

OPEN VPN Server MIKROTIK Cliente Windows



Mikrotik User Meeting – Lima 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



/Comutel

/AcademiaComutel

Soporte: opción 1

Ventas: opción 2



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.

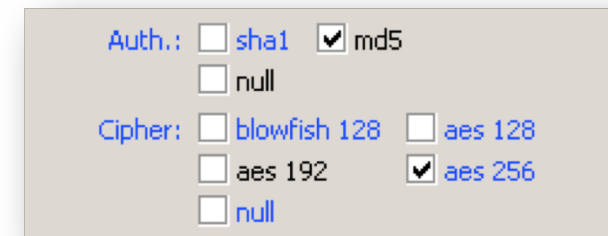


OPEN VPN

- 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 autenticen 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**.



Auth.: sha1 md5
 null

Cipher: blowfish 128 aes 128
 aes 192 aes 256
 null



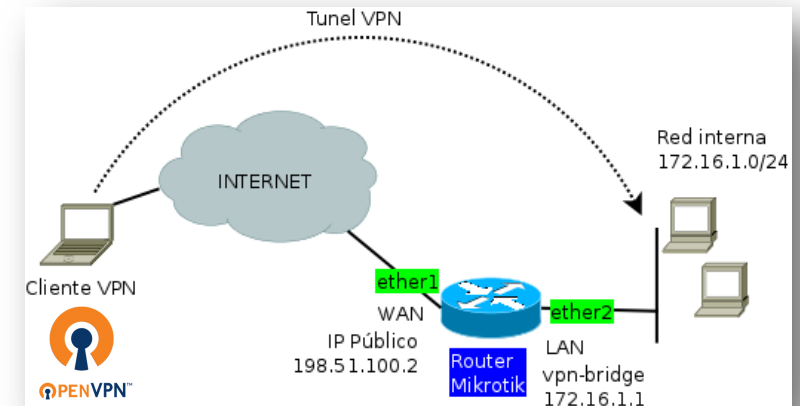
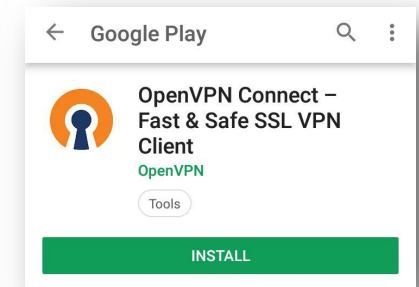
OPEN VPN vs Otros Protocolos

| | 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, dispositivos 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 |

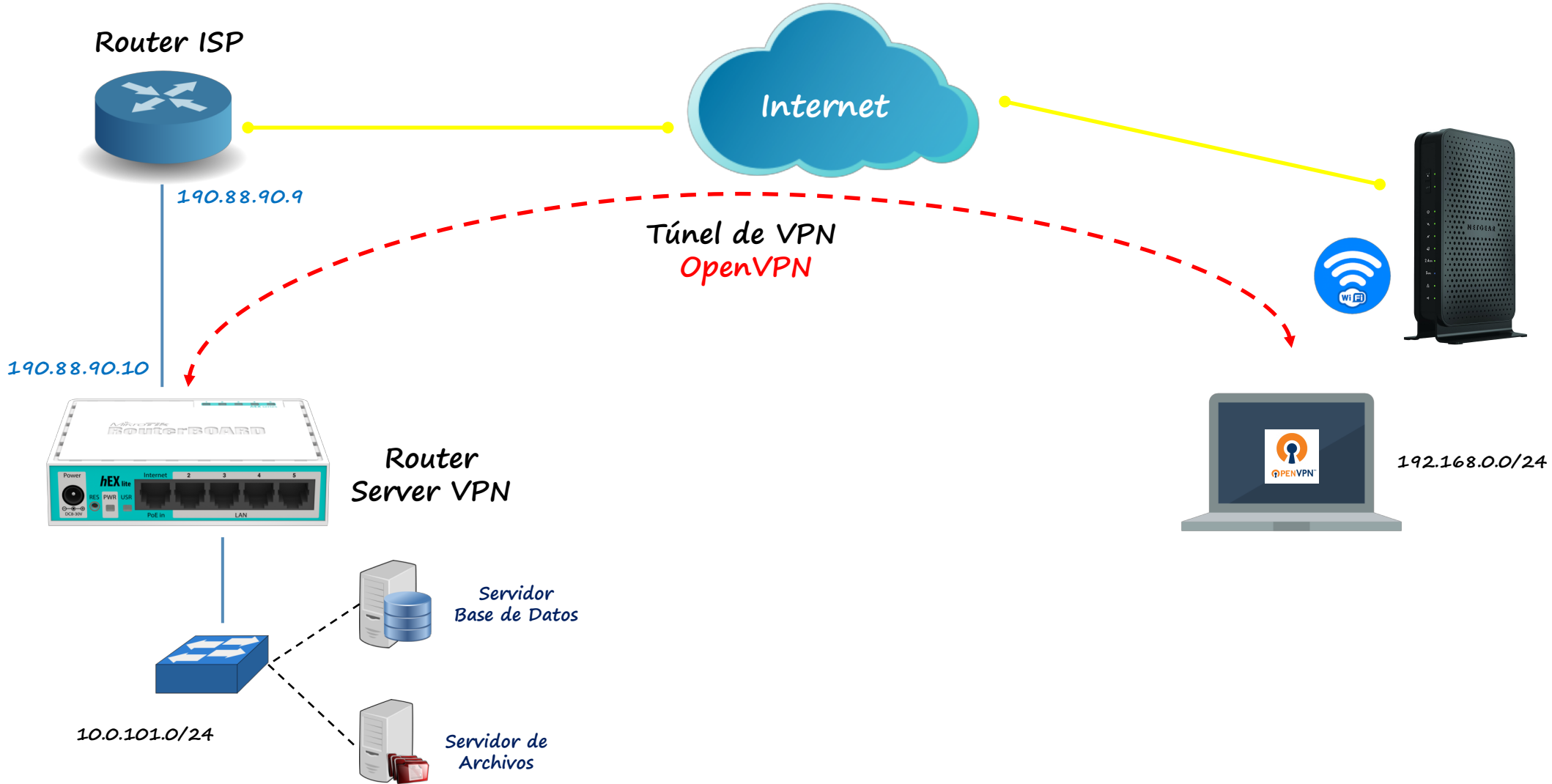


OpenVPN Cliente

- 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**

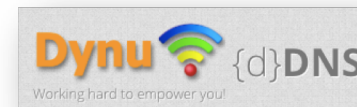
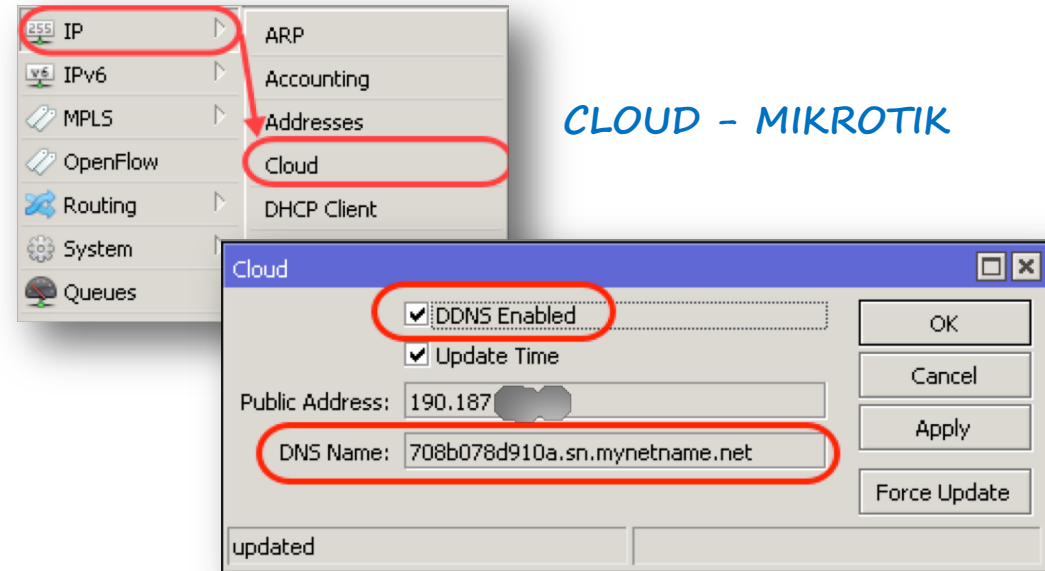


Topología de RED



Requisitos – OpenVPN Server

- Es necesario tener una dirección IP Pública 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.



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-tp1 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-tp1 ca-crl-host=127.0.0.1 name=CA
```

CPU: 100%

Ojo: se elevara a la hora de firmar.

Días de valides

| | |
|-------------|------|
| Key Size: | 4096 |
| Days Valid: | 3650 |

Fecha de expiración

| | |
|-----------------|----------------------|
| Invalid Before: | Feb/05/2019 12:55:19 |
| Invalid After: | Feb/02/2029 12:55:19 |
| Expires After: | 3644d 03:51:26 |



Generar Certificado Servidor VPN

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

```
[admin@Router.Principal] > /certificate add name=SERVER-tp1 country=PE state=PE locality=Lince
organization=IPH unit=IT common-name=mymikrotik.freedom.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-tp1 ca=CA name=SERVER
```

CPU: 100%

Ojo: se eleva 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
█
```

CPU: 100%

Ojo: se elevara a la hora de firmar.



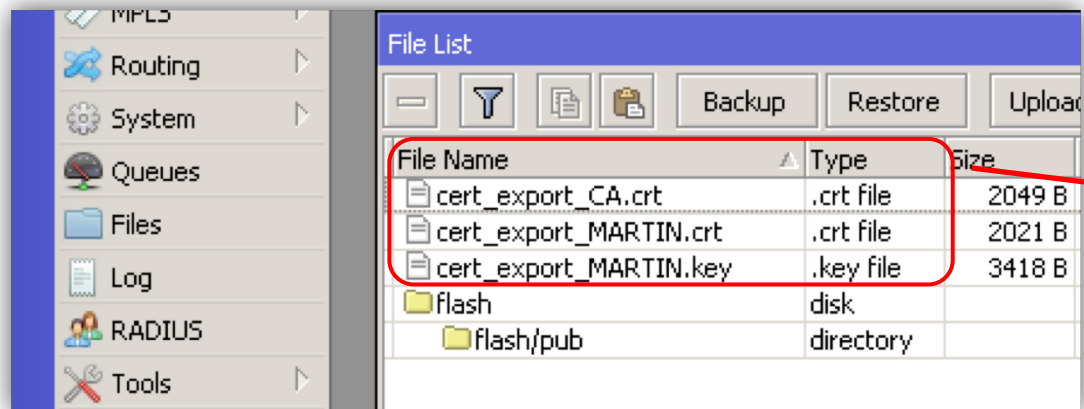
Exportar los certificados

- 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



| File Name | Type | Size |
|------------------------|-----------|--------|
| cert_export_CA.crt | .crt file | 2049 B |
| cert_export_MARTIN.crt | .crt file | 2021 B |
| cert_export_MARTIN.key | .key file | 3418 B |
| flash | disk | |
| flash/pub | directory | |



Habilitar OpenVPN Server

OVPN Server

Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:42:EC:DC:D9:60

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: default-encryption

Certificate: SERVER

Require Client Certificate

Auth.: sha1 md5
 null

Cipher: blowfish 128 aes 128
 aes 192 aes 256
 null

OK
Cancel
Apply

- 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)

The screenshot shows a dialog box titled "PPP Secret <martin>". It contains several input fields and buttons. A red box highlights the "Name" field (containing "martin"), the "Password" field (containing "12345678"), and the "Service" dropdown menu (set to "ovpn"). Another red box highlights the "Local Address" field (containing "10.0.101.254") and the "Remote Address" field (containing "10.0.101.9"). A red arrow points from the "Cancel" button to the text "Se indica la contraseña del usuario creado." in the list below. Another red arrow points from the "Local Address" field to the text "Especificar la dirección IP LOCAL del túnel VPN." in the list below.

| | |
|-----------------|--------------|
| Name: | martin |
| Password: | 12345678 |
| Service: | ovpn |
| Caller ID: | |
| Profile: | default |
| Local Address: | 10.0.101.254 |
| Remote Address: | 10.0.101.9 |

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

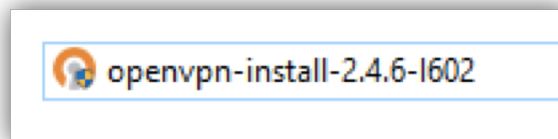
- **Name:** Indica el nombre de usuario del empleado.
- **Password:** Se indica la contraseña del usuario creado.
- **Servicio:** Se debe indicar el protocolo que se esta utilizando **ovpn**.
- **Local Address:** Especificar la dirección IP **LOCAL** del túnel VPN.
- **Remote Address:** Especificar la dirección IP Remota del túnel VPN, sitio Remoto.

Instalación de OpenVPN Cliente

| | | |
|--------------------------|-----------------|--------------------------------|
| SOURCE TARBALL (GZIP) | GnuPG Signature | openvpn-2.4.6.tar.gz |
| SOURCE TARBALL (XZ) | GnuPG Signature | openvpn-2.4.6.tar.xz |
| SOURCE ZIP | GnuPG Signature | openvpn-2.4.6.zip |
| WINDOWS INSTALLER (NSIS) | GnuPG Signature | openvpn-install-2.4.6-i602.exe |

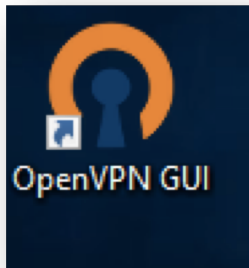
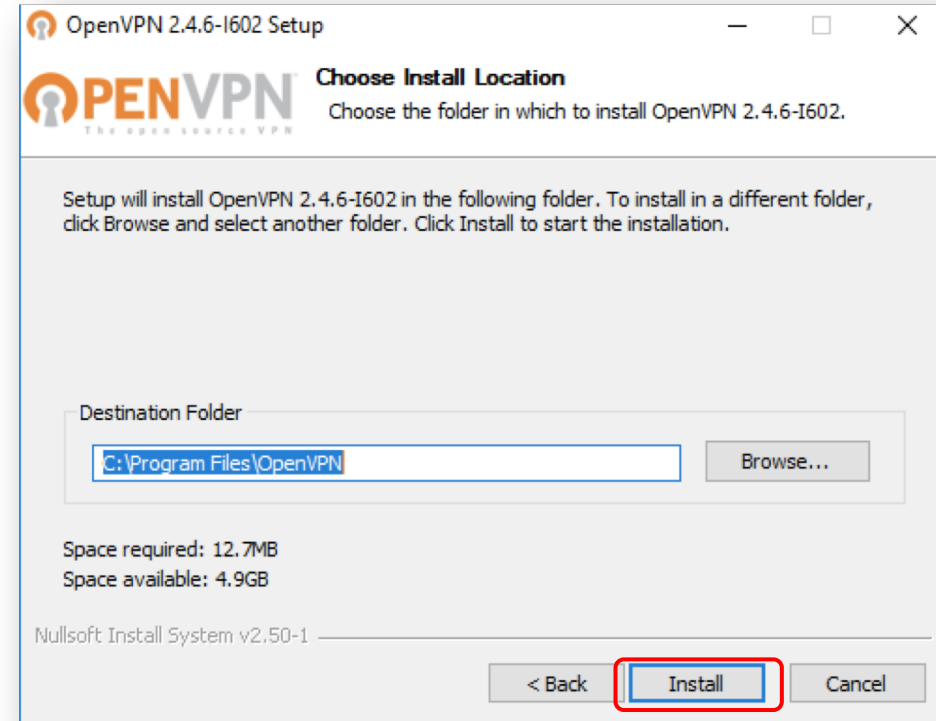
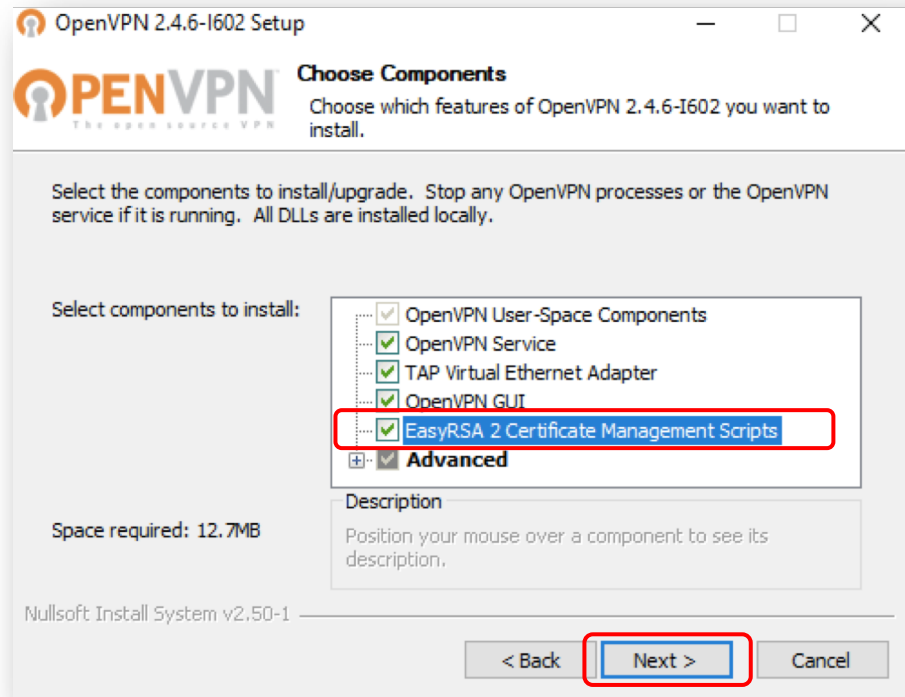
Ingreso a pagina web de la comunidad de OpenVPN

Descarga la versión de Windows Installer 2.4.6



* Ejecutar como Administrador

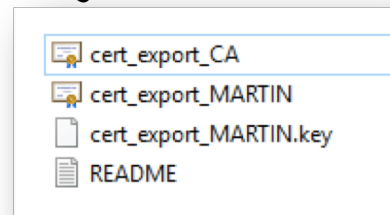
Instalación de OpenVPN Cliente



*** Nota:**

Luego de haber instalado el software se debe de dirigir a la Ruta: C:\Archivos de Programas\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.freedom.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
```

```
# Check server certificate 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".

```
cert_export_CA  
cert_export_MARTIN  
cert_export_MARTIN.key  
README
```



Crear un MTVPN.ovpn

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

```
client
```

1

```
# 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
```

2

```
# Are we connecting to a TCP or  
# UDP server? Use the same setting as  
# on the server. For Mikrotik only TCP
```

```
proto tcp-client
```

3

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

```
remote mymikrotik.freedom.org
```

4

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

```
port 1194
```

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
```

6

```
# Check server certificate in key-usage  
remote-cert-tls server
```

7

```
# 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
```

8

Información de la carpeta
"config".

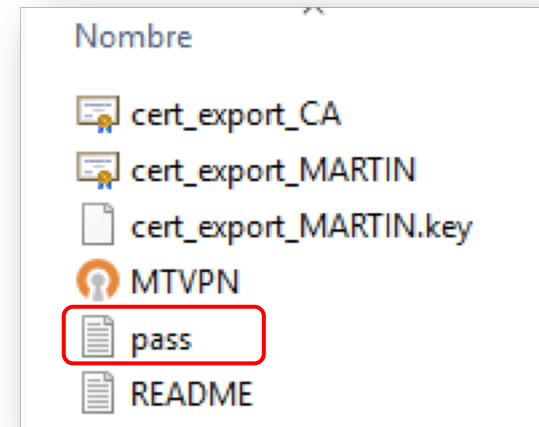
```
cert_export_CA  
cert_export_MARTIN  
cert_export_MARTIN.key  
README
```



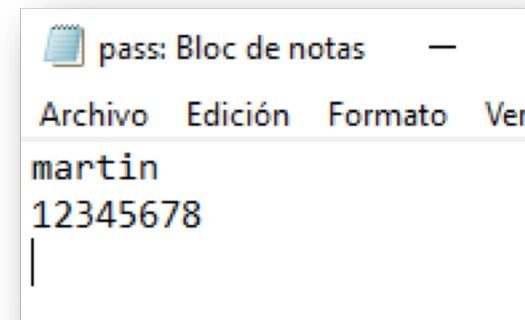
Crear un MTVPN.ovpn

```
# Select a cryptographic cipher.  
# If the cipher option is used on the server  
# then you must also specify it here.  
cipher AES-256-CBC 9  
  
# cipher algorithm  
auth SHA1 10  
  
# Username and password file  
auth-user-pass pass.txt 11
```

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

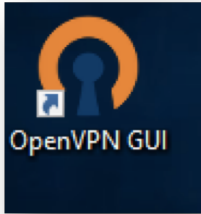


En file "config", debe de estar guardado el archivo de las credenciales.



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

Iniciar Sesión : Cliente OpenVPN



1 Ejecutar el aplicativo OpenVPN.

The screenshot shows the OpenVPN Connection (MTVPN) window. The main log area displays the following text:

```
Thu Feb 07 01:46:06 2019 show_digests = DISABLED
Thu Feb 07 01:46:06 2019 show_engines = DISABLED
Thu Feb 07 01:46:06 2019 genkey = DISABLED
Thu Feb 07 01:46:06 2019 key_pass_file = [UNDEF]
Thu Feb 07 01:46:06 2019 show_tls_ciphers = DISABLED
Thu Feb 07 01:46:06 2019 Connection profiles [default]:
Thu Feb 07 01:46:06 2019 NOTE: OpenVPN
Thu Feb 07 01:46:06 2019 278 variables suppressed by --mute
Thu Feb 07 01:46:06 2019 OpenVPN [OpenSSL] [LZO] [PKCS11] [IPv6]
Thu Feb 07 01:46:06 2019 Windows bit
Thu Feb 07 01:46:06 2019 library version LZO 2.10
Thu Feb 07 01:46:06 2019 MANAGEMENT: [MANAGEMENT]127.0.0.1:25340
Thu Feb 07 01:46:06 2019 Need handshake waiting...
Thu Feb 07 01:46:06 2019 MANAGEMENT: [MANAGEMENT]127.0.0.1:25340
Thu Feb 07 01:46:06 2019 MANAGEMENT: CMD 'state on'
Thu Feb 07 01:46:06 2019 M
Thu Feb 07 01:46:06 2019 M
```

An "Enter Password:" dialog box is overlaid on the log, with a red box around the password input field. The dialog has "OK" and "Cancel" buttons.

At the bottom of the window, there are "Disconnect", "Reconnect", and "Hide" buttons.

On the right side of the screenshot, a portion of the log is visible, showing the following text:

```
MTU=1500
Windows TUN subnet mode network/local/netmask = 10.0.101.0/10.0.101.9/255.255.255.0 [SUCCESS]
Windows driver to set a DHCP IP/netmask of 10.0.101.9/255.255.255.0 on interface {8EC1BB07-B71
P Flush on interface [12] {8EC1BB07-B7DB-4272-AA68-132F5A99A6D1}
S: 0/0 succeeded len=0 ret=1 a=0 u/d=up
Sequence Completed
T: >STATE:1549522024,CONNECTED,SUCCESS,10.0.101.9,190.235.188.104
```

A red box highlights the IP address "10.0.101.9,190.235.188.104" in the log.

Se debe de ingresar las credenciales del certificado

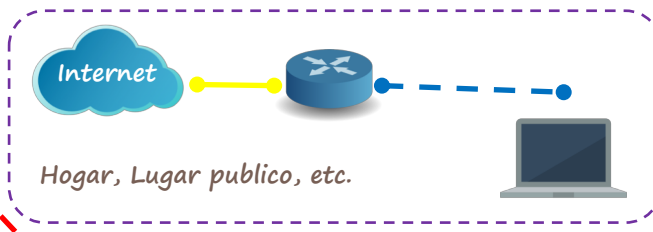
Se verifica que allá sido registrado correcto y entregado la dirección IP de la VPN.



Pruebas de Conectividad

The screenshot shows the Mikrotik WinBox interface. On the left, the 'PPP' menu item is highlighted with a red circle. A red dashed arrow points from this menu item to the 'Active Connections' tab in the main window. Below the tabs, a table lists active PPP connections:

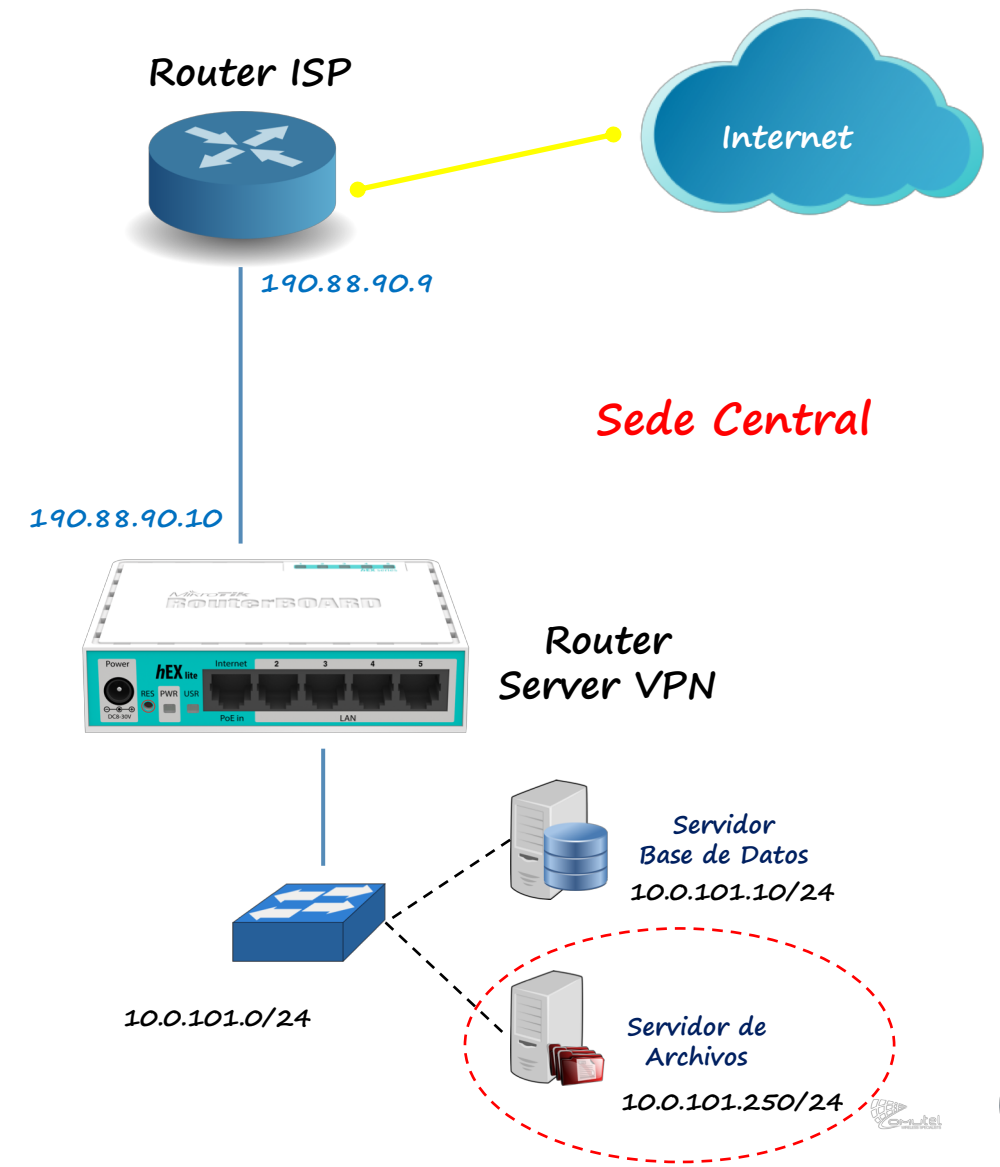
| Name | Service | Caller ID | Encoding | Address | Uptime |
|--------|---------|---------------|------------------|------------|----------|
| martin | ovpn | 192.168.199.1 | AES-256-CBC/SHA1 | 10.0.101.9 | 00:02:24 |



```

C:\> Administrador: Símbolo del sistema
Respuesta desde 10.0.101.250: bytes=32 tiempo=178ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=174ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=154ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=162ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=171ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=177ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=85ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=126ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=48ms TTL=127
Respuesta desde 10.0.101.250: bytes=32 tiempo=53ms TTL=127
    
```

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 !!!

