

Redes privadas virtuales

Álvaro González Sotillo

9 de septiembre de 2023

Índice

1. VPN	1
2. Tipos de VPN	2
3. Tunnelling	2
4. Tunnelling (ejemplo a nivel de red)	5
5. Tunneling: Nivel	5
6. VPN: Protocolos	6
7. Referencias	8

1. VPN

- *Virtual Private Network*
- La interconexión entre dos sistemas se realiza a través de una red insegura
- Pero garantizando la seguridad de la comunicación
 - Confidencialidad
 - Integridad

1.1. Encriptación

- Consiste en ocultar la información que se envía
- Sólo el receptor puede interpretar la información del emisor
- Para el resto de sistemas intermedios los datos no significan nada
- Esto aumenta la **confidencialidad**
- Al dificultar la modificación de la información por sistemas intermedios, mejora la **integridad**

1.2. Autenticación

- Consiste en saber con quién nos conectamos
- El sistema remoto deben autenticarse
 - Los clientes suelen usar contraseñas
 - Los servidores suelen usar certificados
- Aumenta la **confidencialidad**
- Al evitar que otras personas operen en nuestra red mejora **integridad**

1.3. Datos sobre los datos (*metadatos*)

- La encriptación oculta los datos que se transmitan
 - Pero los routers intermedios siguen enrutando cada paquete
 - Pueden saber
 - Cuántos paquetes se envían
 - A qué horas
 - Con cuántos datos
- Para evitar este problema se puede usar **tráfico de relleno**
 - No se podrá distinguir información real de la de relleno
 - Problema: mayor consumo de ancho de banda

2. Tipos de VPN

- Acceso remoto
- Punto a punto
- Interna (VPN over LAN)

2.1. Acceso remoto

- Usuarios finales utilizan una VPN para conectarse a la LAN de su empresa
- Se utiliza cualquier red final disponible
 - Particular, 3G, aeropuertos, hoteles...

By [Ludovic.ferre Own work CC BY-SA 4.0](#)

2.2. Punto a punto

- Los LAN de la misma empresa utilizan un enlace de VPN a modo de red local
- Permite a diferentes sedes trabajar como si estuviesen en la central

By [Ludovic.ferre Own work CC BY-SA 4.0](#)

2.3. VPN over LAN

- Los accesos a la LAN pueden ser poco seguros
 - Wifi
 - Puntos de red no vigilados
- La LAN puede segmentarse (por ejemplo, VLAN), y permitir solo conexiones a la LAN más interna por una VPN

By [Ludovic.ferre Own work CC BY-SA 4.0](#)

3. Tunnelling

3.1. Encapsulación de protocolos

- Según el modelo ISO/OSI, unos protocolos se encapsulan dentro de otros
- Los protocolos superiores solo son datos para los inferiores

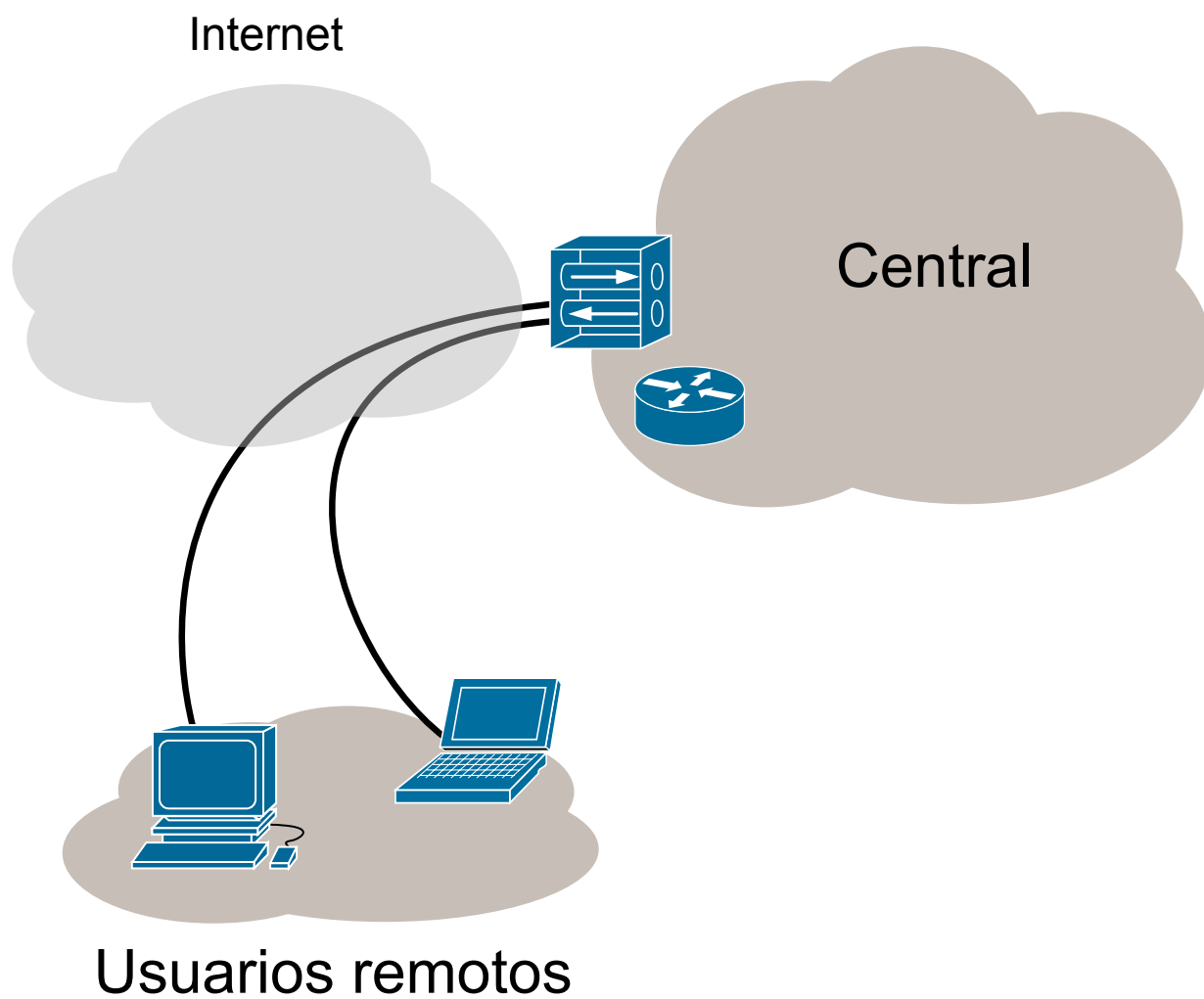


Figura 1: VPN de acceso remoto

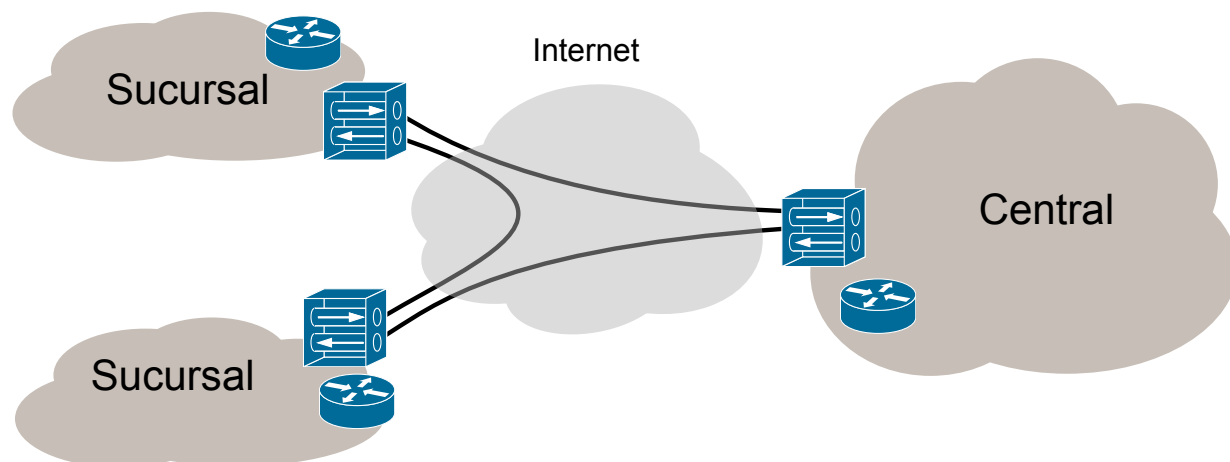


Figura 2: VPN de acceso punto a punto

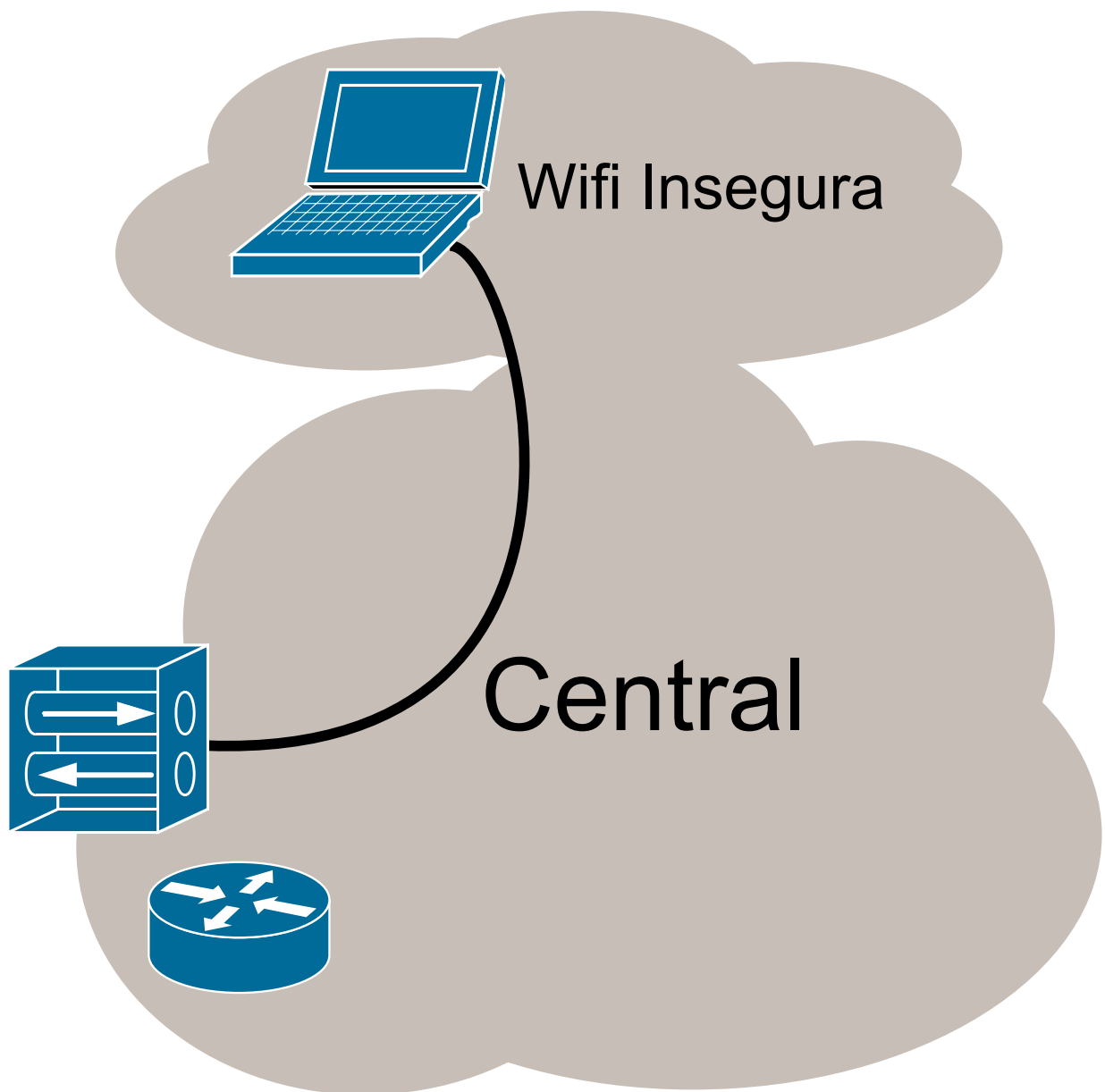


Figura 3: VPN over LAN

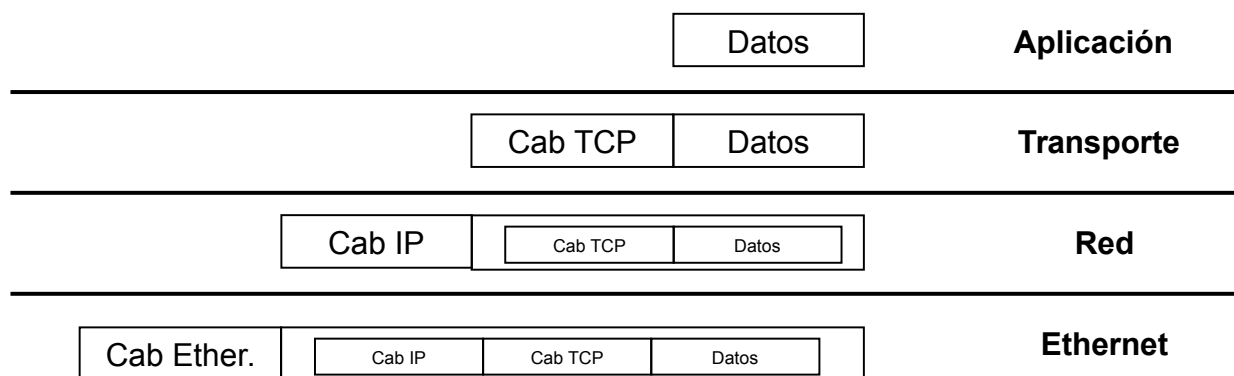


Figura 4: Pila típica de protocolos

3.2. Encriptación de datos

- Cualquier capa puede encriptar los datos que envía
- Y los datos son los protocolos superiores

3.3. Tunnelling

- Un nivel de red puede encriptarse y volver a meterse como datos a cualquier nivel
- Los extremos de la comunicación utilizan interfaces virtuales
 - Los datos enviados por esa interfaz se encriptan y se envían por una interfaz real

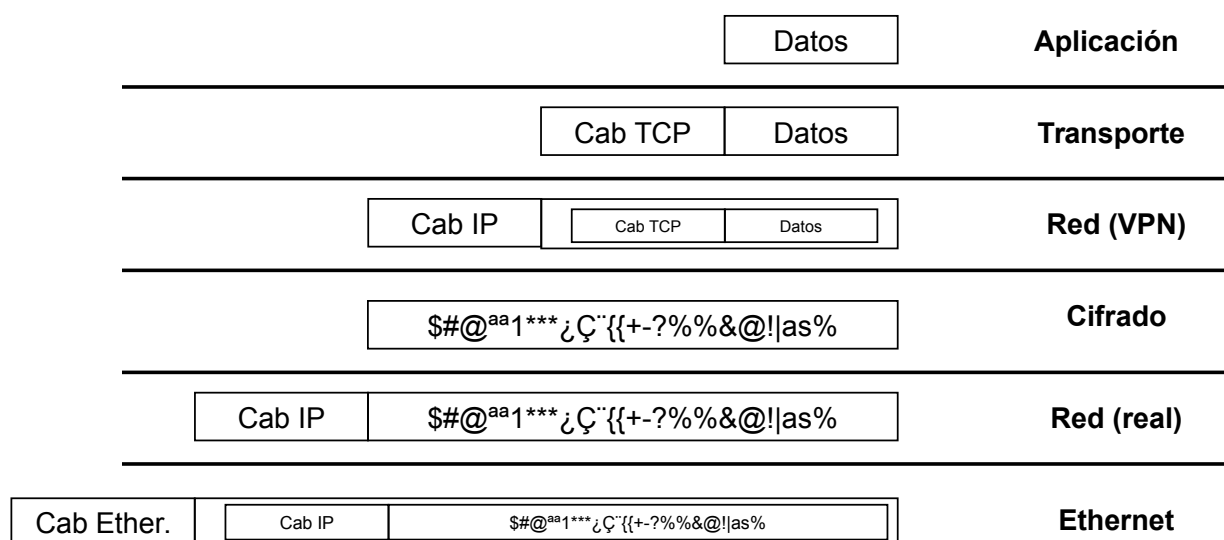


Figura 5: Ejemplo de *tunneling* en el nivel 3

4. Tunnelling (ejemplo a nivel de red)

5. Tunneling: Nivel

- VPN a nivel de enlace (ethernet)
 - Se transmiten los broadcasts de ethernet
 - Funcionan: DHCP, ARP,...
 - Drivers **TAP**
- VPN a nivel de red (IP)
 - Se transmiten paquetes IP y broadcasts IP
 - Funcionan: TCP, UDP, ICMP, enrutamiento...
 - Drivers **TUN**
- VPN a nivel de transporte (TCP)
 - La VPN conecta con un programa en la otra red (dirección IP y puerto TCP)

Túneles SSH

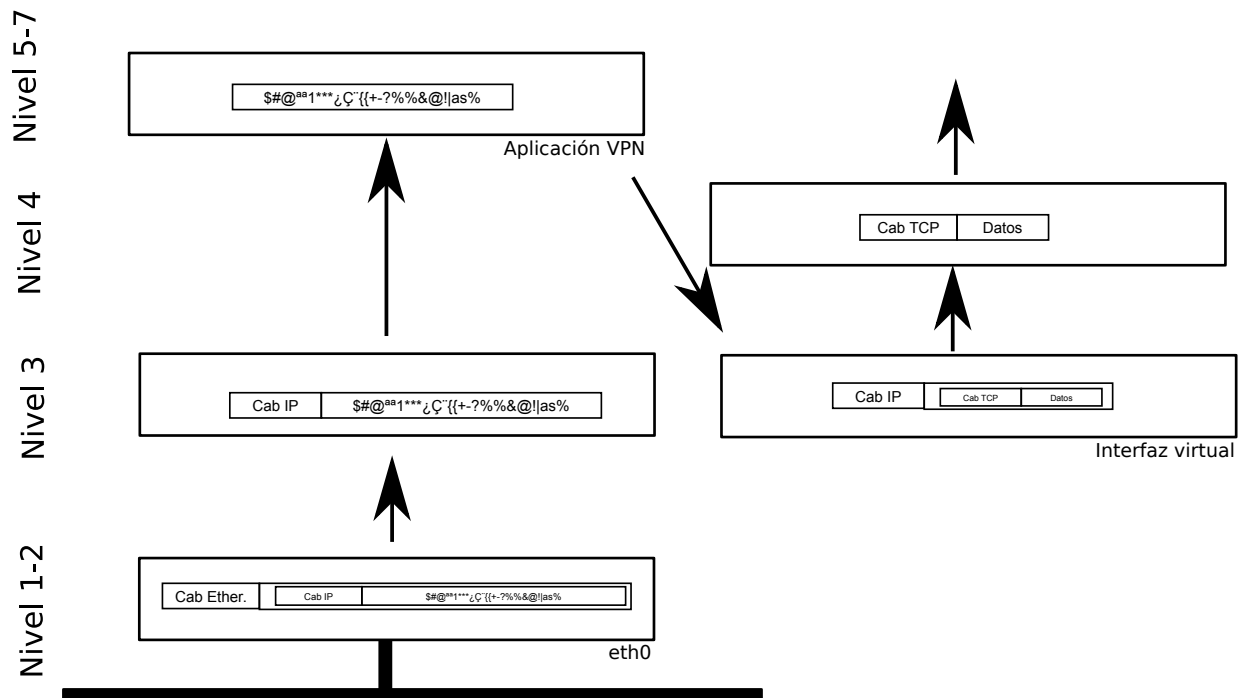


Figura 6: Ejemplo de proceso para *tunneling* a nivel 3

6. VPN: Protocolos

- PPTP
 - Muy extendido
 - Puede encapsular cualquier protocolo
 - Seguridad más débil
- L2TP
 - Utiliza IPSec para el cifrado
- IPSec
 - Soportado por OSI
 - Más complejo, pero más flexible
 - Fácil implementación en sistemas Windows

6.1. Ejercicio: VPN en Windows

- Crea un servidor VPN Windows en la *red interna 1*
- Conéctate desde un cliente VPN en la *red interna 2*
- Comprueba con `pathping` que a través de la VPN solo se da un salto
- Red interna 1: `192.168.1.0/24`
- Red interna 2: `192.168.2.0/24`
- Los ordenadores son los primeros de la red. El router es el último de la red.

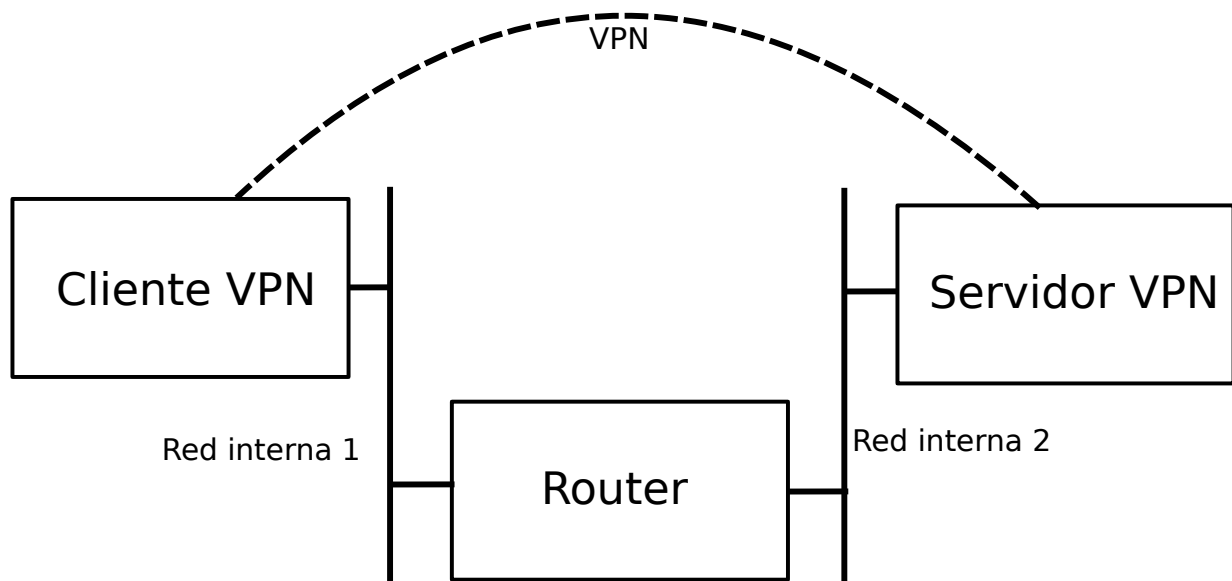


Figura 7: Diagrama lógico de la red con VPN

6.2. Ejercicio: VPN con SSH

- Crea un servidor VPN SSH en la *red interna 1*
- Conéctate desde un cliente VPN en la *red interna 2*
- Comprueba con `pathping` que a través de la VPN solo se da un salto

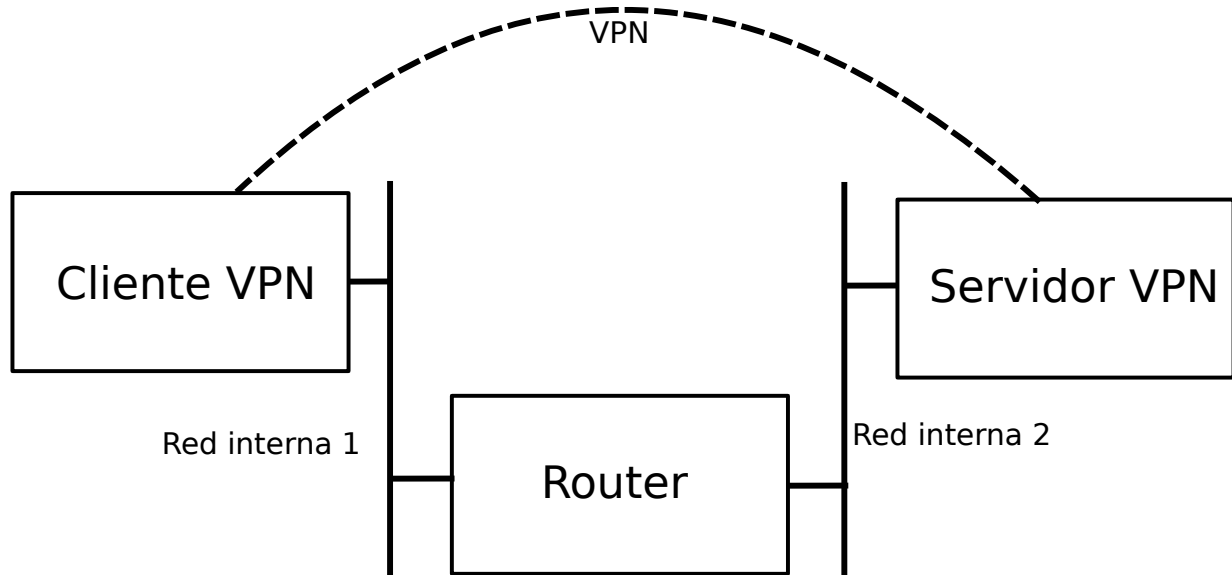


Figura 8: Diagrama lógico de la red con VPN

- Red interna 1: `192.168.1.0/24`
- Red interna 2: `192.168.2.0/24`
- Los ordenadores son los primeros de la red. El router es el último de la red.
- Red VPN: `10.0.0.0/24`

https://help.ubuntu.com/community/SSH_VPN

7. Referencias

- Formatos:
 - [Transparencias](#)
 - [PDF](#)
 - [EPUB](#)
- Creado con:
 - [Emacs](#)
 - [org-re-reveal](#)
 - [Latex](#)
- Alojado en [Github](#)