SoftEther VPN

Autor: Sergio Ibáñez Núñez
Curso: 2ºASIR

Indice

Introducción

¿Que es una VPN?

VPN (Virtual Private Network) es una tecnología de red que permite conectar uno o más ordenadores en una red privada virtual, a través de una red pública como Internet, sin necesidad de que los ordenadores estén conectados físicamente entre sí o de que estén en un mismo lugar.

De esta forma, dos dispositivos o más pueden conectarse e intercambiar datos de forma segura y privada a través de un usuario y contraseña.

¿Que es Softether?

Softether VPN es uno de los softwares VPN multiprotocolo mas potentes y rápidos del mundo actualmente. Funciona en sistemas Windows, Solaris, Mac, FreeBSD y algunas distribuciones de Linux. Ademas de ser de software libre, tambien es una alternativa muy buena a openvpn y a los servidores VPN de microsoft.

Una de las funciones con las que cuenta este software es la de clonación de openvpn server, mediante la cual si se tiene un server openvpn, este se puede convertir rápidamente en un server Softether.

Características de SoftEther

- De código abierto.
- Fácil de establecer conexiones VPN tanto remotas como de sitio a sitio.
- Tunelacion SSL-VPN en HTTPS para pasar a través de NAT y Firewalls.
- Funciones VPN sobre ICMP y DNS.
- 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.
- Rendimiento de rendimiento de alta velocidad de clase 1Gbps con bajo uso de memoria y CPU.

- SSL-VPN (HTTPS) y los 6 protocolos principales de VPN (OpenVPN, IPsec, L2TP, MS-SSTP, L2TPv3 y EtherIP) son compatibles como protocolos subyacentes de tunelización VPN.
- La función de clonación de OpenVPN admite clientes de OpenVPN heredados.
- Función de autenticación de usuario de dominio RADIUS / NT
- Función de autenticación de certificado RSA
- Función de registro de paquetes de inspección profunda
- Función de lista de control de dirección IP de origen
- Función de transferencia de syslog

DNS Integrado

La función DDNS registra la dirección IP de su servidor VPN en el registro DNS de ".softether.net", que es el sufijo de dominio operado por SoftEther Corporation y la Universidad de Tsukuba, de forma gratuita.

Se asignará un DDNS FQDN a su servidor VPN SoftEther. Puede decirle el nombre de host DDNS a los usuarios de su servidor VPN. Un usuario de su servidor VPN ahora puede especificar el nombre de host DDNS como destino. Si la dirección IP correspondiente se cambiará repentinamente en el futuro, la dirección IP registrada del nombre de host DDNS seguirá a la nueva IP.

NAT Transversal

Al utilizar los sistemas VPN existentes, se debe pedir al admin del firewall de la empresa que abra un punto final (puerto TCP o UDP) en el firewall / NAT en la frontera entre la empresa e Internet. Para reducir la necesidad de abrir un punto final en el firewall, SoftEther VPN Server tiene la función "NAT Traversal".

NAT Traversal está habilitado de forma predeterminada. Mientras está habilitado, las maquinas del Cliente VPN SoftEther pueden conectarse a su Servidor VPN detrás del firewall / NAT. No se necesitan configuraciones especiales en el firewall / NAT.

Protocolos que usa softether

- **L2TP/IPsec** - Internet Protocol security - Esta función es para aceptar conexiones VPN desde iPhone, iPad, Android, Windows y Mac OS X.
- **MS-SSTP** - Microsoft Secure Socket Tunneling Protocol - Implementa PPP sobre HTTPS (SSL). Encapsula todos los paquetes de usuario en TCP. Para que pueda pasar el cortafuegos fácilmente.
- **L2TPv3** - puede establecer un túnel cifrado con IPsec entre el enrutador Cisco del sitio remoto y el servidor VPN SoftEther.
- **EtherIP** - protocolo de tunelacion ethernet.
- **SSL-VPN** - para segurizar las conexiones.

Diferencias con Open VPN y Wireguard

	OpenVPN	Wireguard	SoftetherVPN
Rendimiento (velocidad de conexión)	100 mbps	900 mbps (aprox)	1 Gbps
Configuración	sencilla	sencilla	sencilla
Seguridad	baja	media-alta	alta
Estabilidad	buena	buena	buena
Transmisión de contenido	medio	alto	alto

Tipos de autentificaciones

- **UserNTLMSet** - Autentificación de dominio Windows NT haciendo uso de AD.
- **UserSignedSet** - Autentificación por certificado firmado.
- **Anónimo** - Autentificación usada en servidores públicos donde no es necesario saber quien se conecta al servidor.
- **Contraseña** - Autentificacion por contraseña de toda la vida.
- **Certificado** - Autentificacion haciendo uso de un certificado creado en el propio servidor softether a traves del comando certcreate o bien haciendo uso de otras herramientas como let's encrypt.
- **Radius** - Es un protocolo cliente-servidor mediante el cual, en la maquina cliente si quiere autenticarse para acceder a un servidor, manda primero un mensaje al servidor Radius, este si esta bien configurado dará o no el visto bueno al usuario, si el usuario tiene permitido el acceso se confirmara y se establecera la conexion con el servior mientras que si el usuario no tiene permitida la conexion se rechazara el intento de autentificacion.

Server SoftEther VPN (Ubuntu Xenial)

Empezamos actualizando el sistema:

```
root@server-vpn:/home/vagrant# apt update
root@server-vpn:/home/vagrant# apt upgrade
```

Instalamos los paquetes necesarios para poder compilar softether y asi hacer uso del server:

```
root@server-vpn:/home/vagrant# apt install build-essential
```

Para descargar softether vpn mediante comandos podemos hacer uso de los comandos lynx, wget o curl, en mi caso he usado el comando lynx:

```
root@server-vpn:/home/vagrant# apt install lynx
root@server-vpn:/home/vagrant# lynx http://www.softether-download.com/files/softether/
```

Cuando tengamos el fichero descargado, primero lo descomprimimos y despues entramos en el directorio vpnserver que se nos crea y compilamos los ficheros de forma que softether pueda ser usado:

```
root@server-vpn:/home/vagrant# tar xzvf softether-vpnserver-v4.34-9745-rtm-2020.04.05-linux-x64-64bit.tar.gz
vpnserver/
vpnserver/Makefile
vpnserver/.install.sh
vpnserver/ReadMeFirst_License.txt
vpnserver/Authors.txt
vpnserver/ReadMeFirst_Important_Notices_ja.txt
vpnserver/ReadMeFirst_Important_Notices_en.txt
vpnserver/ReadMeFirst_Important_Notices_cn.txt
```

vpnserver/code/

vpnserver/code/vpnserver.a

vpnserver/code/vpncmd.a

vpnserver/lib/

vpnserver/lib/libcharset.a

vpnserver/lib/libcrypto.a

vpnserver/lib/libedit.a

vpnserver/lib/libiconv.a

vpnserver/lib/libintelaes.a

vpnserver/lib/libncurses.a

vpnserver/lib/libssl.a

vpnserver/lib/libz.a

vpnserver/lib/License.txt

vpnserver/hamcore.se2

root@server-vpn:/home/vagrant# cd vpnserver/

root@server-vpn:/home/vagrant/vpnserver# make

SoftEther VPN Server (Ver 4.34, Build 9745, Intel x64 / AMD64) for Linux Install Utility

---

Do you want to read the License Agreement for this software ?

1. Yes
2. No

Please choose one of above number:

1

DISCLAIMER

==========

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

THIS SOFTWARE IS DEVELOPED IN JAPAN, AND DISTRIBUTED FROM JAPAN, UNDER JAPANESE LAWS. YOU MUST AGREE IN ADVANCE TO USE, COPY, MODIFY, MERGE, PUBLISH, DISTRIBUTE, SUBLICENSE, AND/OR SELL COPIES OF THIS SOFTWARE, THAT ANY JURIDICAL DISPUTES WHICH ARE CONCERNED TO THIS SOFTWARE OR ITS CONTENTS, AGAINST US (SOFTETHER PROJECT, SOFTETHER CORPORATION, DAIYUU NOBORI OR OTHER SUPPLIERS), OR ANY JURIDICAL DISPUTES AGAINST US WHICH ARE CAUSED BY ANY KIND OF USING, COPYING, MODIFYING, MERGING, PUBLISHING, DISTRIBUTING, SUBLICENSING, AND/OR SELLING COPIES OF THIS SOFTWARE SHALL BE REGARDED AS BE CONSTRUED AND CONTROLLED BY JAPANESE LAWS, AND YOU MUST FURTHER CONSENT TO EXCLUSIVE JURISDICTION

AND VENUE IN THE COURTS SITTING IN TOKYO, JAPAN. YOU MUST WAIVE ALL DEFENSES OF LACK OF PERSONAL JURISDICTION AND FORUM NON CONVENIENS. PROCESS MAY BE SERVED ON EITHER PARTY IN THE MANNER AUTHORIZED BY APPLICABLE LAW OR COURT RULE.

USE ONLY IN JAPAN. DO NOT USE THIS SOFTWARE IN ANOTHER COUNTRY UNLESS YOU HAVE A CONFIRMATION THAT THIS SOFTWARE DOES NOT VIOLATE ANY CRIMINAL LAWS OR CIVIL RIGHTS IN THAT PARTICULAR COUNTRY. USING THIS SOFTWARE IN OTHER COUNTRIES IS COMPLETELY AT YOUR OWN RISK. THE SOFTETHER VPN PROJECT HAS DEVELOPED AND DISTRIBUTED THIS SOFTWARE TO COMPLY ONLY WITH THE JAPANESE LAWS AND EXISTING CIVIL RIGHTS INCLUDING PATENTS WHICH ARE SUBJECTS APPLY IN JAPAN. OTHER COUNTRIES' LAWS OR CIVIL RIGHTS ARE NONE OF OUR CONCERNS NOR RESPONSIBILITIES. WE HAVE NEVER INVESTIGATED ANY CRIMINAL REGULATIONS, CIVIL LAWS OR INTELLECTUAL PROPERTY RIGHTS INCLUDING PATENTS IN ANY OF OTHER 200+ COUNTRIES AND TERRITORIES. BY NATURE, THERE ARE 200+ REGIONS IN THE WORLD, WITH DIFFERENT LAWS. IT IS IMPOSSIBLE TO VERIFY EVERY COUNTRIES' LAWS, REGULATIONS AND CIVIL RIGHTS TO MAKE THE SOFTWARE COMPLY WITH ALL COUNTRIES' LAWS BY THE PROJECT. EVEN IF YOU WILL BE SUED BY A PRIVATE ENTITY OR BE DAMAGED BY A PUBLIC SERVANT IN YOUR COUNTRY, THE DEVELOPERS OF THIS SOFTWARE WILL NEVER BE LIABLE TO RECOVER OR COMPENSATE SUCH DAMAGES, CRIMINAL OR CIVIL

RESPONSIBILITIES. NOTE THAT THIS LINE IS NOT LICENSE RESTRICTION BUT JUST A STATEMENT FOR WARNING AND DISCLAIMER.

READ AND UNDERSTAND THE 'src/WARNING.TXT' FILE BEFORE USING THIS SOFTWARE. SOME SOFTWARE PROGRAMS FROM THIRD PARTIES ARE INCLUDED ON THIS SOFTWARE WITH LICENSE CONDITIONS WHICH ARE DESCRIBED ON THE 'src/THIRD_PARTY.TXT' FILE.

Did you read and understand the License Agreement ?

(If you couldn't read above text, Please read 'ReadMeFirst_License.txt'

file with any text editor.)

1. Yes
2. No

Please choose one of above number:

1

Did you agree the License Agreement ?

1. Agree

2. Do Not Agree

Please choose one of above number:

1

make[1]: Entering directory '/home/vagrant/vpnserver'

Preparing SoftEther VPN Server...

ranlib lib/libcharset.a

ranlib lib/libcrypto.a

ranlib lib/libedit.a

ranlib lib/libiconv.a

ranlib lib/libintelaes.a

ranlib lib/libncurses.a

ranlib lib/libssl.a

ranlib lib/libz.a

ranlib code/vpnserver.a

gcc code/vpnserver.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpnserver

ranlib code/vpncmd.a

gcc code/vpncmd.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpncmd

./vpncmd /tool /cmd:Check

vpncmd command - SoftEther VPN Command Line Management Utility

SoftEther VPN Command Line Management Utility (vpncmd command)

Version 4.34 Build 9745   (English)

Compiled 2020/04/05 23:39:56 by buildsan at crosswin

VPN Tools has been launched. By inputting HELP, you can view a list of the commands that can be used.

VPN Tools>Check

Check command - Check whether SoftEther VPN Operation is Possible

---

SoftEther VPN Operation Environment Check Tool

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...

Checking 'Kernel System'...

Pass

Checking 'Memory Operation System'...

Pass

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

Pass

Checking 'File system'...

Pass

Checking 'Thread processing system'...

Pass

Checking 'Network system'...

Pass

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

The command completed successfully.

The preparation of SoftEther VPN Server is completed !

*** How to switch the display language of the SoftEther VPN Server Service ***

SoftEther VPN Server supports the following languages:

- Japanese
- English
- Simplified Chinese

You can choose your prefered language of SoftEther VPN Server at any time.

To switch the current language, open and edit the 'lang.config' file.

Note: the administrative password is not set on the VPN Server. Please set your own administrative password as soon as possible by vpncmd or the GUI manager.

*** How to start the SoftEther VPN Server Service ***

Please execute './vpnserver start' to run the SoftEther VPN Server Background Service.

And please execute './vpncmd' to run the SoftEther VPN Command-Line Utility to configure SoftEther VPN Server.

Of course, you can use the VPN Server Manager GUI Application for Windows / Mac OS X on the other Windows / Mac OS X computers in order to configure the SoftEther VPN Server remotely.

*** For Windows users ***

You can download the SoftEther VPN Server Manager for Windows

from the http://www.softether-download.com/ web site.

This manager application helps you to completely and easily manage the VPN server services running in remote hosts.

*** For Mac OS X users ***

In April 2016 we released the SoftEther VPN Server Manager for Mac OS X.

You can download it from the http://www.softether-download.com/ web site.

VPN Server Manager for Mac OS X works perfectly as same as the traditional Windows versions. It helps you to completely and easily manage the VPN server services running in remote hosts.

*** PacketiX VPN Server HTML5 Web Administration Console (NEW) ***

This VPN Server / Bridge has the built-in HTML5 Web Administration Console.

After you start the server daemon, you can open the HTML5 Web Administration Console is available at

https://127.0.0.1:5555/

or

https://ip_address_of_the_vpn_server:5555/

This HTML5 page is obviously under construction, and your HTML5 development contribution is very appreciated.

---

make[1]: Leaving directory '/home/vagrant/vpnserver'

A la hora de compilar softether hay que tener en cuenta dos cosas, la primera que tenemos que responder a las preguntas que se nos muestran con la opción 1 para aceptar los términos de licencia, la segunda que a la hora de checkear la compilación, debe tener aprobadas todas las configuraciones, sino el programa no se compilara y no podrá usarse.

Ahora podemos ejecutar nuestro servidor ejecutando ./vpnserver start, pero en su lugar configuraremos softether como un daemon:

```
root@server-vpn:/home/vagrant/vpnserver# cd ..
root@server-vpn:/home/vagrant# mv vpnserver /usr/local
root@server-vpn:/home/vagrant# cd /usr/local/vpnserver/
root@server-vpn:/usr/local/vpnserver# sudo chmod 600 *
root@server-vpn:/usr/local/vpnserver# sudo chmod 700 vpnserver
root@server-vpn:/usr/local/vpnserver# sudo chmod 700 vpncmd
```

Creamos el servicio systemd para softether creando el servicio vpnserver en /lib/systemd/system/ con el siguiente contenido:

```
[Unit]
Description=SoftEther VPN Server
After=network.target

[Service]
Type=forking
ExecStart=/usr/local/vpnserver/vpnserver start
ExecStop=/usr/local/vpnserver/vpnserver stop

[Install]
WantedBy=multi-user.target
```

```
root@server-vpn:/usr/local/vpnserver# systemctl status vpnserver
● vpnserver.service - SoftEther VPN Server
   Loaded: loaded (/lib/systemd/system/vpnserver.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-11-28 10:42:35 UTC; 5s ago
  Process: 8395 ExecStart=/usr/local/vpnserver/vpnserver start (code=exited, status=0/SUCCESS)
 Main PID: 8400 (vpnserver)
```

```
 Tasks: 33
Memory: 17.1M
   CPU: 348ms
CGroup: /system.slice/vpnserver.service
        ├─8400 /usr/local/vpnserver/vpnserver execsvc
        └─8401 /usr/local/vpnserver/vpnserver execsvc

Nov 28 10:42:35 server-vpn systemd[1]: Starting SoftEther VPN Server...
Nov 28 10:42:35 server-vpn vpnserver[8395]: The SoftEther VPN Server service has been started.
Nov 28 10:42:35 server-vpn vpnserver[8395]: Let's get started by accessing to the following URL from your PC:
Nov 28 10:42:35 server-vpn vpnserver[8395]: https://10.0.2.15:5555/
Nov 28 10:42:35 server-vpn vpnserver[8395]:    or
Nov 28 10:42:35 server-vpn vpnserver[8395]: https://10.0.2.15/
Nov 28 10:42:35 server-vpn vpnserver[8395]: Note: IP address may vary. Specify your server's IP address.
Nov 28 10:42:35 server-vpn vpnserver[8395]: A TLS certificate warning will appear because the server uses self signed certificate by default. That is natural. Continue with
Nov 28 10:42:35 server-vpn systemd[1]: Started SoftEther VPN Server.
```

Configuración inicial del servidor

Empezamos poniéndole una contraseña de administrador:

```
root@server-vpn:/usr/local/vpnserver# ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.34 Build 9745   (English)
Compiled 2020/04/05 23:39:56 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

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

1. Management of VPN Server or VPN Bridge

2. Management of VPN Client

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

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is operating on.

By specifying according to the format 'host name:port number', you can also specify the port number.

(When the port number is unspecified, 443 is used.)

If nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer).

Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.

If connecting by server admin mode, please press Enter without inputting anything.

Specify Virtual Hub Name:

Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>ServerPasswordSet

ServerPasswordSet command - Set VPN Server Administrator Password

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

Password: ********** #admin-server

Confirm input: **********

The command completed successfully.

Para poder usar Softether lo primero será crear un concentrador virtual o hub al que posteriormente se puedan conectar los clientes.

```
VPN Server>HubCreate Empresa

HubCreate command - Create New Virtual Hub

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


Password: ********** #admin-server

Confirm input: **********



The command completed successfully.
```

Por otro lado, empezaremos a configurar un puente local para que los clientes en la misma red puedan conectarse sin problemas. Este puente local se puede hacer de dos formas, la primera es usando la función de SecureNAT:

```
VPN Server/VPN1>SecureNatEnable

SecureNatEnable command - Enable the Virtual NAT and DHCP Server Function (SecureNat Function)

The command completed successfully.
```

En el caso de hacerlo creando la interfaz tap, tendríamos que hacer lo siguiente:

```
VPN Server>BridgeCreate /DEVICE:"soft" /TAP:yes Empresa

BridgeCreate command - Create Local Bridge Connection

While in the condition that occurs immediately after a new bridge connection is made when bridging to a physical network adapter, depending on the type of network adapter, there are cases where it will not be possible to communicate using TCP/IP to the network adapter using a bridge connection from a computer on the virtual network.

(This phenomenon is known to occur for Intel and Broadcom network adapters.)
```

If this issue arises, remedy the situation by restarting the computer on which VPN Server / Bridge is running. Normal communication will be possible after the computer has restarted.

Also many wireless network adapters will not respond to the sending of packets in promiscuous mode and when this occurs you will be unable to use the Local Bridge. If this issue arises, try using a regular wired network adapter instead of the wireless network adapter.

Instructions for Local Bridge on VM

It has been detected that the VPN Server might be running on a VM (Virtual Machine) suchlike VMware or Hyper-V. Read the following instructions carefully. If you are not using a VM, please ignore this message.

Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by default.

If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled, the Local Bridge function between a Virtual Hub on the VPN Server and a physical network adapter on the physical computer does not work well. You should allow the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM.

For details please refer the documents of your VM. If it is a shared-VM and administrated by other person, please request the administrator to permit the use of the Promiscuous (MAC Address Spoofing) Mode to your VM.

The command completed successfully.

Esta creación de puente local es posible que muestre un error de privilegios insuficientes, es necesario asegurarse de que el controlador de red usado este configurado en modo promiscuo.

Ahora una vez creado el puente local, crearemos los usuarios necesarios que tendrán acceso a el, dichos usuarios pueden tener distintos métodos de autentificación (contraseña, certificado, RADIUS, NTLM y otros) metiendolos en un grupo.

VPN Server/Empresa>UserCreate sergio

UserCreate command - Create User

Assigned Group Name:

User Full Name: sergio

User Description: sergio

The command completed successfully.

VPN Server/Empresa>UserPasswordSet sergio
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
Please enter the password. To cancel press the Ctrl+D key.

Password: ********** #usuario-01
Confirm input: **********

The command completed successfully.

VPN Server/Empresa>UserCreate invitado
UserCreate command - Create User
Assigned Group Name:

User Full Name: prueba

User Description: usuario de pruebas

The command completed successfully.

VPN Server/Empresa>UserPasswordSet invitado
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
Please enter the password. To cancel press the Ctrl+D key.

Password: ********** #usuario-02

```
Confirm input: **********


The command completed successfully.
```

Ahora configuramos L2TP/IPSec para que de esta forma puedan conectarse dispositivos Android, Iphone o Mac:

```
VPN Server/Empresa>IPsecEnable
IPsecEnable command - Enable or Disable IPsec VPN Server Function
Enable L2TP over IPsec Server Function (yes / no): yes

Enable Raw L2TP Server Function (yes / no): yes

Enable EtherIP / L2TPv3 over IPsec Server Function (yes / no): yes

Pre Shared Key for IPsec (Recommended: 9 letters at maximum): softether

Default Virtual HUB in a case of omitting the HUB on the Username: Empresa

The command completed successfully.
```

Generamos un certificado para que los clientes puedan acceder al servidor a través de un certificado:

```
VPN Server/Empresa>ServerCertRegenerate
ServerCertRegenerate command - Generate New Self-Signed Certificate with Specified CN (Common Name) and Register on VPN Server
Value of Common Name (CN): server-vpn


A new server certificate has been set.
```

If you are using OpenVPN protocols, please mind that you may have to update the inline certificate data in the OpenVPN configuration file.

The command completed successfully.

VPN Server/Empresa>ServerCertGet ~/cert.cer

ServerCertGet command - Get SSL Certificate of VPN Server

The command completed successfully.

Habilitamos la función sstp para poder enviar los certificados creados a los clientes:

VPN Server/Empresa>SstpEnable yes

SstpEnable command - Enable / Disable Microsoft SSTP VPN Clone Server Function

The command completed successfully.

Habilitamos openvpn para que si algún cliente usa openvpn pueda conectarse:

VPN Server/Empresa>OpenVpnEnable yes /PORTS:1194

OpenVpnEnable command - Enable / Disable OpenVPN Clone Server Function

The command completed successfully.

Creamos una configuración openvpn por si se da el caso de que los clientes tengan openvpn:

VPN Server/Empresa>OpenVpnMakeConfig ~/openvpn_config.zip

OpenVpnMakeConfig command - Generate a Sample Setting File for OpenVPN Client

The sample setting file was saved as "~/openvpn_config.zip". You can unzip this file to extract setting files.

The command completed successfully.

Habilitamos tanto icmp como dns (En caso de haber creado la interfaz tap, con SecureNAT no es necesario):

```
VPN Server/Empresa>VpnOverIcmpDnsEnable /ICMP:yes /DNS:yes

VpnOverIcmpDnsEnable command - Enable / Disable the VPN over ICMP / VPN over DNS Server Function

The command completed successfully.
```

Configuramos dns y dhcp

```
root@server-vpn:/usr/local/vpnserver# service vpnserver stop

root@server-vpn:/usr/local/vpnserver# echo interface=tap_soft >> /etc/dnsmasq.conf

root@server-vpn:/usr/local/vpnserver# echo dhcp-range=tap_soft,192.168.1.50,192.168.1.200,12h >> /etc/dnsmasq.conf

root@server-vpn:/usr/local/vpnserver# echo dhcp-option=tap_soft,3,192.168.1.1 >> /etc/dnsmasq.conf

root@server-vpn:/usr/local/vpnserver# echo port=0 >> /etc/dnsmasq.conf

root@server-vpn:/usr/local/vpnserver# echo dhcp-option=option:dns-server,8.8.8.8 >> /etc/dnsmasq.conf

root@server-vpn:/usr/local/vpnserver# echo net.ipv4.ip_forward = 1 >> /etc/sysctl.d/ipv4_forwarding.conf
```

Aplicamos los cambios:

```
root@server-vpn:/usr/local/vpnserver# sysctl -n -e --system

* Applying /etc/sysctl.d/10-console-messages.conf ...

4 4 1 7

* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...

2

2

* Applying /etc/sysctl.d/10-kernel-hardening.conf ...

1

* Applying /etc/sysctl.d/10-link-restrictions.conf ...

1
```

```
1
* Applying /etc/sysctl.d/10-lxd-inotify.conf ...
1024
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
176
* Applying /etc/sysctl.d/10-network-security.conf ...
1
1
1
* Applying /etc/sysctl.d/10-ptrace.conf ...
1
* Applying /etc/sysctl.d/10-zeropage.conf ...
65536
* Applying /etc/sysctl.d/99-cloudimg-ipv6.conf ...
0
0
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.d/ipv4_forwarding.conf ...
1
* Applying /etc/sysctl.conf ...
```

Instalación del cliente1

Actualizamos el cliente:

```
root@cliente-vpn:/home/vagrant# apt update
root@cliente-vpn:/home/vagrant# apt upgrade
```

Instalamos softether con lynx:

```
root@cliente-vpn:/home/vagrant# lynx http://www.softether-download.com/files/softether/
```

Instalamos los paquetes necesarios:

```
root@cliente-vpn:/home/vagrant# apt install build-essential
```

Descomprimimos el fichero:

```
root@cliente-vpn:/home/vagrant# tar xzvf softether-vpnclient-v4.34-9745-rtm-2020.04.05-linux-x64-64bit.tar.gz
vpnclient/
vpnclient/Makefile
vpnclient/.install.sh
vpnclient/ReadMeFirst_License.txt
vpnclient/Authors.txt
vpnclient/ReadMeFirst_Important_Notices_ja.txt
vpnclient/ReadMeFirst_Important_Notices_en.txt
vpnclient/ReadMeFirst_Important_Notices_cn.txt
vpnclient/code/
vpnclient/code/vpnclient.a
vpnclient/code/vpncmd.a
vpnclient/lib/
vpnclient/lib/libcharset.a
vpnclient/lib/libcrypto.a
vpnclient/lib/libedit.a
vpnclient/lib/libiconv.a
vpnclient/lib/libintelaes.a
vpnclient/lib/libncurses.a
vpnclient/lib/libssl.a
vpnclient/lib/libz.a
vpnclient/lib/License.txt
vpnclient/hamcore.se2
```

Compilamos el fichero:

```
root@cliente-vpn:/home/vagrant# cd vpnclient/
root@cliente-vpn:/home/vagrant/vpnclient# make
--------------------------------------------------------------------

SoftEther VPN Client (Ver 4.34, Build 9745, Intel x64 / AMD64) for Linux Install Utility
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Reserved.

--------------------------------------------------------------------



Do you want to read the License Agreement for this software ?

 1. Yes
 2. No

Please choose one of above number:
1

Copyright (c) all contributors on SoftEther VPN project in GitHub.
Copyright (c) Daiyuu Nobori, SoftEther Project at University of Tsukuba, and SoftEther Corporation.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0
```

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

DISCLAIMER

==========

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

THIS SOFTWARE IS DEVELOPED IN JAPAN, AND DISTRIBUTED FROM JAPAN, UNDER JAPANESE LAWS. YOU MUST AGREE IN ADVANCE TO USE, COPY, MODIFY, MERGE, PUBLISH, DISTRIBUTE, SUBLICENSE, AND/OR SELL COPIES OF THIS SOFTWARE, THAT ANY JURIDICAL DISPUTES WHICH ARE CONCERNED TO THIS SOFTWARE OR ITS CONTENTS, AGAINST US (SOFTETHER PROJECT, SOFTETHER CORPORATION, DAIYUU NOBORI OR OTHER SUPPLIERS), OR ANY JURIDICAL DISPUTES AGAINST US WHICH ARE CAUSED BY ANY KIND OF USING, COPYING, MODIFYING, MERGING, PUBLISHING, DISTRIBUTING, SUBLICENSING, AND/OR SELLING COPIES OF THIS SOFTWARE SHALL BE REGARDED AS BE CONSTRUED AND CONTROLLED BY JAPANESE LAWS, AND YOU MUST FURTHER CONSENT TO EXCLUSIVE JURISDICTION AND VENUE IN THE COURTS SITTING IN TOKYO, JAPAN. YOU MUST WAIVE ALL DEFENSES OF LACK OF PERSONAL JURISDICTION AND FORUM NON CONVENIENS. PROCESS MAY BE SERVED ON EITHER PARTY IN THE MANNER AUTHORIZED BY APPLICABLE LAW OR COURT RULE.

USE ONLY IN JAPAN. DO NOT USE THIS SOFTWARE IN ANOTHER COUNTRY UNLESS YOU HAVE A CONFIRMATION THAT THIS SOFTWARE DOES NOT VIOLATE ANY CRIMINAL LAWS OR CIVIL RIGHTS IN THAT PARTICULAR COUNTRY. USING THIS SOFTWARE IN OTHER COUNTRIES IS COMPLETELY AT YOUR OWN RISK. THE SOFTETHER VPN PROJECT HAS DEVELOPED AND DISTRIBUTED THIS SOFTWARE TO COMPLY ONLY WITH THE JAPANESE LAWS AND EXISTING CIVIL RIGHTS INCLUDING PATENTS WHICH ARE SUBJECTS APPLY IN JAPAN. OTHER COUNTRIES' LAWS OR CIVIL RIGHTS ARE NONE OF OUR CONCERNS NOR RESPONSIBILITIES. WE HAVE

NEVER INVESTIGATED ANY CRIMINAL REGULATIONS, CIVIL LAWS OR INTELLECTUAL PROPERTY RIGHTS INCLUDING PATENTS IN ANY OF OTHER 200+ COUNTRIES AND TERRITORIES. BY NATURE, THERE ARE 200+ REGIONS IN THE WORLD, WITH DIFFERENT LAWS. IT IS IMPOSSIBLE TO VERIFY EVERY COUNTRIES' LAWS, REGULATIONS AND CIVIL RIGHTS TO MAKE THE SOFTWARE COMPLY WITH ALL COUNTRIES' LAWS BY THE PROJECT. EVEN IF YOU WILL BE SUED BY A PRIVATE ENTITY OR BE DAMAGED BY A PUBLIC SERVANT IN YOUR COUNTRY, THE DEVELOPERS OF THIS SOFTWARE WILL NEVER BE LIABLE TO RECOVER OR COMPENSATE SUCH DAMAGES, CRIMINAL OR CIVIL

RESPONSIBILITIES. NOTE THAT THIS LINE IS NOT LICENSE RESTRICTION BUT JUST A STATEMENT FOR WARNING AND DISCLAIMER.

READ AND UNDERSTAND THE 'src/WARNING.TXT' FILE BEFORE USING THIS SOFTWARE. SOME SOFTWARE PROGRAMS FROM THIRD PARTIES ARE INCLUDED ON THIS SOFTWARE WITH LICENSE CONDITIONS WHICH ARE DESCRIBED ON THE 'src/THIRD_PARTY.TXT' FILE.

Did you read and understand the License Agreement ?

(If you couldn't read above text, Please read 'ReadMeFirst_License.txt'

file with any text editor.)

1. Yes
2. No

Please choose one of above number:

1

Did you agree the License Agreement ?

1. Agree
2. Do Not Agree

Please choose one of above number:

```
1


make[1]: Entering directory '/home/vagrant/vpnclient'
Preparing SoftEther VPN Client...
ranlib lib/libcharset.a
ranlib lib/libcrypto.a
ranlib lib/libedit.a
ranlib lib/libiconv.a
ranlib lib/libintelaes.a
ranlib lib/libncurses.a
ranlib lib/libssl.a
ranlib lib/libz.a
ranlib code/vpnclient.a
gcc code/vpnclient.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpnclient
ranlib code/vpncmd.a
gcc code/vpncmd.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpncmd


---------------------------------------------------------------
The preparation of SoftEther VPN Client is completed !



*** How to switch the display language of the SoftEther VPN Client Service ***
SoftEther VPN Client supports the following languages:
  - Japanese
  - English
  - Simplified Chinese


You can choose your prefered language of SoftEther VPN Client at any time.
To switch the current language, open and edit the 'lang.config' file.
```

Note: the administrative password is not set on the VPN Server. Please set your own administrative password as soon as possible by vpncmd or the GUI manager.

*** How to start the SoftEther VPN Client Service ***

Please execute './vpnclient start' to run the SoftEther VPN Client Background Service.

And please execute './vpncmd' to run the SoftEther VPN Command-Line Utility to configure SoftEther VPN Client.

Of course, you can use the VPN Server Manager GUI Application for Windows / Mac OS X on the other Windows / Mac OS X computers in order to configure the SoftEther VPN Client remotely.

*** For Windows users ***

You can download the SoftEther VPN Server Manager for Windows

from the http://www.softether-download.com/ web site.

This manager application helps you to completely and easily manage the VPN server services running in remote hosts.

*** For Mac OS X users ***

In April 2016 we released the SoftEther VPN Server Manager for Mac OS X.

You can download it from the http://www.softether-download.com/ web site.

VPN Server Manager for Mac OS X works perfectly as same as the traditional Windows versions. It helps you to completely and easily manage the VPN server services running in remote hosts.

*** PacketiX VPN Server HTML5 Web Administration Console (NEW) ***

This VPN Server / Bridge has the built-in HTML5 Web Administration Console.

After you start the server daemon, you can open the HTML5 Web Administration Console is available at

https://127.0.0.1:5555/

or

https://ip_address_of_the_vpn_server:5555/

This HTML5 page is obviously under construction, and your HTML5 development contribution is very appreciated.

---

make[1]: Leaving directory '/home/vagrant/vpnclient'

Movemos el fichero a /usr/local y modificamos los permisos:

```
root@cliente-vpn:/usr/local/vpnclient# chmod 600 *
root@cliente-vpn:/usr/local/vpnclient# chmod 700 vpnclient
root@cliente-vpn:/usr/local/vpnclient# chmod 700 vpncmd
```

Iniciamos el cliente:

```
root@cliente-vpn:/usr/local/vpnclient# ./vpnclient start
```

Configuración del cliente1

Creamos un adaptador virtual:

```
VPN Client>NicCreate R1
NicCreate command - Create New Virtual Network Adapter
The command completed successfully.
```

```
VPN Client>AccountCreate Local

AccountCreate command - Create New VPN Connection Setting

Destination VPN Server Host Name and Port Number: 192.168.1.100:443


Destination Virtual Hub Name: Empresa


Connecting User Name: sergio


Used Virtual Network Adapter Name: R1


The command completed successfully.
```

```
VPN Client>AccountPasswordSet Local

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

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


Password: ********** #usuario-01

Confirm input: **********



Specify standard or radius: standard


The command completed successfully.
```

Conectamos el adaptador y comprobamos que se ha establecido una conexión con el servidor:

```
VPN Client>accountconnect Local

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

The command completed successfully.


VPN Client>AccountStatusGet Local
```

AccountStatusGet command - Get Current VPN Connection Setting Status

Item |Value

VPN Connection Setting Name |Local

Session Status |Connection Completed (Session Established)

VLAN ID |-

Server Name |192.168.1.100

Port Number |TCP Port 443

Server Product Name |SoftEther VPN Server (64 bit)

Server Version |4.34

Server Build |Build 9745

Connection Started at |2021-11-28 (Sun) 14:15:59

First Session has been Established since |2021-11-28 (Sun) 14:15:59

Current Session has been Established since|2021-11-28 (Sun) 14:15:59

Number of Established Sessions |1 Times

Half Duplex TCP Connection Mode |No (Full Duplex Mode)

VoIP / QoS Function |Enabled

Number of TCP Connections |2

Maximum Number of TCP Connections |2

Encryption |Enabled (Algorithm: TLS_AES_256_GCM_SHA384)

Use of Compression |No (No Compression)

Physical Underlay Protocol |Standard TCP/IP (IPv4)

|IPv4 UDPAccel_Ver=2 ChachaPoly_OpenSSL UDPAccel_MSS=1309

UDP Acceleration is Supported |Yes

UDP Acceleration is Active |Yes

Session Name |SID-SERGIO-2

Connection Name |CID-12

Session Key (160 bit) |DD15D51435FE05B59D80B97FF4AE0BB7FDC23D8F

Bridge / Router Mode |No

Monitoring Mode |No

Outgoing Data Size |9,713 bytes

Incoming Data Size |6,618 bytes

```
Outgoing Unicast Packets                |24 packets
Outgoing Unicast Total Size             |1,984 bytes
Outgoing Broadcast Packets              |8 packets
Outgoing Broadcast Total Size           |648 bytes
Incoming Unicast Packets                |10 packets
Incoming Unicast Total Size             |860 bytes
Incoming Broadcast Packets              |0 packets
Incoming Broadcast Total Size           |0 bytes
The command completed successfully.
```

A la hora de hacer dhclient comprobamos como el servidor nos da una ip del rango 192.168.30.X (que es la configuración por defecto que ofrece SecureNat y que podremos cambiar en cualquier momento):

```
root@cliente-vpn:/usr/local/vpnclient# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:be:82:6b:cc:1d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::be:82ff:fe6b:cc1d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:e5:01:cd brd ff:ff:ff:ff:ff:ff
```

```
    inet 192.168.1.150/24 brd 192.168.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:1cd/64 scope link
       valid_lft forever preferred_lft forever
5: vpn_r1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN group default qlen 1000
    link/ether 5e:e3:d0:fa:69:b9 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::5ce3:d0ff:fefa:69b9/64 scope link
       valid_lft forever preferred_lft forever
```

```
root@cliente-vpn:/usr/local/vpnclient# dhclient vpn_r1
root@cliente-vpn:/usr/local/vpnclient# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 02:be:82:6b:cc:1d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::be:82ff:fe6b:cc1d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:e5:01:cd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:1cd/64 scope link
       valid_lft forever preferred_lft forever
```

```
5: vpn_r1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 5e:e3:d0:fa:69:b9 brd ff:ff:ff:ff:ff:ff
   inet 192.168.30.10/24 brd 192.168.30.255 scope global vpn_r1
       valid_lft forever preferred_lft forever
    inet6 fe80::5ce3:d0ff:fefa:69b9/64 scope link
       valid_lft forever preferred_lft forever
```

Si en nuestro servidor hacemos un dhclient al igual que en el cliente de la interfaz tap, comprobamos que al servidor la ip 192.168.30.11. Al estar ambas maquinas en la misma red de forma local esta configuración no sirve de nada, sin embargo, esto quiere decir que de forma remota ya se pueden conectar equipos sin ningún problema por lo que ahora se probara a poner Softether en practica creando otras dos maquinas, una que configurara como cliente y otra que se configurara como puente entre el cliente2 y el servidor, de forma que cuando el cliente2 solicite una ip con dhclient, aun estando en redes distintas podrá interactuar con el cliente1 como si estuviese en la misma red.

Instalación del puente

Al igual que con las otras maquinas empezamos actualizando el sistema:

```
root@puente-vpn:/home/vagrant# apt update
root@puente-vpn:/home/vagrant# apt upgrade
```

Instalamos lynx y los paquetes necesarios para el uso de softether:

```
root@puente-vpn:/home/vagrant# apt install build-essential
```

Descomprimimos softether:

```
root@puente-vpn:/home/vagrant# tar xzvf softether-vpnbridge-v4.34-9745-rtm-2020.04.05-linux-x64-64bit.tar.gz
vpnbridge/
vpnbridge/Makefile
vpnbridge/.install.sh
```

vpnbridge/ReadMeFirst_License.txt

vpnbridge/Authors.txt

vpnbridge/ReadMeFirst_Important_Notices_ja.txt

vpnbridge/ReadMeFirst_Important_Notices_en.txt

vpnbridge/ReadMeFirst_Important_Notices_cn.txt

vpnbridge/code/

vpnbridge/code/vpnbridge.a

vpnbridge/code/vpncmd.a

vpnbridge/lib/

vpnbridge/lib/libcharset.a

vpnbridge/lib/libcrypto.a

vpnbridge/lib/libedit.a

vpnbridge/lib/libiconv.a

vpnbridge/lib/libintelaes.a

vpnbridge/lib/libncurses.a

vpnbridge/lib/libssl.a

vpnbridge/lib/libz.a

vpnbridge/lib/License.txt

vpnbridge/hamcore.se2

root@puente-vpn:/home/vagrant#

root@puente-vpn:/home/vagrant# cd vpnbridge/

root@puente-vpn:/home/vagrant/vpnbridge# make

SoftEther VPN Bridge (Ver 4.34, Build 9745, Intel x64 / AMD64) for Linux Install Utility

---

Do you want to read the License Agreement for this software ?

1. Yes

2. No

Please choose one of above number:

1

DISCLAIMER

==========

THIS SOFTWARE IS DEVELOPED IN JAPAN, AND DISTRIBUTED FROM JAPAN, UNDER JAPANESE LAWS. YOU MUST AGREE IN ADVANCE TO USE, COPY, MODIFY, MERGE, PUBLISH, DISTRIBUTE, SUBLICENSE, AND/OR SELL COPIES OF THIS SOFTWARE, THAT ANY JURIDICAL DISPUTES WHICH ARE CONCERNED TO THIS SOFTWARE OR ITS CONTENTS, AGAINST US (SOFTETHER PROJECT, SOFTETHER CORPORATION, DAIYUU NOBORI OR OTHER SUPPLIERS), OR ANY JURIDICAL DISPUTES AGAINST US WHICH ARE CAUSED BY ANY KIND OF USING, COPYING, MODIFYING, MERGING, PUBLISHING, DISTRIBUTING, SUBLICENSING, AND/OR SELLING COPIES OF THIS SOFTWARE SHALL BE REGARDED AS BE CONSTRUED AND CONTROLLED BY JAPANESE LAWS, AND YOU MUST FURTHER CONSENT TO EXCLUSIVE JURISDICTION AND VENUE IN THE COURTS SITTING IN TOKYO, JAPAN. YOU MUST WAIVE ALL DEFENSES OF LACK OF PERSONAL JURISDICTION AND FORUM NON CONVENIENS. PROCESS MAY BE SERVED ON EITHER PARTY IN THE MANNER AUTHORIZED BY APPLICABLE LAW OR COURT RULE.

USE ONLY IN JAPAN. DO NOT USE THIS SOFTWARE IN ANOTHER COUNTRY UNLESS YOU HAVE A CONFIRMATION THAT THIS SOFTWARE DOES NOT VIOLATE ANY CRIMINAL LAWS OR CIVIL RIGHTS IN THAT PARTICULAR COUNTRY. USING THIS SOFTWARE IN OTHER COUNTRIES IS COMPLETELY AT YOUR OWN RISK. THE SOFTETHER VPN PROJECT HAS DEVELOPED AND DISTRIBUTED THIS SOFTWARE TO COMPLY ONLY WITH THE JAPANESE LAWS AND EXISTING CIVIL RIGHTS INCLUDING PATENTS WHICH ARE SUBJECTS APPLY IN JAPAN. OTHER COUNTRIES' LAWS OR CIVIL RIGHTS ARE NONE OF OUR CONCERNS NOR RESPONSIBILITIES. WE HAVE NEVER INVESTIGATED ANY CRIMINAL REGULATIONS, CIVIL LAWS OR INTELLECTUAL PROPERTY RIGHTS INCLUDING PATENTS IN ANY OF OTHER 200+ COUNTRIES AND TERRITORIES. BY NATURE, THERE ARE 200+ REGIONS IN THE WORLD, WITH DIFFERENT LAWS. IT IS IMPOSSIBLE TO VERIFY EVERY COUNTRIES' LAWS, REGULATIONS AND CIVIL RIGHTS TO MAKE THE SOFTWARE COMPLY WITH ALL COUNTRIES' LAWS BY THE PROJECT. EVEN IF YOU WILL BE SUED BY A PRIVATE ENTITY OR BE DAMAGED BY A PUBLIC SERVANT IN YOUR COUNTRY, THE DEVELOPERS OF THIS SOFTWARE WILL NEVER BE LIABLE TO RECOVER OR COMPENSATE SUCH DAMAGES, CRIMINAL OR CIVIL

RESPONSIBILITIES. NOTE THAT THIS LINE IS NOT LICENSE RESTRICTION BUT JUST A STATEMENT FOR WARNING AND DISCLAIMER.

READ AND UNDERSTAND THE 'src/WARNING.TXT' FILE BEFORE USING THIS SOFTWARE. SOME SOFTWARE PROGRAMS FROM THIRD PARTIES ARE INCLUDED ON THIS SOFTWARE WITH LICENSE CONDITIONS WHICH ARE DESCRIBED ON THE 'src/THIRD_PARTY.TXT' FILE.

Did you read and understand the License Agreement ?

(If you couldn't read above text, Please read 'ReadMeFirst_License.txt'

file with any text editor.)

1. Yes
2. No

Please choose one of above number:

1

Did you agree the License Agreement ?

1. Agree
2. Do Not Agree

Please choose one of above number:

1

make[1]: Entering directory '/home/vagrant/vpnbridge'

Preparing SoftEther VPN Bridge...

ranlib lib/libcharset.a

ranlib lib/libcrypto.a

ranlib lib/libedit.a

ranlib lib/libiconv.a

ranlib lib/libintelaes.a

ranlib lib/libncurses.a

ranlib lib/libssl.a

ranlib lib/libz.a

ranlib code/vpnbridge.a

gcc code/vpnbridge.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpnbridge

```
ranlib code/vpncmd.a

gcc code/vpncmd.a -fPIE -O2 -fsigned-char -pthread -m64 -lm -lrt -lpthread -L./ lib/libssl.a lib/libcrypto.a lib/libiconv.a lib/libcharset.a lib/libedit.a lib/libncurses.a lib/libz.a lib/libintelaes.a -ldl -o vpncmd

./vpncmd /tool /cmd:Check

vpncmd command - SoftEther VPN Command Line Management Utility

SoftEther VPN Command Line Management Utility (vpncmd command)

Version 4.34 Build 9745   (English)

Compiled 2020/04/05 23:39:56 by buildsan at crosswin

Copyright (c) SoftEther VPN Project. All Rights Reserved.


VPN Tools has been launched. By inputting HELP, you can view a list of the commands that can be used.


VPN Tools>Check

Check command - Check whether SoftEther VPN Operation is Possible

--------------------------------------------------

SoftEther VPN Operation Environment Check Tool


Copyright (c) SoftEther VPN Project.

All Rights Reserved.


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...


Checking 'Kernel System'...

        Pass

Checking 'Memory Operation System'...

        Pass

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

        Pass

Checking 'File system'...

        Pass
```

Checking 'Thread processing system'...

Pass

Checking 'Network system'...

Pass

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

The command completed successfully.

The preparation of SoftEther VPN Bridge is completed !

*** How to switch the display language of the SoftEther VPN Bridge Service ***

SoftEther VPN Bridge supports the following languages:

- Japanese
- English
- Simplified Chinese

You can choose your prefered language of SoftEther VPN Bridge at any time.

To switch the current language, open and edit the 'lang.config' file.

Note: the administrative password is not set on the VPN Server. Please set your own administrative password as soon as possible by vpncmd or the GUI manager.

*** How to start the SoftEther VPN Bridge Service ***

Please execute './vpnbridge start' to run the SoftEther VPN Bridge Background Service.

And please execute './vpncmd' to run the SoftEther VPN Command-Line Utility to configure SoftEther VPN Bridge.

Of course, you can use the VPN Server Manager GUI Application for Windows / Mac OS X on the other Windows / Mac OS X computers in order to configure the SoftEther VPN Bridge remotely.

*** For Windows users ***

You can download the SoftEther VPN Server Manager for Windows

from the http://www.softether-download.com/ web site.

This manager application helps you to completely and easily manage the VPN server services running in remote hosts.

*** For Mac OS X users ***

In April 2016 we released the SoftEther VPN Server Manager for Mac OS X.

You can download it from the http://www.softether-download.com/ web site.

VPN Server Manager for Mac OS X works perfectly as same as the traditional Windows versions. It helps you to completely and easily manage the VPN server services running in remote hosts.

*** PacketiX VPN Server HTML5 Web Administration Console (NEW) ***

This VPN Server / Bridge has the built-in HTML5 Web Administration Console.

After you start the server daemon, you can open the HTML5 Web Administration Console is available at

https://127.0.0.1:5555/

or

https://ip_address_of_the_vpn_server:5555/

This HTML5 page is obviously under construction, and your HTML5 development contribution is very appreciated.

```
-----------------------------------------------------------------


make[1]: Leaving directory '/home/vagrant/vpnbridge'
```

Movemos el directorio y cambiamos los permisos como en los demas:

```
root@puente-vpn:/home/vagrant/vpnbridge# cd ..
root@puente-vpn:/home/vagrant# mv vpnbridge/ /usr/local/
root@puente-vpn:/home/vagrant# cd /usr/local/vpnbridge/
root@puente-vpn:/usr/local/vpnbridge# chmod 600 *
root@puente-vpn:/usr/local/vpnbridge# chmod 700 vpnbridge
root@puente-vpn:/usr/local/vpnbridge# chmod 700 vpncmd
root@puente-vpn:/usr/local/vpnbridge#
```

Configuración para el puente

```
root@puente-vpn:/home/vagrant# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:be:82:6b:cc:1d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::be:82ff:fe6b:cc1d/64 scope link
       valid_lft forever preferred_lft forever
```

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:bb:ac:4f brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.20/24 brd 10.10.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febb:ac4f/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:7e:4a:25 brd ff:ff:ff:ff:ff:ff
    inet 172.22.10.10/24 brd 172.22.10.255 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:4a25/64 scope link
       valid_lft forever preferred_lft forever
```

Arrancamos el servicio y comprobamos el puente:

```
root@puente-vpn:/home/vagrant# ./vpnbridge start
bash: ./vpnbridge: No such file or directory
root@puente-vpn:/home/vagrant# cd /usr/local/vpnbridge/
root@puente-vpn:/usr/local/vpnbridge# ./vpnbridge start
The SoftEther VPN Bridge service has been started.

Let's get started by accessing to the following URL from your PC:

https://10.0.2.15:5555/
  or
https://10.0.2.15/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certificate by default. That
is natural. Continue with ignoring the TLS warning.
```

```
root@puente-vpn:/usr/local/vpnbridge# ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.34 Build 9745   (English)
Compiled 2020/04/05 23:39:56 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also specify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Password: **********

Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.
```

```
VPN Server>hublist
HubList command - Get List of Virtual Hubs
Item              |Value
------------------+------------------
Virtual Hub Name  |BRIDGE
Status            |Online
Type              |Standalone
Users             |0
Groups            |0
Sessions          |1
MAC Tables        |0
IP Tables         |0
Num Logins        |0
Last Login        |2021-11-28 15:58:19
Last Communication|2021-12-04 11:57:03
Transfer Bytes    |8,067,782,709
Transfer Packets  |152,211,372
The command completed successfully.
```

Al contrario que con el servidor Softether, el puente solo puede tener un único hub bastante limitado ya que tampoco permite la creación de usuarios.

Creamos la conexión en cascada con el equipo servidor:

```
VPN Server/BRIDGE>cascadecreate R1
CascadeCreate command - Create New Cascade Connection
Destination VPN Server Host Name and Port Number: 10.10.10.10:443

Destination Virtual Hub Name: Empresa

Connecting User Name: prueba
```

```
The command completed successfully.


VPN Server/BRIDGE>cascadepasswordset prueba
CascadePasswordSet command - Set User Authentication Type of Cascade Connection to Password Authentication
Please enter the password. To cancel press the Ctrl+D key.

Password: ****** #prueba
Confirm input: ******

Specify standard or radius: standard

The command completed successfully.
```

Comprobamos que se ha creado correctamente:

```
VPN Server/BRIDGE>cascadelist
CascadeList command - Get List of Cascade Connections
Item                |Value
--------------------+----------------
Setting Name        |R1
Status              |Offline (Stopped)
Established at      |(None)
Destination VPN Server|10.10.10.10
Virtual Hub         |
The command completed successfully.

VPN Server/BRIDGE>cascadeonline R1
CascadeOnline command - Switch Cascade Connection to Online Status
The command completed successfully.

VPN Server/BRIDGE>cascadelist
```

```
CascadeList command - Get List of Cascade Connections
Item                |Value
--------------------+------------------------
Setting Name        |R1
Status              |Online (Established)
Established at      |2021-12-04 (Sat) 15:56:53
Destination VPN Server|10.10.10.10
Virtual Hub         |
The command completed successfully.
```

Ahora crearemos la interfaz que recibirá la ip del servidor, para ello empezamos instalando bridge-utils

```
apt install bridge-utils
root@puente-vpn:/usr/local/vpnbridge# brctl addbr br0
```

```
VPN Server>bridgecreate BRIDGE /DEVICE:enp0s9 /TAP:yes
BridgeCreate command - Create Local Bridge Connection
While in the condition that occurs immediately after a new bridge connection is made when bridging to a physical network adapter, depending on the type of network adapter, there are cases where it will not be possible to communicate using TCP/IP to the network adapter using a bridge connection from a computer on the virtual network.
(This phenomenon is known to occur for Intel and Broadcom network adapters.)

If this issue arises, remedy the situation by restarting the computer on which VPN Server / Bridge is running. Normal communication will be possible after the computer has restarted.

Also many wireless network adapters will not respond to the sending of packets in promiscuous mode and when this occurs you will be unable to use the Local Bridge. If this issue arises, try using a regular wired network adapter instead of the wireless network adapter.
```

Instructions for Local Bridge on VM

It has been detected that the VPN Server might be running on a VM (Virtual Machine) suchlike VMware or Hyper-V. Read the following instructions carefully. If you are not using a VM, please ignore this message.

Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by default.

If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled, the Local Bridge function between a Virtual Hub on the VPN Server and a physical network adapter on the physical computer does not work well. You should allow the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM.

For details please refer the documents of your VM. If it is a shared-VM and administrated by other person, please request the administrator to permit the use of the Promiscuous (MAC Address Spoofing) Mode to your VM.

The command completed successfully.

VPN Server>bridgelist

BridgeList command - Get List of Local Bridge Connection

Number|Virtual Hub Name|Network Adapter or Tap Device Name|Status

------+---------------+---------------------------------+---------

1 |Local |172.22.10.20:443 |Offline

2 |BRIDGE |enp0s9 |Operating

3 |BRIDGE |enp0s9 |Operating

root@puente-vpn:/usr/local/vpnbridge# brctl addif br0 tap_enp0s9

root@puente-vpn:/usr/local/vpnbridge# brctl addif br0 enp0s8

root@puente-vpn:/usr/local/vpnbridge# ip link set br0 up

Hacemos dhclient y comprobamos como el puente recibe ip del servidor:

root@puente-vpn:/usr/local/vpnbridge# ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 02:be:82:6b:cc:1d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::be:82ff:fe6b:cc1d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0
state UP group default qlen 1000
    link/ether 08:00:27:bb:ac:4f brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.20/24 brd 10.10.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febb:ac4f/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
    link/ether 08:00:27:7e:4a:25 brd ff:ff:ff:ff:ff:ff
    inet 172.22.10.10/24 brd 172.22.10.255 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:4a25/64 scope link
       valid_lft forever preferred_lft forever
5: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default qlen 1000
    link/ether 08:00:27:bb:ac:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.10/24 brd 192.168.30.255 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febb:ac4f/64 scope link
       valid_lft forever preferred_lft forever
```

```
6: tap_enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UNKNOWN group default qlen 1000
    link/ether 5e:a8:f3:c1:4b:78 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::5ca8:f3ff:fec1:4b78/64 scope link
       valid_lft forever preferred_lft forever
root@puente-vpn:/usr/local/vpnbridge# dhclient tap_enp0s9
```

```
root@puente-vpn:/usr/local/vpnbridge# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:be:82:6b:cc:1d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::be:82ff:fe6b:cc1d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP group default qlen 1000
    link/ether 08:00:27:bb:ac:4f brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.20/24 brd 10.10.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febb:ac4f/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:7e:4a:25 brd ff:ff:ff:ff:ff:ff
    inet 172.22.10.10/24 brd 172.22.10.255 scope global enp0s9
```

```
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:4a25/64 scope link
       valid_lft forever preferred_lft forever
5: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default qlen 1000
    link/ether 08:00:27:bb:ac:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.10/24 brd 192.168.30.255 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febb:ac4f/64 scope link
       valid_lft forever preferred_lft forever
6: tap_enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master
br0 state UNKNOWN group default qlen 1000
    link/ether 5e:a8:f3:c1:4b:78 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::5ca8:f3ff:fec1:4b78/64 scope link
       valid_lft forever preferred_lft forever


root@puente-vpn:/usr/local/vpnbridge# ping 192.168.30.12
PING 192.168.30.12 (192.168.30.12) 56(84) bytes of data.
64 bytes from 192.168.30.12: icmp_seq=1 ttl=64 time=1.35 ms
64 bytes from 192.168.30.12: icmp_seq=2 ttl=64 time=1.37 ms
^C
--- 192.168.30.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 1.358/1.368/1.379/0.038 ms
```

Podemos ver que el puente puede hacerle ping al cliente de la red1 sin problemas. En este punto solo falta que el cliente reciba una ip mediante el puente.