Redes WAN

VPN

Esteban De La Fuente Rubio
esteban@delaf.cl
LaTeX

Universidad Andrés Bello

13 may 2011

Tabla de contenidos

Trabajadores a distancia

- Empleados de forma remota.
- Disponer de trabajadores en sucursales.
- Oportunidades mediante telefonía IP y aplicaciones web.

Trabajadores a distancia (2)

Beneficios:

- Mayor capacidad de respuesta.
- Acceso a la información desde cualquier punto.
- Integración de datos, voz y video.
- Mayor productividad, satisfacción y retención de empleados.

Trabajadores a distancia (3)

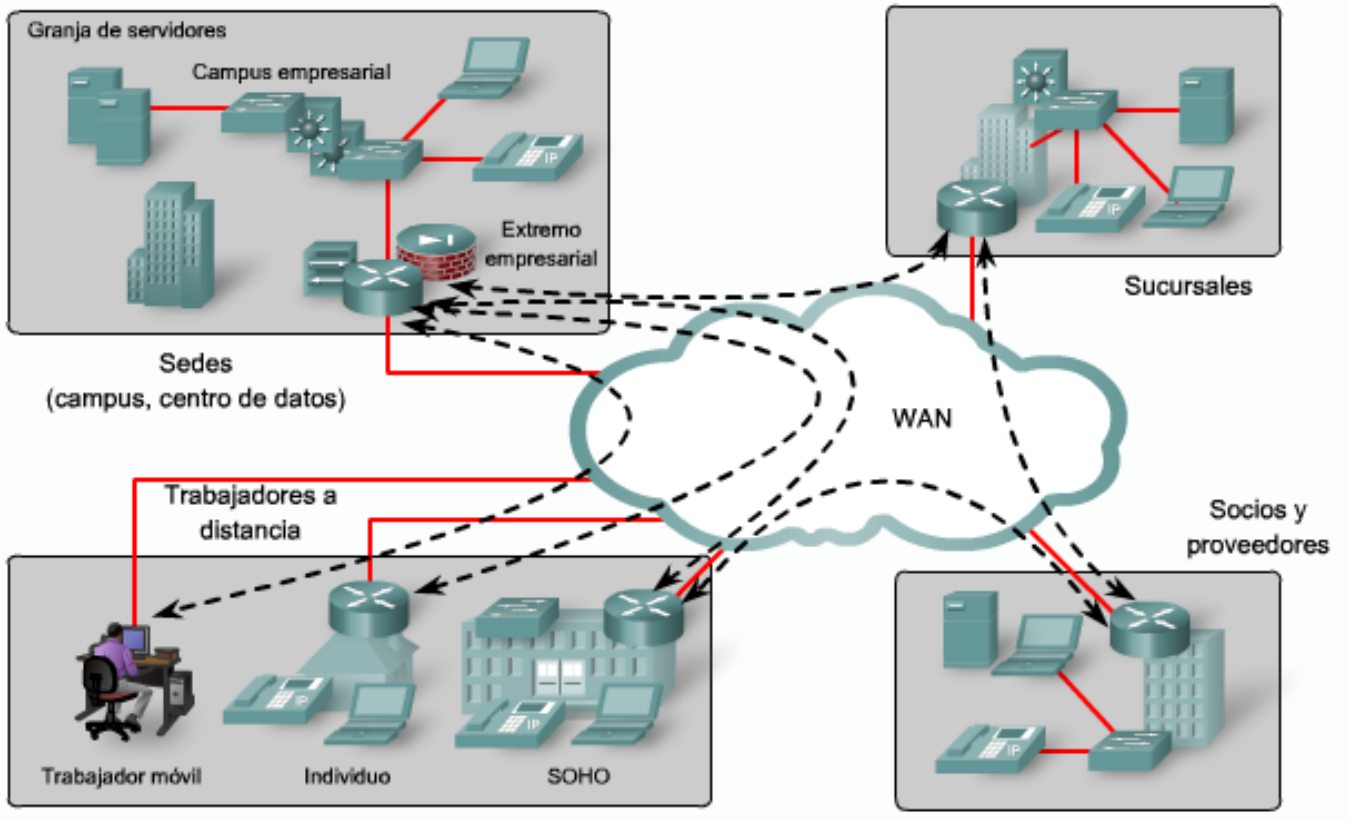

Figura: Opciones de conexión remota

Trabajadores a distancia (4)

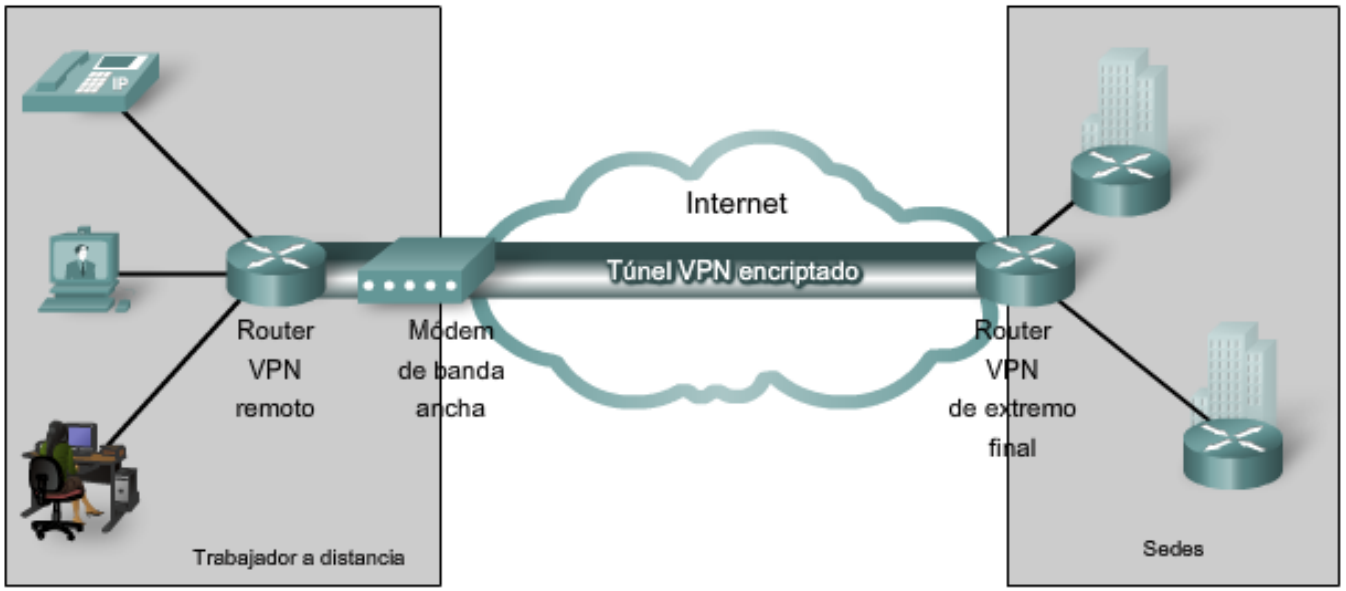

Figura: Requisitos de conexión remota

Trabajadores a distancia (5)

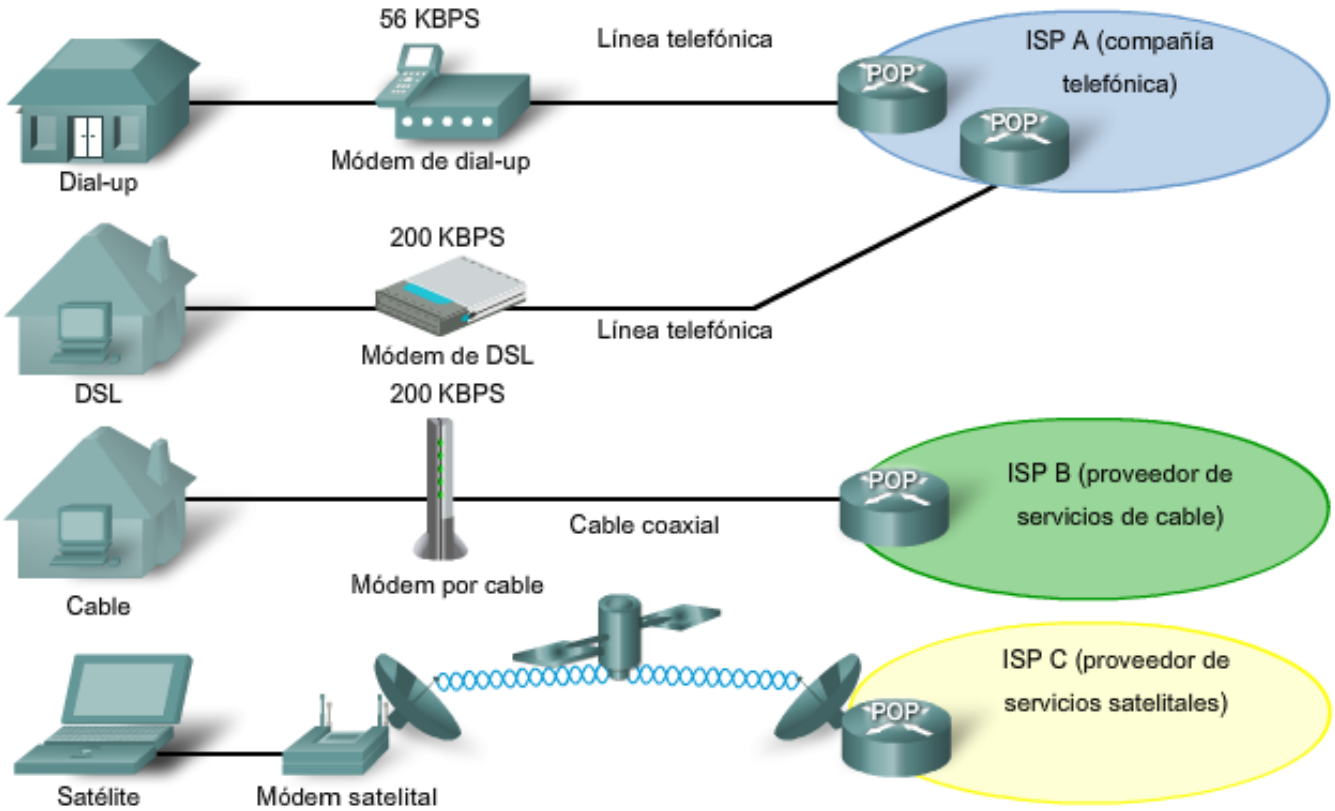

Figura: Opciones de conexión WAN

Redes VPN

- Red privada virtual.
- Utilizado por las empresas para proveer de servicios a sucursales y trabajadores a distancia.
- Evita tener que utilizar una conexión de capa 2 exclusiva (como Frame Relay).
- Se enrutan a través de Internet.

Redes VPN (2)

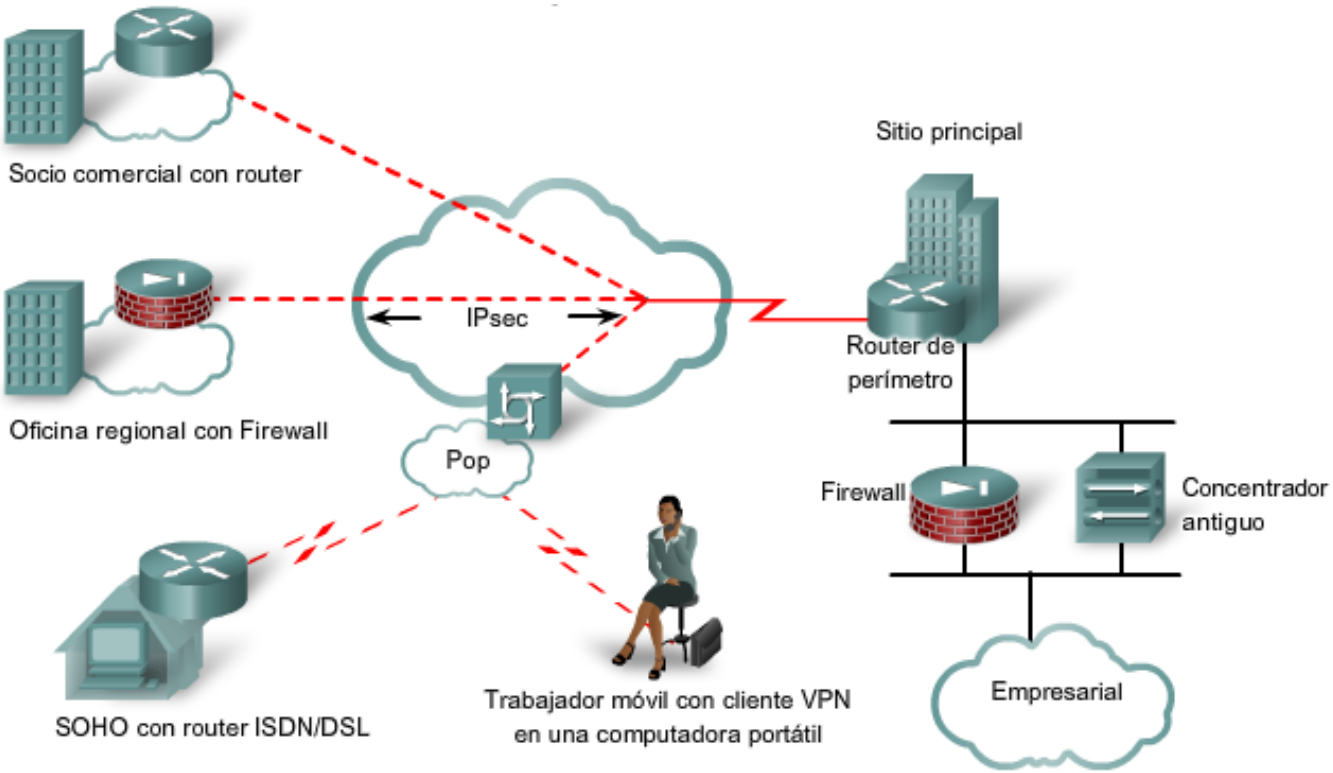

Figura: VPN

Redes VPN (3)

- Uso de internet para transportar tráfico de la empresa.
- Ofrece seguridad al utilizar métodos de cifrado y autenticación.
- Es un sistema escalable ya que se utilizan los mismos equipos ya adquiridos.

Sitio a sitio

- Permiten conectar 2 extremos fijos.
- Utilizado para unir redes de sucursales.

Roadwarrior

- Permite conectar a una persona a una red o ordenador.
- Usuario iniciará sesión de VPN y podrá acceder a los servicios del extremo.

Seguridad

Al ser una conexión segura debe proveer:

- Confidencialidad.
- Integridad.
- Autenticación.

Encapsulación

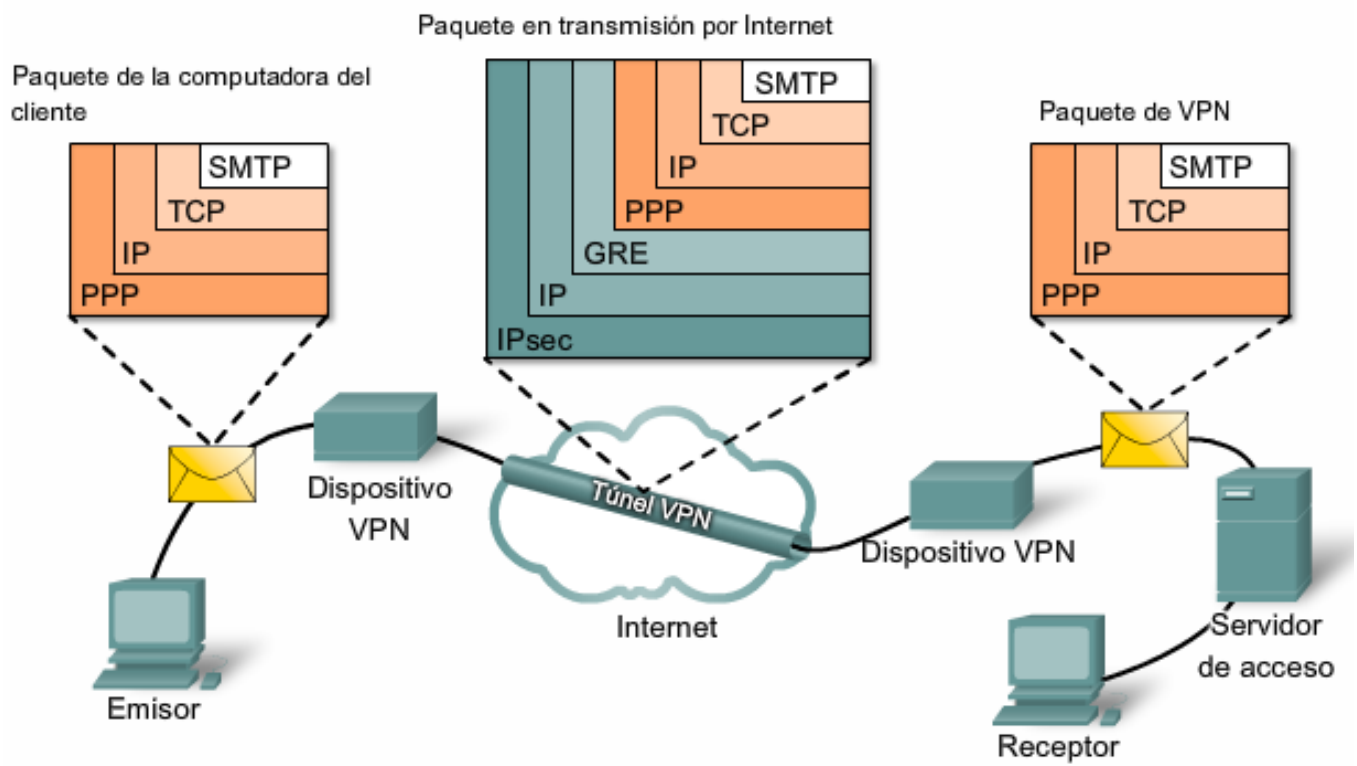

Figura: Encapsulación usanto un túnel GRE

Encriptación

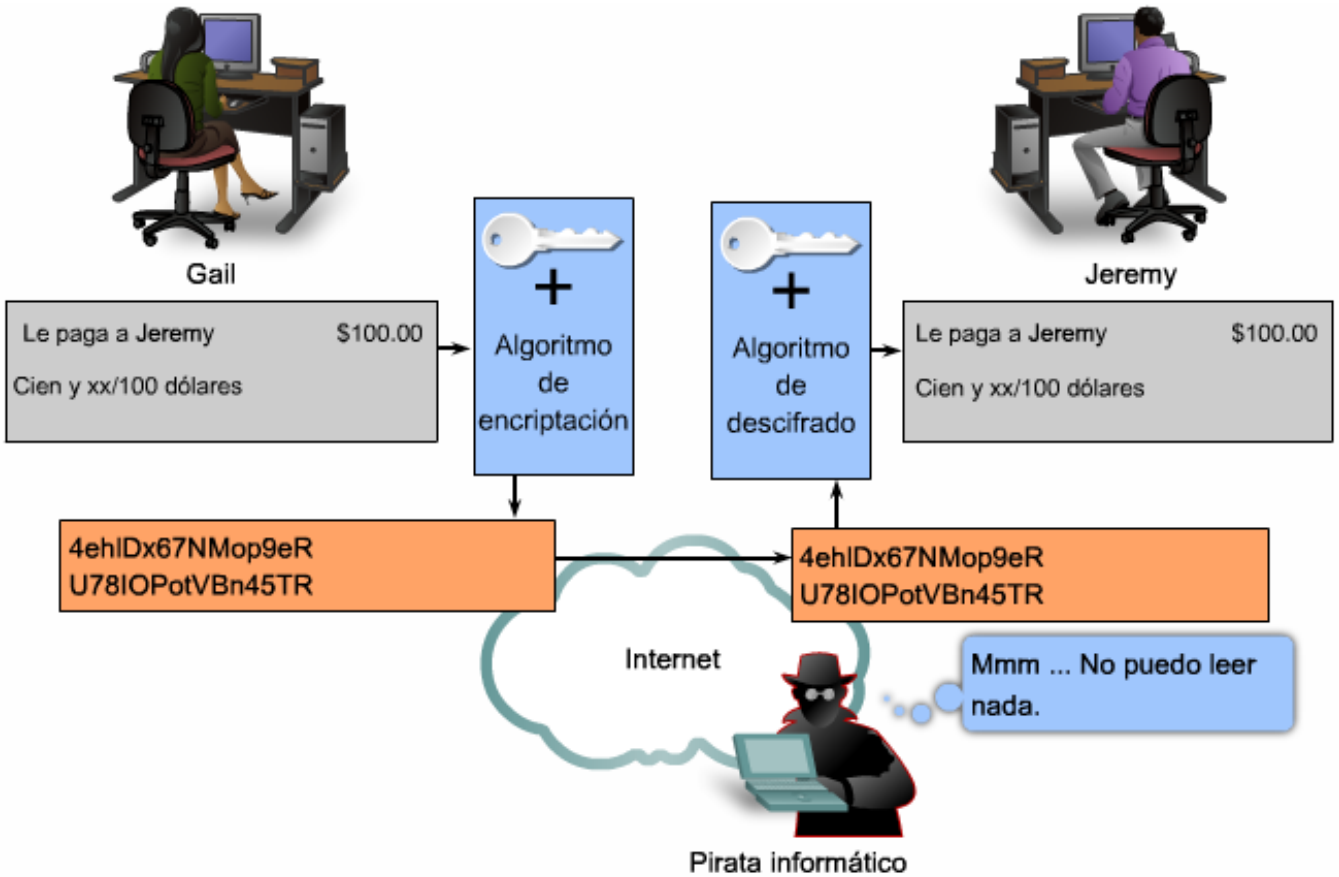

Figura: Encriptación de datos del túnel VPN

Hash

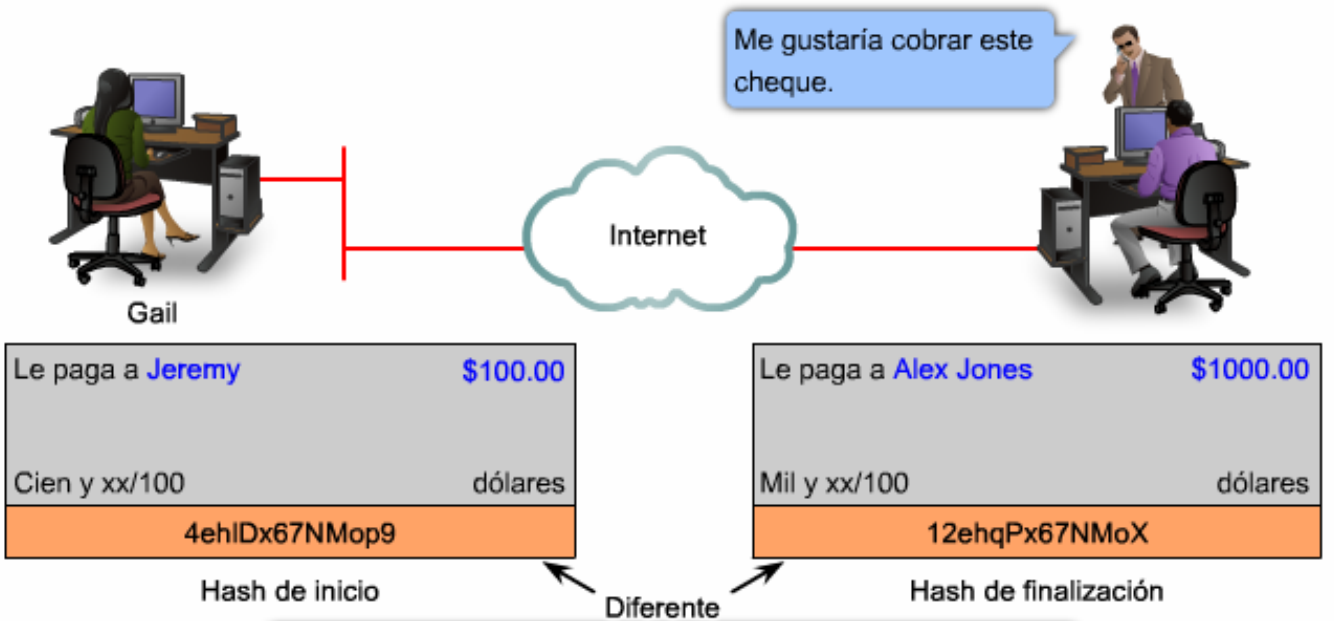

Figura: Hash

Autenticación

Figura: Autenticación mediante Firmas RSA o PSK.

IPSec

- Conjunto de protocolos para asegurar las comunicaciones.
- Funciona en capa 3.
- Estándar.
- Permite la creación de VPN.

IPSec (2)

IPSec permite:

- Cifrar el tráfico.
- Validar integridad.
- Autenticar los extremos.
- Evitar repetición de sesiones.

IPSec (3)

Modos de funcionamiento:

- Modo transporte.
- Modo túnel.

Modo transporte

- Ordenador a ordenador.
- Solo datos son cifrados.
- Enrutamiento se mantiene.
- Problemas al usar NAT (ya que se modifica el hash del paquete).

Modo túnel

- Red a red, ordenador a red u ordenador a ordenador.
- Todo el paquete es cifrado.
- Encapsulado en un nuevo paquete IP.
- No hay problemas al usar NAT.

OpenVPN

- Solución basada en software usando SSL.
- Publicado bajo licencia GPL.
- Más simple de configurar que IPSec.
- Puede utilizar cifrado simétrico y asimétrico.

Cifrado

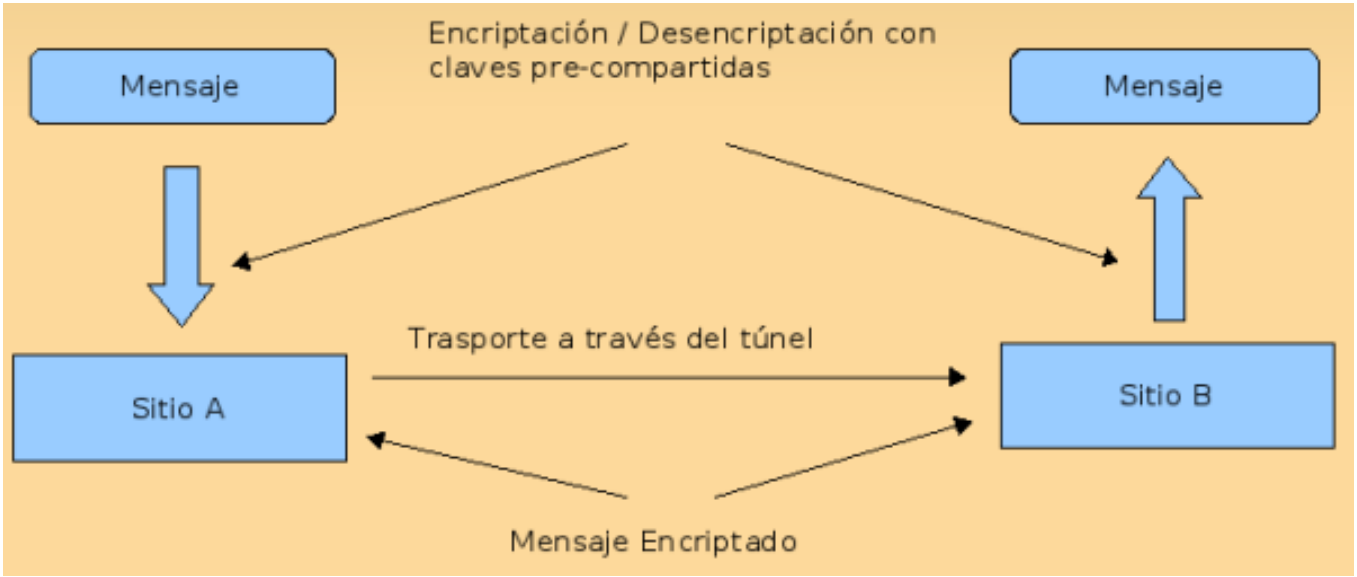

Figura: Uso de pre-sharedkey (PSK)

Cifrado (2)

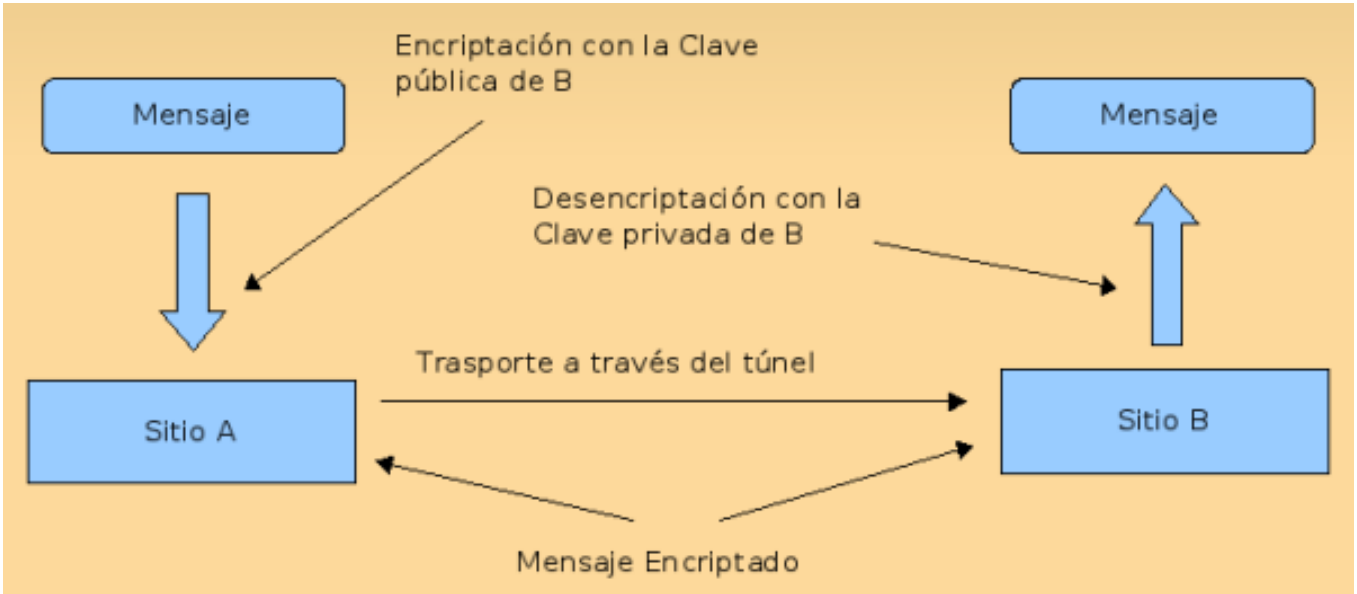

Figura: Uso de llaves públicas y privadas.

Ventajas

- Funcionamiento en capa 2 o capa 3.
- No tiene problema al utilizar NAT.
- No se requieren IP estáticas en ambos lados del túnel.
- Fácil de implementar.

Desventajas

- No tiene compatibilidad con IPSec.
- Poco masivo (gente que no lo sabe utilizar).
- Pocos dispositivos con OpenVPN integrado (WRT54GL + OpenWRT).

Comparación con IPSec

- Tecnología sencilla.
- Se ejecuta en el espacio del usuario (sin ser root).
- Tecnologías de cifrado estandarizada.
- Utiliza solo un puerto en el firewall.