OPEN VPN Server MIKROTIK
Cliente Windows

Mikrotik User Meeting – Lima Perú 2019

MUM
Perú
2019

Presentación Personal

- **Nombre:** Ruben Cabrera Neciosup
- **Profesión:** Especialista Redes y Comunicaciones
  - Instructor TI – **Comutel**
  - Experiencia con **RouterOS** – 2010
  - Desarrollo de Proyectos TI – 2012

- **Certificaciones:**
  - **Cisco:** CCNA
  - **Mikrotik:** MTCNA / MTCUME / MTCTCE / MTCRE / MTCWE

COMUTEL - 2008

- Venta de equipos de **Redes y Telecomunicaciones**
- Soporte y Post-Venta - **MIKROTIK**
- Desarrollo de Proyectos **llave en mano**
- Academia de Entrenamiento:
  - *Certificaciones Oficiales **MIKROTIK***
  - *Cursos y Tallares prácticos – **MIKROTIK***
- Canales de Atención:

✓ ***Central Telf.:*** *01 4801010*

Soporte: *opción **1***
Ventas: *opción **2***

/Comutel

/AcademiaComutel

www.comutelperu.com

+51 960195934
+51 991939577

Comutel Academia

Certificación MTCNA

Certificación MTCTCE

Objetivos de esta exposición

- Presentar el concepto y características del protocolo OPEN VPN, y además sus diferencias de otros protocolos de VPN.

- Proponer una versión resumida de la solución que a sido realizado para la empresa de Logística.

- Proveer una planificación de la configuración de lado de VPN Server y VPN Cliente.

OPEN VPN

- Es un protocolo de **software de código abierto** que permite implementar una **VPN** (red privada virtual) para crear una conexión segura entre **sitios remotos.**

- Presenta una conexión segura por qué utiliza el cifrado **SSL / TLS**, para el intercambio de claves.

- Permite que los usuarios se autentiquen mediante una **clave secreta** y **certificado**, esta configuración lo realiza en el **Router Server VPN.**

Protocolo	Descripción
SSL SSLv2, SSLv3	Secure Sockets Layer
TLS	Transport Layer Security

- Es difícil diferenciar entre una conexión HTTPS sobre SSL.
- Utiliza los protocolos **UDP** y **TCP**, pero tenga en cuenta que **RouterOS** no soporta **UDP**.
- Soporta **Autenticación** y **Cifrado:** Se recomienda utilizar **AES** y **MD5**.

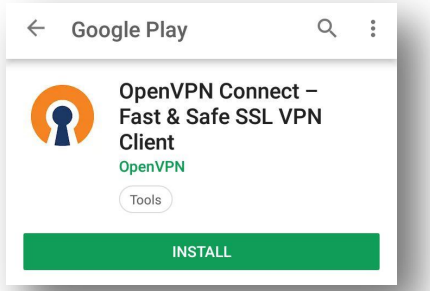
OPEN VPN vs Otros Protocolos

	Open VPN	PPTP	L2TP / IPsec	SSTP
Cifrado	160-bit, 256-bit	128-bit	256-bit	256-bit
Seguridad	Muy Alto	Muy débil	Alta Seguridad	Alto
Velocidad	Rápido	Rápido, debido al bajo cifrado.	Medio, debido al doble encapsulación	Rápido
Estabilidad	Muy estable	Muy estable	Estable	Muy Estable
Compatibilidad	Soporte con multiples plataformas, incluyendo windows, MAC, Linux, dispositvos moviles. Requiere software de terceros.	Soporte en múltiples dispositivos, mayor en OS Windows.	Soporte para múltiples dispositivos y plataformas.	Plataforma Windows, pero funciona en otras distribuciones de Linux.
Notas	Es protocolo recomendado y muy rápido.	- Nativo en Windows. - Seguridad débil.	Versátil y seguro. Una alternativa decente para OpenVPN.	Alternativa más rápida y segura a PPTP y L2TP.
Protocolo / Puerto	TCP / 1194	TCP / 1723	UDP / 1701	TCP / 443

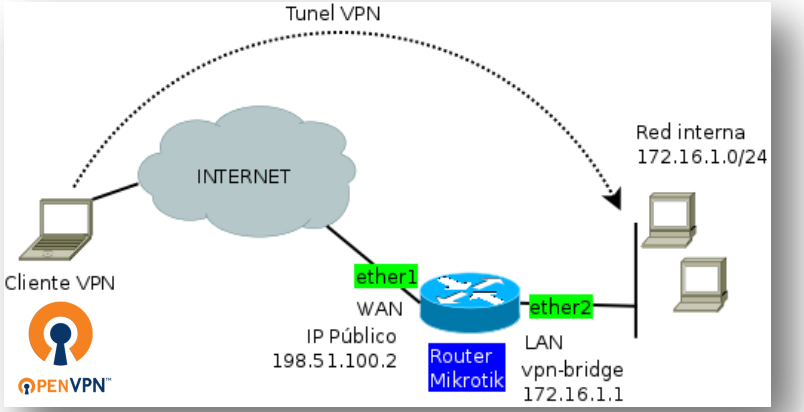
* https://thebestvpn.com/pptp-l2tp-openvpn-sstp-ikev2-protocols/

OpenVPN Cliente

- Se requiere utilizar un software de tercero para la conexión de usuarios dispositivos finales, es compatible OS: **Windows**, **Android**, **iOS**, etc.

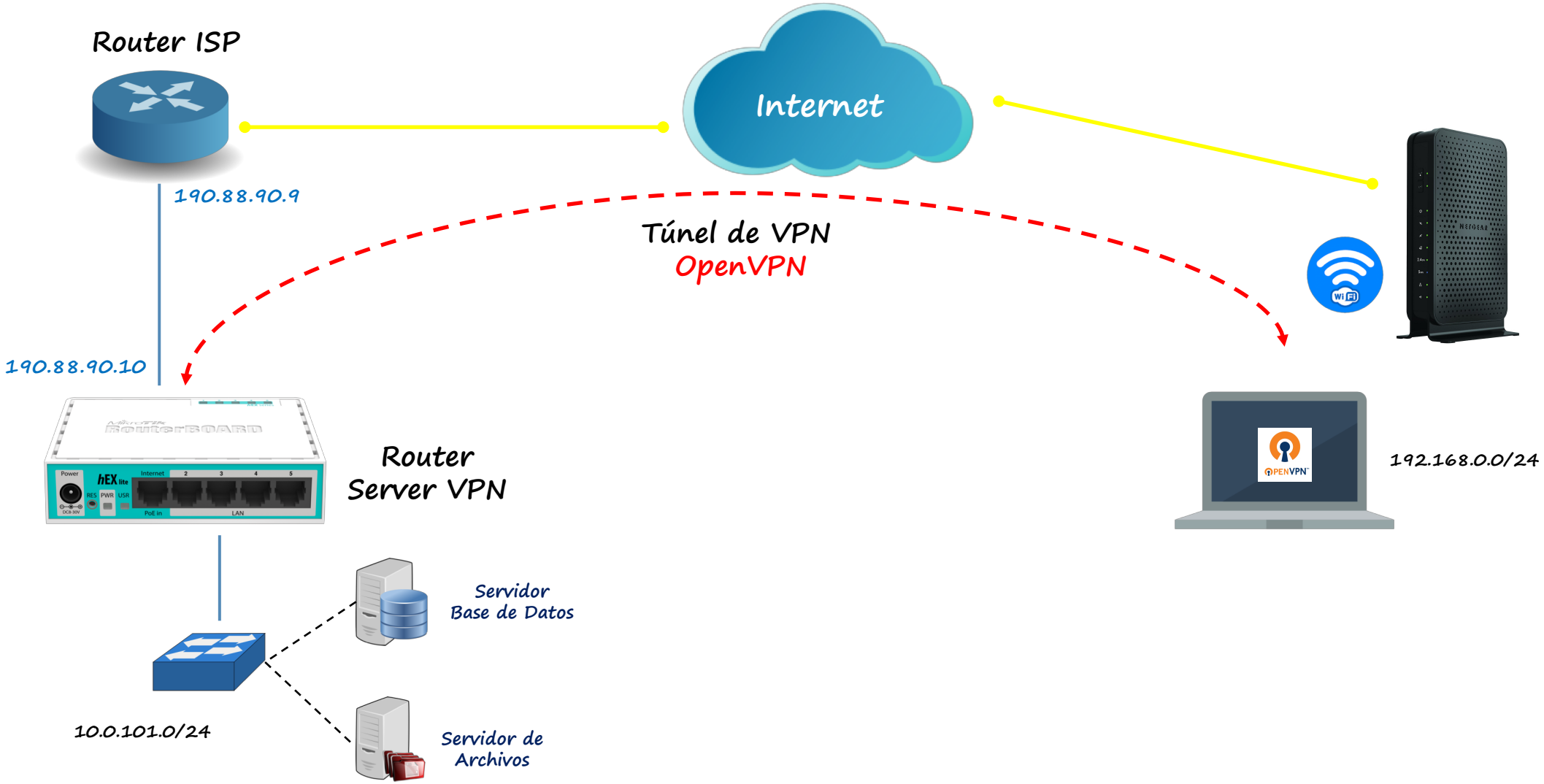


- Para la solución se deberá instalar la aplicación **OpenVPN Connect Client on windows.** Es necesario que el ordenador se encuentre los certificados creador por **RouterOS**.



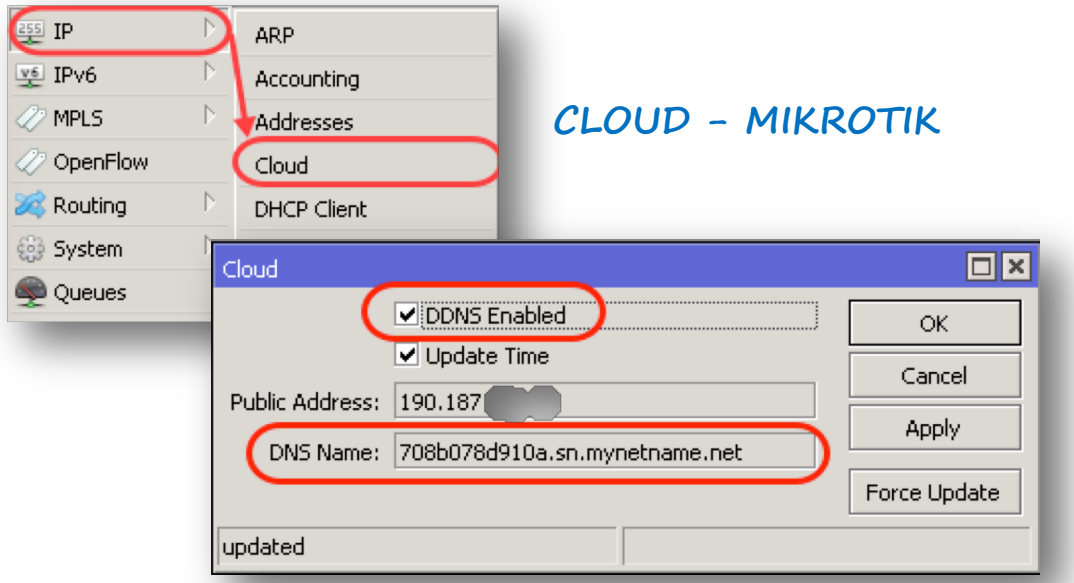
- Es compatible con estos sistemas operativos de **Windows**:
  - **Windows 10, Windows 8, Windows 7**

Topología de RED



Requisitos – OpenVPN Server

- Es necesario tener una dirección IP Publica fija.
- De lo contrario si es IP dinámica se puede utilizar **DDNS** (Mikrotik) o **Dynu.com**
- Generar los certificados para el Router VPN – CA
- Generar certificados para los usuarios finales.



CLOUD – MIKROTIK

Dynu {d}DNS
Working hard to empower you!

Permite tener hasta 4 dominios gratuitos, donde se puede utilizar un script que pueda realizar un UPDATE de actualización de IP Dinámica.

Link script

https://www.dynu.com/DynamicDNS/IPUpdateClient/Mikrotik-Dynamic-DNS

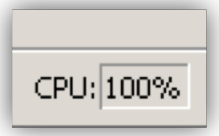
Generar Certificado CA

- Crear el certificado de autoridad (CA), con una validez de **10 Años**

```
/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@Router.Principal] > /certificate add name=CA-tpl country=PE state=PE locality=Lince organization=IPH
 unit=IT common-name=CA key-size=4096 days-valid=3650 key-usage=crl-sign,key-cert-sign
[admin@Router.Principal] >
```

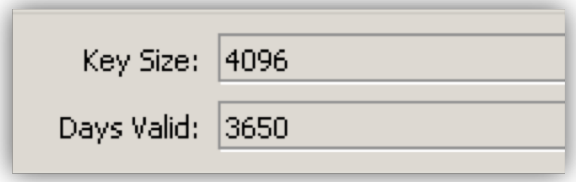
  - Firma del certificado **CA**

```
/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@Router.Principal] >
[admin@Router.Principal] > /certificate sign CA-tpl ca-crl-host=127.0.0.1 name=CA
```

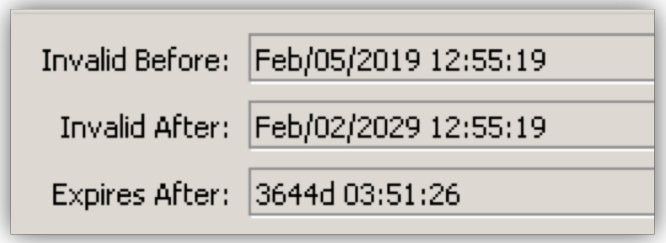


Ojo: se elevara a la hora de firmar.

Días de valides



Fecha de expiración



Generar Certificado Servidor VPN

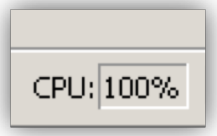
- Crear el certificado del Servidor, con una validez de **10 Años**

```
[admin@Router.Principal] > /certificate add name=SERVER-tpl country=PE state=PE locality=Lince
organization=IPH unit=IT common-name=mymikrotik.freeddns.org key-size=4096 days-valid=3650 key-
usage=digital-signature,key-encipherment,tls-server
[admin@Router.Principal] >
```

  - **Nota:**
    - Common-name= Si tiene una **IP publica Fija** se debe configurar la IP, si es dinámica el **Dominio.**

  - Firma del certificado **Servidor**

```
/                Move up to base level
..               Move up one level
/command         Use command at the base level
[admin@Router.Principal] >
[admin@Router.Principal] > /certificate sign SERVER-tpl ca=CA name=SERVER
```



Ojo: se elevara a la hora de firmar.

Generar Certificado – Cliente

- Crear la plantilla del empleado, con una validez de **10 Años**

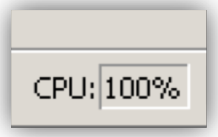
```
/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@Router.Principal] > /certificate add name=CLIENT-tpl country=PE state=PE locality=Lince organization=IPH
unit=IT common-name=CLIENT key-size=4096 days-valid=3650 key-usage=tls-client
[admin@Router.Principal] >
```

- Crear el certificado con el nombre del Empleado

```
[admin@Router.Principal] > /certificate add name=MARTIN copy-from=CLIENT-tpl common-name=MARTIN
[admin@Router.Principal] >
```

- Firma del certificado **MARTIN** (empleado)

```
[admin@Router.Principal] > /certificate sign MARTIN ca=CA name=MARTIN
```



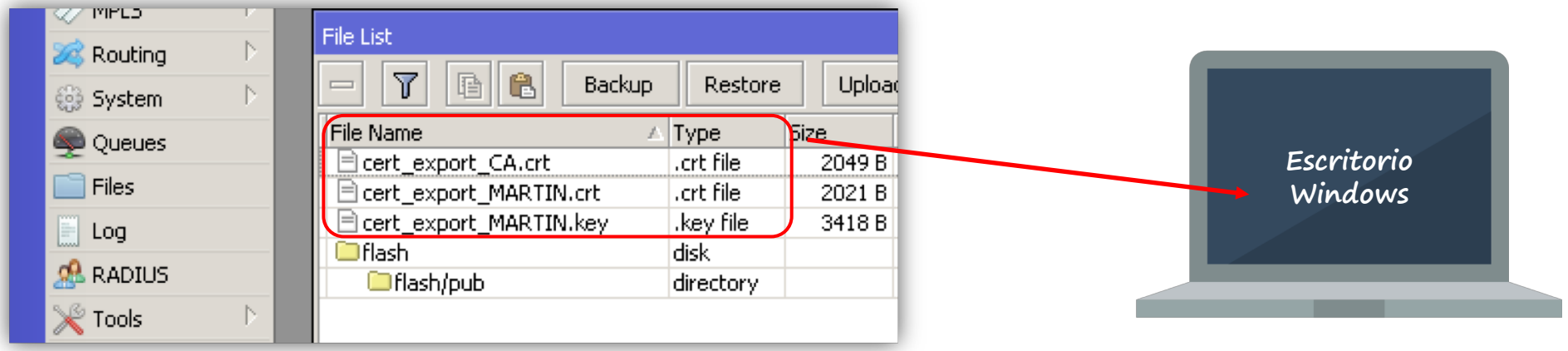
Ojo: se elevara a la hora de firmar.

Exportar los certificados

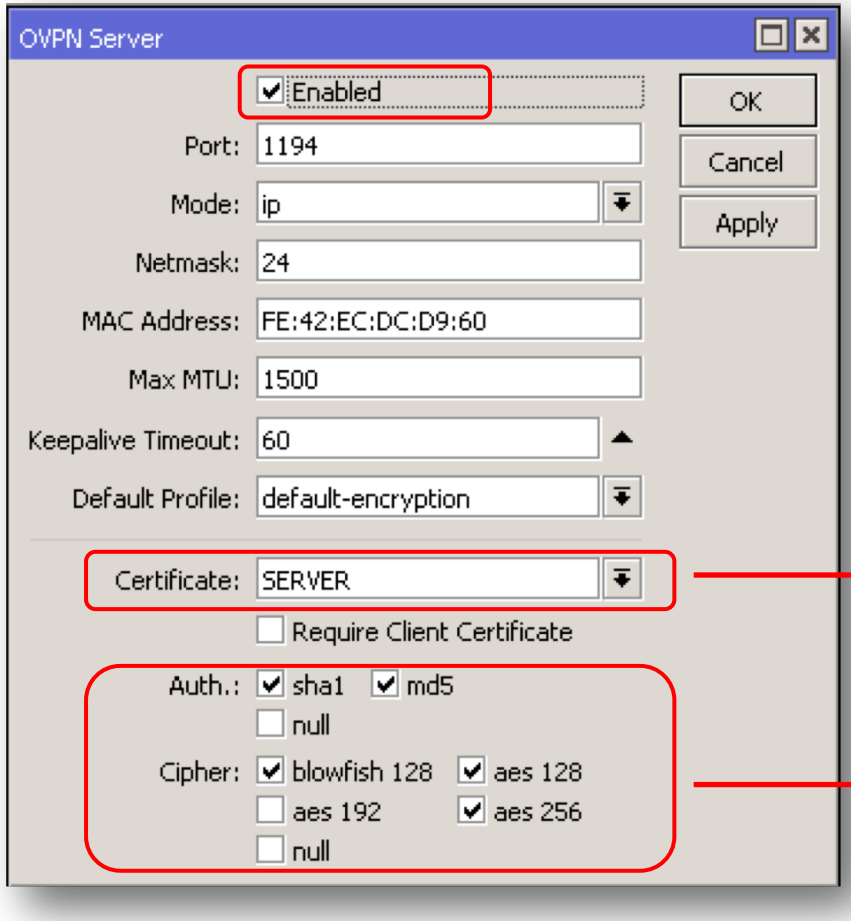
- Como requerimiento de OpenVPN Cliente en Windows se requiere los siguientes archivos:
  - CA.ca
  - MARTIN.crt.
  - CLIENT.key.

```
/                Move up to base level
..               Move up one level
/command         Use command at the base level
[admin@Router.Principal] >
[admin@Router.Principal] > /certificate export-certificate CA export-passphrase=
[admin@Router.Principal] > /certificate export-certificate MARTIN export-passphrase=666777888
[admin@Router.Principal] >
```

** La contraseña del certificado del empleador MARTIN es : 666777888*



Habilitar OpenVPN Server

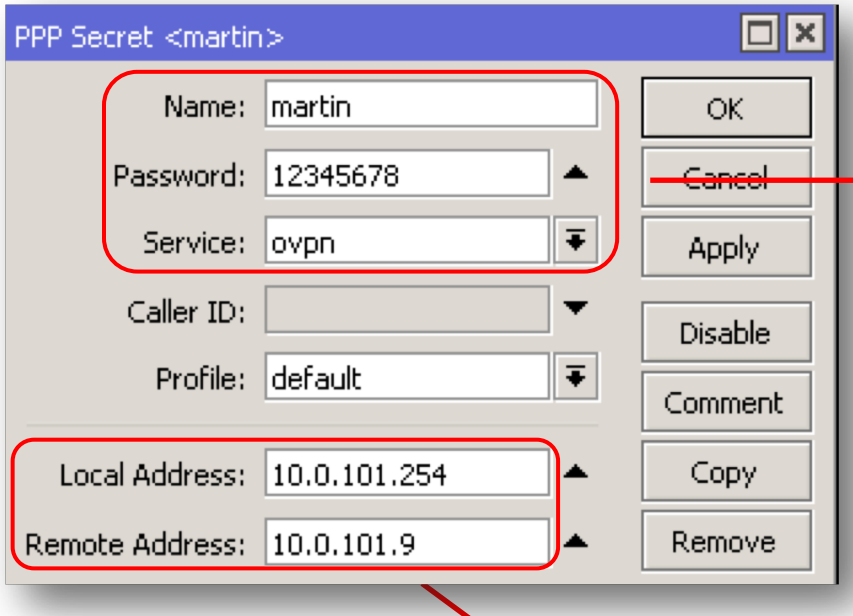


- Se va a omitir la **configuración del acceso a internet** del **Router VPN Server.**
- Se debe habilitar el protocolo **OVPN Server**, para eso se debe tomar en cuenta el **paquete PPP** que se encuentre instalado.

Se debe elegir el certificado del **SERVER**, que es el que se encuentra validado con el **CA.**

Se debe activar la autenticación y cifrado, tomando en cuenta el **AES256**, para mayor encriptación.

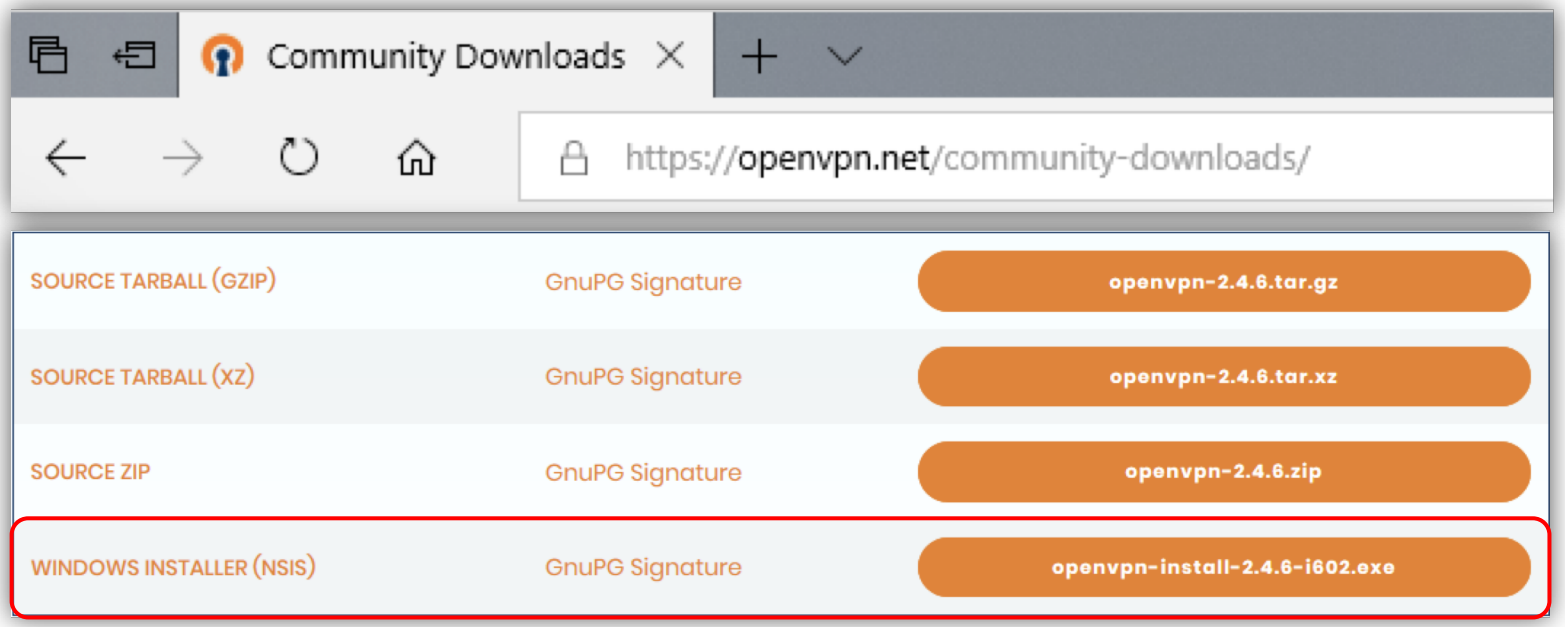
Crear user y password (empleado)



- **Name:** Indica el nombre de usuario del empleado.
- **Password:** Se indica la contraseña del usuario creado.
- **Servicio:** Se debe indicar el protocolo que se esta utilizando **ovpn**.

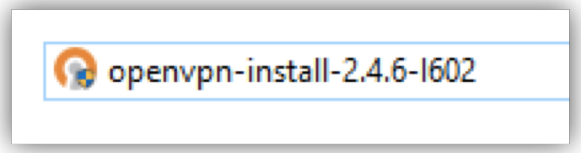
- **Local Address:** Especificar la dirección **IP LOCAL** del túnel VPN.
- **Remote Address:** Especificar la dirección **IP Remota** del túnel VPN, sitio Remoto.

Instalación de OpenVPN Cliente



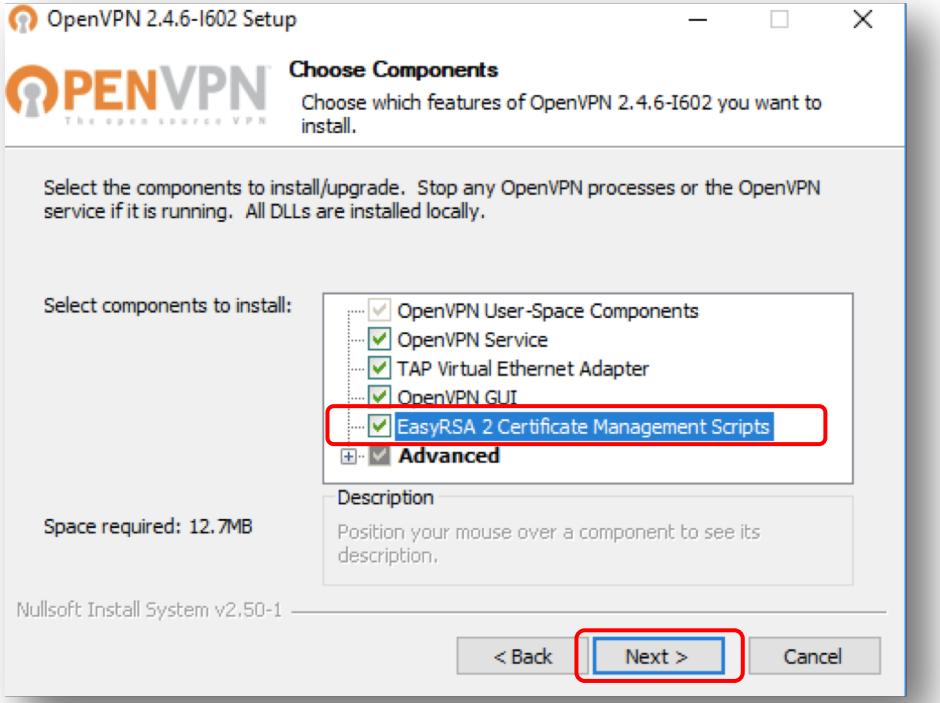
Ingreso a pagina web de la comunidad de OpenVPN

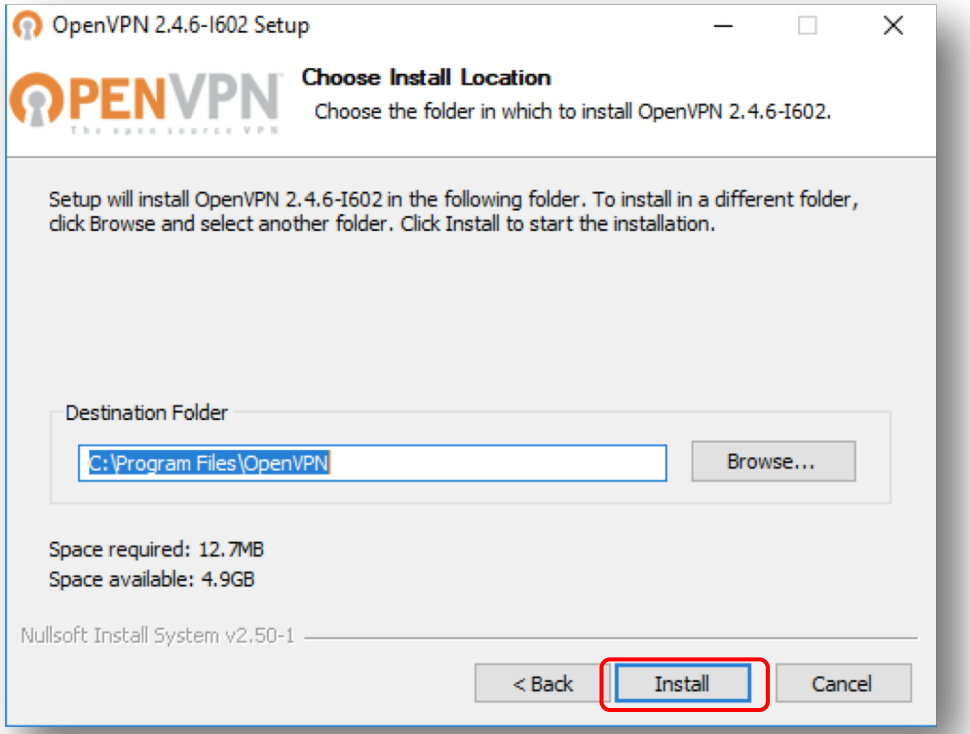
Descarga la versión de Windows Installer 2.4.6



* Ejecutar como Administrador

Instalación de OpenVPN Cliente

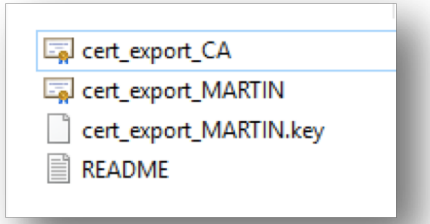




* *Nota:*

Luego de haber instalado el software se debe de dirigir a la Ruta: C:\Archivos de Progarmas\OpenVPN\config

Y pegar los certificados exportados.



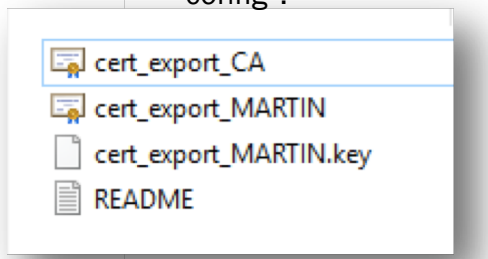
Crear un MTVPN.ovpn

```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On some systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
#dev tap
dev tun

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.  For MikroTik only TCP
proto tcp-client
```

```
# Change 'myremote' to be your remote host,
# or comment out to enter a listening
# server mode.
remote mymikrotik.freeddns.org

# Reconfigure this line to use a different
# port number than the default of 1194.
port 1194
```

```
# Most clients don't need to bind to
# a specific local port number.
nobind

# Try to preserve some state across restarts.
persist-key
persist-tun

# SSL/TLS client
tls-client

# Chech server serificate in key-usage
remote-cert-tls server

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca cert_export_CA.crt
cert cert_export_MARTIN.crt
key cert_export_MARTIN.key
```

Información de la **carpeta** “config”.



Crear un MTVPN.ovpn

```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On some systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
#dev tap
dev tun

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.  For MikroTik only TCP
proto tcp-client
```

1

2

3

```
# Change 'myremote' to be your remote host,
# or comment out to enter a listening
# server mode.
remote mymikrotik.freeddns.org

# Reconfigure this line to use a different
# port number than the default of 1194.
port 1194
```

4

5

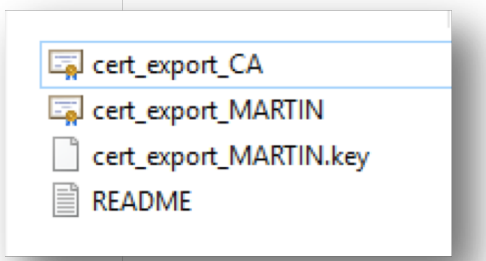
```
# Most clients don't need to bind to
# a specific local port number.
nobind

# Try to preserve some state across restarts.
persist-key
persist-tun

# SSL/TLS client
tls-client

# Chech server serificate in key-usage
remote-cert-tls server

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca cert_export_CA.crt
cert cert_export_MARTIN.crt
key cert_export_MARTIN.key
```

6

7

8

Información de la **carpeta "config".**



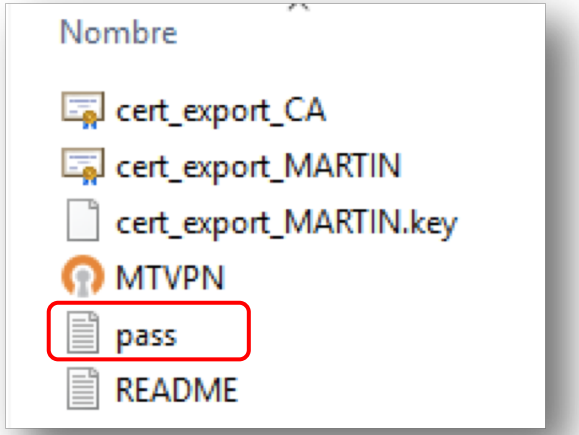
Crear un MTVPN.ovpn

```
# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
cipher AES-256-CBC

# cipher algorithm
auth SHA1

# Username and password file
auth-user-pass pass.txt
```

9

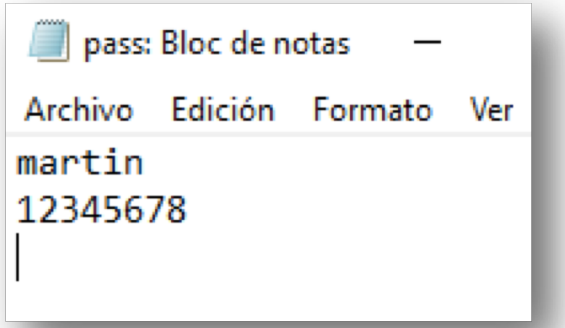
10

11



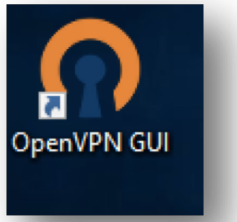
En file "config", debe de estar guardado el archivo de las credenciales.

Se debe de crear un archivo de texto con el usuario y contraseña creado en el ROUTER VPN.

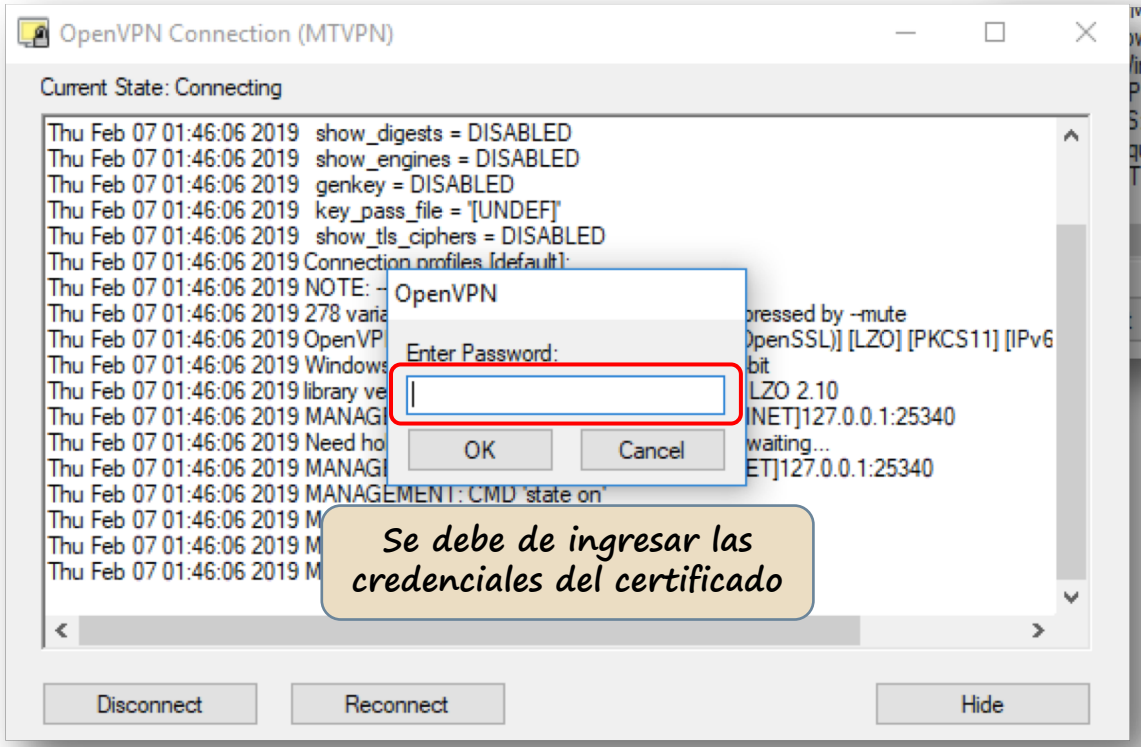


En un archivo de texto escribir las credenciales del usuario y contraseña

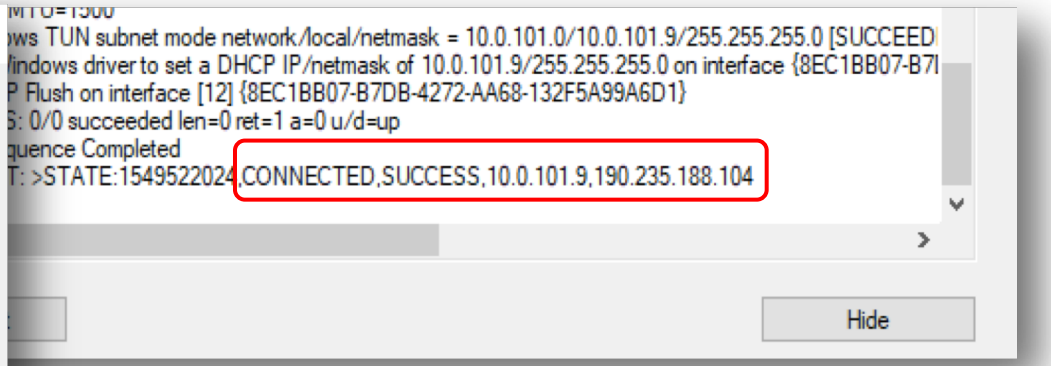
Iniciar Sesión : Cliente OpenVPN



1 *Ejecutar el aplicativo OpenVPN.*

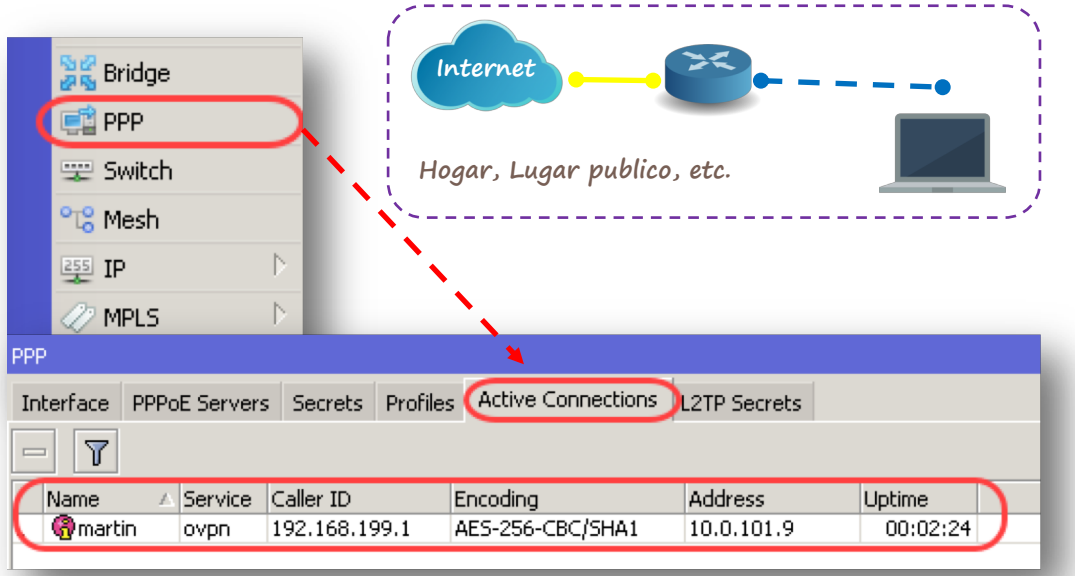


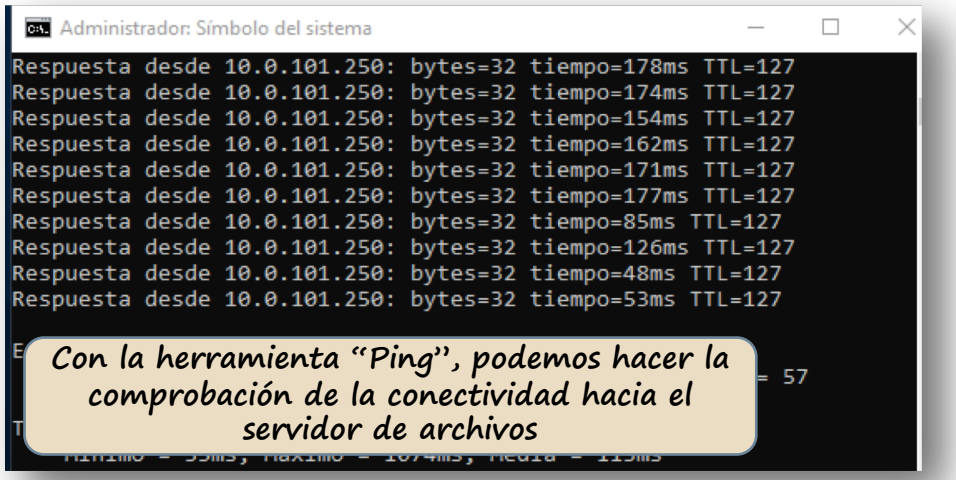
Se debe de ingresar las credenciales del certificado



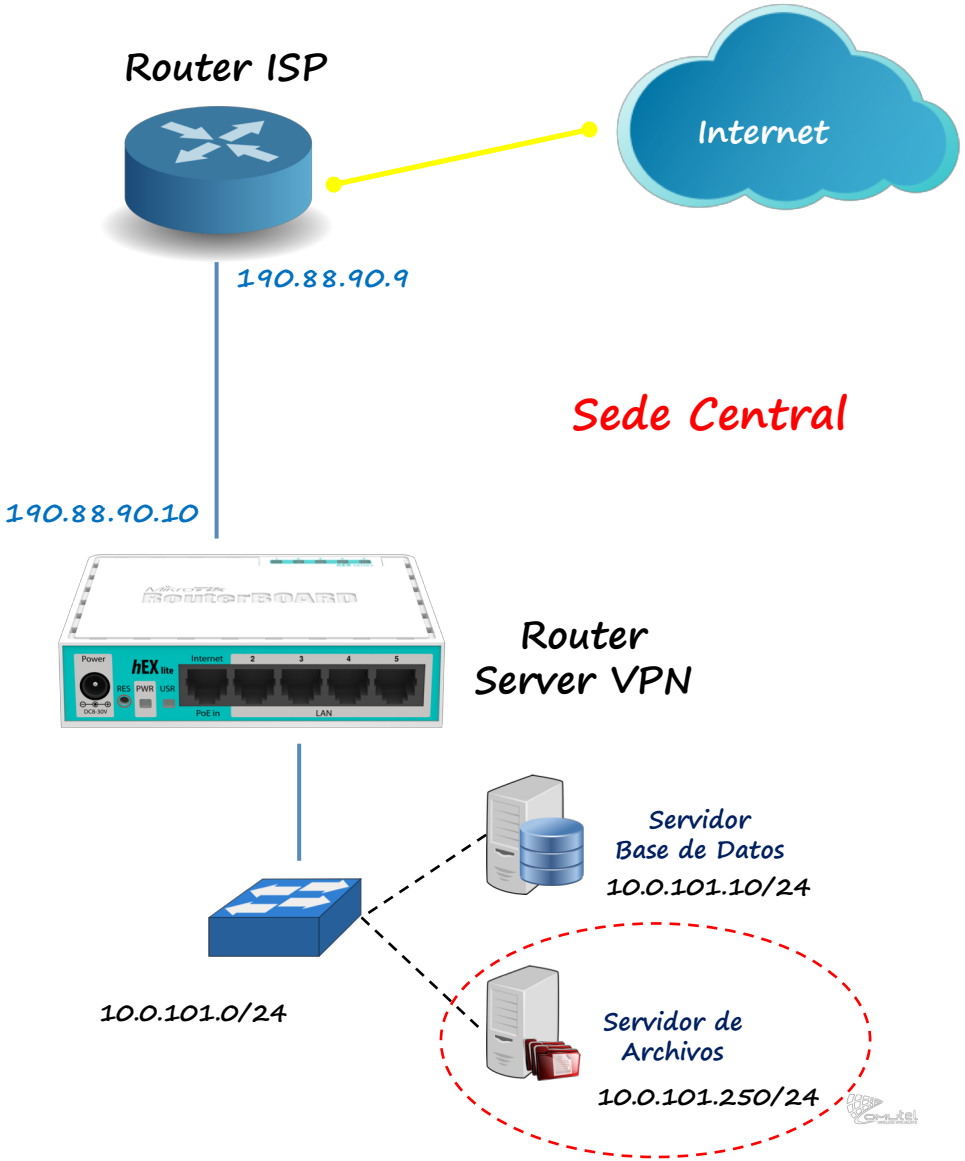
Se verifica que allá sido registrado correcto y entregado la dirección IP de la VPN.

Pruebas de Conectividad





Con la herramienta "Ping", podemos hacer la comprobación de la conectividad hacia el servidor de archivos



Conclusiones

- **OpenVPN** , presenta una solución de VPN de mayor encriptación, por ello es que emplea la biblioteca de **OpenSSL** y protocolos **SSLv3** / **TLSv1.**
- RouterOS facilidad la configuración en que permite **crear certificados** y en habilitar el **Server OpenVPN**, solo demandaría el OS del empleado para la configuración.
- **Dynu.com**, definitivamente es una mejor opción si tienes IP dinámica, puede omitir el **doble NAT** con un **script.**
- El software cliente, es compatible para diferentes OS, incluso lo puedes en **PlayStore.**

Referencias

- https://mikrotik.unibit.bg/articles/mikrotik-openvpn-server-windows-client/
- https://mum.mikrotik.com/presentations/VN17/presentation_4102_1493726768.pdf
- https://mum.mikrotik.com/presentations/KH17/presentation_4166_1493374693.pdf

¿Preguntas?

¡¡¡ Muchas Gracias !!!