

VPN VS. TÚNEL SSH: ¿CUÁL ES MÁS SEGURO?

Las VPN y los túneles SSH pueden "tunelizar" el tráfico de red de forma segura a través de una conexión cifrada. Son similares en algunos aspectos, pero diferentes en otros.

Un túnel SSH a menudo se denomina "VPN para pobres" porque puede proporcionar algunas de las mismas funciones que una VPN sin el proceso de configuración del servidor más complicado; sin embargo, tiene algunas limitaciones.

CÓMO FUNCIONA UN TÚNEL SSH

SSH, que significa "shell seguro", no está diseñado únicamente para reenviar tráfico de red. Generalmente, SSH se utiliza para adquirir y utilizar de forma segura una sesión de terminal remota, pero **SSH tiene otros usos**. SSH también utiliza un cifrado sólido y puede configurar su cliente SSH para que actúe como un proxy SOCKS. Una vez que lo haya hecho, puede configurar aplicaciones en su computadora, como su navegador web, para usar el proxy SOCKS. El tráfico ingresa al proxy SOCKS que se ejecuta en su sistema local y el cliente SSH lo reenvía a través de la conexión SSH; esto se conoce como tunelización SSH. Esto funciona de manera similar a navegar por la web a través de una VPN: desde la perspectiva del servidor web, su tráfico parece provenir del servidor SSH. El tráfico entre su computadora y el servidor SSH está encriptado, por lo que puede navegar a través de una conexión encriptada como lo haría con una VPN.

Sin embargo, un túnel SSH no ofrece todos los beneficios de una VPN. A diferencia de una VPN, debe configurar cada aplicación para que utilice el proxy del túnel SSH. Con una VPN, tiene la seguridad de que todo el tráfico se enviará a través de la VPN, pero no tiene esta garantía con un túnel SSH. Con una VPN, su sistema operativo se comportará como si estuviera en la red remota, lo que significa que conectarse a los recursos compartidos de archivos en red de Windows sería fácil. Es considerablemente más difícil con un túnel SSH.

CÓMO FUNCIONA UNA VPN

VPN significa "red privada virtual"; como su nombre lo indica, se utiliza para conectarse a redes privadas a través de redes públicas, como Internet. En un caso de uso común de VPN, una empresa puede tener una red privada con archivos compartidos, impresoras en red y otras cosas importantes. Algunos de los empleados de la empresa pueden viajar y, con frecuencia, necesitan acceder a estos recursos desde la carretera. Sin embargo, la empresa no quiere exponer sus importantes recursos a la Internet pública. En cambio, la empresa puede configurar un servidor VPN y los empleados que viajan pueden conectarse a la VPN de la empresa. Una vez que un empleado está conectado, su computadora parece ser parte de la red privada de la empresa: puede acceder a archivos compartidos y otros recursos de red como si realmente estuvieran en la red física.

El cliente VPN se comunica a través de la Internet pública y envía el tráfico de red de la computadora a través de la conexión cifrada al servidor VPN. El cifrado proporciona una conexión segura, lo que significa que la competencia de la empresa no puede fisgonear en la conexión y ver información empresarial confidencial. Dependiendo de la VPN, todo el tráfico de la red de la computadora puede enviarse a través de la VPN, o solo una parte (generalmente, sin embargo, todo el tráfico de la red pasa por la VPN). Si todo el tráfico de navegación web se envía a través de la VPN, las personas entre el cliente y el servidor VPN no pueden espiar el tráfico de navegación web. Esto proporciona protección cuando se utilizan redes Wi-

Fi públicas y permite a los usuarios acceder a servicios geográficamente restringidos; por ejemplo, el empleado podría eludir la censura de Internet si trabaja desde un país que censura la web. Para los sitios web a los que accede el empleado a través de la VPN, el tráfico de navegación web parece provenir del servidor VPN.

Fundamentalmente, una VPN funciona más a nivel de sistema operativo que a nivel de aplicación. En otras palabras, cuando ha configurado una conexión VPN, su sistema operativo puede enrutar todo el tráfico de red a través de ella desde todas las aplicaciones (aunque esto puede variar de una VPN a otra, dependiendo de cómo esté configurada la VPN). No es necesario configurar cada aplicación individual.

¿CUÁL ES MÁS SEGURO?

Si le preocupa cuál es más seguro para el uso empresarial, la respuesta es claramente una VPN: puede forzar todo el tráfico de red del sistema a través de ella. Sin embargo, si solo desea una conexión encriptada para navegar por la web desde redes públicas de Wi-Fi en cafeterías y aeropuertos, un servidor VPN y SSH tienen un cifrado sólido que le será de gran utilidad.

También hay otras consideraciones. Los usuarios novatos pueden conectarse fácilmente a una VPN, pero configurar un servidor VPN es un proceso más complejo. Los túneles SSH son más desalentadores para los usuarios novatos, pero configurar un servidor SSH es más simple; de hecho, muchas personas ya tendrán un servidor SSH al que acceden de forma remota. Si ya tiene acceso a un servidor SSH, es mucho más fácil usarlo como túnel SSH que configurar un servidor VPN. Por esta razón, los túneles SSH se han denominado una "VPN para pobres".

Las empresas que buscan redes más sólidas querrán invertir en una VPN. Por otro lado, si eres un geek con acceso a un servidor SSH, un túnel SSH es una forma fácil de cifrar y canalizar el tráfico de red, y el cifrado es tan bueno como el cifrado de una VPN.

SOFTETHER VPN: QUÉ ES Y CÓMO INSTALAR ESTE PROGRAMA EN WINDOWS

Al navegar por Internet podemos hacer uso de muchas herramientas para cifrar nuestra conexión y evitar problemas que dañen la seguridad y privacidad. Un ejemplo son los servicios VPN, que nos ayudan a navegar por redes inalámbricas públicas con más seguridad y ocultar la dirección IP real. En este artículo vamos a hablar de SoftEther, una interesante opción que podemos tener en cuenta. Vamos a explicar cómo usarlo en Windows.

QUÉ ES SOFTETHER VPN

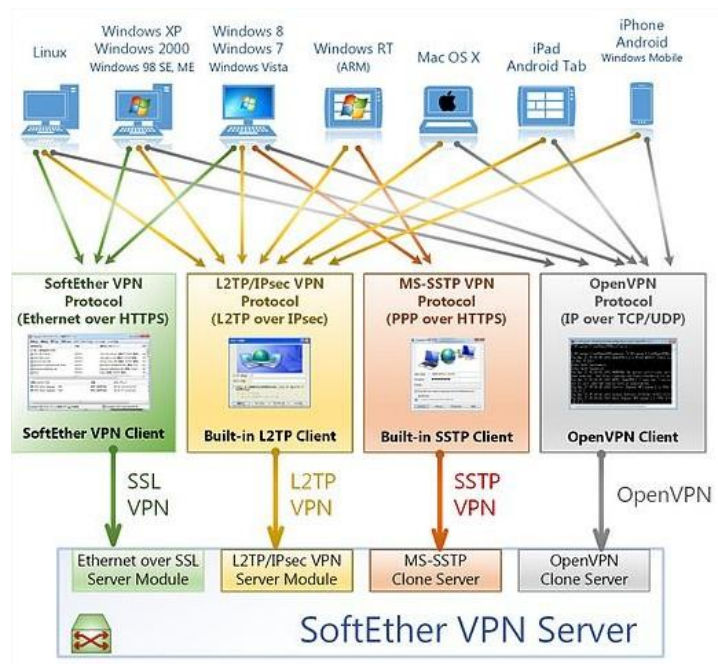
SoftEther VPN es un software VPN multiprotocolo que podemos utilizar en sistemas operativos como Windows, Linux o macOS, entre otros. Su nombre viene de Software Ethernet. Es de código abierto y totalmente gratuito. Supone una alternativa a otras opciones como OpenVPN y servidores de Microsoft.

Es considerada una opción más rápida que OpenVPN y además hay que indicar que es compatible con Microsoft SSTP VPN para las diferentes versiones de Windows. Cuenta con un protocolo propio: SSL-VPN. Está optimizado totalmente para esta herramienta, por lo que ofrece un rendimiento muy rápido, baja latencia y resistencia al firewall.

Permite virtualizar Ethernet a través de la enumeración de software. SoftEther VPN Client implementa Virtual Network Adapter y SoftEther VPN Server implementa Virtual Ethernet Switch. Podemos crear fácilmente VPN de acceso remoto y VPN de sitio a sitio, como una expansión de la VPN L2 basada en Ethernet. También permite crear una VPN tradicional basada en L3 con enrutamiento IP.

SoftEther VPN tiene una gran compatibilidad con los productos VPN más populares de la actualidad a nivel global. Tiene interoperabilidad con OpenVPN, L2TP, IPsec, EtherIP, L2TPv3, Cisco VPN Routers y MS-SSTP VPN Clients. En la actualidad es el único del mundo que admite SSL-VPN, OpenVPN, L2TP, EtherIP, L2TPv3 e IPsec, como un único software VPN.

SoftEther (Software Ethernet) es desarrollado en Japón y soporta múltiples protocolos de VPN, como L2TP, OpenVPN y SSTP. Desde el 2014 es uno de los softwares escritos de VPN más sofisticados en software libre. A continuación, se muestra una imagen con algunos de los protocolos que soporta:



CARACTERÍSTICAS PRINCIPALES DE SOFTETHER

Hemos visto qué es SoftEther y ahora vamos a ver cuáles son sus características principales. Un repaso por los puntos que debemos tener en cuenta de este software. Ya hemos mencionado algunos aspectos, como que es gratuito y de código abierto.

- Facilidad para establecer VPN de sitio a sitio y de acceso remoto
- Tunelización SSL-VPN en HTTPS para pasar a través de NAT y cortafuegos
- Funciones innovadoras de VPN sobre ICMP y VPN sobre DNS
- Es resistente a firewalls altamente restringidos
- DNS dinámico y NAT transversal integrados para que no se requiera una dirección IP fija o estática
- Cifrados AES de 256 bits y RSA de 4096 bits
- Funciones de seguridad, como registro y túnel VPN
- Alto rendimiento con 1 Gbps con bajo uso de memoria y CPU
- Admite Windows, Linux, macOS, iOS o Android, entre otros
- Compatibilidad con SSL-VPN (HTTPS) y los seis principales protocolos VPN (OpenVPN, IPsec, L2TP, MS-SSTP, L2TPv3 y EtherIP)
- La función de clonación de OpenVPN admite clientes OpenVPN heredados
- IPv4 y IPv6

Otra de las grandes características con las que cuenta, es la posibilidad de implementarlo en Windows Server 2022. Esto beneficia directamente al lugar donde se de uso de este sistema operativo, ya que cualquier usuario que pase por este servidor para su conexión a internet, tendrá esta protección disponible con las opciones que citamos previamente. Por lo cual la protección de los datos será mucho más elevada, lo cual se agradece especialmente si se trata de información muy sensible. A mayores, si se puede combinar con soluciones que se implementan a nivel de servidor, por lo cual se puede extrapolar a las aplicaciones que cuentan con sus bases de datos en este. Como puede ser Citrix, que permite realizar gestión de usuarios en multitud de aplicaciones diferentes.

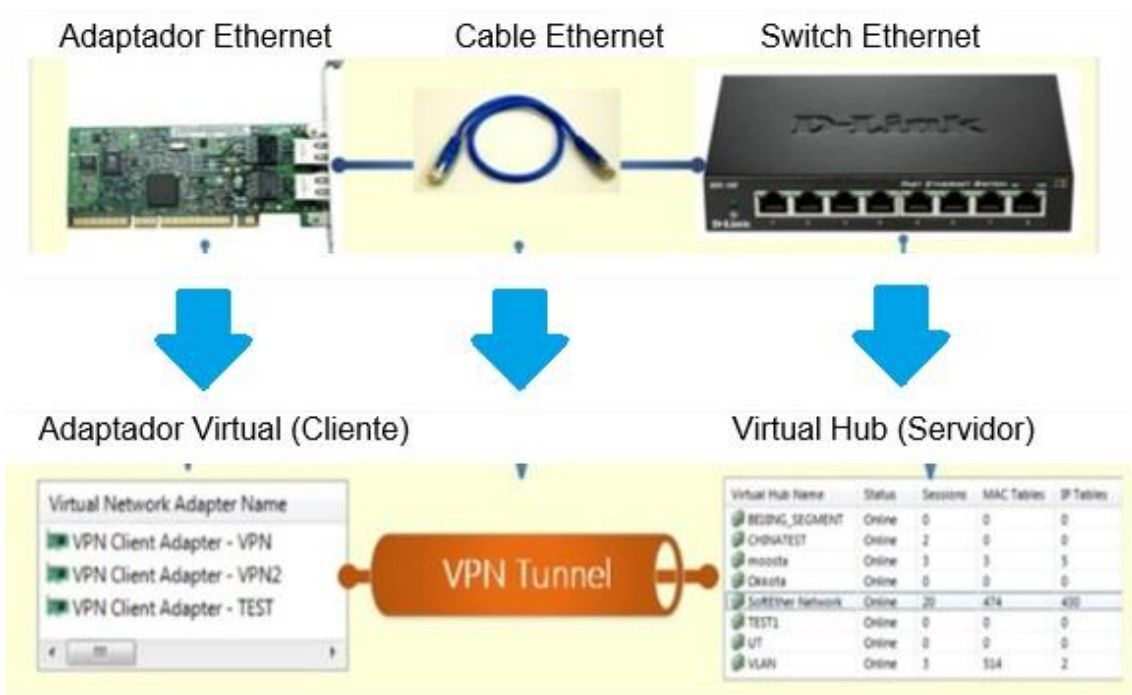
En definitiva, estas son las principales características con las que cuenta SoftEther. Este software de VPN servidor y cliente multiplataforma ofrece un amplio abanico de opciones. Cuenta con un gran rendimiento en los diferentes sistemas operativos donde es compatible.

A continuación, se muestra una comparación entre SoftEther y OpenVPN:

Aspectos a comparar	OpenVPN	SoftEther
Release inicial	2002	2014
Licencia	GNU GPL	GNU GPL
Código fuente	C 91,000 líneas	C/C++ 378,000 líneas
Desarrollado por	OpenVPN technologies	SoftetherVPN project, University of Tsukuba, Japan
Protocolos soportados	Sólo OpenVPN	OpenVPN L2TP/IPsec L2TPv3/IPsec EtherIP Microsoft SSTP VPN over HTTPS VPN over DNS VPN over ICMP
Cientes VPN nativos del Sistema Operativo soportados	No	Windows (L2TP, SSTP) Mac OS x (L2TP) iOS (L2TP) Android (L2TP)
Ancho de banda	<100 Mbps (Generalmente 10 Mbps)	>900 Mbps (Generalmente 100 Mbps)
Función de NAT traversal	No	Sí
Función de DNS dinámico	No	Sí
VPN via proxy HTTP	Sí	Sí
IPv6	Sí	Sí
Filtrado de paquetes	No	Sí
Soporte para Multi-tenants (multi-inquilino)	No	Sí
Generador de retraso, Jitter y pérdida de paquetes (Función de simulación)	No	Sí
Asignación fija de IP por DHCP	Sí	No
Escucha en múltiples puertos TCP/UDP	No	Sí
Capa de Seguridad	OpenSSL	OpenSSL
Smartcards & Tokens USB	No	Sí (VPN Server GUI manager)
Gestión CUI	Limitada	Sí
Gestión RPC sobre HTTPS	No	Sí
Interfaz de usuario multilinguaje	Sólo Inglés	Inglés, Japonés, Chino
Plataformas	Windows Linux FreeBSD Solaris Mac OS X iOS Android NetBSD QNX	Windows Linux FreeBSD Solaris Mac OS X iOS Android

ARQUITECTURA DEL SOFTETHER

El SoftEther VPN Client levanta en la máquina un nuevo adaptador de red con un direccionamiento interno e independiente a la dirección ip de nuestra tarjeta de red física. Esta dirección ip es asignada por el DHCP que posee el servidor VPN, el cual constituye el DNS y el Gateway de la nueva subred interna creada. Para lograr un mejor entendimiento de este tema las siguientes figuras hacen una analogía con una red física.



CÓMO INSTALAR SOFETHER EN WINDOWS

Vamos a explicar paso a paso cómo instalar SoftEther en Windows. Vamos a probarlo en el que es el sistema operativo más utilizado en equipos de escritorio, aunque hay que indicar que el proceso para su instalación y uso es similar en el resto de sistemas operativos donde podemos utilizarlo.

Lo primero que tenemos que hacer es ir a la sección de descargas de su [web oficial](#). Allí encontraremos las diferentes opciones para descargar el programa. Tenemos también el enlace a GitHub y poder consultar el código fuente del software. Hay varios servidores para elegir de dónde descargarlo.

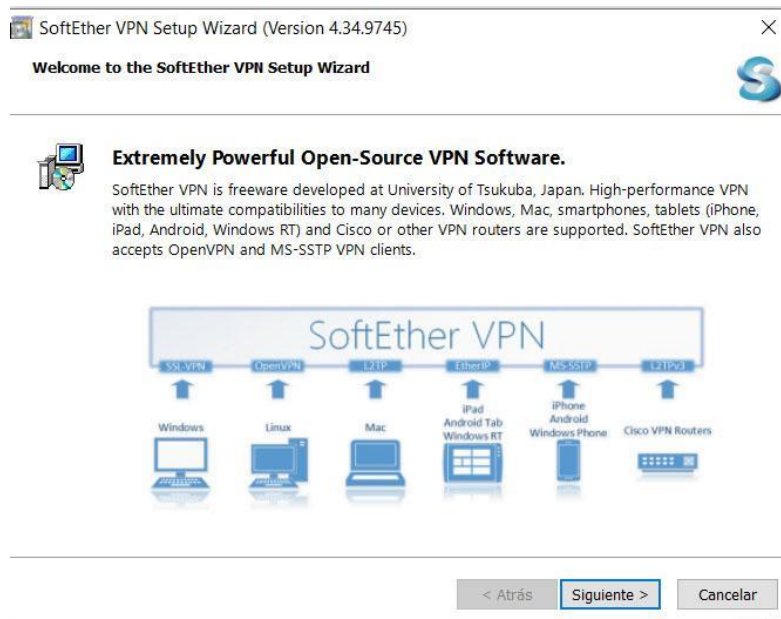
The screenshot shows the SoftEther VPN website. The main content area is titled 'Download' and provides information about the open-source software. It lists several download sources:

- Primary Download Server (hosted by Windows Azure):**
 - Download SoftEther VPN
- Download from CNET Download.com:**
 - Download SoftEther VPN from CNET Download.com
- Download from Softpedia.com:**
 - Download SoftEther VPN from Softpedia.com

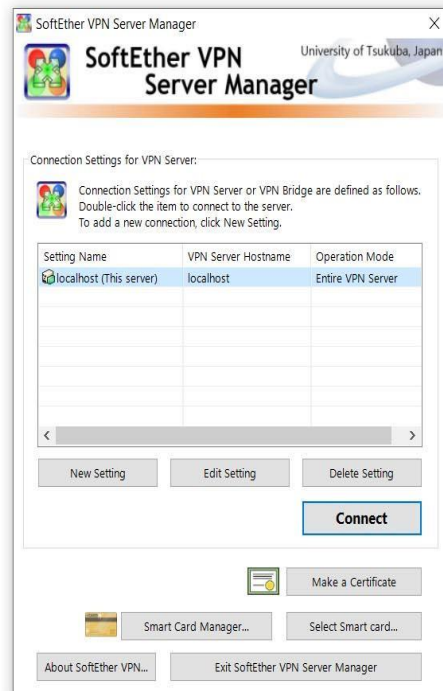
At the bottom, it states 'Source Code is Available!' and provides a link to the source code.

Hay que tener en cuenta que podremos descargar la opción servidor, cliente, puente, así como elegir la plataforma. El **archivo de instalación** ocupa unos 50 MB. Una vez lo hemos descargado lo siguiente

que tenemos que hacer es ejecutarlo en el sistema. Comenzará con la instalación, un proceso sencillo e intuitivo. Nos solicitará permisos para su instalación y debemos aceptar.



Una vez lo hayamos instalado y ejecutado por primera vez nos aparecerá una ventana como la que vemos en la imagen de abajo. Tenemos que darle a **Connect** para empezar a usarlo. Nos solicitará contraseña de administrador.



cionado 12,7 KB

Si queremos **crear un servidor remoto VPN** con SoftEther tenemos que marcar esa opción en la nueva ventana que se abrirá posteriormente y darle a siguiente. Nos pedirá confirmación y le damos a aceptar. También tendremos que crear un nombre.

SoftEther VPN Server / Bridge Easy Setup

SoftEther VPN Server / Bridge Easy Setup

By using this setup you can easily setup a SoftEther VPN Server or VPN Bridge for the following use and purpose. After exiting the setup, you can use the VPN Server Manager to freely configure more advanced settings.

Select the type of VPN server you want to build. Multiple types can be selected together.

☒ **Remote Access VPN Server**

The Remote Access VPN Server allows VPN Client computers in remote locations to access to the existing Ethernet segments, for example company LAN.
Any VPN Clients who is connecting to the VPN Server will be able to access to the network as if they are connected directly and physically to the network.

☐ **Site-to-site VPN Server or VPN Bridge**

Site-to-site VPN is a VPN configuration to connect between two or more remote Ethernet segments.
Each of the sites are connected together, and become the same segment at Layer-2 level. It enables any computers of each sites to communicate to each other as if there is a single network.

Select the role of this VPN Server:

☐ VPN Server that Accepts Connection from Other Sites (Center)

☐ VPN Server or VPN Bridge at Each Site (Edge)

☐ **Other Advanced Configuration of VPN**

Select this if you are planning to build a VPN system that provides advanced functions such as a clustering function and a Virtual Layer 3 Switch function.

Click Next to start Setup. Click Close if you want to exit the setup and manually configure all settings.

Next > Close

Hecho esto nos creará una función de **Dynamic DNS**. Asignará un Hostname, dirección global IPv4 y todo como vemos en la imagen de abajo. Podemos cambiar el nombre y asignar el que queramos. Pinchamos en Set to Above Hostname.

Dynamic DNS Function

Dynamic DNS Function

This VPN Server has a Built-in Dynamic DNS Function.

The Dynamic DNS assigns a unique and permanent DNS hostname for this VPN Server. You can use that hostname to specify this VPN Server on the settings for VPN Client and VPN Bridge. You need not to register and keep a domain name.

Also, if your ISP assigns you a dynamic (not-fixed) IP address, the corresponding IP address of your Dynamic DNS hostname will be automatically changed. It enables you to keep running the VPN Server by using only a dynamic IP address. Therefore, you need not any longer to keep static global IP addresses with expenses monthly costs.

Moreover, this VPN Server version supports 'NAT-Traversal' function. If the VPN Server is inside the NAT and is assigned only a private IP address, you can connect to that VPN Server from the Internet side without any special settings on the NAT beforehand.

Current Status:

Assigned Dynamic DNS Hostname:
vpn .softether.net Hint

Global IPv4 Address:
81.

Global IPv6 Address:
Unable to reach the IPv6 DDNS Server.

DNS Key 0 Hint

Modify the Settings:

Change the Dynamic DNS Hostname:
VPN_RedesModule .softether.net

Hostname is with only alphabets numeric, and dashes '-'.
Three letters at least.
You can change it any time later.

Set to Above Hostname Restore

If you are not connected to IPv6 Internet, "Global IPv6 Address" should show an error.
A few countries or territories might prohibit Dynamic DNS Service.

Connect via Proxy Server... Exit

Una vez creado tenemos que darle a salir y en la ventana que aparece marcar la opción de **Enable L2TP Server Function** (L2TP over IPsec). Hay que elegir también el nombre de usuario, pero como tendremos únicamente uno creado ya vendrá marcado de forma predeterminada. Le damos a OK.

IPsec / L2TP / EtherIP / L2TPv3 Settings

IPsec / L2TP / EtherIP / L2TPv3 Server Settings


Virtual Hubs on the VPN Server can accept Remote-Access VPN connections from L2TP-compatible PCs, Mac OS X and Smartphones, and also can accept EtherIP / L2TPv3 Site-to-Site VPN Connection.

L2TP Server (Remote-Access VPN Server Function)

VPN Connections from Smartphones suchlike iPhone, iPad and Android, and also from built-in VPN Clients on Mac OS X and Windows can be accepted.

☒ **Enable L2TP Server Function (L2TP over IPsec)**
Make VPN Connections from iPhone, iPad, Android, Windows, and Mac OS X acceptable.

☐ **Enable L2TP Server Function (Raw L2TP with No Encryptions)**
It supports special VPN Clients which uses L2TP with no IPsec encryption.

 Users should specify their username such as "Username@Target Virtual Hub Name" to connect this L2TP Server. If designation of a Virtual Hub is omitted, the below Hub will be used as the target.

Default Virtual Hub in a case of omitting a name of Hub on the Username:

EtherIP Server Function (Site-to-Site VPN Connection)

Router products which are compatible with EtherIP / L2TPv3 over IPsec can connect to Virtual Hub on the VPN Server and establish Layer-2 (Ethernet) Bridging.

☐ **Enable EtherIP / L2TPv3 over IPsec Server Function** [EtherIP / L2TPv3 Detail Settings](#)

IPsec Common Settings:

IPsec Pre-Shared Key:

IPsec Pre-Shared Key is also called "PSKs" or "Secrets". Specify it with around eight ASCII characters, and let all VPN users know.

En la siguiente ventana le damos a **deshabilitar VPN Azure** y marcamos OK nuevamente. Tras esto le damos a crear un nuevo usuario y rellenamos los datos correspondientes. Tenemos que poner el nombre y el tipo de autenticación, básicamente, además de la contraseña.

Create New User

User Name:

Full Name:

Note:

Group Name (Optional): [Browse Groups...](#)

☐ Set the Expiration Date for This Account
13/02/2021 0:00:00

Auth Type: **Anonymous Authentication**

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

☐ Specify User Name on Authentication Server
User Name on Authentication Server:

Security Policy

☐ Set Security Policy [Security Policy](#)

Password Authentication Settings:

Password:

Confirm Password:

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

[Specify Certificate](#) [View Certificate](#) [Create Certificate](#)

Signed Certificate Authentication Settings:

Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

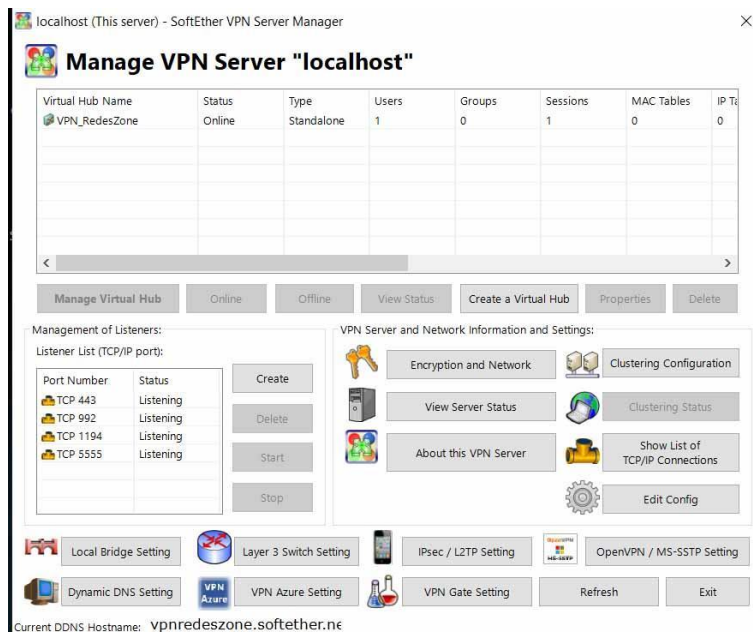
☐ Limit Common Name (CN) Value

☐ Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

Hint: Define a user object with username "*" (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.

Automáticamente veremos en la nueva ventana que ya aparece el usuario que hemos creado. Podemos simplemente cerrar esa ventana dando a Exit y en la ventana anterior, en el paso 3 elegir el **controlador Ethernet** y cerramos. Podremos comprobar que el estado es Online, como vemos en la imagen de abajo.



Si seleccionamos el usuario y hacemos clic en **Manage Virtual Hub** podremos entrar en los diferentes puntos que podemos modificar. Podemos pinchar en Virtual NAT and Virtual DCHP y habilitar SecureNAT. Posteriormente entramos en SecureNAT Configuration y allí veremos las opciones de la interfaz de la tarjeta, como la dirección MAC o dirección IP.

Podemos ver en la ventana principal la lista de puertos TCP/IP en escucha. Podemos crear, eliminar o pausar los que hay.

INSTALAR SOFTETHER CLIENT

También podemos instalar la versión del **cliente de SoftEther VPN**. El proceso es el mismo. Tenemos que ir a su página web y allí en esta ocasión seleccionar Client. Hay que elegir el sistema operativo donde lo queremos instalar. Al abrirlo nos encontraremos con una ventana como la que vemos en la imagen de abajo.



Tenemos que darle a **Add VPN Connection**. Hay que ponerle un nombre y comenzará a crear la nueva red virtual en Windows. Esto tardará unos segundos. Automáticamente aparecerá en la parte de debajo de la ventana principal, con el nombre que hemos creado. Hay que asegurarse de que pone estado Enabled.

Hecho esto hay que ir a Connect, le damos a New VPN y aparecerá una nueva ventana para rellenar los datos como vemos en la imagen.

New VPN Connection Setting Properties

Please configure the VPN Connection Setting for VPN Server.

Setting Name:

Destination VPN Server:

Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.

Host Name:

Port Number: ☐ Disable NAT-T

Virtual Hub Name:

Proxy Server as Relay:

You can connect to a VPN Server via a proxy server.

Proxy Type:

☒ Direct TCP/IP Connection (No Proxy)

☐ Connect via HTTP Proxy Server

☐ Connect via SOCKS Proxy Server

Server Certificate Verification Option:

☐ Always Verify Server Certificate

☐ Hide Status and Errors Screens ☐ Hide IP Address Screens

Virtual Network Adapter to Use:

☒ VPN Client Adapter - VPN2

User Authentication Setting:

Set the user authentication information that is required when connecting to the VPN Server.

Auth Type:

User Name:

Password:

You can change the user's password on the VPN Server.

Advanced Setting of Communications:

☒ Reconnects Automatically After Disconnected

Reconnect Count: times

Reconnect Interval: seconds

☒ Infinite Reconnects (Keep VPN Always Online)

☐ Use SSL 3.0 (1)

Allí tenemos que poner datos como el nombre del host, que en nuestro caso como lo configuramos antes sería vpnredeszone.softether.net. También elegir el puerto y deshabilitar NAT-T.

Hay que poner nombre de usuario y contraseña a la derecha y damos a OK. Nos aparecerá ahora en la ventana principal la conexión en offline. Simplemente con hacer clic derecho y darle a Conectar establecerá la conexión y nos aparecerá la IP. Ya veremos que aparece como conectado.

En definitiva, siguiendo estos pasos que hemos ido explicando podemos descargar y configurar SoftEther como servidor y cliente. Podemos crear una VPN fácilmente y de manera segura.

IMPLEMENTANDO SOFTETHER VPN SERVER EN LINUX

PAQUETES NECESARIOS

- softether-vpnserver-v4.28-9669-beta-2018.09.11-linux-x64-64bit.tar.gz

```
1 wget https://www.softether-download.com/files/softether/v4.28-9669-beta-2018.09.11-  
tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.28-9669-beta-  
2018.09.11-linux-x64-64bit.tar.gz
```

Preparando el escenario:

```
1 apt install build-essential  
2 mkdir /opt/instaladores
```

Copiar el compilador de softether en el directorio y acceder para su instalación:

```
1 cd /opt/instaladores  
2 tar -xzf softether-vpnserver-v4.28-9669-beta-2018.09.11-linux-x64-64bit.tar.gz  
3 cd vpnserver  
4 make
```

Seguir los siguientes pasos:

```
1 Do you want to read the License Agreement for this software ?  
2 1. Yes  
3 Did you read and understand the License Agreement ?  
4 (If you couldn't read above text, Please read 'ReadMeFirst_License.txt'  
5 file with any text editor.)  
6 1. Yes  
7 Did you agree the License Agreement ?  
8 1. Agree
```

Configurar el servicio como un demonio:

```
1 cd ..  
2 mv vpnserver /usr/local  
3 cd /usr/local/vpnserver/  
4 chmod 600 *  
5 chmod 700 vpnserver  
6 chmod 700 vpncmd
```

Antes de continuar, verifiquemos que el servidor vpn opera con normalidad. Es importante realizar este chequeo antes de inicializar el servidor vpn:

```
1./vpncmd
```

Seguir los siguientes pasos:

```
1By using vpncmd program, the following can be achieved.
```

```
23. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)
```

```
3check
```

Si todo está bien, debe devolver lo siguiente:

```
1All checks passed. It is most likely that SoftEther VPN Server / Bridge can operate normally on this system.
```

```
2
```

```
3The command completed successfully.
```

Crear un servicio de systemd para softether vpn server:

```
1nano /lib/systemd/system/softether.service
```

Agregar lo siguiente:

```
1 [Unit]
```

```
2 Description=SoftEther VPN Server
```

```
3 After=network.target
```

```
4
```

```
5 [Service]
```

```
6 Type=forking
```

```
7 ExecStart=/usr/local/vpnserver/vpnserver start
```

```
8 ExecStop=/usr/local/vpnserver/vpnserver stop
```

```
9
```

```
10[Install]
```

```
11WantedBy=multi-user.target
```

Ahora el servidor vpn inicia automáticamente cuando inicie el sistema, y podemos gestionar el servidor via systemctl. Si al reiniciar no levanta el demonio, hacer lo siguiente:

```
1mkdir -p /config/scripts
```

```
2nano /config/scripts/softether.startup.sh
```

Agregar lo siguiente:

```
1#!/bin/sh
```

```
2
```

```
3#-----
```

```
4# El objetivo de este script es iniciar el servicio de softether
```

```
5#-----
```

```
6
```

```
7systemctl start softether
```

Damos los permisos de ejecución:

```
1chmod +x /config/scripts/softether.startup.sh
```

Editamos el cron para una tarea programada al inicio del sistema:

```
1crontab -e
```

Seleccionar el editor preferido, y agregar lo siguiente y agregamos lo siguiente:

```
1 #####
```

```
2 # LEYENDA #
```

```
3 #####
```

```
4
```

```
5 # "m": minutos (0-59)
```

```
6 # "h": horas (0-23)
```

```
7 # "dow": dia de la semana (0-6)
```

```
8 # "dom": dia del mes (1-28/1-30/1-31)
```

```
9 # "mon": mes (1-12)
```

```
10# "*" : cualquiera
```

```
11# ",": separa valores dentro de la misma variable (0,5,10)
```

```
12# "-": define rangos dentro de la misma variable (0-5)
```

```
13# m h dom mon dow ruta_hacia_script
```

```
14
```

```
15#####
```

```
16# SOFTETHER #
```

```
17#####
```

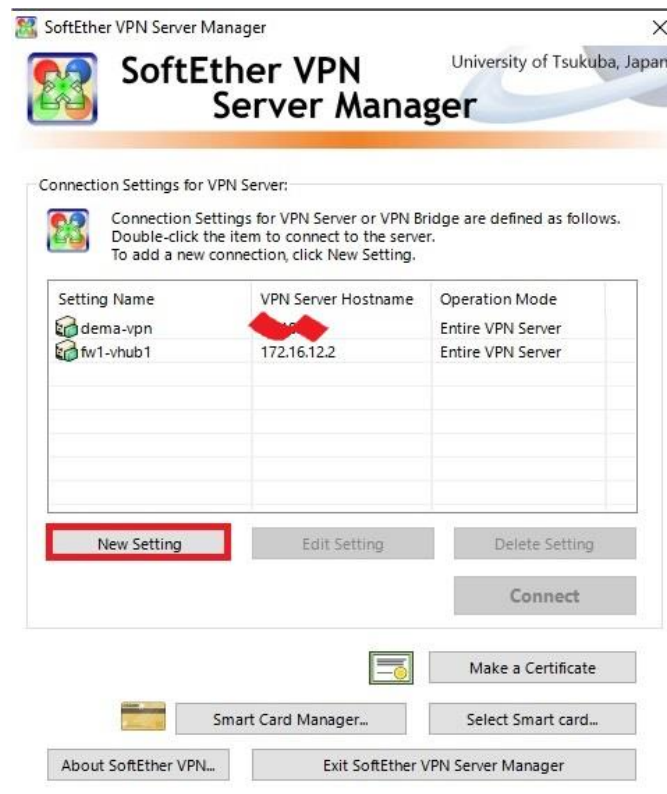
```
18
```


19# AL iniciar el sistema

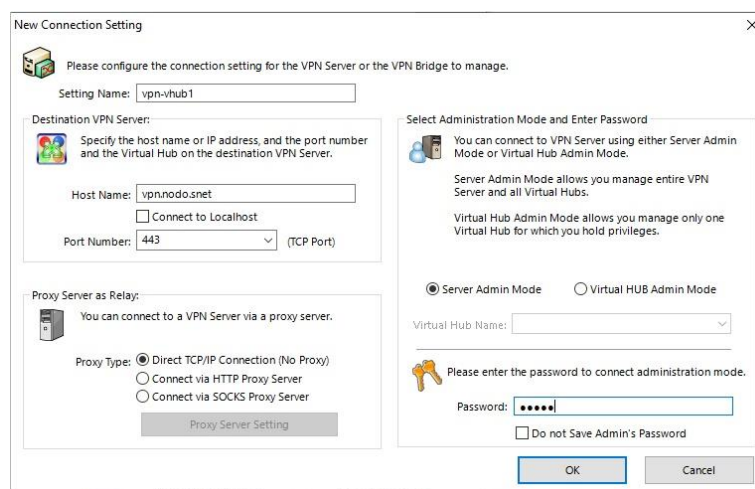
20@reboot /config/scripts/softether.startup.sh

CONFIGURANDO EL SERVIDOR DE SOFTETHER MEDIANTE «SE-VPN SERVER MANAGER (TOOLS)»

Seguir el procedimiento descrito por las siguientes imágenes y adaptar a su red, según convenga. Abrimos el «SoftEther VPN Manager» desde nuestra PC en Windows y damos click en «New Settings» para añadir una nueva configuración:



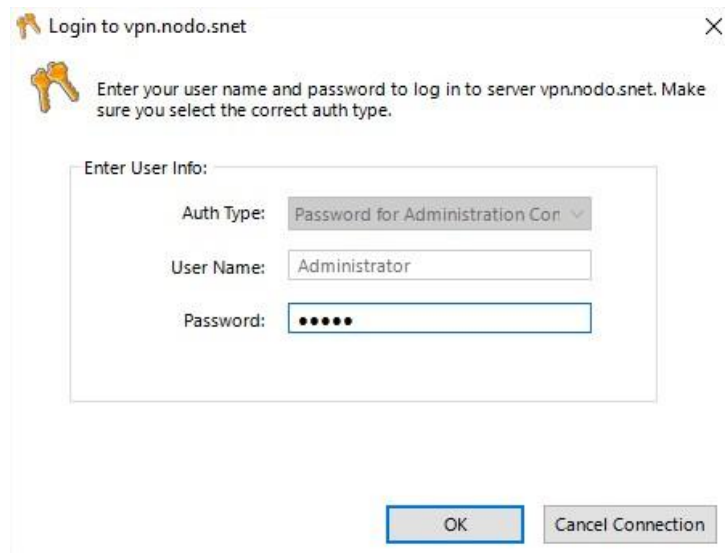
Configuramos la vpn, adaptando a su red:



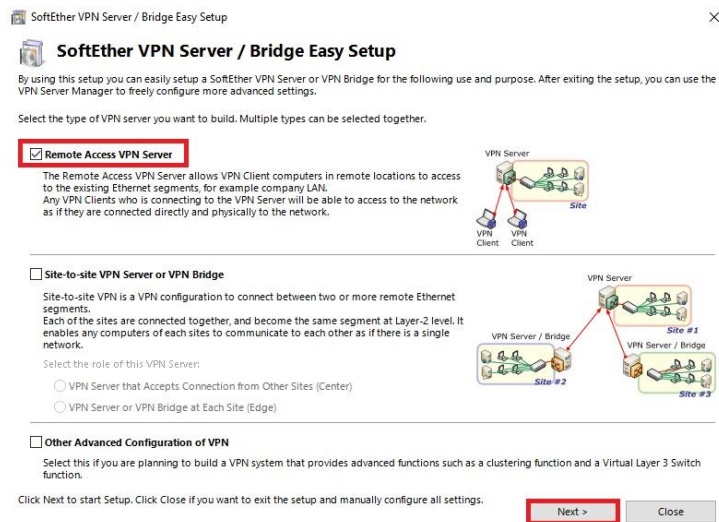
De vuelta a la vista inicial, ahora seleccionamos la nueva vpn creada y damos click en «Connect»:



Acto seguido pedirá definir una contraseña para la vpn:



En este caso configuraremos una vpn para acceso remoto:



Aceptamos la indicación del servidor:



Definimos el nombre que recibirá el «Virtual Hub»:



Deshabilitamos el servicio de «VPN Azure»:

VPN Azure Service Settings

The diagram illustrates the VPN Azure Cloud VPN Service architecture. A central cloud labeled "VPN Azure Cloud" connects two locations: "Office" and "Home".

- Office Side:** A "Your PC with VPN Server" is connected to a "Private Network". A box labeled "Penetrates Firewall" indicates the connection path. A box labeled "VPN Session is Relayed" shows the connection to the cloud. A box labeled "No Need Net Admin Privileges" and "No Need Global IP" and "No Need Open Ports" are shown.
- Home Side:** A "Windows Vista / 7 / 8 / RT" PC is connected to a "Home" user. A box labeled "Establish a SSTP VPN" shows the connection path. A box labeled "Use Built-in Windows VPN Client" is shown.

VPN Azure Cloud VPN Service (Free)

VPN Azure makes it easier to establish a VPN Session from your home PC to your office PC. While a VPN connection is established, you can access to any other servers on the private network of your company.

You don't need a global IP address on the office PC (VPN Server). It can work behind firewalls or NATs. No network administrator's configuration required. You can use the built-in SSTP-VPN Client of Windows in your home PC.

VPN Azure VPN Azure is a cloud VPN service operated by SoftEther VPN Project. VPN Azure is free of charge and available to anyone. Press the right button to see details and how-to-use instructions.

VPN Azure Setting

☐ Enable VPN Azure
Status: Not Connected

☒ Disable VPN Azure

How to Use VPN Azure (Visit the Web)

OK

Creamos un usuario para la vpn:

VPN Easy Setup Tasks

To complete the setup of this VPN Server / VPN Bridge, you must complete the following tasks.

Step 1. Create a User to Accept VPN Connection

When this VPN Server accepts a remote access VPN, or becomes the central site-to-site VPN server that accepts connections from other sites, create users to accept the VPN connection.

Create Users

Step 2. Define a Connection to Destination VPN Server

When this VPN Server is installed on a particular site (edge) of a site-to-site VPN, you have to specify the address of the center VPN Server that accepts the connections, and establish a connection to that central VPN Server.

Configure Connection Setting

Step 3. Set Local Bridge

For an site-to-site VPN, use the Local Bridge Function to connect a bridge between the virtual Ethernet segment on the VPN side and the physical Ethernet segment on the local side. Select an existing Ethernet device (Network Adapter) that will be provide the bridge connection to the VPN.

Select the Ethernet device to establish the bridge connection.

Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.

Close

Llenamos los datos correspondientes para el usuario:

Create New User

User Name:

Full Name:

Note:

Group Name (Optional):

Browse Groups...

☐ Set the Expiration Date for This Account

30/ 7/2019

12:00:00

Auth Type:

☒ Anonymous Authentication
 ☐ Password Authentication
 ☐ Individual Certificate Authentication
 ☐ Signed Certificate Authentication
 ☐ RADIUS Authentication
 ☒ NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

☐ Specify User Name on Authentication Server

User Name on Authentication Server:

Security Policy

☐ Set Security Policy

Security Policy

Password Authentication Settings:

Password:

Confirm Password:

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Specify Certificate

View Certificate

Create Certificate

Signed Certificate Authentication Settings:

Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

☐ Limit Common Name (CN) Value


☐ Limit Values of the Certificate Serial Number


Note: Enter hexadecimal values. (Example: 0155ABCDFF)


OK


Cancel

[illegible]

VPN Easy Setup Tasks


To complete the setup of this VPN Server / VPN Bridge, you must complete the following tasks.

Step 1. Create a User to Accept VPN Connection

When this VPN Server accepts a remote access VPN, or becomes the central site-to-site VPN server that accepts connections from other sites, create users to accept the VPN connection.


Create Users

Step 2. Define a Connection to Destination VPN Server

When this VPN Server is installed on a particular site (edge) of a site-to-site VPN, you have to specify the address of the center VPN Server that accepts the connections, and establish a connection to that central VPN Server.

Configure Connection Setting

Step 3. Set Local Bridge

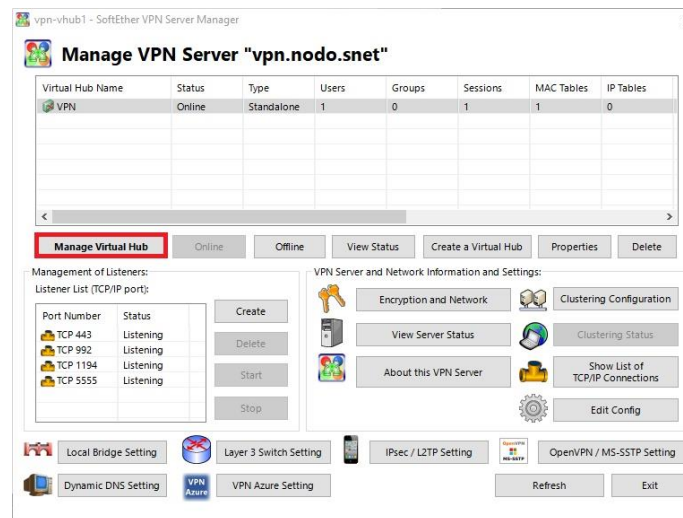
For an site-to-site VPN, use the Local Bridge Function to connect a bridge between the virtual Ethernet segment on the VPN side and the physical Ethernet segment on the local side. Select an existing Ethernet device (Network Adapter) that will be provide the bridge connection to the VPN.

Select the Ethernet device to establish the bridge connection.

Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.

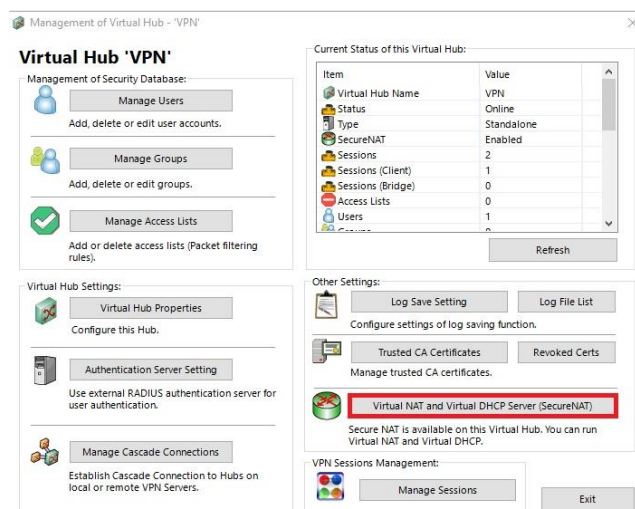
Close

Damos click en «Manage Virtual Hub» para configurar el servidor:

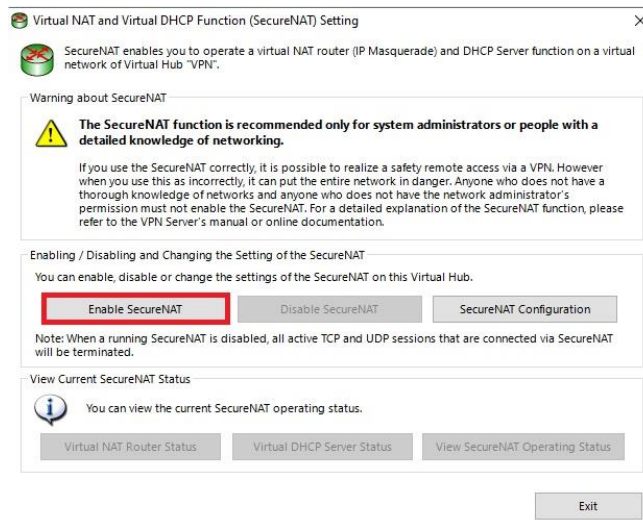


Configuramos el servidor DHCP virtual:

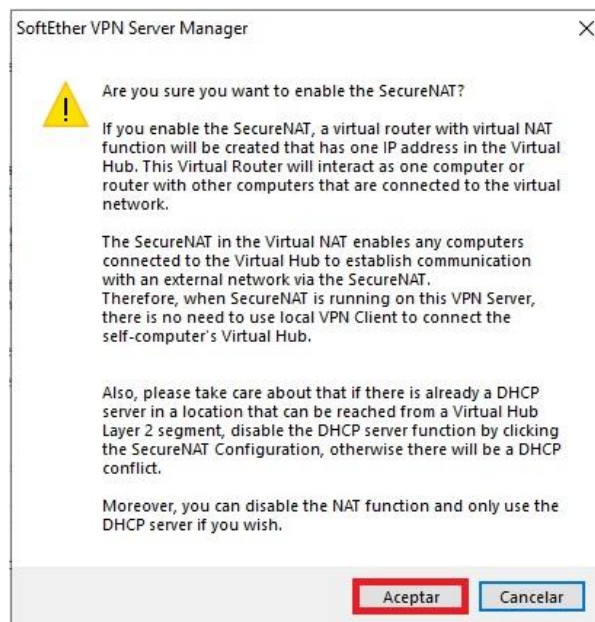
NOTA: Si configuramos el DHCP virtual, tenemos cuando un usuario se conecte al servidor vpn perderá conexión con la red externa, si no se tiene configurado las subredes que será nateadas con la IP del servidor vpn. En cambio, si no se configura el servidor DHCP, los clientes Windows obtendrán un rango de IP propio, no así los clientes Linux (probado y verificado). En este caso optaremos por configurar el DHCP virtual para hacer las configuraciones del cliente vpn, tanto en Linux como en Windows.



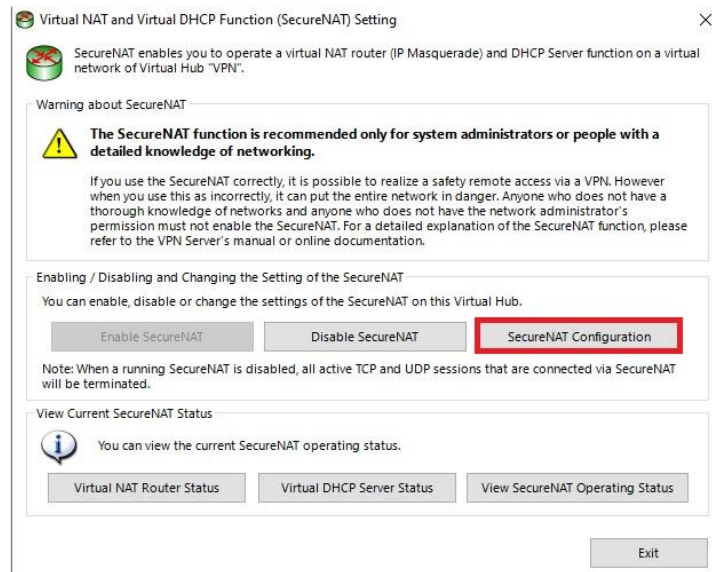
Es necesario habilitar el «SecureNAT»:



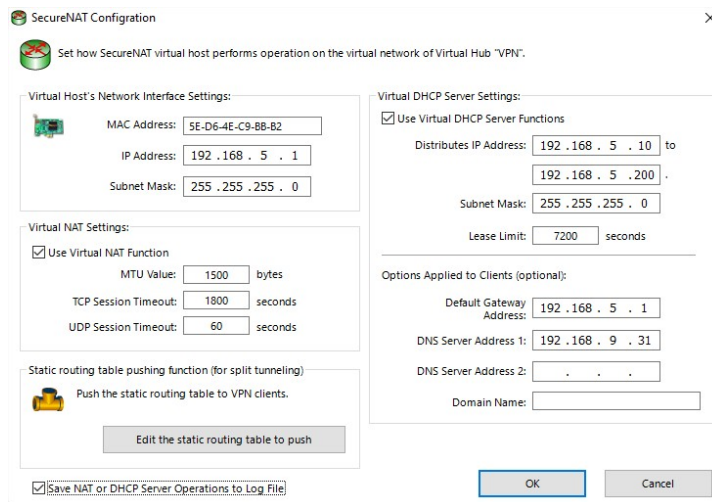
Aceptamos la notificación del servidor:



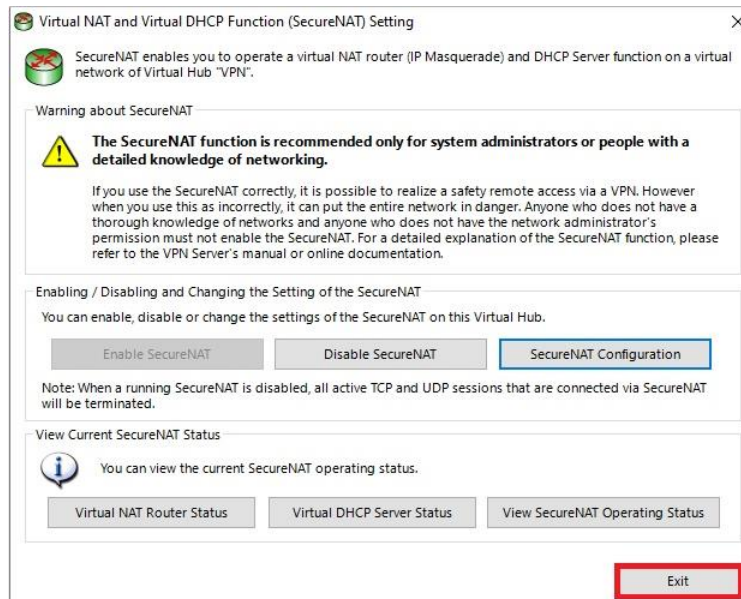
Accedemos a la ventana de configuración del servidor DHCP virtual:



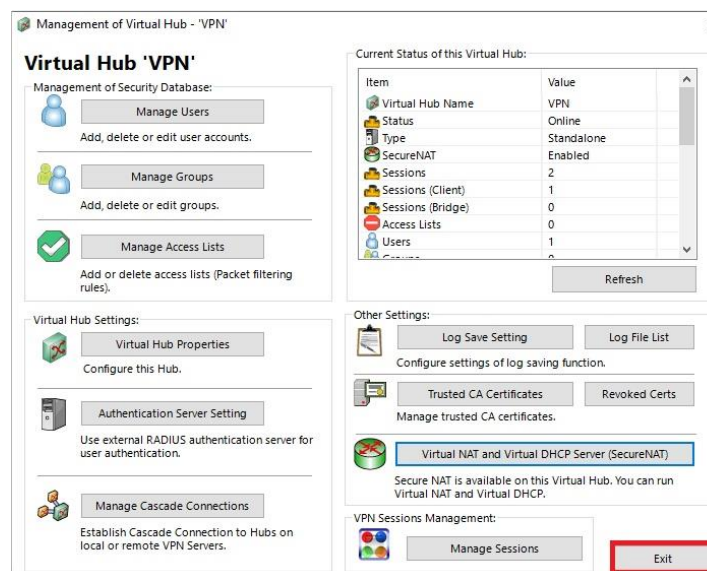
Editamos el servidor según los datos de la red:



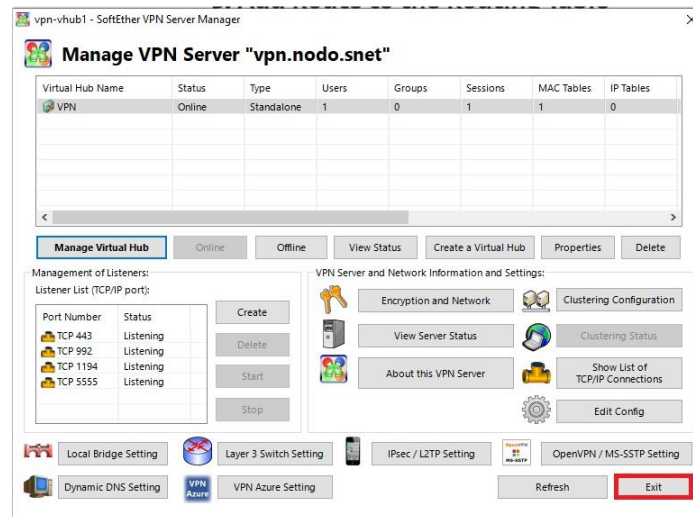
Salimos de la configuración del servidor DHCP virtual:



Salimos de la configuración del «Virtual Hub»:



Salimos de la ventana de configuración del servidor:



IMPLEMENTANDO SOFTETHER VPN CLIENT EN LINUX

PAQUETES NECESARIOS

softether-vpnclient-v4.28-9669-beta-2018.09.11-linux-x64-64bit.tar.gz

Obtenemos el paquete anterior y lo ubicamos en «/usr/local/»

```
1 wget https://www.softether-download.com/files/softether/v4.28-9669-beta-2018.09.11-
  tree/Linux/SoftEther_VPN_Client/64bit_-_Intel_x64_or_AMD64/softether-vpnclient-v4.28-9669-beta-
  2018.09.11-linux-x64-64bit.tar.gz
```

COMPILANDO SOFTETHER VPN CLIENT

Accedemos al directorio, desempaquetamos el paquete del cliente y accedemos al directorio del cliente:

```
1 cd /usr/local
```

```
2 tar -xvzf softether-vpnclient-v4.28-9669-beta-2018.09.11-linux-x64-64bit.tar.gz
```

```
3 cd /usr/local/vpnclient/
```

Damos los permisos necesarios:

```
1 chmod 600 *
```

Compilamos el cliente:

```
1 make
```

Seleccione «Yes» como respuesta a todas las preguntas:

```
1 -----
```

```
2
```

```
3 SoftEther VPN Client (Ver 4.28, Build 9669, Intel x64 / AMD64) for Linux Install Utility
```

```
4 Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Reserved.
```

```
5
6 -----
7
8
9 Do you want to read the License Agreement for this software ?
10
11 1. Yes
12 2. No
13
14 Please choose one of above number: 1
15
16 Did you read and understand the License Agreement ?
17 (If you couldn't read above text, Please read 'ReadMeFirst_License.txt'
18 file with any text editor.)
19
20 1. Yes
21 2. No
22
23 Please choose one of above number: 1
24
25 Did you agree the License Agreement ?
26
27 1. Agree
28 2. Do Not Agree
29
30 Please choose one of above number: 1
```

Damos los permisos necesarios a los nuevos ficheros creados:

```
1 chmod 700 vpnclient
```

Iniciamos el cliente con el script «vpnclient» estando dentro del directorio del cliente:

```
1 ./vpnclient start
```

Deberá devolver lo siguiente:

1The SoftEther VPN Client service has been started.

Ejecutamos el cliente:

1./vpncmd

Antes de ir a la parte de configuración, debemos hacer una prueba de verificación a la instalación del cliente, seleccionando la opción 3:

1By using vpncmd program, the following can be achieved.

2

31. Management of VPN Server or VPN Bridge

42. Management of VPN Client

53. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

6

7Select 1, 2 or 3: 3

Corremos el comando «check»:

1VPN Tools>check

Si todas las pruebas fueron superadas satisfactoriamente, debería salir lo siguiente:

1 Check command - Check whether SoftEther VPN Operation is Possible

2

3 SoftEther VPN Operation Environment Check Tool

4

5 Copyright (c) SoftEther VPN Project.

6 All Rights Reserved.

7

8 If this operation environment check tool is run on a system and that system passes, it is most likely that
SoftEther VPN software can operate on that system. This check may take a while. Please wait...

9

10
11 Checking 'Kernel System'...

12 Pass

13 Checking 'Memory Operation System'...

14 Pass

15 Checking 'ANSI / Unicode string processing system'...


```
16Pass
17Checking 'File system'...
18Pass
19Checking 'Thread processing system'...
20Pass
21Checking 'Network system'...
22Pass
23
24All checks passed. It is most likely that SoftEther VPN Server / Bridge can operate normally on this system.
25
The command completed successfully.
```

Presionamos Ctrl+C para terminar ese proceso, o escribimos «exit»:

CONFIGURANDO EL SOFTETHER VPN CLIENT

Ejecutamos «./vpncmd» dentro del directorio del cliente:

```
1./vpncmd
```

Seleccionamos la opción 2 y establecemos una conexión con el «localhost», sólo con presionar la tecla «ENTER», ya que estableceremos una conexión local al cliente:

```
1 By using vpncmd program, the following can be achieved.
2
3 1. Management of VPN Server or VPN Bridge
4 2. Management of VPN Client
5 3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)
6
7 Select 1, 2 or 3: 2
8
9 Specify the host name or IP address of the computer that the destination VPN Client is operating on.
10 If nothing is input and Enter is pressed, connection will be made to localhost (this computer).
11 Hostname of IP Address of Destination: ENTER
12
13 Connected to VPN Client "localhost"
```

Habilitamos gestión remota del cliente vpn:

```
1VPN Client>remoteenable
```

Creamos la interfaz virtual «se» para conectarnos al servidor vpn:

```
1VPN Client>niccreate
```

```
2NicCreate command - Create New Virtual Network Adapter
```

```
3Virtual Network Adapter Name: se
```

```
4The command completed successfully.
```

Configuramos el nombre al cual va a responder esta vpn en el cliente:

```
1VPN Client>accountcreate
```

```
2AccountCreate command - Create New VPN Connection Setting
```

```
3Name of VPN Connection Setting: vpn-vhub1
```

Configuramos la cuenta con los detalles ofrecidos por el servidor (Ip del servidor, puerto del servicio y usuario e la cuenta) y por el cliente (nombre del adaptador virtual):

```
1Destination VPN Server Host Name and Port Number: vpn.nodo.snet:443
```

```
2Destination Virtual Hub Name: VPN
```

```
3Connecting User Name: usuario1
```

```
4Used Virtual Network Adapter Name: se
```

Si hizo todo bien, debería poder salirle los siguiente:

```
1The command completed successfully
```

Establecemos la contraseña para la cuenta creada (en este caso fue «123456») y se trata de una cuenta con «Standar Password Authentication»:

```
1 VPN Client>accountpassword
```

```
2 AccountPasswordSet command - Set User Authentication Type of VPN Connection Setting to Password Authentication
```

```
3  
4 Name of VPN Connection Setting: vpn-vhub1
```

```
5  
6 Please enter the password. To cancel press the Ctrl+D key.
```

```
7  
8 Password: 123456
```

```
9 Confirm input: 123456
```

```
10
```

```

11 Specify standard or radius: standard
12
The command completed successfully.

```

Verificamos todas las configuraciones que hemos realizado en el cliente para esta conexión de vpn:

```

1 VPN Client>accountget
2 AccountGet command - Get Setting of VPN Connection Setting
3 Name of VPN Connection Setting: vpn-vhub1
4
5 Item |Value
6 -----+-----
7 VPN Connection Setting Name          |vpn-vhub1
8 Destination VPN Server Host Name      |vpn.nodo.snet
9 Destination VPN Server Port Number    |443
10 Destination VPN Server Virtual Hub Name |VPN
11 Proxy Server Type                    |Direct TCP/IP Connection
12 Verify Server Certificate             |Disable
13 Device Name Used for Connection       |se
14 Authentication Type                  |Standard Password Authentication
15 User Name                            |usuario1
16 Number of TCP Connections to Use in VPN Communication|1
17 Interval between Establishing Each TCP Connection  |1
18 Connection Life of Each TCP Connection  |Infinite
19 Use Half Duplex Mode                  |Disable
20 Encryption by SSL                     |Enable
21 Data Compression                      |Disable
22 Connect by Bridge / Router Mode       |Disable
23 Connect by Monitoring Mode             |Disable
24 No Adjustment for Routing Table        |Disable
25 Do not Use QoS Control Function        |Disable
26 The command completed successfully.

```

Ahora podremos conectarnos al SoftEther VPN Client a través de la cuenta creada:

```
1VPN Client>accountconnect
```

```
2AccountConnect command - Start Connection to VPN Server using VPN Connection Setting
```

```
3Name of VPN Connection Setting: vpn-vhub1
```

```
4
```

```
5The command completed successfully.
```

Verificamos la conectividad con el servidor:

```
1 VPN Client>accountlist
```

```
2 Si obtenemos en "status" el valor "Connected" será bueno para nosotros en el siguiente paso:
```

```
3 AccountList command - Get List of VPN Connection Settings
```

```
4 Item |Value
```

```
5 -----+-----
```

```
6 VPN Connection Setting Name |vpn-vhub1
```

```
7 Status |Connected
```

```
8 VPN Server Hostname |vpn.nodo.snet:443 (Direct TCP/IP Connection)
```

```
9 Virtual Hub |VPN
```

```
10Virtual Network Adapter Name|se
```

```
11The command completed successfully.
```

Salvaremos la configuración echa para esta conexión en el directorio «/home/»:

```
1VPN Client>accountexport
```

```
2AccountExport command - Export VPN Connection Setting
```

```
3Name of VPN Connection Setting: vpn-vhub1
```

```
4
```

```
5Save Destination File Name (recommended extension: vpn): /home/vpn-vhub1.vpn
```

```
6
```

```
7The command completed successfully.
```

Salimos del SoftEther VPN Client:

```
1exit
```

Verificamos si se guardó correctamente el fichero de configuración exportado por el cliente:

```
1ls -l /home | grep vpn-vhub1.vpn
```

Debe devolver lo siguiente:

```
1-rw----- 1 root root 1323 jul 29 17:06 vpn-vhub1.vpn
```

Para ver la configuración del fichero de configuración, hacer lo siguiente:

```
1cat /home/vpn-vhub1.vpn
```

Debe aparecer algo como esto, según la configuración del cliente:

```
1 ### VPN Client VPN Connection Setting File
2 #
3 # This file is exported using the VPN Client Manager.
4 # The contents of this file can be edited using a text editor.
5 #
6 # When this file is imported to the Client Connection Manager
7 # it can be used immediately.
8
9 declare root
10 {
11     bool CheckServerCert false
12     uint64 CreateDateTime 0
13     uint64 LastConnectDateTime 0
14     bool StartupAccount false
15     uint64 UpdateDateTime 0
16
17     declare ClientAuth
18     {
19         uint AuthType 1
20         byte HashedPassword P5no+IeAptPgCgSiTbR5h0xtph0=
21         string Username usuario1
22     }
23
24     declare ClientOption
25     {
26         string AccountName vpn-vhub1
27         uint AdditionalConnectionInterval 1
28         uint ConnectionDisconnectSpan 0
```

```

28     string DeviceName se
29     bool DisableQoS false
30     bool HalfConnection false
31     bool HideNicInfoWindow false
32     bool HideStatusWindow false
33     string Hostname vpn.nodo.snet
34     string HubName VPN
35     uint MaxConnection 1
36     bool NoRoutingTracking false
37     bool NoTls1 false
38     bool NoUdpAcceleration false
39     uint NumRetry 4294967295
40     uint Port 443
41     uint PortUDP 0
42     string ProxyName $
43     byte ProxyPassword $
44     uint ProxyPort 0
45     uint ProxyType 0
46     string ProxyUsername $
47     bool RequireBridgeRoutingMode false
48     bool RequireMonitorMode false
49     uint RetryInterval 15
50     bool UseCompress false
51     bool UseEncrypt true
52 }
53}

```

Verificamos si se creó correctamente la interfaz de red virtual «se», que deberá salir con el nombre «vpn_se», ya que siempre saldrá el nombre del adaptador virtual con la sintaxis «vpn_<nombre_especificado>»:

```
1 ifconfig | grep vpn_se
```

Debe devolver algo como esto:

```
1 [...]

```



```
2
```

```
3vpn_se: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

CONFIGURACIONES DE RED

En caso de que se decida alcanzar una subred a través de nuestro servidor vpn. Para ello requerirá agregar una ruta hacia esa subred, dando como puerta de enlace la IP del servidor vpn por dentro del tunel y especificando la IP de nuestro cliente por dentro del tunel. Será necesario que esté permitido el forwardo de paquetes. Lo verificamos:

```
1cat /proc/sys/net/ipv4/ip_forward
```

Si la respuesta es «1», puede saltarse el siguiente procedimiento, pero si retorna el valor «0», entonces edite el fichero «/etc/sysctl.conf» y descomente la línea «net.ipv4.ip_forward=1». aplique los cambios con el comando «sysctl -p». Luego verifique nuevamente:

```
1cat /proc/sys/net/ipv4/ip_forward
```

La respuesta ahora debe ser «1».

Si verificamos ahora todos los adaptadores de red, podremos ver que «vpn_se» no tiene una dirección IP.

```
1ifconfig
```

Debe devolver algo como esto:

```
1[...]
```

```
2vpn_se: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
3ether 5e:53:bb:71:6b:61 txqueuelen 1000 (Ethernet)
```

```
4RX packets 0 bytes 0 (0.0 B)
```

```
5RX errors 0 dropped 0 overruns 0 frame 0
```

```
6TX packets 5 bytes 1710 (1.6 KiB)
```

```
7TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Para que la interfaz virtual obtenga una dirección ip, configuramos el cliente dhcp de Linux:

```
1dhclient vpn_se
```

Pasado un momento, volvemos a encuestar el adaptador de red y veremos que ya cuenta con una dirección IP:

```
1ifconfig
```

Debe devolver algo como esto:

```
1[...]
```

```
2vpn_se: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
3inet 192.168.5.10 netmask 255.255.255.0 broadcast 192.168.5.255
```

```
4ether 5e:53:bb:71:6b:61 txqueuelen 1000 (Ethernet)
```

```
5RX packets 316 bytes 25348 (24.7 KiB)
```

```
6RX errors 0 dropped 0 overruns 0 frame 0
```

```
7TX packets 207 bytes 17862 (17.4 KiB)
```

```
8TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Si usted realizó todos los pasos anteriores, usted ya cuenta con un servidor cliente SoftEther para Linux totalmente funcional.

AUTOMATIZANDO UN POCO EL SERVICIO EN EL CLIENTE

Creemos un servicio de systemd para el cliente de softether:

```
1nano /lib/systemd/system/softethervpn-client.service
```

Agregar lo siguiente:

```
1[Unit]
```

```
2Description=SoftEther VPN Server
```

```
3After=network.target
```

```
4
```

```
5[Service]
```

```
6Type=forking
```

```
7ExecStart=/usr/local/vpnclient/vpnclient start
```

```
8ExecStop=/usr/local/vpnclient/vpnclient stop
```

```
9
```

```
10[Install]
```

```
11WantedBy=multi-user.target
```

Ahora el servidor vpn inicia automáticamente cuando inicie el sistema, y podemos gestionar el servidor via systemctl:

NOTA:

Si al reiniciar no levanta el demonio, lo haremos mediante un script:

```
1mkdir -p /config/scripts
```

```
2nano /config/scripts/softethervpn-client.startup.sh
```

Agregar lo siguiente:

```
1#!/bin/sh
```

```
2
```

```
3#-----
```

```
4# El objetivo de este script es iniciar el servicio de softethervpn-client
```

```
5#-----
```

```
6
```

```
7systemctl start softethervpn-client
```

Damos los permisos de ejecución:

```
1chmod +x /config/scripts/softethervpn-client.startup.sh
```

Editamos el cron para una tarea programada al inicio del sistema:

```
1crontab -e
```

Seleccionar el editor preferido, y agregar lo siguiente y agregamos lo siguiente:

```
1 #####
```

```
2 # LEYENDA #
```

```
3 #####
```

```
4
```

```
5 # "m": minutos (0-59)
```

```
6 # "h": horas (0-23)
```

```
7 # "dow": dia de la semana (0-6)
```

```
8 # "dom": dia del mes (1-28/1-30/1-31)
```

```
9 # "mon": mes (1-12)
```

```
10# "*" : cualquiera
```

```
11# ",": separa valores dentro de la misma variable (0,5,10)
```

```
12# "-": define rangos dentro de la misma variable (0-5)
```

```
13# m h dom mon dow ruta_hacia_script
```

```
14
```

```
15#####
```

```
16# SOFTETHER #
```

```
17#####
```

```
18
```

19# Al iniciar el sistema

```
20@reboot /config/scripts/softethervpn-client.startup.sh
```

Automatizamos la conexión al servidor vpn con el inicio del sistema:

```
1/usr/local/vpnclient/vpnclient
```

Seleccionamos la 2da opción y establecemos una conexión al «localhost» como ya hemos hecho anteriormente. Después de haber hecho esto definimos que al iniciar el servicio se inicie la conexión con el servidor vpn especificado:

```
1VPN Client>accountstartupset
```

```
2AccountStartupSet command - Set VPN Connection Setting as Startup Connection
```

```
3Name of VPN Connection Setting: vpn-vhub1
```

```
4
```

```
5The command completed successfully.
```

Con todo esto su sistema iniciará con el sistema el servicio «softethervpn-client» y establecerá una conexión automática con el servidor vpn especificado. Sólo resta ejecutar el cliente dhcp para la interfaz de red virtual «vpn_se».

CONFIGURACIÓN DEL «SOFTETHER VPN CLIENT MANAGER» PARA WINDOWS

PAQUETES NECESARIOS

softether-vpnclient-v4.28-9669-beta-2018.09.11-windows-x86_x64-intel.exe

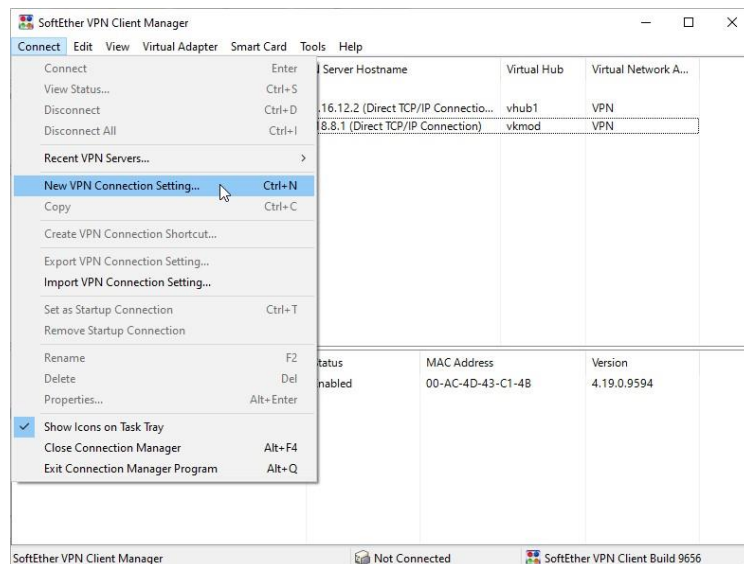
Descargar desde el siguiente enlace:

https://www.softether-download.com/files/softether/v4.28-9669-beta-2018.09.11-tree/Windows/SoftEther_VPN_Client/softether-vpnclient-v4.28-9669-beta-2018.09.11-windows-x86_x64-intel.exe

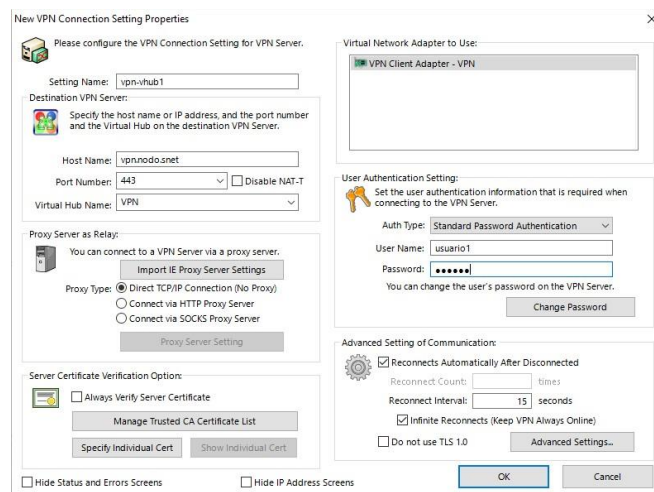
PROCEDIMIENTO

Después de instalado el cliente, cuando se ejecute dará la opción de añadir una nueva conexión VPN. Pedirá crear un adaptador de red virtual, al cual usted debe darle el nombre de «VPN». Si más adelante crea un nuevo adaptador, debe nombrarlo por «VPN2», y así sucesivamente cambiará el número con tantos adaptadores se creen.

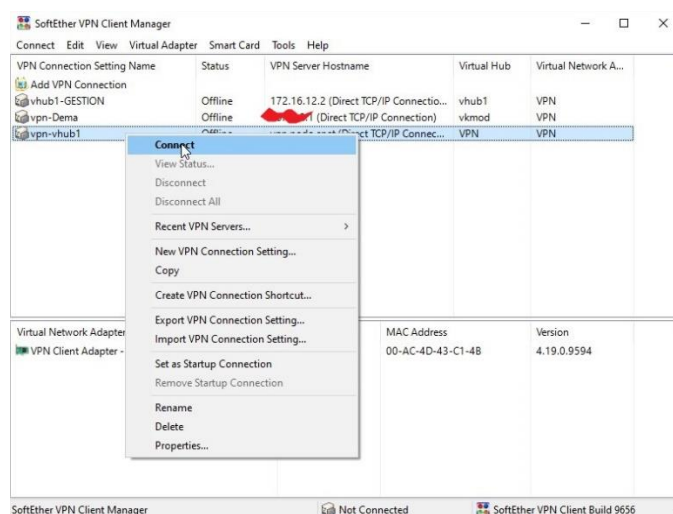
Para configurar una conexión seguir los pasos descritos por las siguientes imágenes: Ejecutamos el cliente y nos desplazamos a la pestaña «Connect» y seleccionamos «New VPN Connection Setting...»:



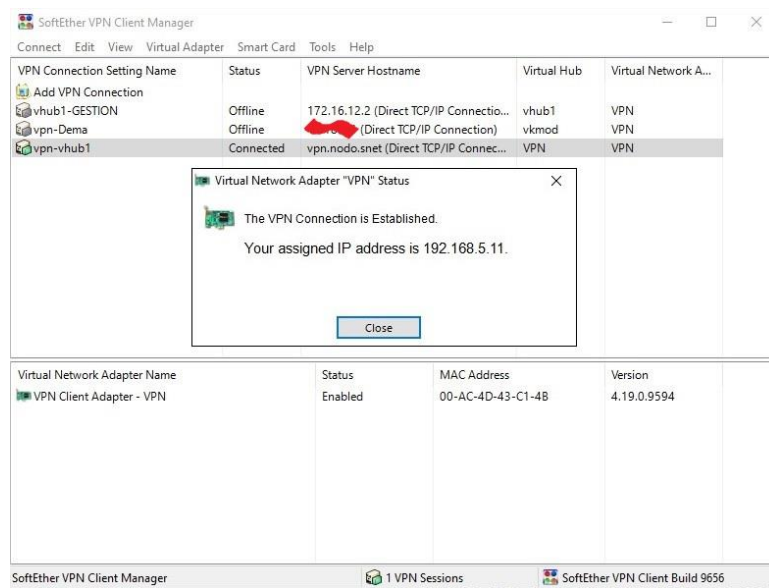
Llenamos los datos necesarios para la conexión con el servidor:



Nos ubicamos encima de la nueva vpn configurada y damos click derecho y «Connect»:



Veremos cómo nos saldrá la nueva IP asignada, tras conectarnos al VPN:



Con esto ya usted tiene su cliente vpn para SoftEther configurado en Windows.