

Túneles VPN L2TP

Conceptos generales



Tunel L2TP

L2TP (*Layer 2 Tunneling Protocol*) es un protocolo utilizado por redes privadas virtuales que fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos.

L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete de datos, incluyendo X.25, Frame Relay y ATM.

Túnel L2TP

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete **UDP**, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos **IPSec** pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

Tunel L2TP

L2TP incluye autenticación(authentication) y contabilidad(accounting) PPP para cada conexión L2TP. Una completa autenticación y contabilidad puede ser administrada por un **RADIUS** o localmente en Mikrotik.

Métodos en encriptación soportados

- **MPPE 40 bits**
- **MPPE 128 bits**

Tunel L2TP

Utiliza claves (keys) de encriptación **AES-256 bit**, o algoritmo de encriptación 3DES. La carga útil (payload) de **L2TP es encriptada por IPSec**.

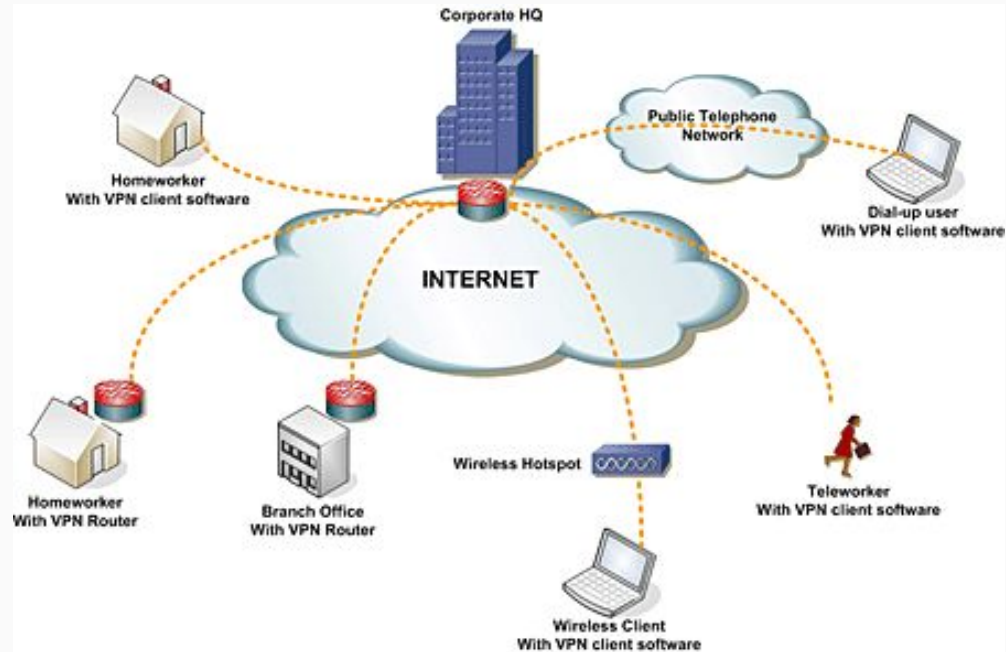
L2TP tiene un overhead más alto comparado con otros estándares debido a la doble encriptación. Todos los sistemas operativos Windows y Mac OS soportan L2TP de forma nativa. También soporta plataformas **Linux, iOS y Android**.

Tunel L2TP

L2TP utiliza los puertos

- **UDP 500** para el intercambio inicial de clave (initial key Exchange)
- **UDP 1701** para configuración
- **UDP 4500** para NAT

VPN L2TP/IPSEC



Laboratorios L2TP

Ahora vamos a configurar
los laboratorios de L2TP
básicos y luego
configuraremos
L2TP/IPSEC



DigitalOcean