Virtual Private Network (VPN's)

Fernando Dagoberto Piche Ramirez

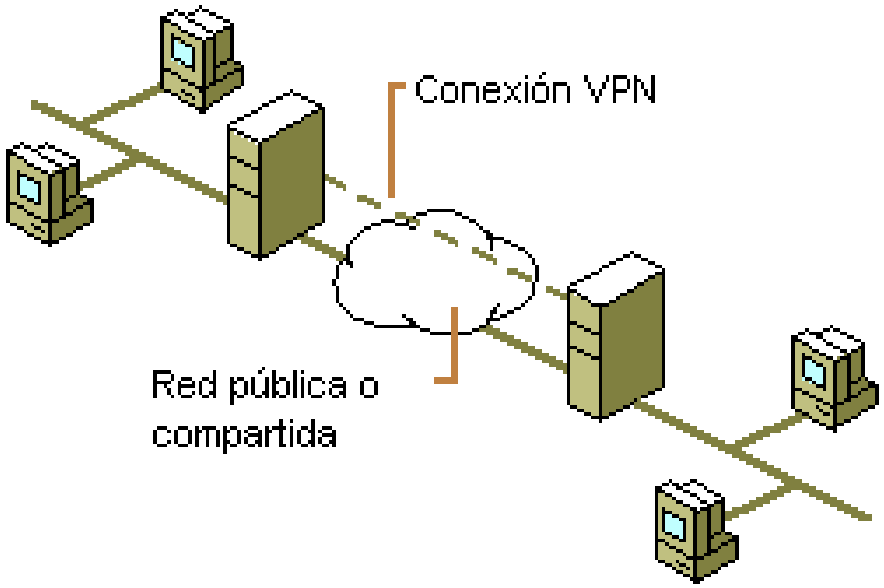
Luis Alfredo Avilés Sánchez

Introducción

- ¿Qué es una VPN?
- Tipos de Enlaces
- ¿Para que sirve?
- Aspectos Técnicos
- Ventajas e Desventajas

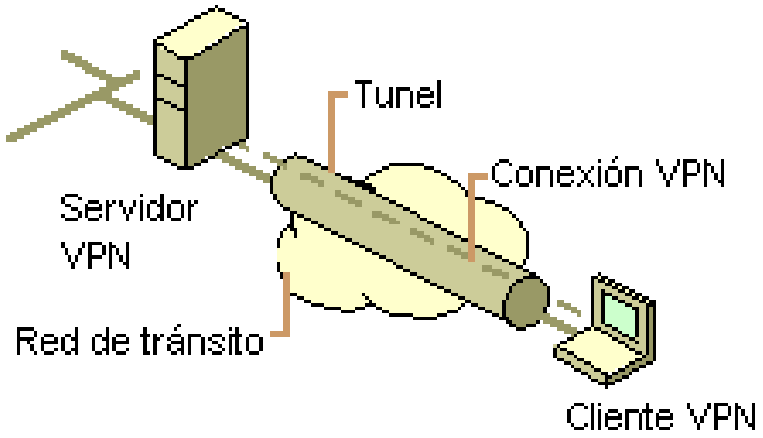
¿Qué es una VPN?

- Red privada y segura sobre red pública y no segura.
- Proporciona un túnel ip encriptado y/o encapsulado a través de internet.



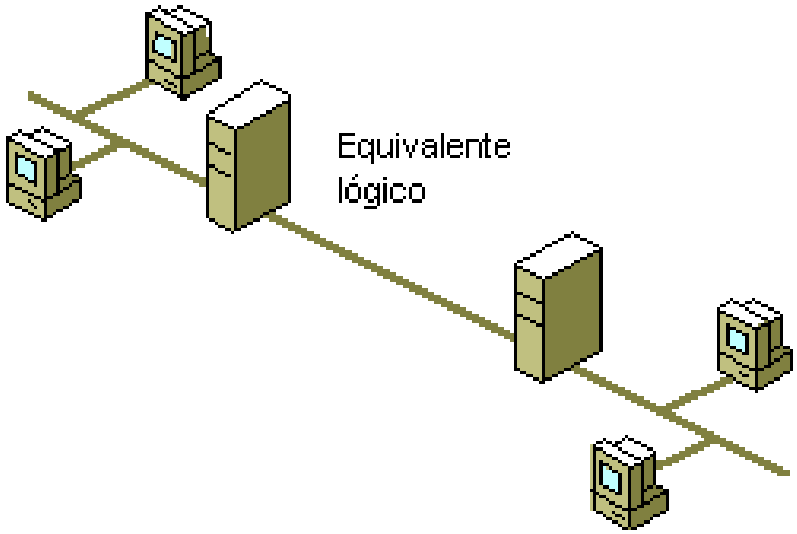
Tipos de Enlaces

- Enlace Cliente - Red:
  - El cliente se conecta remotamente a una LAN.
  - Se usa PPP para establecer una conexión entre el cliente y la LAN.



Tipos de Enlaces

- Enlace Red - Red:
  - Se encapsula el tráfico de una red local.
  - Nos ahorramos el paso PPP (las tramas se encapsulan directamente).



¿*Para que sirven?*

- Permite conectar diferentes redes de una empresa, simulando una red local de una manera segura.
- Da acceso a clientes, socios y consultores a los diferentes recursos de la red de forma remota y segura.

Niveles donde trabajan

- Nivel 2 (OSI)
  - PPTP, L2F, L2TP
- Nivel 3 (OSI)
  - IPSec

PPTP

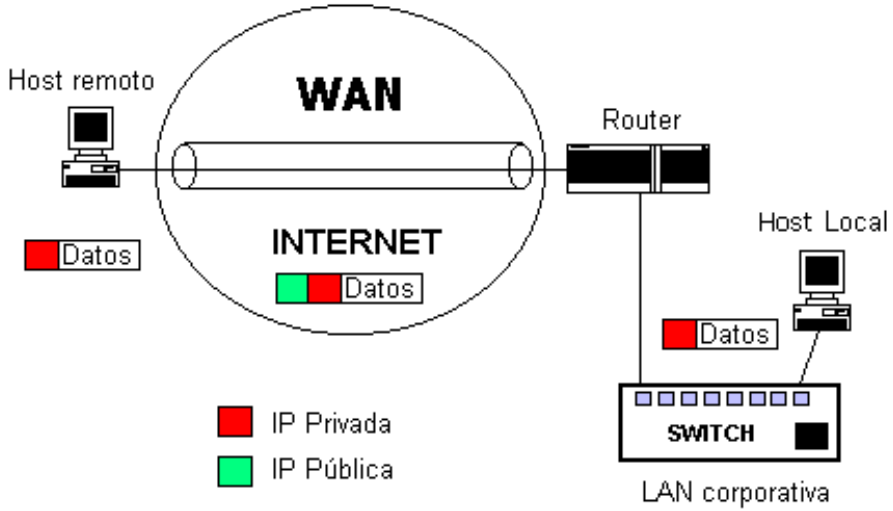
- PPTP (Point-to-Point Tunneling Protocol):
  - Protocolo desarrollado por Microsoft y de facil configuracion.
  - Permite el tráfico seguro de datos desde un cliente remoto a un servidor privado.
  - PPTP soporta protocolos de red (IP, IPX, NetBEUI).
  - Tiene una mala reputación en seguridad por ser de la Microsoft.
  - Muy usado en plataformas Microsoft.

L2TP

- L2F (Layer 2 Forwarding):
  - Protocolo desarrollado por Cisco Systems.
  - Precursor del L2TP.
  - Ofrece métodos de autenticación de usuarios remotos
  - Carece de cifrado de datos

Tunneling

- Tunneling:
  - Añade una cabecera IP adicional (**cabecera del protocolo de transporte**) al paquete original para que éste pueda circular a través de Internet hasta el router de la empresa corporativa donde es eliminada.
  - El router que permite accesos vía tunel a una red privada se denomina **servidor de túneles**.



Seguridad para L2TP

- IPSec :
  - Proporciona servicios de seguridad a nivel 3.
  - Permite seleccionar protocolos de seguridad, algoritmos que se van a utilizar y las claves requeridas para dar estos servicios.
  - Servicios de seguridad que proporciona:
    - Control de acceso
    - Integridad
    - Autenticación del origen de los datos
    - Confidencialidad
  - Es estándar dentro de IPv6 y ha sido adaptado para IPv4.

Ventajas

- Ventajas:
  - Ahorro de los costos.
  - No se compromete la seguridad de la red de la empresa.
  - El cliente remoto adquiere la condición de miembro de la LAN (permisos, directivas de seguridad).
  - El cliente tiene acceso a todos los recursos ofrecidos en la LAN (impresoras, correo electrónico, base de datos).
  - Acceso desde cualquier punto del mundo (siempre y cuando se tenga acceso a internet).

Desventajas

- Desventajas:
  - No se garantiza disponibilidad (NO Internet --> NO VPN).
  - No se garantiza el caudal.
  - Gestión de claves de acceso y autenticación delicada y laboriosa.
  - La fiabilidad es menor que en una linea dedicada
  - Mayor carga en el cliente VPN (encapsulación y encriptación)
  - Mayor complejidad en la configuración del cliente (proxy, servidor de correo, …)
  - Una VPN se considera segura pero no hay que olvidar que viajamos por Internet (no seguro y expuestos a ataques).