

Índice:

Ejercicio 1	2
a) PPTP.....	2
b) IKEv2/IPsec.....	4
c) OpenVPN	6
d) SSTP.....	8
e) WireGuard.....	10
f) Conclusión.....	11

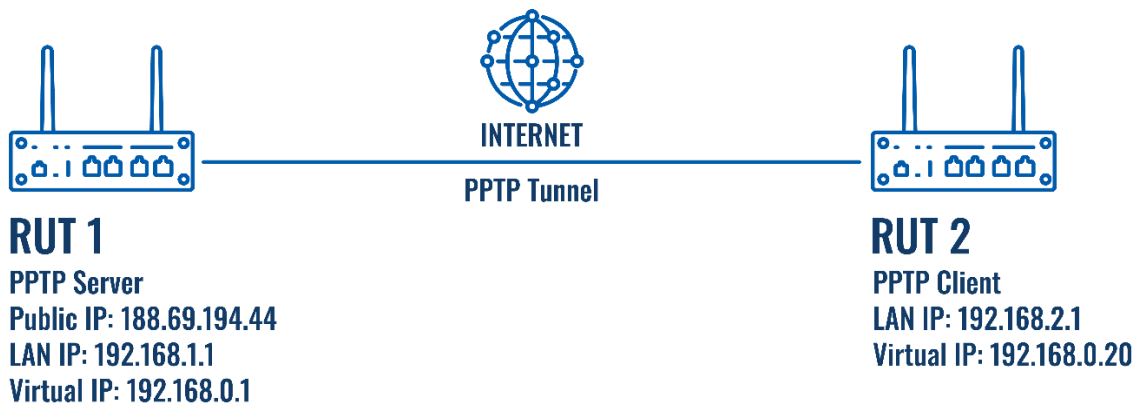
Ejercicio 1

a) PPTP

Solución:

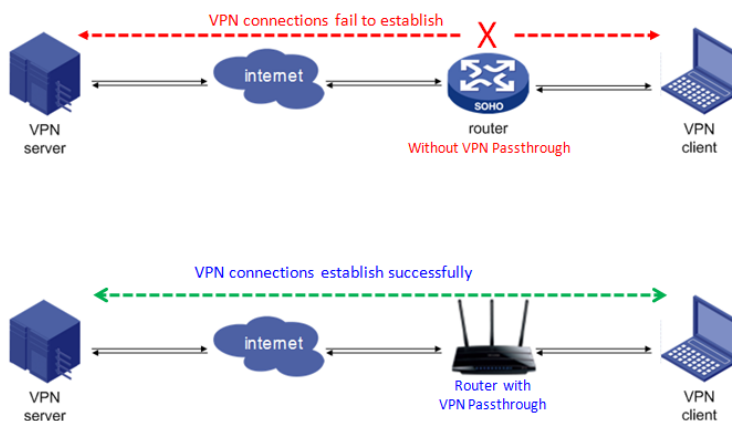


El Protocolo de Tunelización Punto a Punto (PPTP) es uno de los protocolos VPN más antiguos, especificado en el RFC 2637 en 1999. Aunque sigue siendo compatible con muchos sistemas operativos y dispositivos de red, presenta **riesgos significativos de seguridad**. PPTP utiliza una arquitectura **cliente-servidor** y encapsula paquetes de **Protocolo Punto a Punto (PPP)** para permitir la transmisión de datos entre redes privadas a través de Internet.



El funcionamiento de PPTP implica la conexión a un puerto **TCP 1723**, estableciendo una "**Conexión de Control**" y luego creando un **túnel GRE** para transportar paquetes PPP. Se utiliza **Microsoft Point-to-Point Encryption (MPPE)** para el cifrado y **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)** para la autenticación.

A pesar de sus ventajas, como la inclusión en todas las versiones de Windows y velocidades relativamente rápidas, PPTP tiene desventajas significativas. Su principal inconveniente es la **vulnerabilidad a ataques de seguridad**, como cambios de bits en MPPE, la facilidad de descifrar MS-CHAP y la posibilidad de **ataques de denegación de servicio**.



El **PPTP passthrough** es una característica que permite que los protocolos VPN atraviesen el **NAT** en dispositivos de red. Aunque algunas plataformas aún admiten PPTP, muchas han **dejado de hacerlo** debido a preocupaciones de seguridad, como **macOS** y **Android**.

Protocolo VPN	Velocidad	Encriptación	Streaming	Estabilidad	P2P	Disponible en NordVPN
OpenVPN	Rápido	Muy bueno	Bueno	Bueno	Bueno	✓
IPSec/IKEv2	Rápido	Bueno	Bueno	Muy bueno	Bueno	✓
Wireguard	Muy rápido	Bueno	Regular	Pobre	Bueno	✗*
SSTP	Regular	Bueno	Regular	Regular	Bueno	✗
L2TP/IPSec	Regular	Bueno	Pobre	Bueno	Pobre	✗
PPTP	Rápido	Pobre	Pobre	Bueno	Pobre	✗

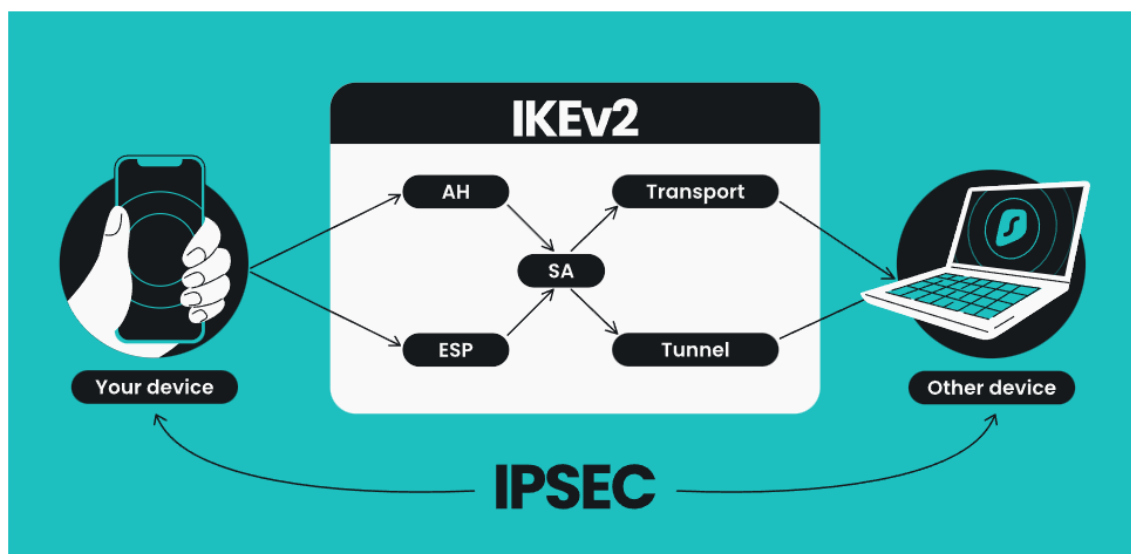
Aunque PPTP puede ser utilizado en casos específicos, se recomienda evitar su uso en entornos de producción críticos. En su lugar, se sugiere optar por protocolos VPN más seguros y modernos, como **IKEv2/IPsec**, **OpenVPN**, **SSTP** o **WireGuard**, para garantizar la seguridad en entornos empresariales actuales plagados de amenazas de seguridad en Internet.

b) IKEv2/IPsec

Solución:



IKEv2 (Internet Key Exchange version 2): Es un protocolo de VPN que combina dos protocolos distintos: IKEv2 gestiona la asociación de seguridad entre el dispositivo y el servidor VPN, mientras que IPsec se encarga de la transmisión de datos. Utiliza certificados X.509 para la identificación y crea un "secreto compartido" mediante Diffie-Hellman.



Integración de IKEv2 e IPsec: La fusión de IKEv2 e IPsec, liderada por Microsoft y Cisco, optimiza la velocidad y eficiencia. IKEv2 opera en el espacio de usuario, accediendo al almacenamiento de datos, mientras que IPsec funciona en el núcleo para procesar datos a velocidades superiores.

Diferencias entre IKEv1 e IKEv2: IKEv2 es más rápido, consume menos ancho de banda, tiene NAT integrada y admite EAP para mayor seguridad.

Seguridad de IKEv2: Considerado seguro, la implementación y la configuración correcta por parte del proveedor de VPN son cruciales para garantizar la seguridad.

Configuración de IKEv2: Puede configurarse fácilmente mediante un servicio VPN compatible. En sistemas como macOS, iOS y Android, la configuración es sencilla a través de la aplicación del proveedor. Para configuración manual, los pasos varían según el sistema operativo.

IKEv2



Other VPN

PPTP
SSTP
L2TP



Comparación con Otros Protocolos: En comparación con otros protocolos como **OpenVPN** y **WireGuard**, **IKEv2 es seguro y rápido**. La elección entre ellos depende de la implementación y preferencias del usuario.

Ventajas de IKEv2: **Cifrado seguro**, **estabilidad de conexión** al cambiar entre redes, **velocidad eficiente** con recursos limitados y **compatibilidad** con diversos dispositivos.

Inconvenientes: En comparación con **WireGuard**, un **protocolo más reciente y rápido**, **IKEv2** puede considerarse **menos avanzado**.

Compatibilidad con Dispositivos: Compatible con **Android**, **iOS** y **macOS**, **Windows** y **Linux**.

c) OpenVPN

Solución:



Gestiona las comunicaciones cliente-servidor, estableciendo un "túnel" seguro entre ellos. Utiliza extensamente la biblioteca OpenSSL para cifrado y autenticación. Opera sobre UDP o TCP para la transmisión de datos.

TCP es más estable con corrección de errores; UDP es más rápido pero menos estable. OpenVPN prefiere conexiones UDP por velocidad, con la opción de TCP si es necesario.



Emplea cifrado de 256 bits con varios cifrados como AES, Camellia, 3DES, CAST-128 o Blowfish. Usa un protocolo personalizado basado en TLS y SSL, diferente de L2TP, IPSec y PPTP. Admite procesos de inicio de sesión y autenticación mejorados mediante complementos de terceros y scripts.

OpenVPN opera en el espacio de usuario, no en el espacio del núcleo, mejorando la seguridad. Superó auditorías de seguridad en 2017 con hallazgos mínimos.

Aunque no es el más rápido, OpenVPN ofrece velocidades decentes, afectadas por el cifrado fuerte. UDP generalmente proporciona velocidades más rápidas en comparación con TCP.

Requiere archivos de configuración proporcionados por un servicio VPN. La instalación implica configurar el cliente OpenVPN, importar datos VPN y establecer conexiones.

Ventajas: Alta seguridad, evasión de firewall, flexibilidad de protocolo (UDP/TCP), soporte multiplataforma, Secreto Perfecto Hacia Adelante.

Desventajas: Posiblemente velocidades más lentas, complejidad en la configuración.

- OpenVPN vs. SSTP: La naturaleza de código abierto y el amplio soporte de plataforma dan a OpenVPN una ventaja.
- OpenVPN vs. WireGuard: WireGuard es más rápido pero puede carecer de la extensa trayectoria de OpenVPN.
- OpenVPN vs. SoftEther: Ambos seguros, SoftEther afirma velocidades más altas, pero la confiabilidad y madurez de OpenVPN a menudo son preferidas.

OpenVPN es ampliamente considerado como uno de los protocolos VPN más seguros. Su naturaleza de código abierto permite una inspección y mejora continua.

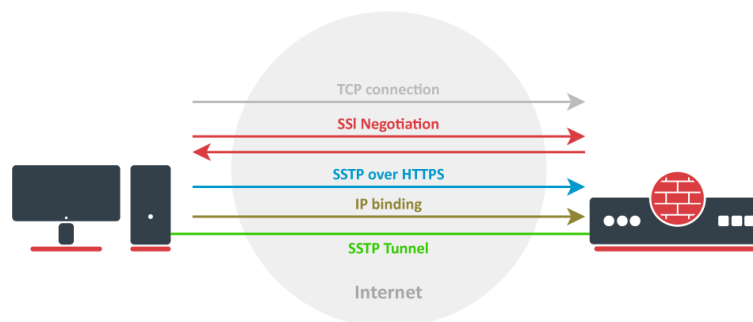
La configuración implica obtener archivos de configuración, instalar el cliente OpenVPN y, si es necesario, ajustar configuraciones. Adecuado para diversas actividades en línea que requieren privacidad, seguridad y evasión de firewall. Recomendado para escenarios como juegos, descargas de torrents y eludir restricciones geográficas.

d) SSTP

Solución:



SSTP significa Protocolo de Tunelización de Conector Seguro (Secure Socket Tunneling Protocol en inglés). A diferencia de otros protocolos, SSTP es propiedad directa de Microsoft y fue introducido con Windows Vista.



Transporte a través de SSL: SSTP transporta el tráfico a través del protocolo de Capa de Conectores Seguros (SSL), utilizando el puerto TCP 443. Esto reduce la probabilidad de ser bloqueado por cortafuegos en comparación con L2TP.

Propiedad de Microsoft: Aunque no cuenta con las ventajas de código abierto como OpenVPN, SSTP suele ser considerado como uno de los protocolos más seguros, al ser propiedad de Microsoft.

Adaptación en Routers Mikrotik: Después de su introducción en Windows Vista, RouterOS adaptó SSTP para su uso en routers Mikrotik.

Enfoque en Clientes: SSTP fue diseñado principalmente para clientes, no para conexiones de sitio a sitio (Site-to-Site), aunque Mikrotik ha proporcionado adaptaciones para este propósito.

Autenticación mediante Certificados: Para establecer un túnel SSTP, se requieren certificados. En el servidor, la autenticación se realiza mediante usuario y contraseña, mientras que en el cliente se autentica mediante el certificado del servidor.

Requisito para Clientes Windows: Si el cliente SSTP es una PC con Windows, la única manera de configurar un túnel SSTP es importando un certificado auto-firmado.

e) WireGuard

Solución:



WireGuard es un protocolo VPN de código abierto introducido en 2016, destacado por su rapidez, facilidad de uso y seguridad. Utiliza criptografía avanzada para conectar dispositivos a servidores VPN, creando túneles privados y cifrados para mantener la privacidad de los datos y comunicaciones.

Protocolo y Capa de Transporte: Basado en la capa de transporte UDP, proporcionando comunicación rápida entre hosts y clientes. A diferencia de TCP, no requiere un apretón de manos, lo que acelera la conexión VPN.

Diseño Optimizado y Ligero: Con aproximadamente 4000 líneas de código, WireGuard es más simple que alternativas como OpenVPN (600,000 líneas). Su diseño minimalista y eficiente mejora la velocidad y seguridad, siendo menos exigente con los recursos de la CPU.

Ventajas:

- **Velocidad:** Combina rapidez y seguridad al utilizar métodos criptográficos avanzados como ChaCha20.
- **Seguridad:** Código fuente abierto, diseño mínimo, y cifrado moderno mejoran la seguridad.
- **Facilidad de Uso:** Configuración sencilla y conexión rápida, ideal para usuarios que se desplazan entre redes.

Inconvenientes:

- **Privacidad:** La capa de transporte UDP puede hacer evidente el uso de una VPN, posiblemente limitando la elusión de cortafuegos.
- **Compatibilidad:** Aunque crece, WireGuard aún no es compatible con todos los servicios VPN en todas las plataformas.
- **Comparación con Otros Protocolos VPN:**

WireGuard vs. OpenVPN: WireGuard destaca por su diseño más sencillo, uso de UDP, y cifrado moderno, ofreciendo ventajas de velocidad. OpenVPN puede ser preferido para ocultar el uso de la VPN.

WireGuard vs. IKEv2/IPsec: WireGuard es más rápido y seguro, mientras que IKEv2/IPsec es más versátil pero con cifrado más antiguo. La elección depende de las necesidades de la red.

Código Fuente Abierto y Mínimo: La simplicidad del código y su naturaleza de código abierto facilitan auditorías y mejoras continuas. WireGuard utiliza cifrado moderno, priorizando tanto la seguridad como la velocidad.

f) Conclusión

En resumen, cada protocolo VPN, como PPTP, IKEv2/IPsec, OpenVPN, SSTP y WireGuard, presenta ventajas y desventajas. PPTP, a pesar de su compatibilidad, es obsoleto y menos seguro. IKEv2/IPsec ofrece versatilidad pero puede ser más vulnerable. OpenVPN es un estándar popular y seguro, aunque menos eficiente. SSTP es sólido pero principalmente compatible con entornos Windows. WireGuard destaca por su eficiencia y seguridad moderna. La elección depende de las necesidades individuales, considerando factores como seguridad, rendimiento y compatibilidad.