Manual
Elastix-EasyVPN
V1.1

Última actualización:
22 de mayo de 2014

Conexión y Enlace de Comunicación Profesional S.A. de C.V.
Mier y Pesado 329 Int. 203 Col. Del Valle, Benito Juárez, México D.F. | Tel. (55) 50.181.181 | ventas@enlaza.mx | http://enlaza.mx

Tabla de contenidos

¡Gracias!

Sí, gracias por descargar el addon Elastix-EasyVPN. Éste te permitirá crear de forma sencilla, rápida e intuitiva una red privada virtual basada en el popular software de código abierto OpenVPN. Al finalizar la instalación y configuración podrás crear certificados para clientes Linux, Windows, teléfonos Yealink y teléfonos SNOM.

Dependencias.

Paquete	Dependencias	Descripción
Elastix-easyvpn-0.1-5	Openvpn, easy-rsa, framework 2.4	Brinda la posibilidad de crear una red privada virtual de manera fácil.

Instalación.

Puedes descargar el addon a través del Marketplace de Elastix, desde la página de addons de su PBX o bien ejecutando el siguiente comando desde la consola de Linux como el usuario *root:*

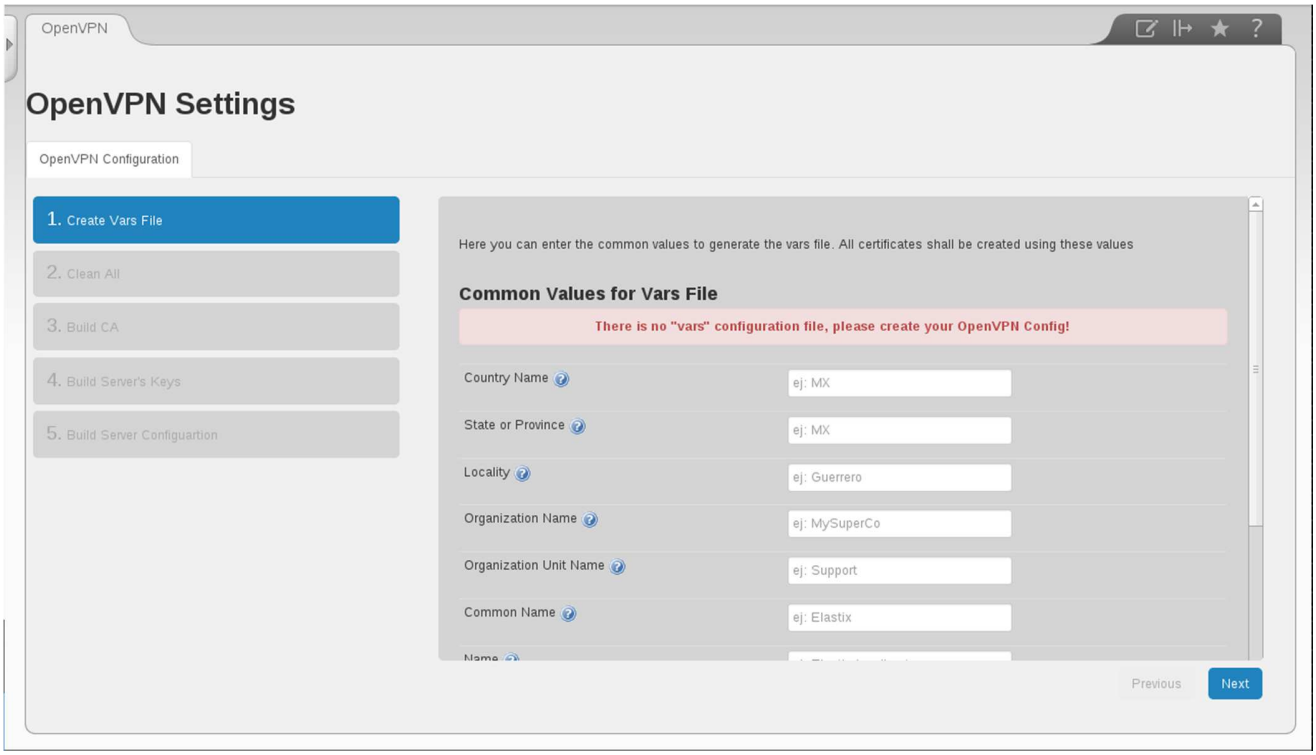
```
# yum install elastix-easyvpn
```

Configuración y uso.

Al terminar la instalación del Addon elastix-easyvpn deberás ingresar a la página web de administración de Elastix como Administrador para poder ver el módulo recién instalado, de lo contrario no serás capaz de usarlo.

La ubicación del módulo es: `Security ---> OpenVPN/Seguridad ---> OpenVPN`.

Una vez en el menú anteriormente mencionado verás una página como la siguiente:

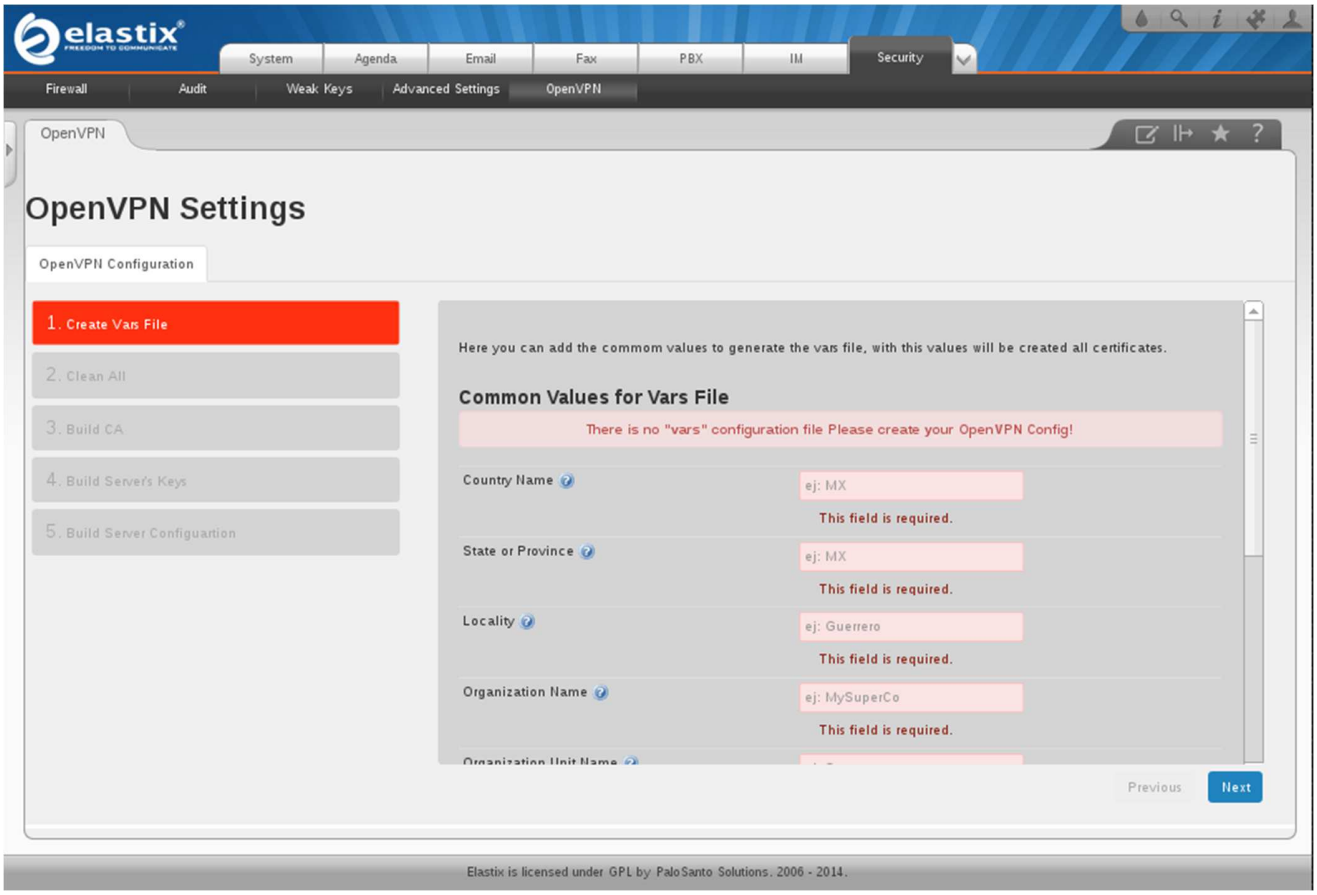


En esta sección deberás completar 5 pasos para poder iniciar el servicio de OpenVPN y poder crear certificados para los clientes que se conectarán a la VPN.

Paso 1. Creación del Archivo “Vars”.

Si estás familiarizado con la puesta en marcha del servicio de OpenVPN sabes de antemano que existe un archivo llamado vars, el cual contiene la información como: nombre del país, estado o provincia, nombre de la organización, nombre común, etcétera. Esta información será utilizada para crear los certificados tanto del cliente como del servidor.

Este paso necesita completarse para poder avanzar al paso 2. Si no completas este paso verás la página de la siguiente manera:

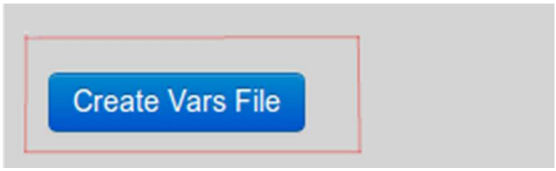


Deberás llenar los siguientes campos para poder avanzar al paso 2:

Nombre del campo	Descripción del campo	Valores de ejemplo
***Country Name* (nombre del país)**	Es el código del país donde está ubicado el servidor. Tiene una longitud de 2 caracteres y es necesario para poder generar el archivo vars. El valor que puedes usar es el nombre del país reducido a dos letras de acuerdo al RFC ISO 3166 (http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2#Officially_assigned_code_elements).	MX EU AR EC
***State or Province* (Estado o provincia)**	Es el estado o provincia donde se encuentra el servidor. Tiene una longitud de 2 caracteres.	DF TX MO

***Locality* (Localidad)**	Es el nombre de la localidad donde se encuentra el servidor. No tiene límite de longitud.	Acapulco Benito Juárez Buenos Aires
***Organization Name* (Nombre de la organización)**	Es el nombre de la organización que hospeda al servidor. Puedes usar el nombre de tu empresa para llenar este campo. No tiene límite de longitud.	Enlaza Comunicaciones Palosanto Solutions
***Organization Unit* (Departamento de la organización)**	Utiliza el nombre del departamento de tu empresa responsable del manejo de este servidor. No tiene límite de longitud.	Soporte Sistemas Seguridad
***Common Name* (Nombre común)**	Puedes usar cualquier nombre común para llenar este campo.	Elastix
***Name* (Nombre)**	Generalmente este campo se llena con el nombre del host de tu PBX. No tiene límite de longitud.	mipbx.dominio.com
***Email* (correo electrónico)**	Es el correo electrónico que se usará para registrar los certificados del servidor.	soporte@miempresa.com

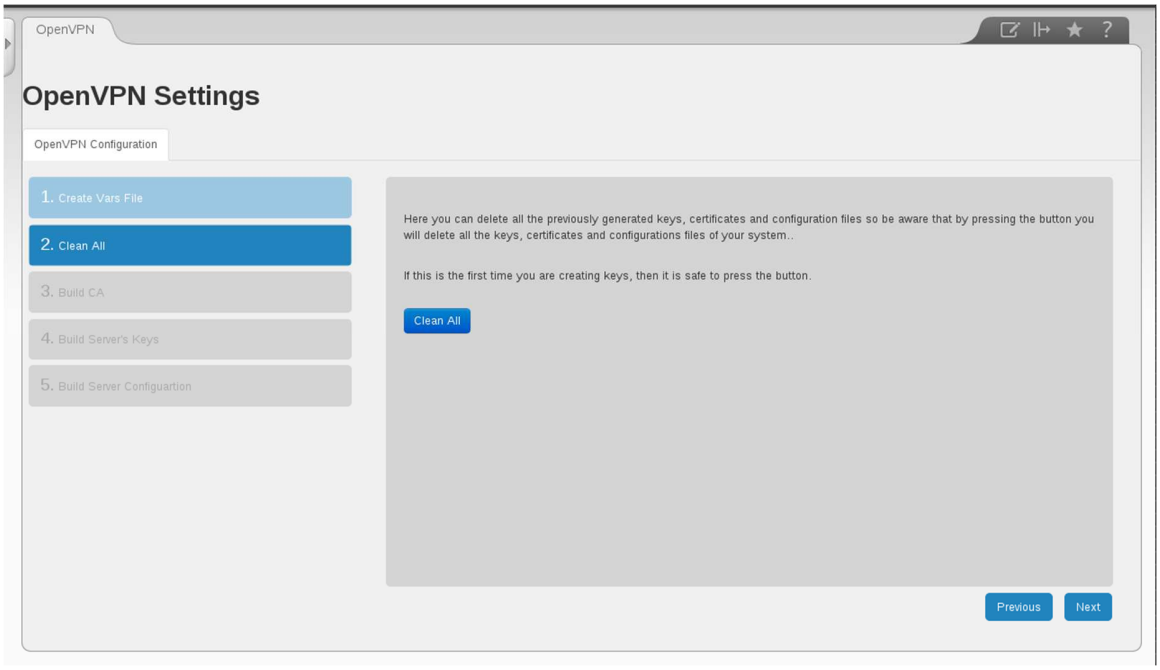
Una vez que hayas completado todos los campos deberás dar clic en el botón ***Create Vars File* (Crear archivo Vars)** para pasar al paso 2.



***Vars Exists?* (¿Existe el archivo Vars?):** Este campo de texto es un campo de sistema, no es editable. Sin embargo, es requerido para avanzar al paso 2. Este campo se llenará con la palabra *YES* (SÍ) una vez que hayas dado clic en el botón "Create vars file". Si este campo aparece vacío deberás generar de nuevo el archivo vars con la información previamente descrita.

Para ir al paso 2 presiona el botón ***Next* (Siguiente)**.

Paso 2. Limpieza de Certificados.

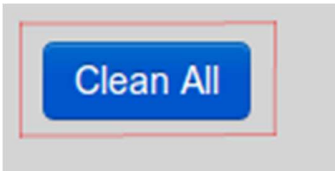


En este paso serás capaz de eliminar llaves y/o certificados previamente creados.

Si has creado previamente certificados (ya sea del servidor o de los clientes), éstos serán borrados del sistema para poder crear los nuevos. Si ésta es tu primera vez creando certificados puedes continuar de manera segura.

Los archivos eliminados son los *.pem, *.crt, *.key, dh1024.pem y las configuraciones del servidor.

Para limpiar el sistema basta con presionar el botón ***Clean All*** **(Borrar todo)**.



Para ir al Paso 3 presiona el botón ***Next*** **(Siguiente).**

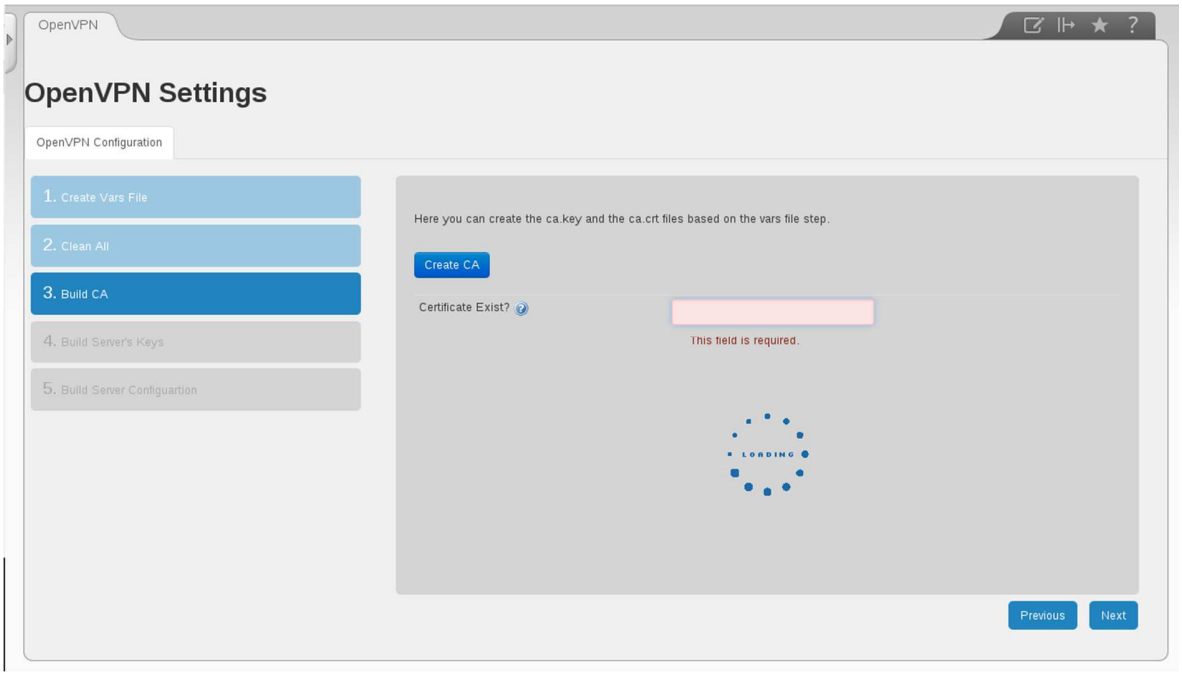
Paso 3. Creación del Certificado “ca.crt”.

En este paso serás capaz de crear el certificado ca.crt el cual es necesario para la implementación de la VPN. Bastará con que presiones el botón ***Create CA*** **(Crear CA)** para generar dicho archivo. Una vez presionado el botón verás una imagen que indica que el sistema está trabajando.

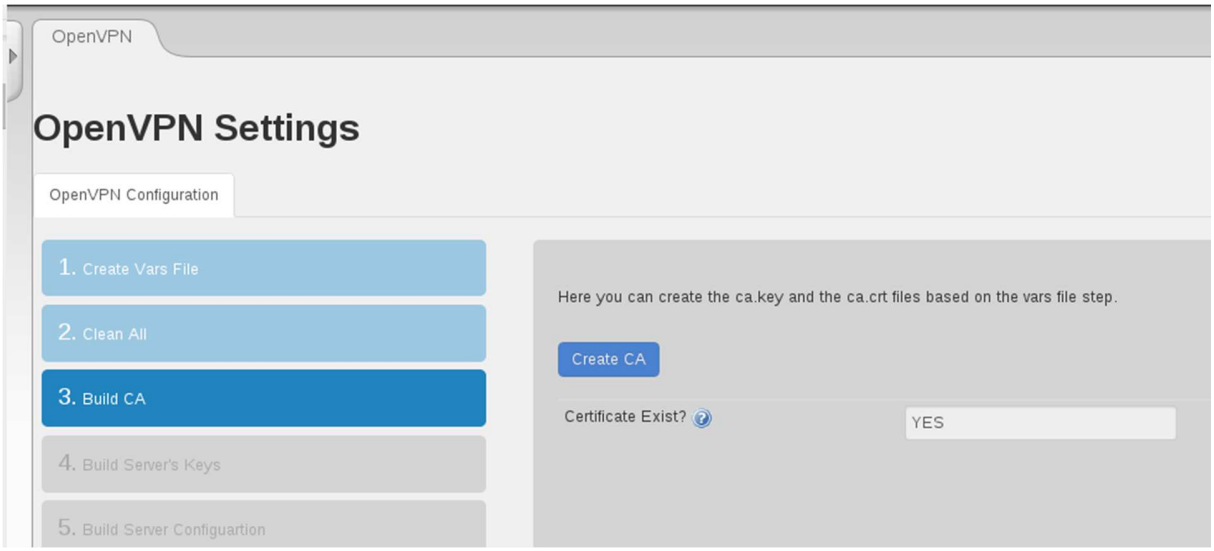
Al finalizar el proceso la imagen desaparecerá y el campo de texto ***Certificate Exist?*** **(¿Existe certificado?)** se llenará

con la palabra *YES*.

***Certificate Exist?* (¿Existe certificado?):** Este campo es un campo de sistema, no es editable pero es requerido para avanzar al paso 4. Para que el sistema llene el campo de texto presiona el botón ***Create CA* (Crear CA)**.



Cuando se haya generado el certificado, el sistema deshabilitará el botón y llenará el campo de texto de sistema, como lo muestra la siguiente imagen:



Para avanzar al paso 4 presiona el botón ***Next* (Siguiente)**.

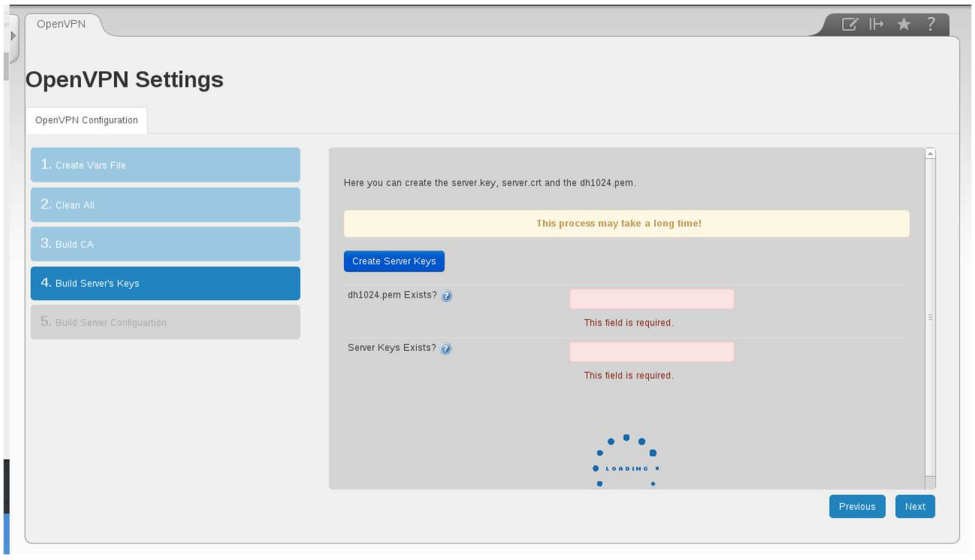
Paso 4. Creación de las llaves del servidor y el Diffie-Hellman.

En este paso crearás las llaves del servidor y el archivo Diffie-Hellman (dh1024.pem).

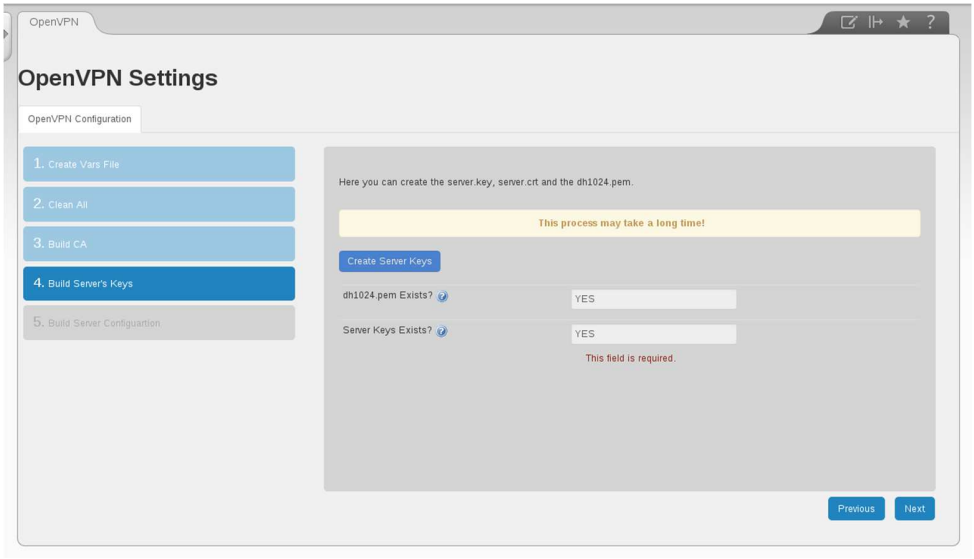
> ***dh1024.pem exists?* (¿Existe archivo dh1024.pem?)**: Este campo es un campo de sistema, no es editable pero es requerido para avanzar al paso 5. Para que el sistema llene este campo presiona el botón ***Create Server Keys* (Crear llaves del servidor)**.
>
> **Server Keys Exists? (¿Existen las llaves del servidor?):** Este campo es un campo de sistema, no es editable pero es requerido para avanzar al paso 5. Para que el sistema llene este campo presiona el botón ***Create Server Keys* (Crear llaves del servidor)**.

Al presionar el botón ***Create Server Keys* (Crear llaves del servidor)**, el sistema desplegará la imagen que indica que el sistema está trabajando en generar las llaves.

Este proceso puede tardar varios minutos dependiendo de la capacidad de su PBX. No cancele ni actualice la página mientras esté activa la imagen que despliega el sistema al presionar el botón "*Create Server Keys*".



Al finalizar el proceso, el sistema deshabilitará el botón ***Create Server Keys* (Crear llaves del servidor)** y llenará los campos de sistema con la palabra ***YES***.

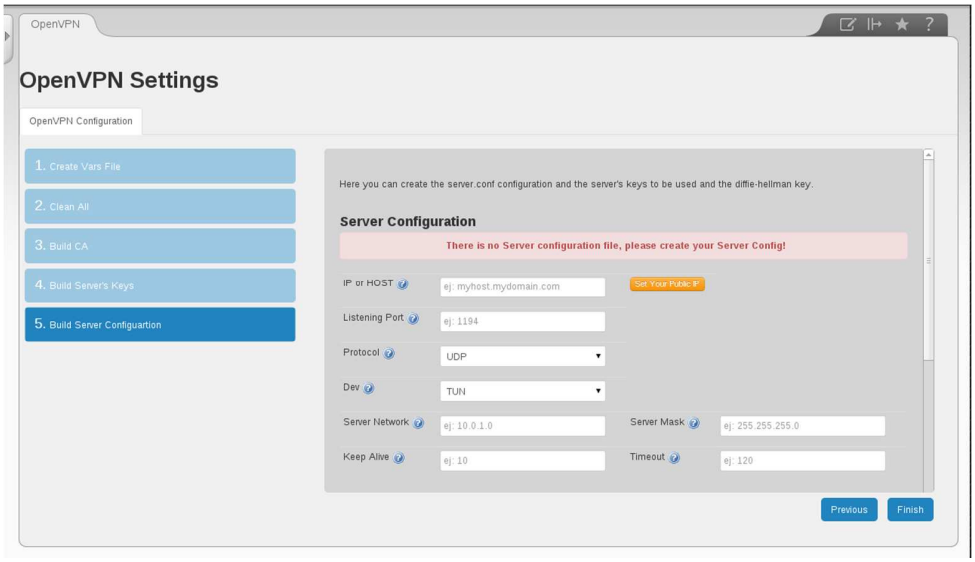


Para ir al paso 5 presiona el botón ***Next* (Siguiente)**.

Paso 5. Configuración del servidor de OpenVPN.

En este paso, serás capaz de crear las reglas de la VPN así como el segmento de RED que la VPN utilizará para crear los túneles de conexión.

Al ingresar al paso 5, verás una página como la siguiente imagen, todos los campos salvo el campo de ***Advanced settings* (Configuraciones avanzadas)** son requeridos.



A continuación se describen los campos con que deberán ser llenados en este apartado de configuración:

***IP or HOST* (IP o HOST):** Este campo no tiene límite de longitud, en éste deberás ingresar la IP (pública o privada) o el nombre del Host al que los clientes se conectarán cuando el servicio esté activo. Este campo es requerido para poder generar los certificados del cliente. Ejemplo: 192.168.1.25 (Dirección interna del servidor) o 189.70.67.09 (Dirección Pública del servidor) o CompuMundoHiperMegaRED.dynds.com.

Si deseas ingresar la IP Publica de tu servidor puedes usar el botón ***Set your public IP* (Usar la Ip Pública)** el cual automáticamente llenará este campo con la dirección pública actual.

Si deseas dar acceso remoto a otros clientes será necesario que uses una IP Pública o un Nombre de Dominio, no podrás tener acceso desde una red externa si usa una IP Privada (por ejemplo 192.168.1.1).

También es importante redireccionar el puerto establecido en la configuración de la dirección interna del servidor para tener acceso remoto, esto desde su ruteador y/o firewall.

***Listening Port* (Puerto):** Este campo no tiene límite de longitud pero espera un valor numérico válido en el rango de puertos UDP o TCP para "escuchar" las conexiones entrantes del servicio de OpenVPN. Generalmente, el valor esperado es el número de puerto 1194. Este campo es necesario para poder generar el archivo de configuración y poder crear certificados del cliente.

***Protocol* (Protocolo):** Esta lista desplegable te permitirá elegir entre el protocolo UDP y TCP para realizar la conexión de los túneles. Este campo es obligatorio y esta seleccionado el valor UDP de forma predeterminada.

Dev (Dispositivo): Esta lista desplegable te permitirá elegir entre 2 dispositivos virtuales de red TUN y TAP. TUN es conocido como un dispositivo TUNnel del Kernel del sistema y opera en la capa 3 usando paquetes IP, mientras el dispositivo TAP es un dispositivo "TAP" del Kernel del sistema y opera en la capa 2 usando tramas ETHERNET.

Este campo lo necesita el sistema para poder generar el archivo de configuración y los certificados del cliente. El valor TUN está seleccionado de forma predeterminada.

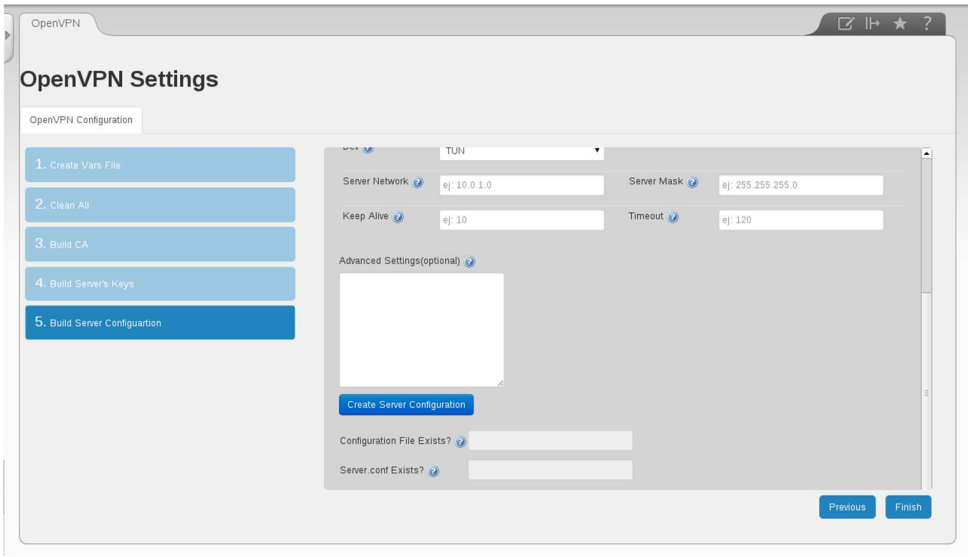
***Server Network* (Red del servidor):** Este campo es obligatorio para el sistema. Se utiliza para establecer el segmento de red que usará el sistema para hacer la conexión entre los túneles de la VPN. Podrás ingresar un segmento de RED para generar el dispositivo de red virtual de la VPN, por ejemplo, para crear un segmento de red 10.0.1.0/24 deberás ingresar el valor: 10.0.1.0.

***Server Mask* (Máscara de red):** Este campo es necesario para el sistema. Se utiliza para establecer la máscara de red que usará la red del servidor. Deberás ingresar un valor válido para el segmento de red previamente establecido, de lo contrario el servicio de OpenVPN no podrá arrancar. Usualmente se genera una máscara de 24 bits: 255.255.255.0.

***Keepalive*:** Este campo es necesario para el sistema. Se utiliza para establecer el tiempo de envío de pings hacia los clientes cada "n" segundos. Deberás ingresar un valor decimal entero para establecer este tiempo, por ejemplo, para enviar cada 10 segundos el *keepalive*, establece el número 10.

***Timeout*:** Este campo es necesario para el sistema. Se utiliza para establecer el tiempo máximo antes de marcar a un cliente como desconectado, es usado en conjunto con el valor *KeepAlive*. Deberás ingresar un valor decimal entero en este campo, por ejemplo, para marcar a un cliente como desconectado al no recibir pings de respuesta después de 140 segundos ingresa el valor 140.

***Advanced Options* (Opciones avanzadas):** Este campo es opcional. Se utiliza para ingresar configuraciones avanzadas en el servidor, deberás conocer las opciones que desees ingresar y crear a su vez las dependencias necesarias para que dichas opciones funcionen correctamente. Por ejemplo: Si deseas usar la directiva client-config-dir deberás añadirla en el área de texto además de asignar el valor y crear dicho directorio en /etc/openvpn, de lo contrario el servicio de OpenVPN no arrancará.



Una vez que hayas llenado los datos de configuración, presiona el botón ***Create Server Configuration* (Crear la configuración del servidor)** y el sistema creará el archivo de configuración y llenará los campos de sistema **Configuration File Exist** y **Server.conf Exist** con la palabra *YES*.

***Configuration File Exist?* (¿Existe el archivo de configuración?):** Este campo es un campo de sistema, no es editable pero es necesario para finalizar la configuración del sistema. Para que el sistema llene este campo es necesario haber concluido el llenado de los campos de la configuración de la VPN y presionar el botón ***Create Server Configuration* (Crear la configuración del servidor)**.

***Server.conf Exists?* (¿Existe el archivo Server.conf?):** Este campo es un campo de sistema, no es editable pero es necesario para finalizar la configuración del sistema. Para que el sistema llene este campo se debe haber concluido el llenado de los campos de la configuración de la VPN y presionar el botón ***Create Server Configuration* (Crear la configuración del servidor)**. Este campo evalúa si el archivo server.conf exist. Este archivo es el que contiene toda la información necesaria para arrancar el servicio de OpenVPN y se llena con una serie de datos predeterminados y los datos que ingresó en la parte superior.

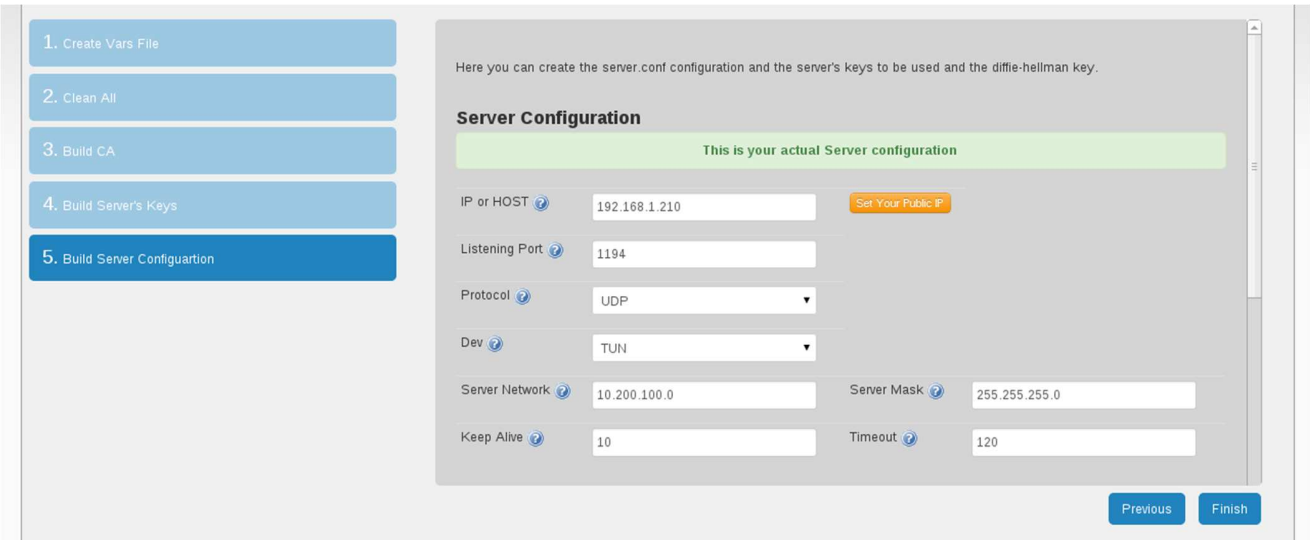
Éstos son los datos con que el archivo server.conf se crea:

```
port <ingresado por usuario>
proto <ingresado por usuario>
dev <ingresado por usuario>
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server <ingresado por usuario>
ifconfig-pool-persist ipp.txt
keepalive <ingresado por usuario>
comp-lzo
user asterisk
group asterisk
persist-key
persist-tun
status openvpn-status.log
verb 3
client-to-client
#111crl-verify /etc/openvpn/crl.pem
```

La parte ingresado por usuario se reemplazará por los datos ingresados en la página web.

La sección #111crl-verify /etc/openvpn/crl.pem será reemplazada por crl-verify /etc/openvpn/crl.pem la primera vez que revoques un certificado.

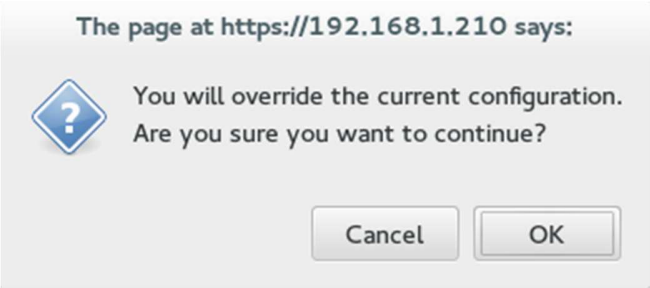
A continuación, se muestra un ejemplo de cómo se verá un archivo creado con los siguientes valores en la página web:



El archivo server.conf tendrá los siguientes datos:

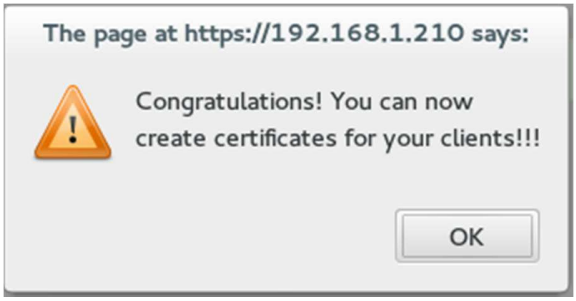
```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.200.100.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 140
comp-lzo
user asterisk
group asterisk
persist-key
persist-tun
status openvpn-status.log
verb 3
client-to-client
#111crl-verify /etc/openvpn/crl.pem
```

Cuando presionas el botón ***Create Server Configuration*** **(Crear la configuración del servidor)**, la página web enviará una alerta preguntando si deseas sobrescribir el archivo actual de configuración, si ésta es la primera vez que lo haces, da clic en aceptar para generar la configuración. Si actualmente existe un archivo de configuración, considera los efectos al sobrescribir este archivo.

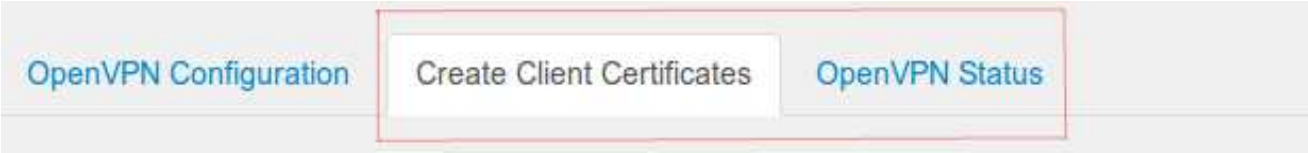


Cuando el sistema termine, verás los campos del sistema llenados con la palabra *YES*.

Para finalizar la configuración de la VPN, deberás presionar el botón ***Finish*** **(Terminar)**. Inmediatamente después aparecerá una ventana indicando que ahora puedes generar los certificados:



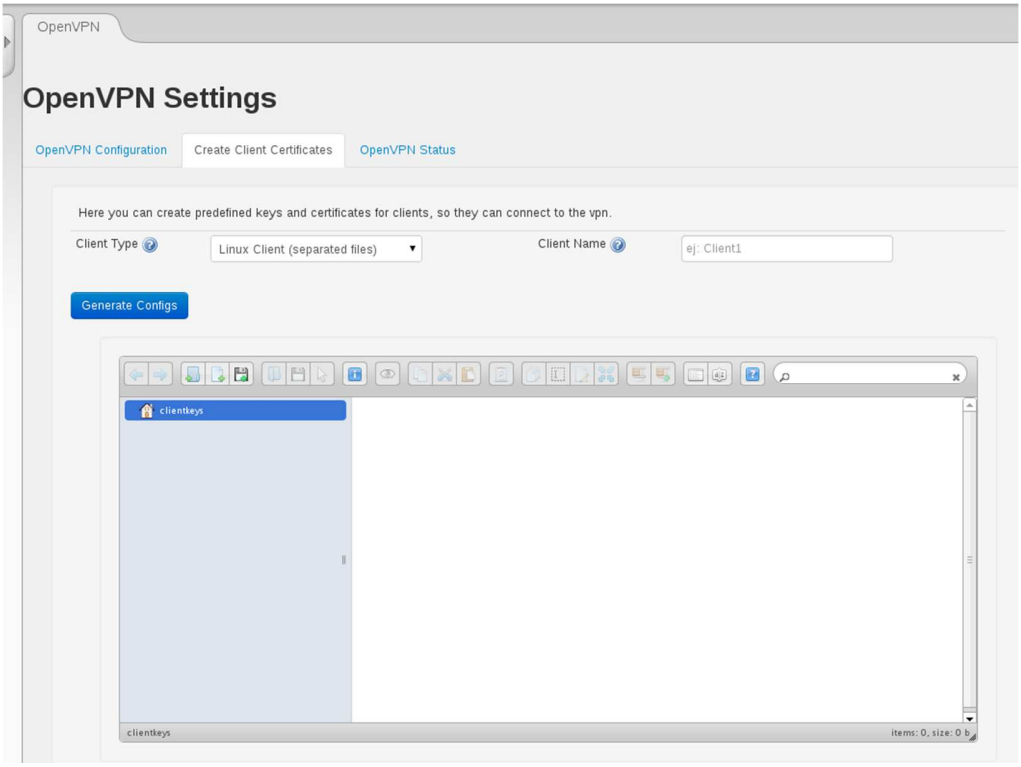
Acto seguido, la página se actualizará y aparecerán 2 nuevas pestañas:



Con estos pasos se da por concluida la configuración general del servidor de OpenVPN. La siguiente tarea es crear los certificados para los clientes (teléfonos) que se conectarán al sistema.

Creación de certificados de clientes

Al ingresar a la pestaña ***Create Client Certificates*** **(Crear certificados de cliente)** verás una página como la siguiente imagen:



En esta sección, podrás obtener certificados para diferentes tipos de cliente con el nombre que indiques, este nombre será usado por el cliente y el servidor para identificar la conexión entrante.

***Client Type* (Tipo de Cliente):** Esta lista desplegable te permite elegir el tipo de cliente y basándose en dicho tipo se generará el certificado. El sistema actualmente cuenta con estos tipos de cliente:

> ***Linux Client* (Cliente Linux):** Este tipo de cliente generará 4 archivos requeridos por los equipos con el sistema operativo Linux: ca.crt, nombre.conf, nombre.crt y nombre.key. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "Linux1" en el manejador de archivos aparecerán 4 archivos llamados: ca.crt, Linux1.conf, Linux1.crt y Linux1.key. Descarga estos archivos a tu equipo Linux para poder conectarte al servidor (El equipo cliente necesita tener instalado el servicio de OpenVPN).
>
> ***Windows Client* (Cliente Windows):** Este tipo de cliente generará 4 archivos requeridos por los equipos con el sistema operativo Windows: ca.crt, nombre.ovpn, nombre.crt y nombre.key. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "Windows1" en el manejador de archivos aparecerán 4 archivos llamados: ca.crt, Windows1.ovpn, Windows1.crt y Windows.key. Descarga estos archivos a tu equipo Windows para poder conectarte al servidor. (El equipo cliente necesita tener instalado el servicio de OpenVPN).

Yealink Phone FW < V71 [TAR] **(Cliente Teléfono Yealink firmware menor a 71):** Este tipo de cliente generará 1 archivo tipo TAR requerido por los teléfonos Yealink con una versión de Firmware menor a la 71 y generará un archivo llamado: nombre.tar. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "Yealink1", en el manejador de archivos aparecerá 1 archivo llamado: Yealink1.tar

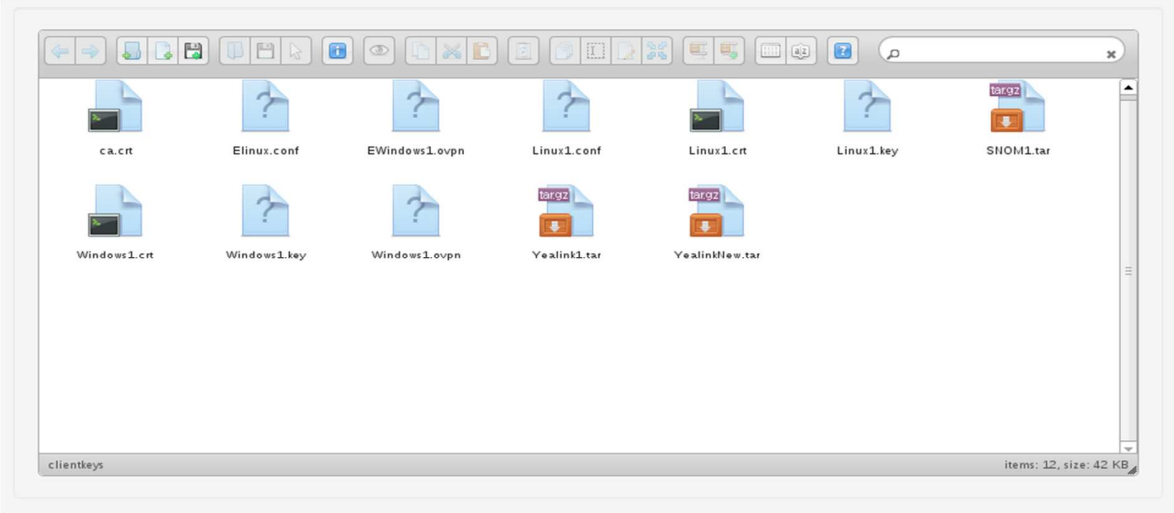
Yealink Phone FW > V71 [TAR] **(Cliente Teléfono Yealink firmware mayor a 71):** Este tipo de cliente generará 1 archivo tipo TAR requerido por los teléfonos Yealink con una versión de Firmware mayor a la 71 y generará un archivo llamado: nombre.tar. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "YealinkNew", en el manejador de archivos aparecerá 1 archivo llamado: YealinkNew.tar

SNOM Phone **[TAR] (Cliente Teléfono SNOM):** Este tipo de cliente generará 1 archivo tipo TAR requerido por los teléfonos SNOM con soporte de OpenVPN y generará un archivo llamado: nombre.tar. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "SNOM1", en el manejador de archivos aparecerá 1 archivo llamado: SNOM1.tar.

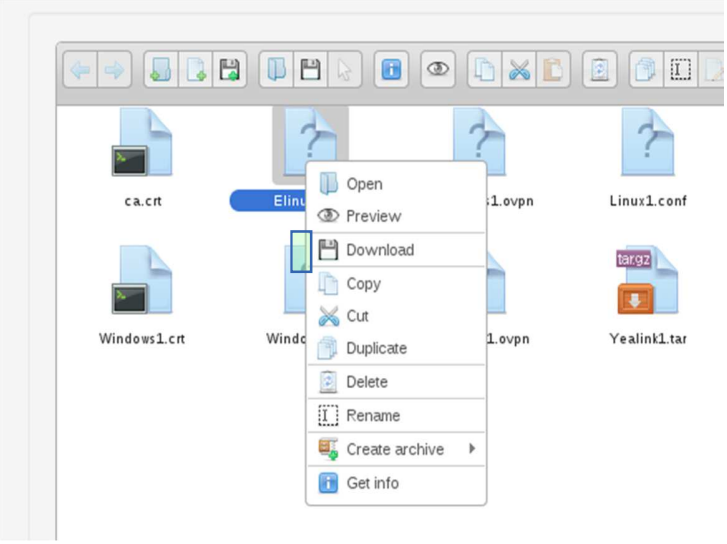
Embedded Linux Client**[One file](Cliente Linux 1 sólo archivo):** Este tipo de cliente generará 1 archivo tipo CONF requerido por el sistema operativo Linux y generará un único archivo el cual contendrá las llaves y certificados embebidos en el mismo y se llamará: nombre.conf. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "Elinux1", en el manejador de archivos aparecerá 1 archivo llamado: Elinux.conf

Embedded Windows Client[One File](Cliente Windows 1 sólo archivo): Este tipo de cliente generará 1 archivo tipo OVPN requerido por el sistema operativo Windows y generará un único archivo el cual contendrá las llaves y certificados embebidos en el mismo y se llamará: nombre.ovpn. La palabra nombre se reemplazará por el nombre elegido por el usuario antes de generar el certificado. Por ejemplo, si ingresaste el nombre "EWindows1", en el manejador de archivos aparecerá 1 archivo llamado: Ewindows1.ovpn.

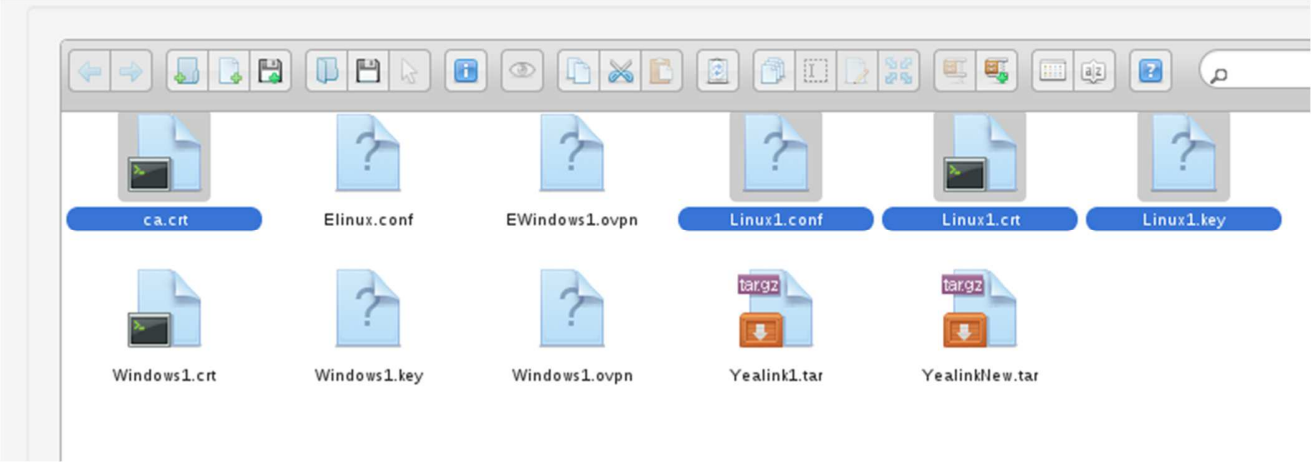
A continuación se muestra una imagen con el manejador de archivos conteniendo los archivos muestra descritos anteriormente:



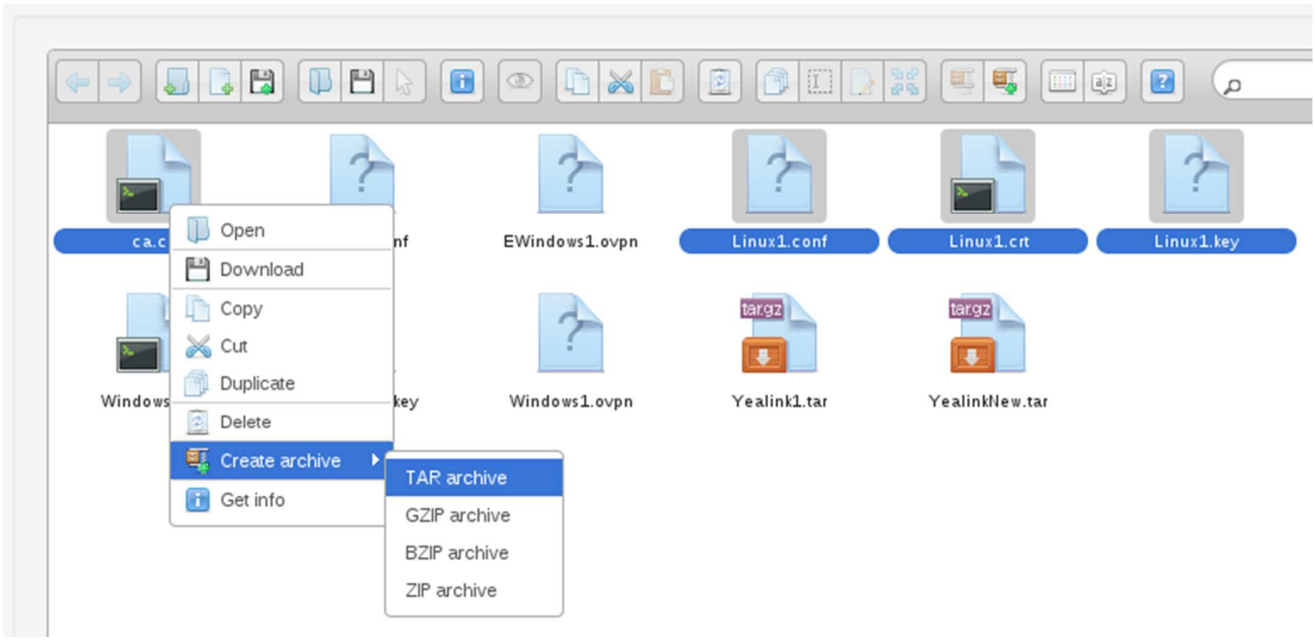
Para descargar los archivos, da clic derecho sobre el archivo deseado y selecciona la opción ***Download*** **(Descargar)**:



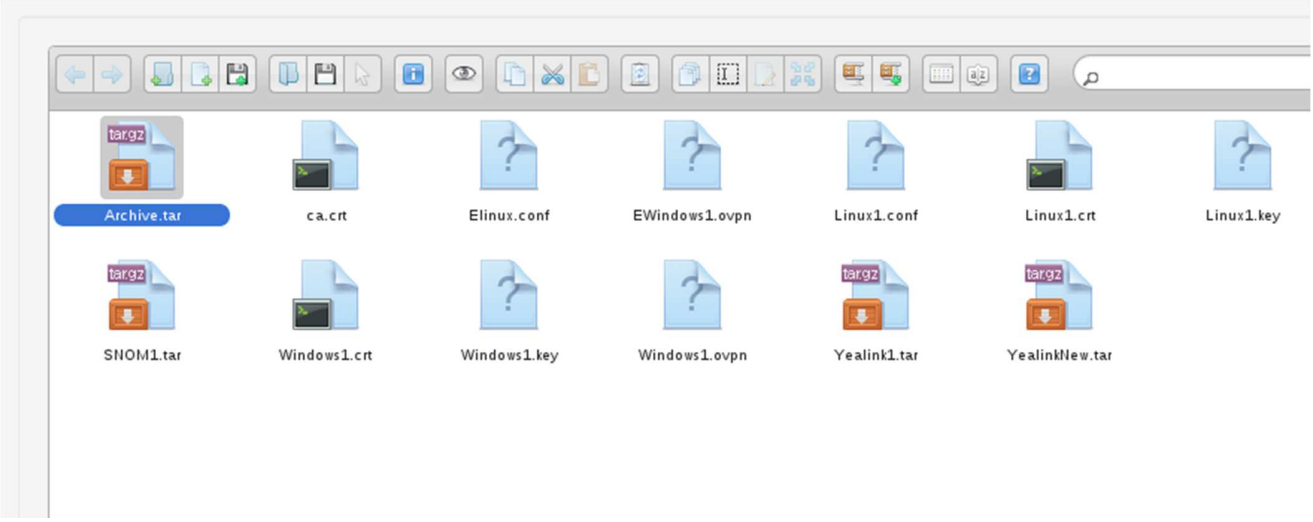
Si deseas descargar varios archivos al mismo tiempo, puedes generar un archivo ZIP, GZIP, TAR o BZIP desde el manejador de archivos. Selecciona los archivos deseados utilizando la tecla CRTL y dando clic sobre ellos:



Como siguiente paso, da clic derecho sobre uno de ellos y selecciona la opción ***Create Archive*** **(Crear Archivo)** para después seleccionar el tipo de archivo comprimido. En este ejemplo es el tipo TAR:

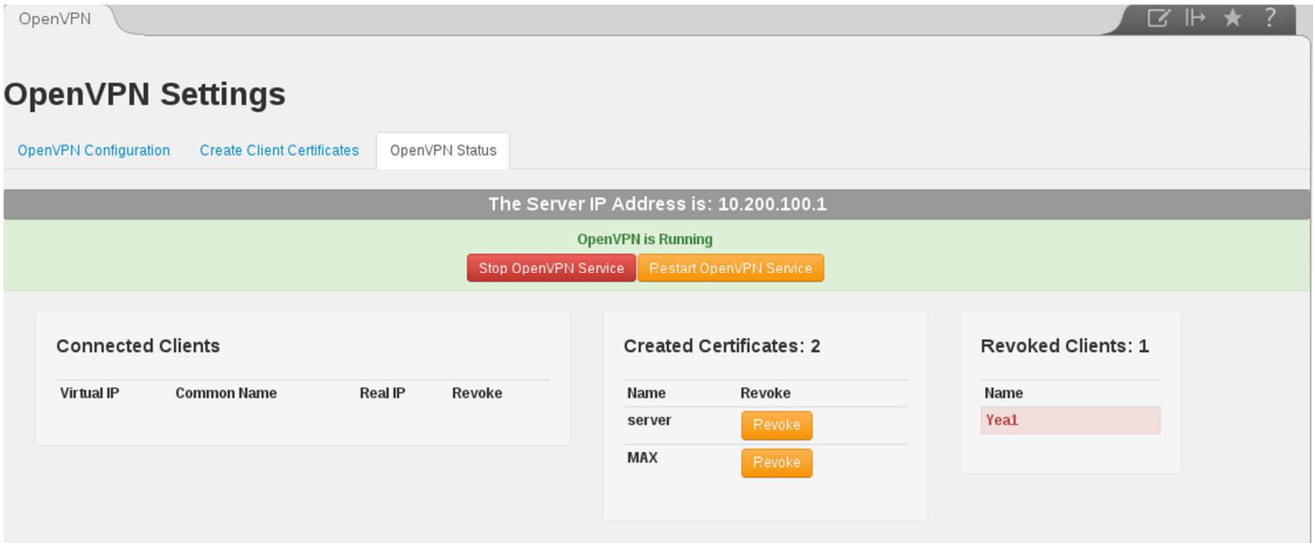


Al finalizar el proceso, encontrarás un archivo llamado: Archive.tar.

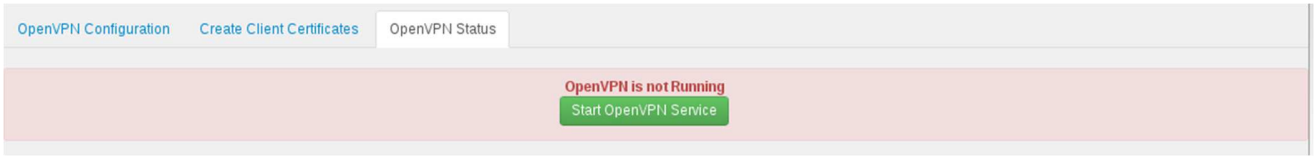


Estado de la VPN.

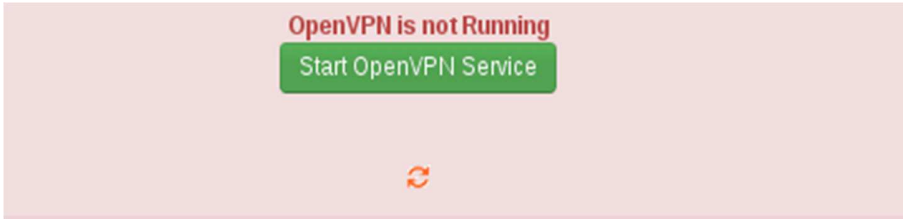
En la pestaña llamada ***OpenVPN Status*** **(Estado OpenVPN)** encontrarás en tiempo real la lista de los clientes conectados al servidor, la lista de todos los certificados creados y la lista de los certificados revocados, así como los botones para iniciar, reiniciar y detener el servicio de OpenVPN.



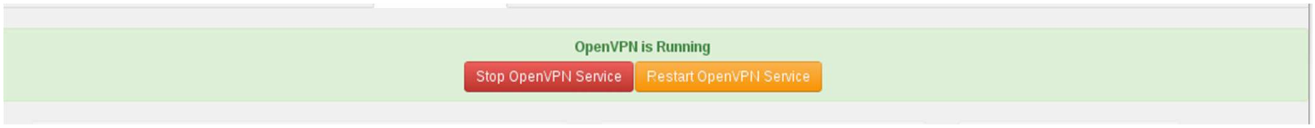
La primera vez que se instala el Addon OpenVPN aparece como que no está en servicio de forma predeterminada, por lo que verás la siguiente imagen:



Para iniciar el servicio deberás presionar el botón llamado ***Start OpenVPN Service*** **(Iniciar el Servicio de OpenVPN)**. El sistema mostrará la siguiente imagen:



Al terminar, el sistema recargará la página y estarás de nueva cuenta en la pestaña de creación de certificados. Da clic en la pestaña de Estado de la VPN y verás la siguiente imagen:

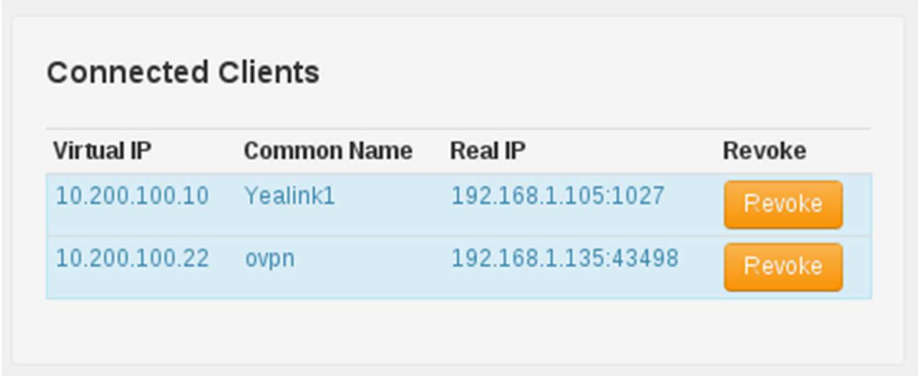


Ahora podrás detener o reiniciar el servicio de la VPN desde esta misma pestaña.

Clientes Conectados.

En la sección de clientes conectados verás la lista de todos los clientes conectados en ese momento al servidor, al iniciar el servicio de OpenVPN es muy probable que sólo veas:

Cuando inicies el servicio de OpenVPN y tus clientes estén conectados, verás una imagen como la siguiente:



Donde encontrarás la siguiente información:

***Virtual IP*(IP Virtual):** Es la IP que el servidor asigna al cliente usando como referencia el campo de la RED asignada en el último paso de la configuración de la VPN.

***Common Name* (Nombre):** Es el nombre con el cual se creó el certificado y, a su vez, es el identificador del equipo cliente.

***Real IP* (IP Real):** Es la IP desde donde el cliente se conecta y puede ser una IP privada o pública.

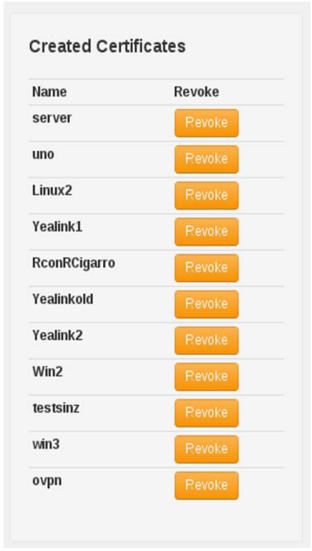
***Revoke* (Revocar):** Este botón te permitirá revocar el certificado de dicho cliente. La revocación consiste en bloquear el acceso al servidor de OpenVPN para el certificado señalado. Cada que revoques un certificado deberás reiniciar el servicio de OpenVPN.

El proceso de revocación no se puede revertir. Una vez revocado el certificado no podrás volver a conectarte con ese certificado y deberás generar otro para poder conectarte; además de que este proceso elimina el certificado revocado.

La revocación del certificado no desconecta al cliente del servidor inmediatamente, tendrás que reiniciar el equipo o esperar a que el sistema lo marque como inválido.

Lista de Certificados Creados.

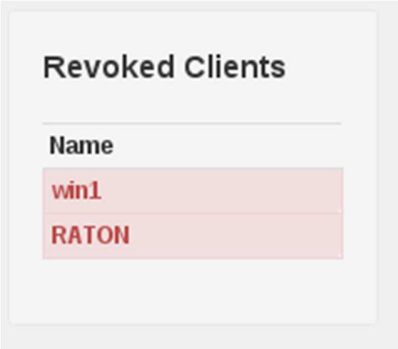
La sección de Certificados credos muestra la lista de todos los certificados creados en el servidor, incluyendo el certificado del servidor. Verás una imagen similar a:



Donde la primera columna refleja el nombre del certificado creado y la segunda columna muestra el botón para revocar el certificado.

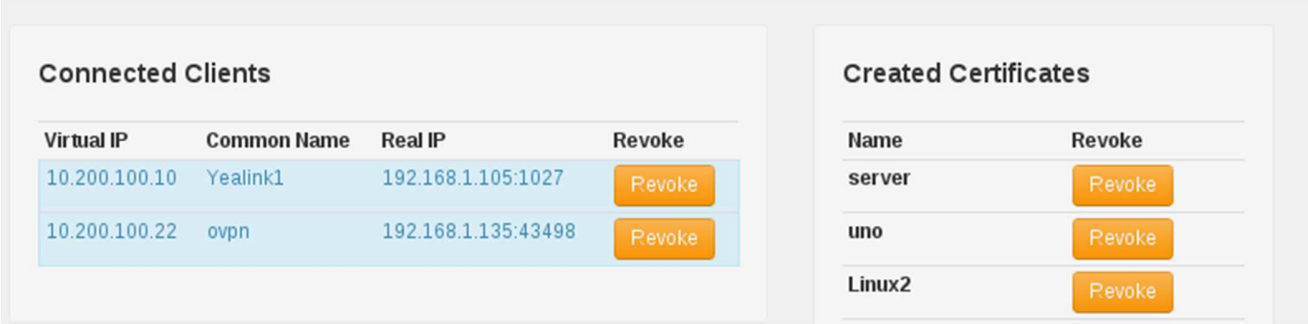
Certificados Revocados.

La sección de Clientes revocados mostrará una lista con todos los certificados que han sido revocados por el administrador y verás una imagen similar a:

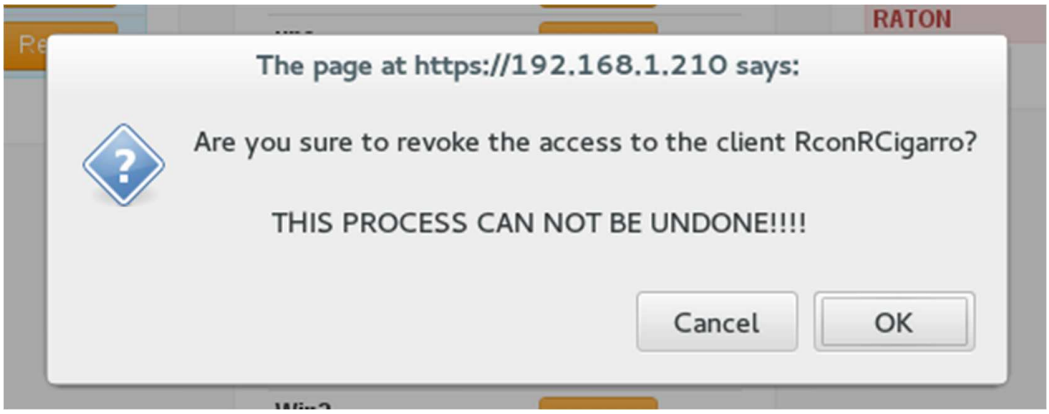


Revocación de Certificados.

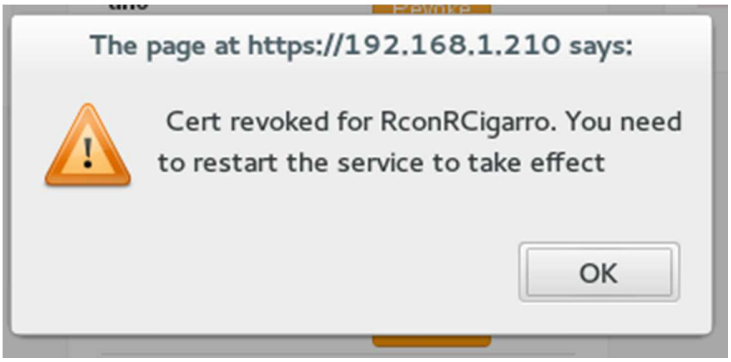
El proceso de revocación de certificados es muy sencillo. Basta con presionar el botón llamado ***Revoke*** **(Revocar)** desde la sección de clientes conectados o desde la sección de certificados creados.



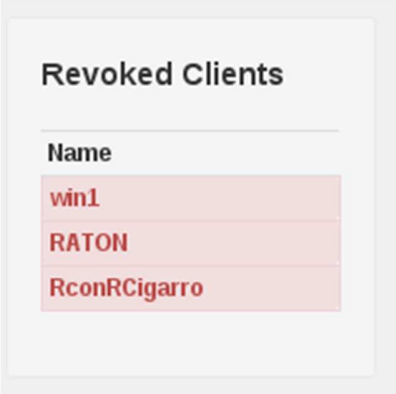
Cuando presionas el botón revocar sobre del cliente deseado, verás una alerta como está:



Está alerta pregunta si estás seguro de realizar el proceso de revocación ya que no se puede revertir en un futuro. Si eliges la opción ***OK*** **(Confirmar)**, verás una nueva alerta como la siguiente:



La cual te indica que el certificado ha sido revocado y para que este cambio tenga efecto deberás reiniciar el servicio de OpenVPN. Segundos después, la página se actualizará y el certificado revocado aparecerá en la lista de certificados revocados:



El proceso de revocación no se puede revertir una vez revocado el certificado. No podrás volver a conectarte con ese certificado y deberás generar otro certificado para poder conectarte; además de que este proceso elimina el certificado revocado.

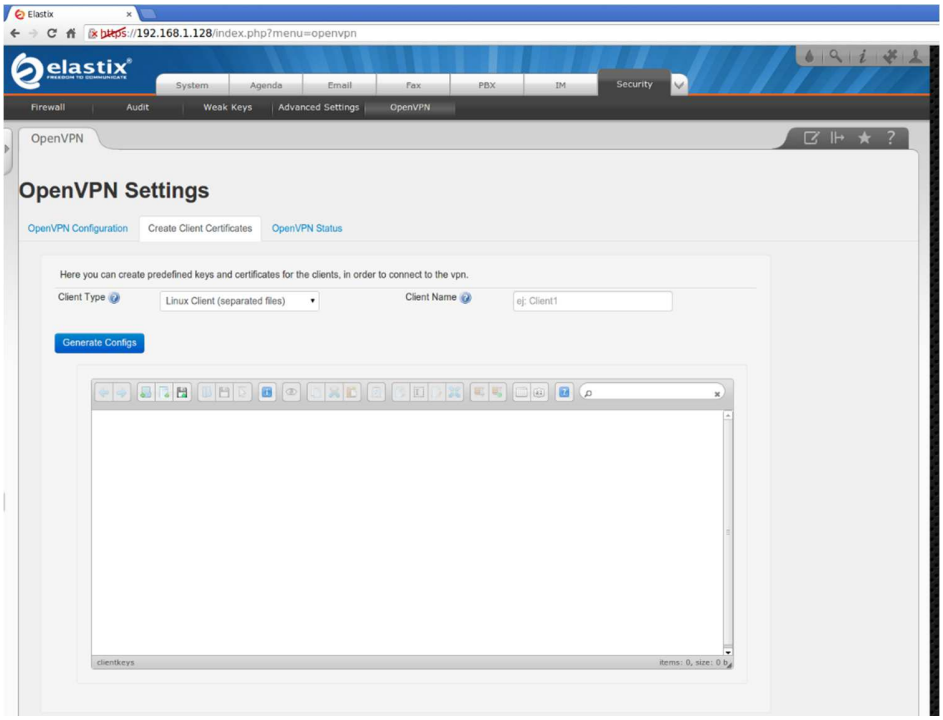
La revocación del certificado no desconecta al cliente del servidor. Tendrás que reiniciar el equipo o esperar a que el sistema lo marque como inválido.

Recuerda reiniciar el servicio de OpenVPN para que estos cambios tengan efecto.

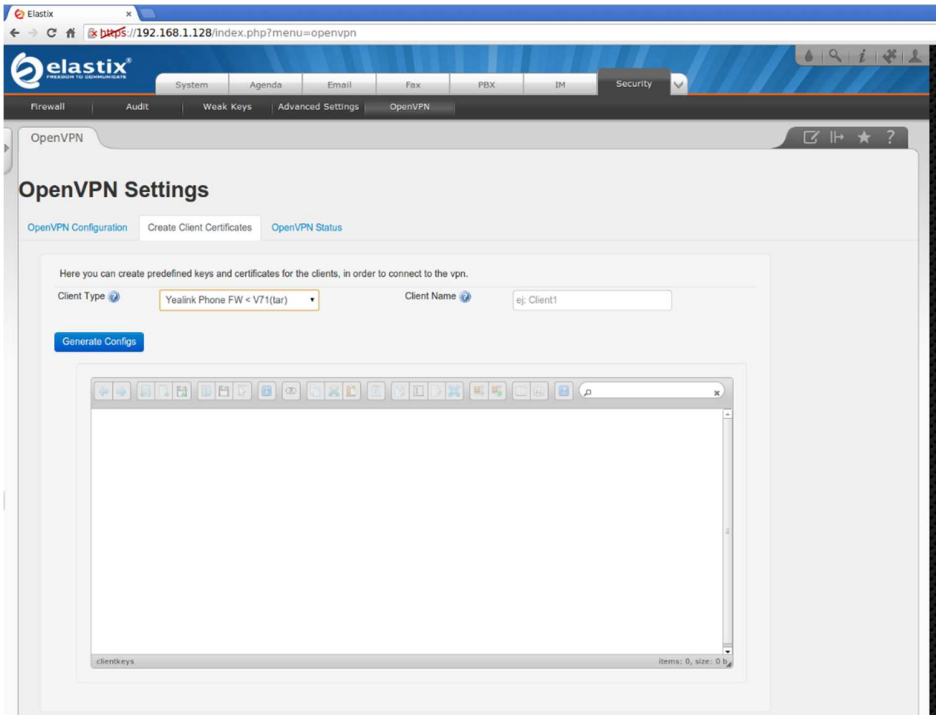
Instalación de certificados

Instalación de Certificado en teléfonos Yealink.

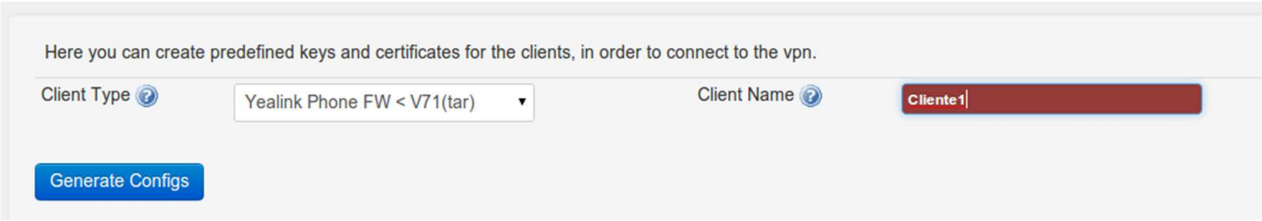
A continuación se describe el proceso para instalar un certificado de OpenVPN en los teléfonos Yealink.



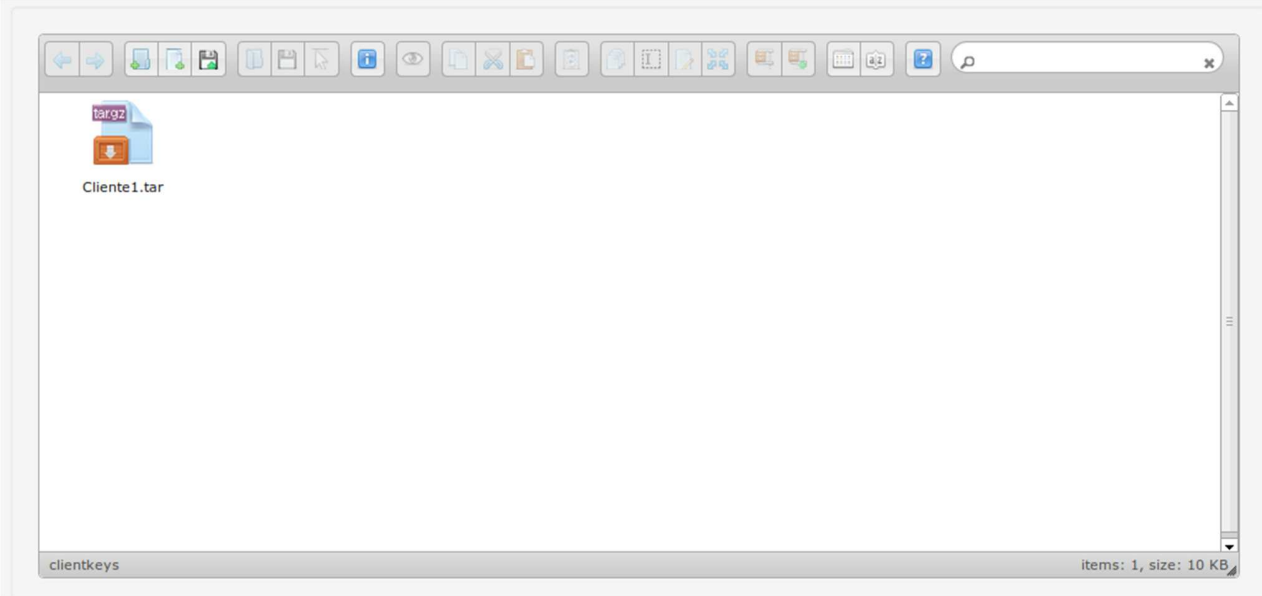
Ve a la pestaña con nombre ***Create Client Certificates*** **(Crear Certificados de Cliente)**. De la lista desplegable, elige la opción de **Yealink Phone FW (Teléfono Yealink)** (Dependiendo de la versión de firmware de tu teléfono, elige mayor o menor a V71.).



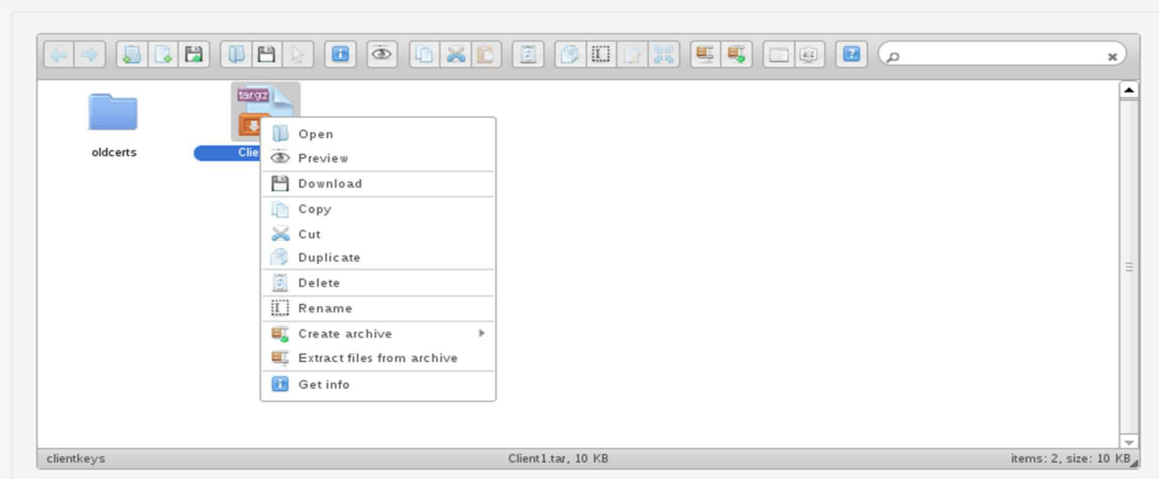
Elige un nombre para el certificado. En este ejemplo usaremos el nombre: Cliente1 y presiona el botón ***Generate Configs*** **(Generar configuraciones)**:



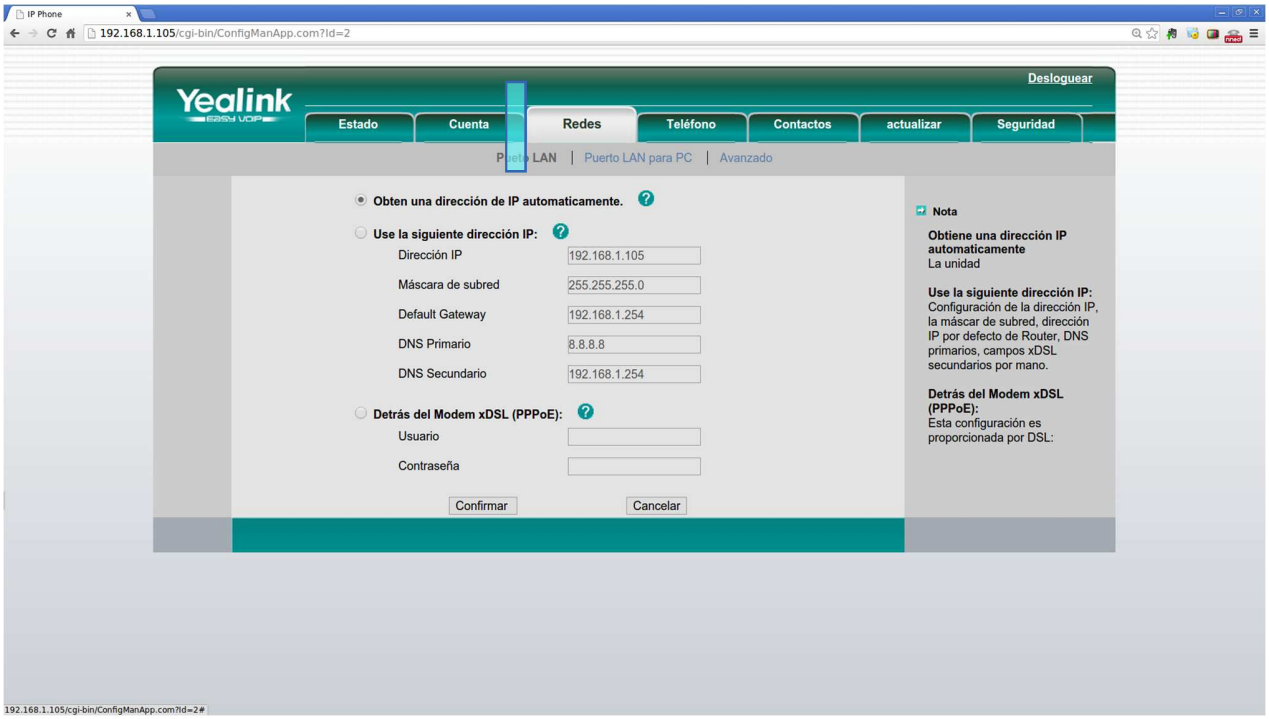
Después de presionar el botón, el sistema generará un archivo comprimido tipo TAR con el nombre elegido. En este ejemplo: Cliente1.tar



Descarga el archivo a tu ordenador para poder usarlo con el teléfono Yealink, selecciona el archivo, da clic derecho sobre él y escoge la opción ***Download*** **(Descargar)**.

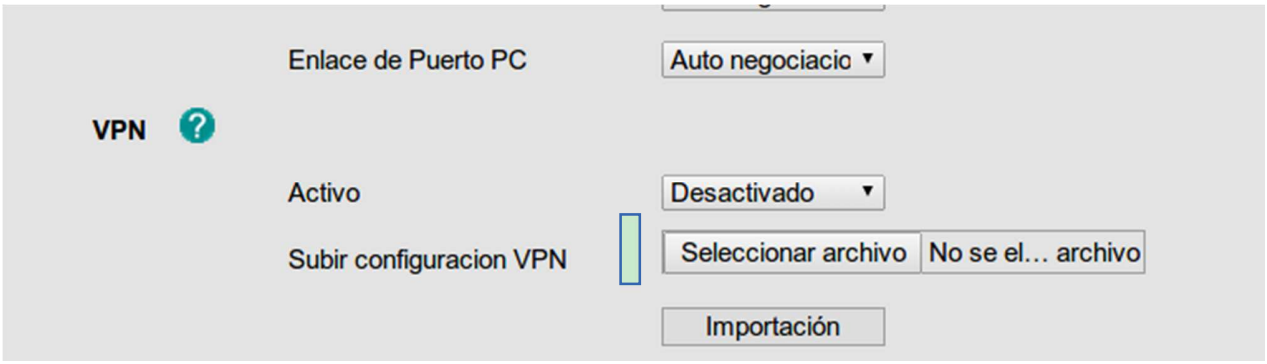


Ingresa a la página de administración del teléfono Yealink y ve a la sección REDES.

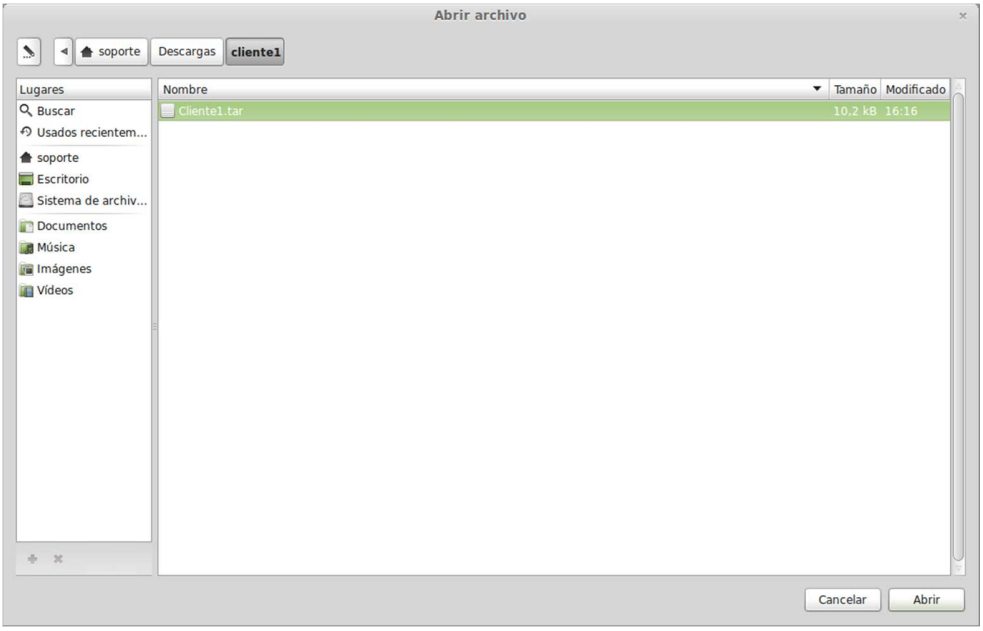


Selecciona el submenú Avanzado.

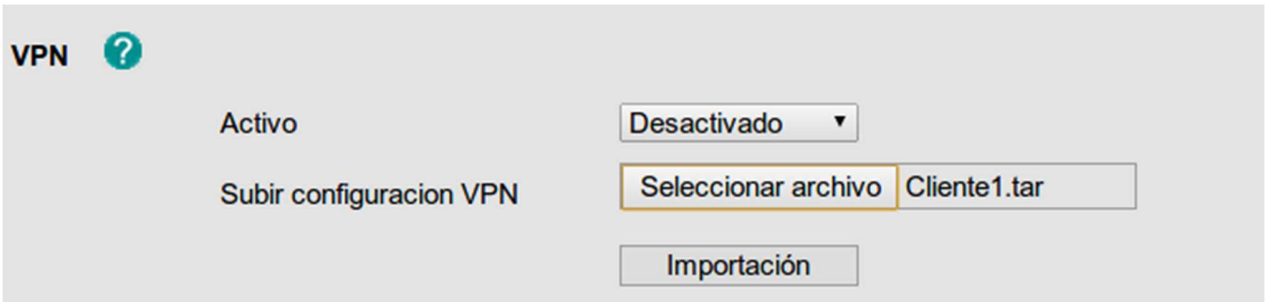
Ve a la sección de VPN y elige seleccionar archivo:



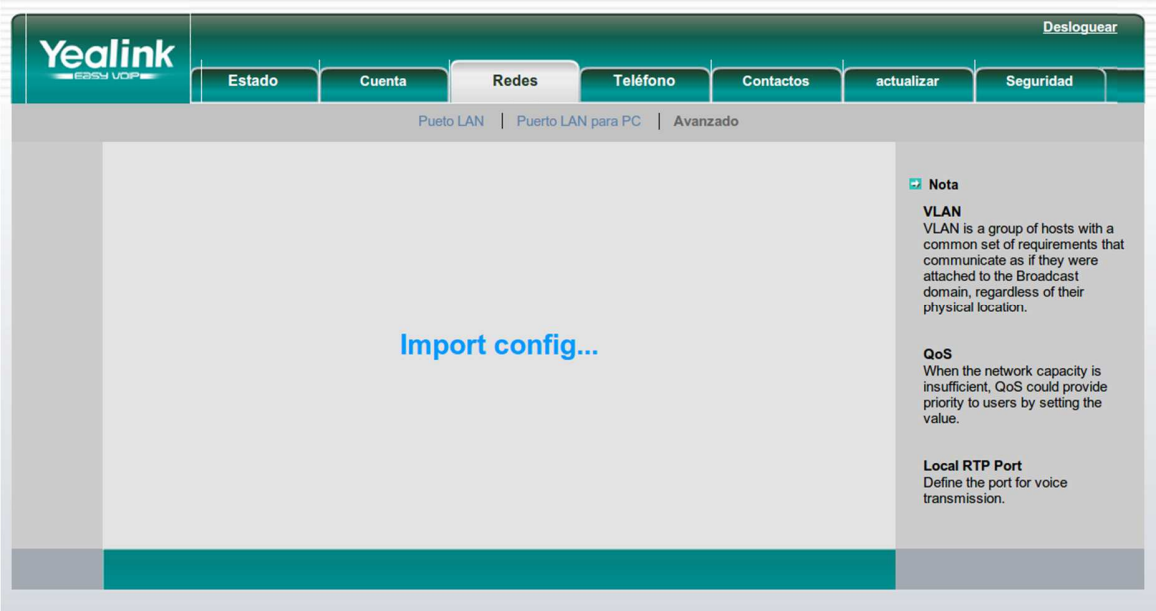
En la ventana que se abrirá, busca el archivo Cliente1.tar recién descargado, selecciónalo y da clic en Abrir:



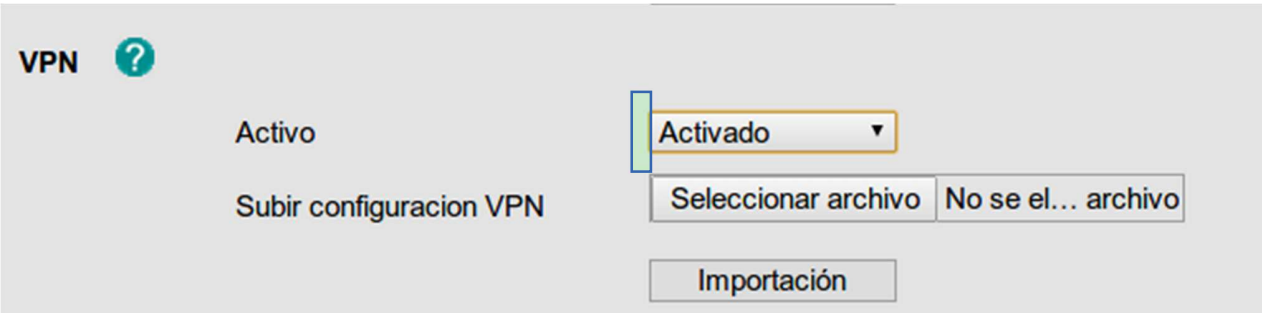
A continuación, da clic en el botón Importación:



El teléfono empezará a importar el archivo comprimido:

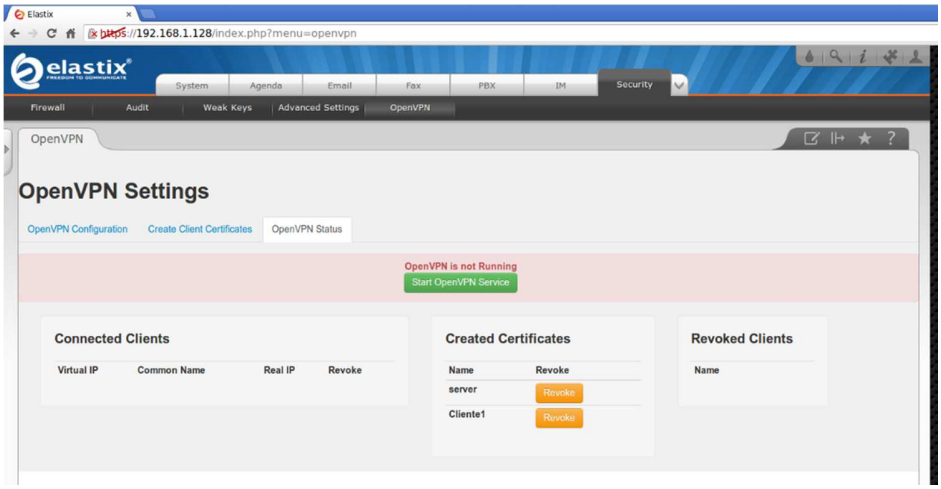


Al finalizar, asegúrate de que el servicio de VPN esté Activado:

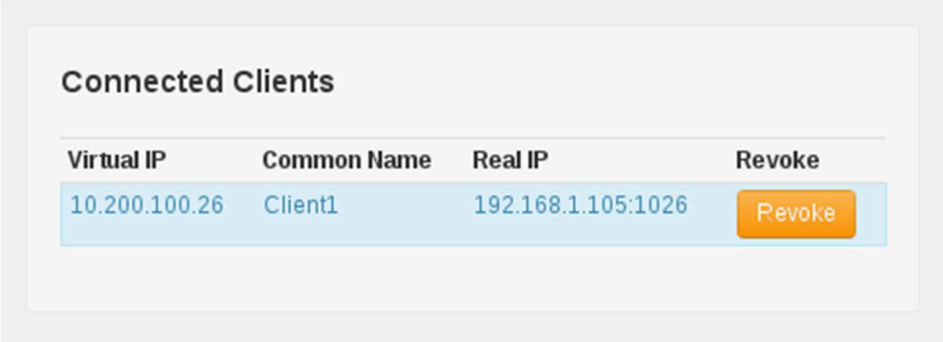


Finalmente, da clic en Guardar Cambios. El teléfono preguntará sobre el reinicio del mismo, acepta y espera a que el teléfono inicie de nuevo.

Ve a la página de tu Elastix, ingresa como administrador, ve al menú Seguridad--->OpenVPN y después a la pestaña OpenVPN Status.

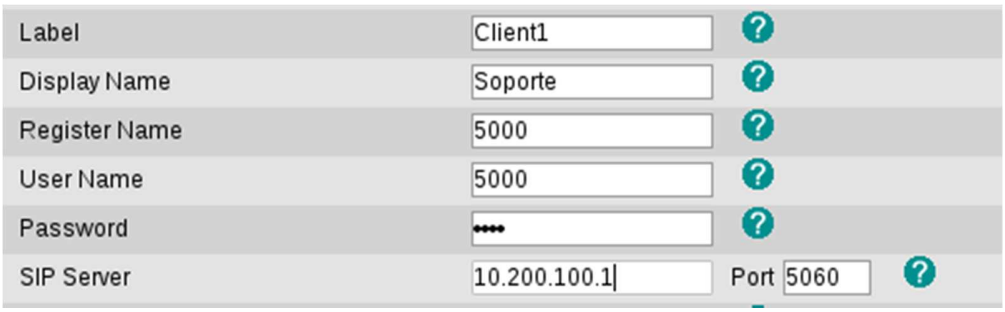


Si no ha arrancado tu servicio de OpenVPN de clic en el botón **Start OpenVPN Service (Arrancar el servicio de OpenVPN)**. Al finalizar, después de un tiempo no mayor a 5 minutos el teléfono se debe ver conectado al servidor como se muestra en la siguiente pantalla:



Y el teléfono deberá mostrar en la pantalla de cristal líquido la palabra VPN:

Ingresa de nuevo en la página de administración de tu teléfono Yealink, ve a la sección de Cuentas, ingresa los datos de la cuenta SIP y apunta a la dirección de la VPN del servidor. Aplica los cambios y usa tu teléfono a través de su VPN.



Instalación del Certificado en plataformas Linux.

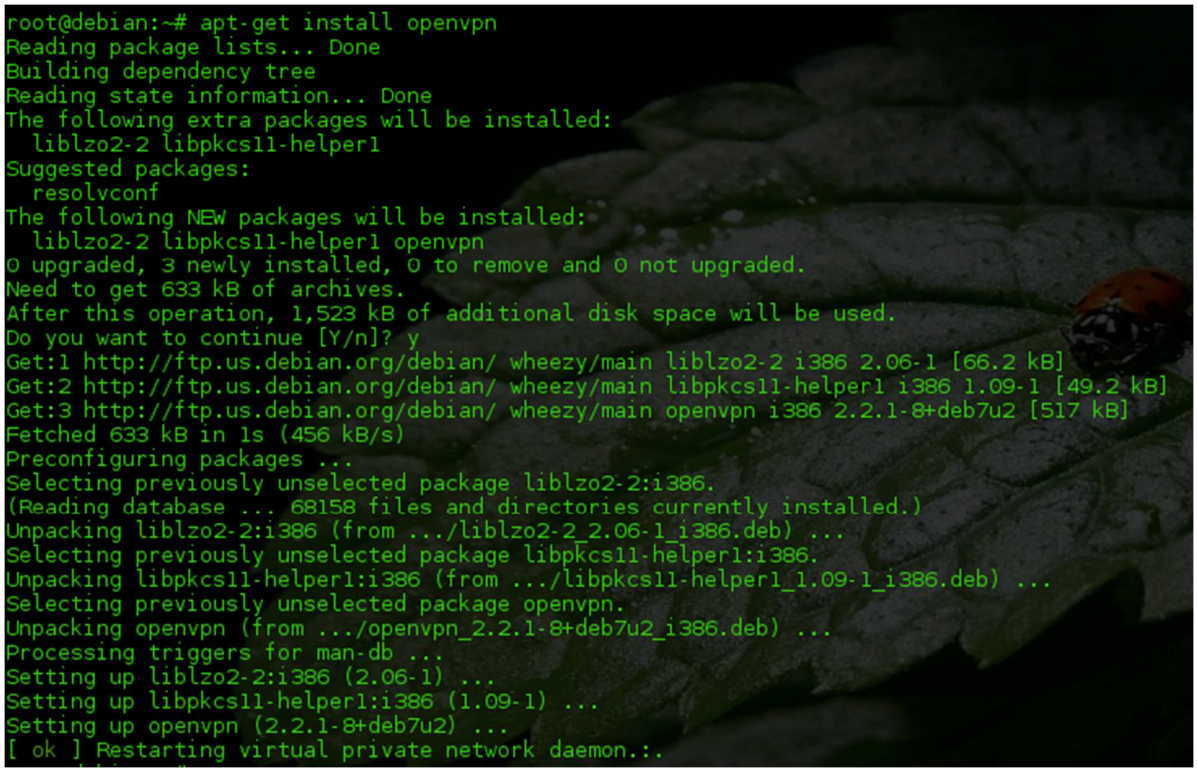
A continuación se describe el proceso para instalar el certificado en plataformas Linux.

Instala el servicio de OpenVPN en tu equipo, en este caso, el ejemplo está desarrollado en Debian por lo que el comando a ejecutar es:

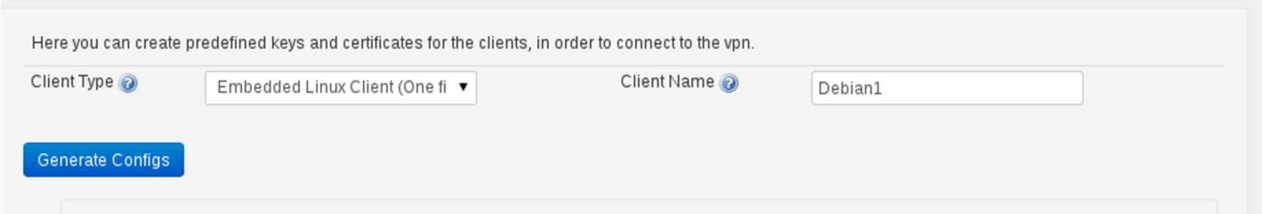
```
# apt-get install openvpn
```

Para CentOS o Fedora puedes usar el comando:

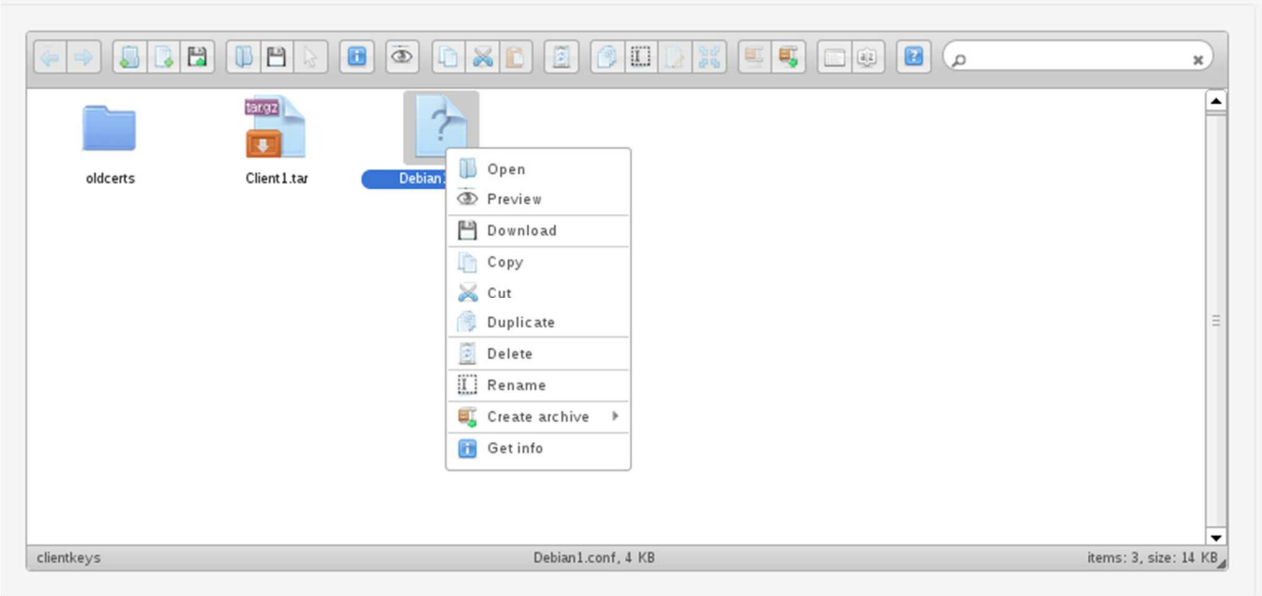
```
# yum install openvpn
```



Ve a la página web de Elastix, ingresa como administrador y ve al menú Seguridad-->OpenVPN. Selecciona el tipo de cliente como *Embedded Linux Client* (Cliente Linux Embebido), asigna el nombre del certificado y da clic en el botón *Generate Configs* (Generar Configuraciones):



Al finalizar el proceso, verás un archivo .conf en el manejador de archivo, para este ejemplo será Debian1.conf, descarga el archivo y cópialo a tu máquina.



Para copiar el archivo, puedes usar scp en Linux o bien un programa como WinSCP o pscp en Windows.

Cuando el archivo .conf esté en la máquina Linux final, copia el archivo al directorio /etc/openvpn

```
# cp Debian1.conf /etc/openvpn
```

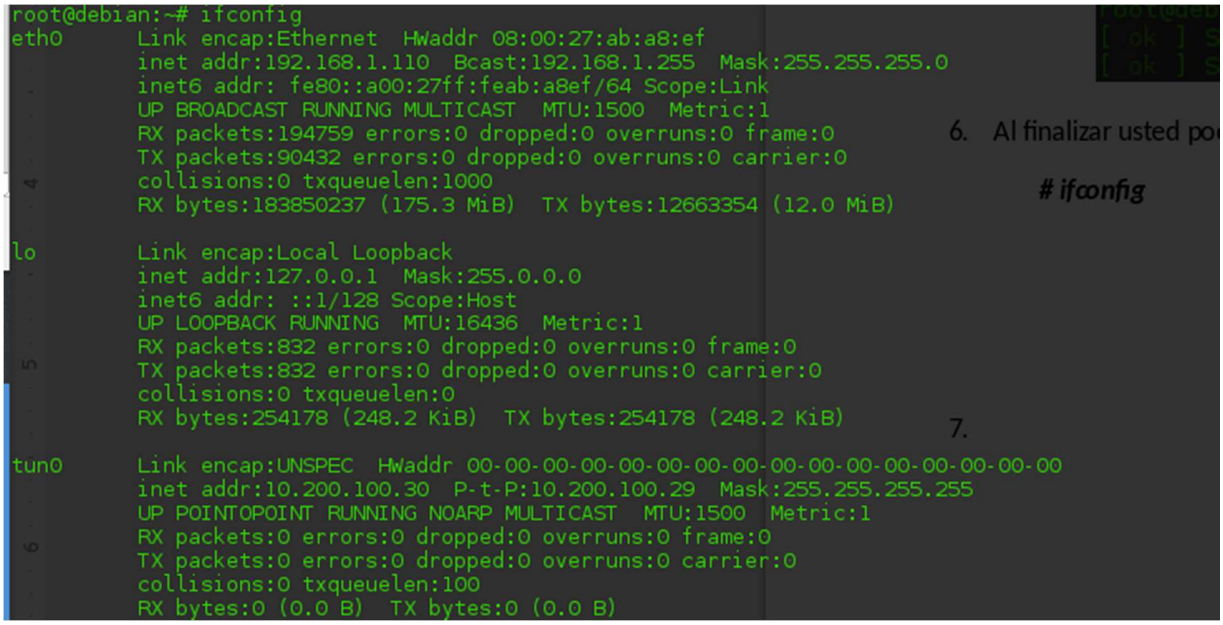
Reinicia el servicio de OpenVPN con el siguiente comando:

```
# /etc/init.d/openvpn restart
```

```
root@debian:~# /etc/init.d/openvpn restart
[ ok ] Stopping virtual private network daemon:.
[ ok ] Starting virtual private network daemon: Debian1.
```

Al finalizar, podrás verificar si se estableció la conexión con el servidor mediante el comando:

```
# ifconfig
```



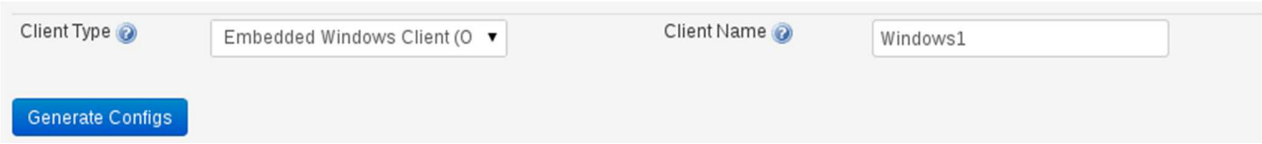
Ahora en la pestaña de *OpenVPN Status* (Estado de la VPN) en la página de Elastix verás al cliente conectado:

Instalación del Certificado en Plataformas Windows.

A continuación se describe el proceso para instalar el certificado en plataformas Windows.

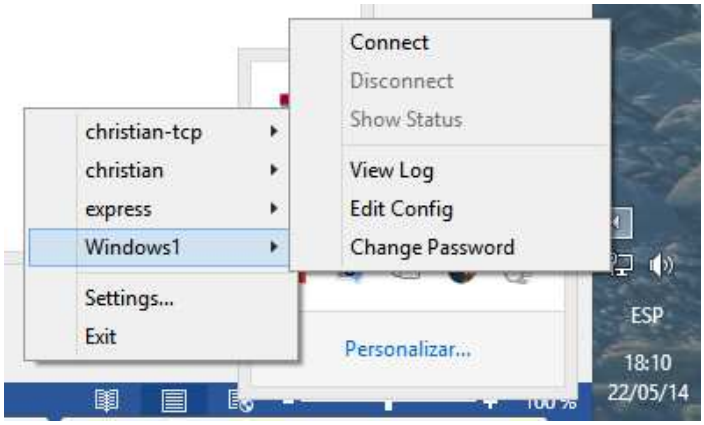
Instala el programa de OpenVPN en tu equipo Windows. Puedes descargar el ejecutable desde el enlace: http://openvpn.net/index.php/download/community-downloads.html

Ve a la página web de Elastix, ingresa como administrador y ve al menú Seguridad-->OpenVPN. Selecciona el tipo de cliente como *Embedded Windows Client* (Cliente Windows Embebido), asigna el nombre del certificado y da clic en el botón *Generate Configs* (Generar Configuraciones):

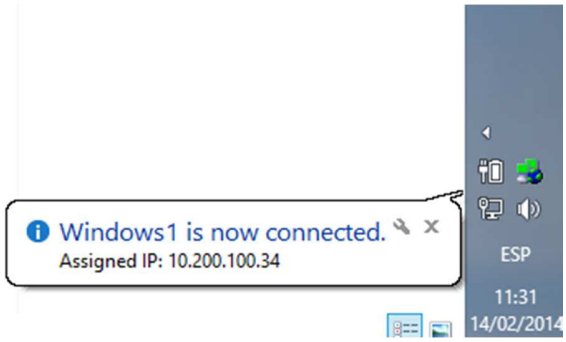


Descarga el archivo a la dirección C:/Archivos de Programa/openvpn/config.

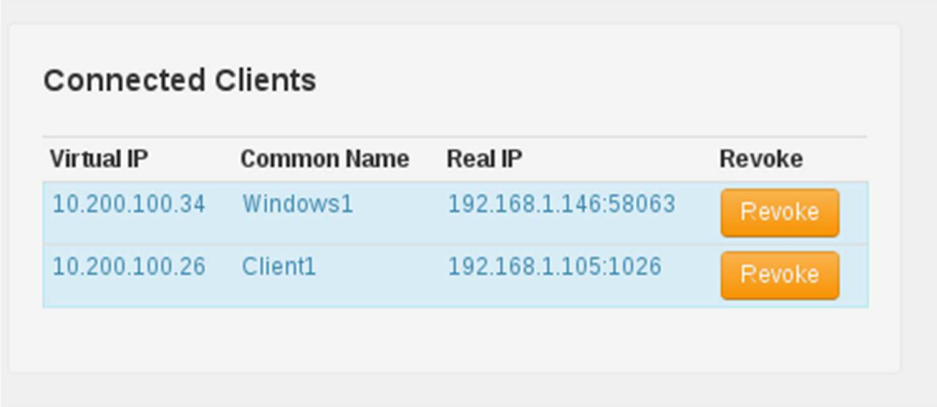
Abre el programa OPENVPN-GUI, da clic derecho sobre el icono y selecciona el nombre del certificado creado. A continuación, da clic en conectar:



Inmediatamente verás la notificación de conectado con la IP asignada:



Y en la página de *OpenVPN Status* (Estado de la VPN) verás al cliente conectado:


Connected Clients
Virtual IP
Common Name
Real IP
Revoke
10.200.100.34
Windows1
192.168.1.146:58063
Revoke
10.200.100.26
Client1
192.168.1.105:1026
Revoke