

Configuración de Clientes VPN con OpenVPN.

Clientes Windows

Para la configuración de clientes OpenVPN utilizaremos el programa OpenVPN GUI para Windows.

OpenVPN GUI para Windows corre normalmente en una ventana de consola, al ser conectado al servidor remoto/local VPN le da un aviso en el área de notificación (el área de abajo a la derecha por el reloj en la barra), desde allí puede tener el control de iniciar/parar el Cliente OpenVPN, consultar los avisos (log), incluso cambiar su contraseña.

Puede ser descargado en el sitio OpenVPN GUI for Windows <http://openvpn.net/index.php/open-source/downloads.html>

Preparativos y configuración

A continuación deberá copiar los siguientes archivos:

- ca.crt.
- cliente1.crt.
- cliente1.csr.
- cliente1.key

Estos fueron creados en el servidor OpenVPN y deberán ser colocados en la máquina cliente dentro de C:\Program Files\OpenVPN\config o a su vez en C:\Archivos de Programa\OpenVPN\config

Se creará un archivo de configuración cliente para el OpenVPN dentro del directorio **C:\Archivos de Programa\OpenVPN\config** con el nombre de **cliente-redes.ovpn**.

Tendrá la siguiente configuración:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#----- SECCION DE LLAVES -----
ca ca.crt
cert cliente.crt
key cliente.key
ns-cert-type server
#-----
comp-lzo
verb 3
```

Descripción:

client: Especifica el tipo de configuración, en este caso tipo cliente OpenVPN.

Port: Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en la conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

remote: Host remoto o dirección IP en el cliente, el cual especifica al servidor OpenVPN.

El cliente OpenVPN puede tratar de conectar al servidor con **host:port** en el orden especificado de las opciones de la opción **--remote**.

float: Este le dice a OpenVPN aceptar los paquetes autenticados de cualquier dirección, no solamente la dirección cuál fue especificado en la opción **--remote**.

resolv-retry: Si la resolución del hostname falla para **-- remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind: No agrega bind a la dirección local y al puerto.

ca: Especifica la ubicación exacta del archivo de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del archivo [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote: Especifica el dominio o IP del servidor así como el puerto que escuchara las peticiones para servicio VPN.

comp-lzo: Especifica los datos que recorren el túnel VPN será compactados durante la transferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb: Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

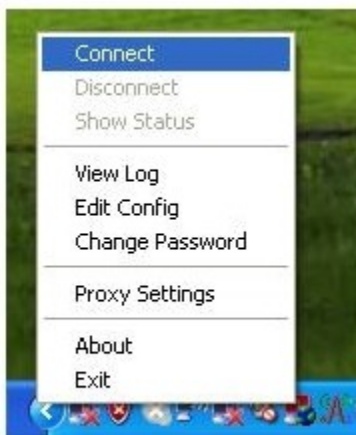
0 --No muestra una salida excepto errores fatales. 1 **to** 4 –Rango de uso normal. 5

--Salida **Ry W**caracteres en la consola por los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

Una vez configurado el cliente VPN con Windows, deberá ir al área de notificación (el área de abajo a la derecha por el reloj en la barra de Windows) y dar un click derecho al icono del cliente OpenVPN, allí aparecerá un menú en el cual podrá elegir la opción **conectar** [connect].

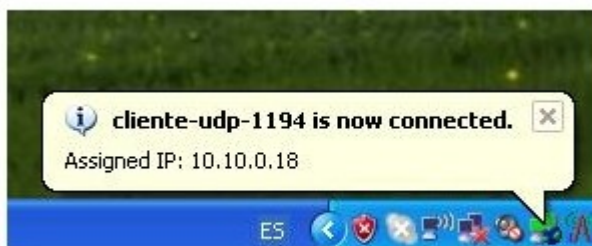


Icono de notificación



Menú del cliente OpenVPN para efectuar la conexión al servidor VPN

Cuando intente conectarse al servidor VPN una vez que haya elegido la opción [**connect**] aparecerá una ventana de notificación en el cual verá los procesos de verificación e intento de conexión al servidor VPN, si todo sale bien, en el icono de notificación del cliente OpenVPN le indicará la correcta conexión y le mostrará el número de IP virtual [**tun**] que se le fue asignado.



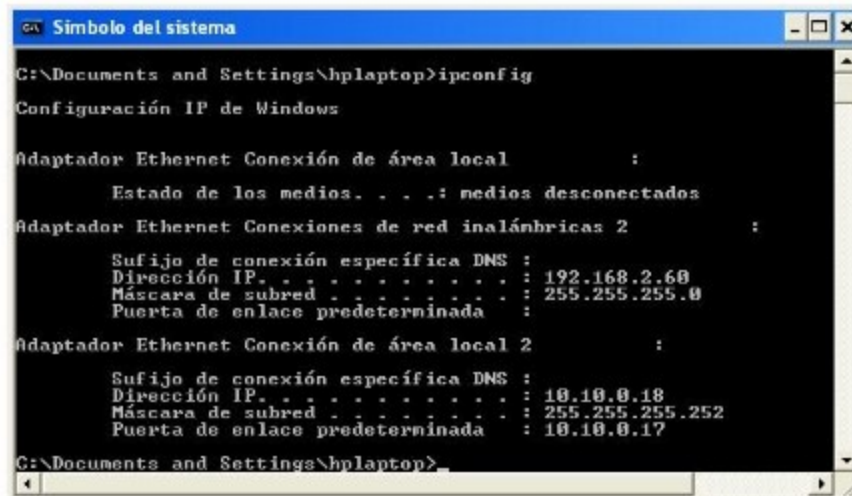
Mensaje de notificación al conectarse al servidor VPN

Pruebas de Conexión

Una vez efectuada la conexión al servidor, para asegurarse que estamos dentro del túnel VPN y tenemos conexión al servidor, podemos realizar una búsqueda de [dirección IP \[Ping\]](#), así como también verificar el número IP asignado por el servidor VPN al estar conectarnos en el túnel.

Para esto utilizaremos el comando **[cmd]** para hacer llamado al MS-Dos de Windows a través de la aplicación [ejecutar].

Una vez estando en la consola en modo texto, utilice el comando **[ipconfig]** para ver que dirección IP se le fue asignado.

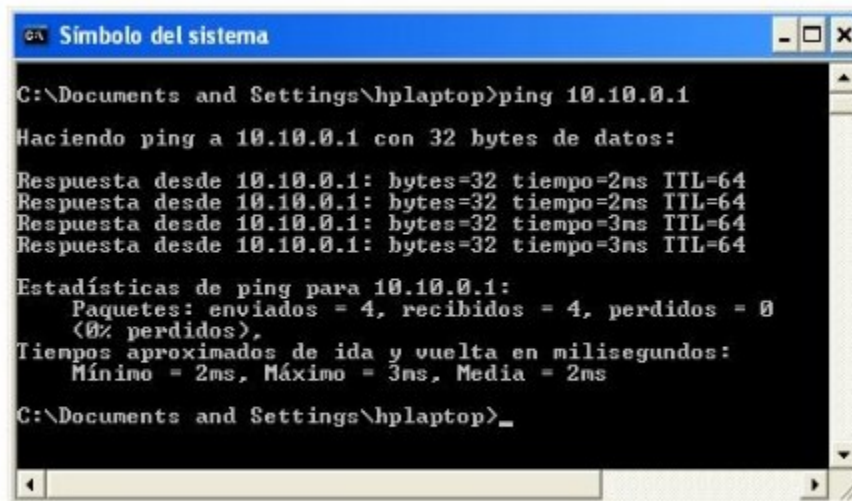


```
Símbolo del sistema
C:\Documents and Settings\hplaptop>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local :
    Estado de los medios. . . .: medios desconectados
Adaptador Ethernet Conexiones de red inalámbricas 2 :
    Sufijo de conexión específica DNS :
    Dirección IP. . . . .: 192.168.2.60
    Máscara de subred . . . . .: 255.255.255.0
    Puerta de enlace predeterminada :
Adaptador Ethernet Conexión de área local 2 :
    Sufijo de conexión específica DNS :
    Dirección IP. . . . .: 10.10.0.18
    Máscara de subred . . . . .: 255.255.255.252
    Puerta de enlace predeterminada : 10.10.0.17
C:\Documents and Settings\hplaptop>
```

Verificación de asignación de dirección IP virtual [tun]



```
Símbolo del sistema
C:\Documents and Settings\hplaptop>ping 10.10.0.1

Haciendo ping a 10.10.0.1 con 32 bytes de datos:

Respuesta desde 10.10.0.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.10.0.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.10.0.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 10.10.0.1: bytes=32 tiempo=3ms TTL=64

Estadísticas de ping para 10.10.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms
C:\Documents and Settings\hplaptop>
```

Verificación de conexión de red a través del túnel VPN

Importante: Deberá desactivar el cortafuego que trae como predeterminado Windows o cual quier otro que este utilizando.

Cientes Linux

Para la configuración de clientes Linux con OpenVPN utilizaremos el modo texto [terminal] y el arranque a través de un **bash**.

Preparativos y configuración

A continuación deberá copiar los siguientes archivos:

- ca.crt
- cliente1.crt
- cliente1.csr
- cliente1.key

Estos fueron creados en el directorio `/etc/openvpn/easy-rsa/2.0/keys` y deberán ser colocados en la máquina cliente dentro del directorio OpenVPN.

Supongamos que las llaves la tenemos en el directorio `/tmp/llaves`, debemos copiar estas en el siguiente directorio `/etc/openvpn/keys`, para esto hay que crearlo antes.

```
mkdir /etc/openvpn/keys

cp -R /tmp/llaves/* /etc/openvpn/keys/

cd /etc/openvpn/
```

A continuación se creará un archivo de configuración cliente para el OpenVPN dentro del directorio `/etc/openvpn/` con el nombre de **cliente1-udp-1194.ovpn**.

Tendrá la siguiente configuración:

```
client
dev tun
proto udp
remote dominio-o-ip.del.servidor.vpn 1194
float
resolv-retry infinite
nobind
persist-key
persist-tun
#----- SECCION DE LLAVES -----
ca ca.crt
cert cliente.crt
key cliente.key
ns-cert-type server
#-----
comp-lzo
verb 3
```

Descripción:

client : Especifica el tipo de configuración, en este caso tipo cliente OpenVPN.

Port : Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en la conexión a través de VPN

dev : Tipo de interfaz de conexión virtual que se utilizará en el servidor openvpn.

remote : Host remoto o dirección IP en el cliente, el cual especifica al servidor OpenVPN.

El cliente OpenVPN puede tratar de conectar al servidor con **host:port** en el orden especificado de las opciones de la opción **--remote**.

float : Este le dice a OpenVPN aceptar los paquetes autenticados de cualquier dirección, no solamente la dirección cuál fue especificado en la opción **--remote**.

resolv-retry : Si la resolución del hostname falla para **-- remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind : No agrega bind a la dirección local y al puerto.

ca : Especifica la ubicación exacta del archivo de Autoridad Certificadora [.ca].

cert : Especifica la ubicación del archivo [.crt] creado para el servidor.

key : Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote : Especifica el dominio o IP del servidor así como el puerto que escuchara las peticiones para servicio VPN.

comp-lzo : Especifica los datos que recorren el túnel VPN serán compactados durante la transferencia de estos paquetes.

persist-key : Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun : Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb : Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 -- No muestra una salida excepto errores fatales.

1 to 4 - Rango de uso normal.

5 -- Salida **R** y **W** caracteres en la consola por los paquetes de lectura y

```
escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP
```

Ahora necesitamos insertar el módulo [**tun**] para controlar los interfaces `/dev/net/tunX` que se necesiten en el sistema para el servicio OpenVPN:

Cargamos el módulo:

```
modprobe tun
```

y habilitamos el IP forwarding:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Comprobamos que tenemos `/dev/net/tun`, si no existe lo creamos con:

```
mknod /dev/net/tun c 10 200
```

Para la ejecución del cliente OpenVPN puede utilizar el siguiente guión y guardarlo con el nombre de `[iniciovpncliente]`, tendrá el siguiente contenido:

```
#!/bin/bash
#
#-- Variables --
RUTACONFIG="/etc/openvpn/"
NOMCONFIG="cliente1-udp-1194.conf"
#
#-- Ejecución de la configuración para el servicio OpenVPN
#
/usr/bin/openvpn $RUTACONFIG./$NOMCONFIG
#
exit 0
```

Y damos los permisos de ejecución correspondientes:

```
chmod +x iniciovpncliente
```

Si desea ejecutar el servicio VPN al inicio del sistema (arranque), puede colocar lo siguiente dentro del archivo `/etc/rc.local`

```
#inicia la configuración OpenVPN
/donde/este/tu/archivo/iniciovpncliente
```

Pruebas de Conexión

Una vez efectuada la conexión al servidor VPN, para asegurarse que estamos dentro del túnel VPN y tenemos conexión al servidor, podemos realizar una búsqueda de dirección IP [**Ping**], así como también verificar el número IP asignado por el servidor VPN al estar conectarnos en el túnel.

Para esto utilizaremos el necesitamos entrar a la terminal de comando, una vez estando en la consola en modo texto, utilice el comando [**ifconfig**] para ver que dirección IP se le fue asignado.

```
root@soporte01:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:04:E2:26:04:7F
          inet addr:192.168.2.51  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::204:e2ff:fe26:47f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42553 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21775 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15261443 (14.5 MiB)  TX bytes:3818721 (3.6 MiB)
          Interrupt:209 Base address:0x2c00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1895 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1895 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4227852 (4.0 MiB)  TX bytes:4227852 (4.0 MiB)

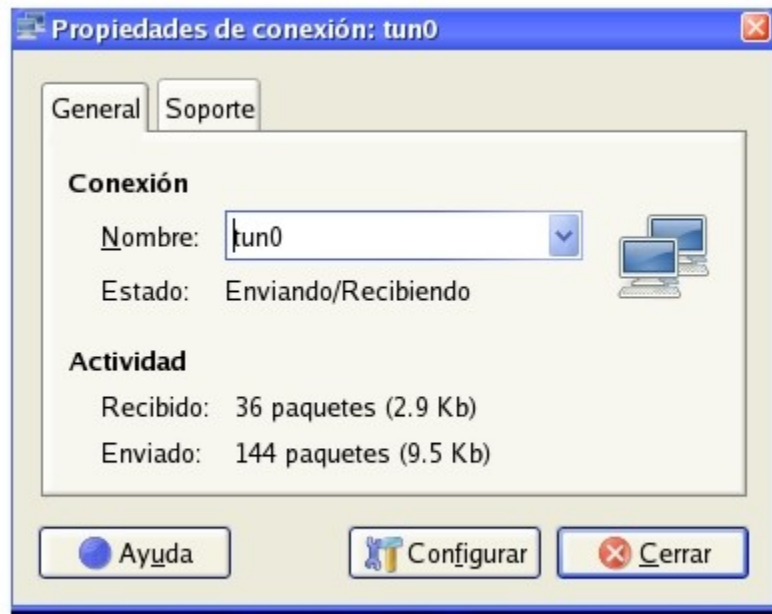
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.10.0.14  P-t-P:10.10.0.13  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:2004 (1.9 KiB)
```

Verificación de asignación de dirección IP [tun] con **ifconfig**

```
root@soporte01:~# ping -c 3 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=0 ttl=64 time=1.17 ms
64 bytes from 10.10.0.1: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=1.18 ms

--- 10.10.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 1.175/1.203/1.250/0.033 ms, pipe 2
root@soporte01:~#
```

Prueba de conexión con el comando [ping] hacia el servidor VPN



Comprobación de conexión hacia el servidor VPN en interfaz gráfica

Si **SELinux** está activo en el sistema y se va a utilizar el componente de OpenVPN para **NetworkManager** (**NetworkManager-openvpn**), y se van a utilizar certificados almacenados en el directorio del usuario, se debe activar la política **openvpn_enable_homedirs**.

```
setsebool -P openvpn_enable_homedirs 1
```

Referencias:

- **Guía de Instalación del acceso de Red Privada Virtual de la UCA (OpenVPN)**
Windows Vista, Universidad de Cádiz, Área de Informática,
<http://www2.uca.es/serv/ai/servicios/vpn/guia-openvpn-vista.html>
- William López Jiménez, VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall, **Creative Commons,**
<http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P1> <<http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P1>>
- William López Jiménez, VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall, **Creative Commons,**
<http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P2> <<http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P2>>