) para extraer su contenido. Aparece el nombre del ejecutable en el escritorio *Tunnelblick*;
- Iniciar el archivo ejecutable *Tunnelblick* con un doble clic. Pulse [Continuar] en el cuadro de diálogo que aparece para avisarle donde quiere poner sus archivos de configuración *Biblioteca / openvpn /*. Cierre la ventana que se abre para permitir que se modifique el ejemplo de archivo de configuración *openvpn.conf*;
- El GUI de OpenVPN Tunnelblick ya está instalado y la barra superior, cerca del reloj, aparece su icono. Ahora, continúe con la configuración necesaria para acceder a un servidor construido con OpenVPN Zeroshell;
- Siga el procedimiento descrito en la sección El archivo de configuración de OpenVPN para obtener el archivo de configuración *zeroshell.ovpn* y el archivo *CA.pem* que contiene el certificado X.509 de la Autoridad de Certificación. Abra el Finder y seleccione el directorio *Biblioteca / openvpn* (el usuario y no el del sistema). Eliminar el ejemplo de archivo de configuración *openvpn.conf* y arrastre los dos archivos en el directorio obtenido anteriormente;
- Cerrar Tunnelblick seleccione [Salir] en el menú contextual que aparece al hacer clic en el icono. A continuación, reinicie haciendo doble clic en el archivo ejecutable *Tunnelblick*. Ahora, al hacer clic en el icono de Tunnelblick aparece cuando [Zeroshell Connect "], que proporciona una conexión a VPN Zeroshell;
- Seleccione el menú [Detalles ...] se abre un cuadro de diálogo y presione [Editar configuración]. Reemplace *zeroshell.example.com* con el nombre de host o dirección IP del servidor VPN. Guarde el archivo de configuración.
- Prueba de la conexión VPN, haga clic en [Zeroshell Connect "]. Aparece un pop-up para introducir nombre de usuario y contraseña (ver Nota *).

Si tiene problemas para conectarse, puede ser útil consultar los registros de OpenVPN para determinar la causa del problema,. Para ello sólo tiene que seleccionar el icono de la Tunnelblick [Detalles].
Si desea verificar que la dirección IP que utiliza la VPN, pertenece realmente a la red LAN remota está conectado, abra una terminal y Mac OS X en el shell del sistema, escriba el comando:

ifconfig tap0

cuya producción es similar a lo siguiente:

```
tap0: flags = 8843 mtu 1500 <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
        inet 192.168.250.1 netmask 0xffffff00 emisión 192168250255
        éter B6: da: D9: 91:22: ff
        abierto 368 (PID)
```

El artículo *inet* indica que la dirección IP es 192.168.250.1 (Zeroshell por defecto si no se configura cedidos a los clientes VPN remotos direcciones que pertenecen a la subred 192.168.250.0/24 con puerta de enlace predeterminada 192.168.250.254). Para estar absolutamente seguro de que el tráfico es realmente enrutado a través del túnel cifrado por la VPN utiliza el comando ***traceroute-n host> ordenador>***. Para que el enrutamiento de VPN sea correcto, el primer salto del router debe ser una LAN remota (192.168.250.254 con la configuración por defecto de OpenVPN Zeroshell configurado).

Kvpnc Linux

Kvpnc Linux es una interfaz que controla la mayor parte de clientes VPN disponibles: Cisco VPN, IPSec, PPTP, OpenVPN, L2TP. Es muy amplio y flexible, de modo que también tiene soporte para tarjetas inteligentes Obviamente, en este contexto, el documento de instalación y configuración única en OpenVPN. Hay paquetes precompilados para la mayoría de distribuciones de Linux como RPMs para SuSE y Fedora. En cuanto a Ubuntu y Kubuntu (o Debian otros derivados), puede instalar kvpnc con OpenVPN simplemente con los comandos:

sudo apt-get install openvpn
sudo apt-get install kvpnc

Tenga en cuenta que a diferencia de otras interfaces gráficas de usuario, el paquete no incluye la kvpnc OpenVPN en cambio, se instalan por separado. A fin de mantener la discusión lo más independiente posible de la distribución de Linux en particular, compilar los fuentes directamente kvpnc, pero si hay un paquete binario para su distribución, se invita a utilizarlos.
Desde kvpnc utiliza la biblioteca Qt, la presencia de estas bibliotecas y de cualquier archivo es un requisito previo para la compilación. En los pasos siguientes, vamos a suponer que OpenVPN ya está instalado. Si no, véase el párrafo Compilación e instalación de OpenVPN.
Ahora se procede con la instalación y configuración de kvpnc:

- Descarga el código fuente desde el sitio http://home.gna.org/kvpnc/. En el siguiente se hará referencia a la versión 0.8.9 de kvpnc, pero aún debe descargar la más reciente disponible;
- Extraiga el contenido del paquete con el comando:
  tar xvfj kvpnc-0.8.9.tar.bz2
- Compilar e instalar kvpnc con la secuencia de comandos:
  kvpnc cd-0.8.9
  . / Configure
  hacer
  sudo make install

  En algunas distribuciones, debe especificar explícitamente la ubicación de los archivos de inclusión y bibliotecas QT. En este caso, agregar los parámetros - *With-qt-includes = / usr/lib64/qt-3.3/include / - with-qt-libraries = / usr/lib64/qt-3.3/lib* / comando *. / Configure*Sustitución */ Usr/lib64/qt-3.3 /* con el camino apropiado para su distribución de Linux;
- Crear el */ Etc / openvpn /* el comando *sudo mkdir / etc / openvpn* y copiar los archivos dentro de *zeroshell.ovpn* y *CA.pem*. Para obtener estos archivos, por favor vaya a El archivo de configuración de OpenVPN;
- Para utilizar kvpnc conun usuario no privilegiado debe utilizar *sudo*. Para ello, tienen privilegios de root, agregar la siguiente línea al final del archivo */ Etc / sudoers*:
  TODOS LOS ALL = NOPASSWD: / usr / bin / kvpnc

  Cuando usted necesite ejecutar el comando kvpnc utiliza la sintaxis:
  / usr / sudo / bin / kvpnc

  De esta manera, *kvpnc* tendrá los privilegios de root que necesita para crear la interfaz virtual Ethernet tap0 y agregar rutas estáticas a la ruta del tráfico de la VPN;

- Importar el perfil para conectarse a un servidor VPN Zeroshell con el siguiente comando:

  kvpnc - openvpnimport = / etc / openvpn / zeroshell.ovpn

  Desde el Administrador de perfil que aparece, utilice las siguientes configuraciones:
  - Desde la pantalla *General* configurar el *Puerta de enlace VPN* con la dirección IP o nombre de host del servidor VPN Zeroshell;
  - Desde la pantalla *OpenVPN* Asegúrese de que la voz de *Método de autenticación* se establece en *SHA1* en lugar de *MD5*;

  Pulse [Aplicar] y luego [Aceptar] en el Administrador de perfiles y [Perfil] -> [Guardar perfil ...] guardar el perfil y cerca de *kvpnc* con el elemento de menú [Archivo] -> [Salir];

- A continuación, ejecute el comando */ usr / sudo / bin / kvpnc* y pulse [Connect] para conectarse a VPN Zeroshell. En este punto se requiere de usuario y contraseña (ver Nota *) Y si la autenticación es satisfactoria, la conexión VPN se establece con la red remota.

Para comprobar que la dirección IP que está utilizando la VPN, lo que realmente pertenece a la red LAN remota está conectado, simplemente abra un intérprete de comandos y escriba el comando:

/ Sbin / ifconfig tap0

cuya producción es similar a lo siguiente:

```
tap0 Link encap: Ethernet HWaddr 26:8 F: 1E: 31:44: DD
          inet addr: 192.168.250.50 Bcast: 192168250255 Mask: 255.255.255.0
          inet6: fe80:: 248F: 1eff: FE31: 44dd/64 Alcance: Vínculo
          UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
          RX packets: 19 errors: 0 dropped: 0 overruns: 0 frame: 0
          TX packets: 25 errors: 0 dropped: 0 overruns: 0 carrier: 0
          collisions: 0 txqueuelen: 100
          RX bytes: 1384 (1.3 MiB) TX bytes: 1668 (1.6 MiB)
```

El artículo *inet* indica que la dirección IP 192.168.250.50 (Zeroshell por defecto si no se configura cedidos a los clientes VPN remotos direcciones que pertenecen a la subred 192.168.250.0/24 con puerta de enlace predeterminada 192.168.250.254). Para estar absolutamente seguro de que el tráfico es realmente enrutado a través del túnel cifrado por la VPN utiliza el comando ***traceroute-n host> ordenador>***. Para que el enrutamiento de VPN sea correcto, el primer salto debe ser una LAN remota (192.168.250.254 con la configuración por defecto de OpenVPN Zeroshell configurado).

OpenVPN para Pocket PC

OpenVPN para Pocket PC software todavía está en versión Alpha, pero después de muchas pruebas demostraron ser lo suficientemente estables y fiables. Las pruebas se realizaron en Microsoft Windows Mobile versión 5.0 instalado en una computadora de mano i-Mate JASJAR (equivalente a un HTC Universal Qtek 9000), sin embargo, no debería haber problemas, incluso corriendo en WM 2003 y otros modelos de PDA. Antes de ver la instalación y configuración, por favor, tenga en cuenta que, al tener que modificar manualmente el archivo de configuración de OpenVPN, usted debe conectar a su PDA a través de ActiveSync y hacer los cambios con un editor de un PC. Alternativamente, si desea hacer cambios directamente en la computadora de mano, debe instalar la *Total Commander CE* , que es un programa gratuito de Administrador de archivos para Pocket PC, disponible en la URL http://www.ghisler.com/pocketpc.htm. Este Filemanager integra, entre otras cosas, un editor sirve a nuestros propósitos.
Éstos son los pasos necesarios para instalar OpenVPN para Pocket PC:

- Transferencia de *OpenVPN para Pocket PC* el sitio http://ovpnppc.ziggurat29.com/ovpnppc-main.htm. El paquete puede ser descargado en dos formatos: en *. Exe* utilizar para la instalación de PC con el PDA conectado a través de ActiveSync, el formato *. Cab* instala directamente desde la computadora de mano en sí. Elija el formato que sea adecuado e instalelo;
- Suponiendo que ha instalado *OpenVPN para Pocket PC* carpeta \ *Archivos de programa* \ *OpenVPN* en la memoria del dispositivo, copiar los archivos *zeroshell.ovpn* y *CA.pem* a *Archivos de programa* \ *OpenVPN* \ *config*. Para obtener estos archivos, por favor vaya a El archivo de configuración de OpenVPN;
- Editar el archivo de configuración \ *Archivos de programa* \ *OpenVPN* \ *config* \ *zeroshell.ovpn* para permitir la conexión a un servidor construido con OpenVPN Zeroshell:
    - Reemplace *zeroshell.example.com* con la dirección IP o nombre de host del servidor OpenVPN;
    - Reemplace *CA.pem* con la ruta completa del archivo que contiene el certificado en formato PEM de la Autoridad de Certificación. En nuestro caso, debemos especificar:

        ca "\ \ Archivos de programa \ \ OpenVPN \ \ config \ \ CA.pem"

        Las comillas y barras dobles son requeridos por la sintaxis;
- Haga clic en el icono de OpenVPN y el elemento de menú *De configuración de arranque.* elegir *zeroshell*. En este punto se requiere de usuario y contraseña (ver Nota *). Si la autenticación es satisfactoria, la conexión VPN se establece y 2 terminales de OpenVPN se iluminan en verde;

Cualquier falta de consulta a los registros de acceso para conectarse \ *Archivos de programa* \ *OpenVPN* \ *log* \ *zeroshell.log*. Por último, para verificar que el tráfico a la red remota o Internet es en realidad encapsulada en el túnel de VPN encriptado, debe realizar una *traceroute* y comprobar que cumple con el primer salto pertenece a la red LAN remota (el valor predeterminado es Zeroshell 192.168.250.254). Sin embargo, Windows Mobile no se ha trazado de forma nativa y por ello es necesario instalar una utilidad externa. El software libre es útil para *ceNetTools* que, además de *traceroute* También le permite realizar comandos *Ping* y el comando *Whois*.

La línea de mando de OpenVPN

Si el sistema que está utilizando no tiene un interfaz gráfico para OpenVPN o la manera en que desea automatizar el inicio de la conexión VPN a través de los scripts de inicio, debe utilizar el comando directamente *OpenVPN*. Sólo tienes que escribir *openvpn hombre* que están disponibles para realizar una serie de parámetros que pueden influir en el comportamiento de la VPN. Estos parámetros se pueden especificar directamente en la línea de comandos precedidos por un guión doble (--), o se inserta en un archivo de configuración. Salvo unos pocos casos, siempre debe utilizar el archivo de configuración porque es más fácil de leer que una línea de comandos agobiados por numerosos parámetros. No es el alcance de este documento responde a los parámetros de OpenVPN, en parte porque las páginas de manual que viene con el comando *hombre* están bien detallados. Ver sólo los pasos para conectarse a un servidor construido con OpenVPN Zeroshell:

- Lugar en un solo directorio (por ejemplo */ Etc / openvpn /*) Archivo de configuración *zeroshell.ovpn* CA.pem y el archivo que contiene el certificado en formato PEM de la Autoridad de Certificación. Para obtener más información acerca de cómo obtener estos archivos, consulte El archivo de configuración de OpenVPN;
- Editar el archivo de configuración *zeroshell.ovpn* sustituir*zeroshell.example.com* con la dirección IP o nombre de host del servidor de VPN;

En el mismo directorio donde se colocan los archivos de configuración, ejecute el comando:

openvpn - config zeroshell.ovpn

Se le pedirá nombre de usuario y contraseña si la autenticación es satisfactoria verá la línea en el registro de:

Inicialización secuencia completa

Compilación e instalación de OpenVPN

Para la mayoría de los sistemas para los que se apoya OpenVPN, están los los paquetes pre-compilados. Sin embargo, especialmente para Linux, dada la gran cantidad de distribuciones que existen, hay casos en que es necesario compilar el código fuente de OpenVPN. Vemos los pasos para hacer esto:

- Descarga desde el sitio http://openvpn.net el paquete que contiene el código fuente de la última versión estable disponible;
- Extraiga el contenido del paquete fuente utilizando el comando *tar* de la siguiente manera:
  tar xvfz openvpn-2.0.9.tar.gz
- Introduzca el directorio directorio *openvpn-2.0.9* a través de comandos
  cd openvpn-2.0.9
- Ejecute el sistema de control para la producción de Makefile con el comando:
  . / Configure - prefix = / usr /

  Si el comando *. / Configure* se queja de la falta de software de compresión *lzo*, Instalarlo de la siguiente manera:
  - Descarga el código fuente desde el sitio lzo http://www.oberhumer.com/ y extraer el contenido con el
    tar xvfz lzo-2.02.tar.gz
  - Entra en el directorio *lzo-2.02* e instalar el software de compresión lzo debido a los siguientes comandos:
    - *. / Configure*
    - *hacer*
    - *make install*(Este comando requiere privilegios de administrador)

    Instalado *lzo*Después de volver al directorio de *openvpn-2.0.9*, Vuelva a ejecutar el comando
    . / Configure - prefix = / usr /

- Compilar el código fuente basado en la recién generada Makefile con el comando:
  hacer
- Instale el programa binario *OpenVPN* y su página de manual mediante el comando:
  make install

  Desde la instalación del sistema de directorio */ Usr /*, Este comando debe ejecutarse con privilegios de administrador.

Notas

(*) La forma en que se validan las credenciales del usuario depende de la configuración del servidor OpenVPN. Zeroshell le permite añadir dominios de autenticación múltiples, cada uno de los cuales pueden ser autenticados en el KDC de Kerberos 5 (local, externo o por medio de la autenticación), o un servidor RADIUS externo. Uno de estos dominios es el valor predeterminado, lo que significa que el usuario que especifica el nombre de usuario no está obligado a declararlo explícitamente. En otros casos, el nombre de usuario debe ser en forma ***nombre de usuario*** @ ***dominio*** (fulvio@example.com por ejemplo). Tenga en cuenta que el dominio no es sensible a mayúsculas, porque si es un Kerberos V, Zeroshell lo convierte automáticamente a mayúsculas.