# OpenVPN

José Domingo Muñoz

IES Gonzalo Nazareno

Febrero 2021


# Introducción

- El proyecto OpenVPN desarrolla una implementación de VPNs basadas SSL/TLS
- Las razones de su desarrollo son las limitaciones y problemas de IPSec y el rápido desarrollo de SSL
- Se trata de un producto de software libre liberado bajo los términos de la GPL que fue creado por James Johan en el año 2001

# Características principales

- El componente principal es el driver tun/tap utilizado para simular interfaces de red, que se encarga de levantar el túnel y encapsular los paquetes a través del enlace virtual
- Encriptación y autenticación con OpenSSL
- Utiliza un único puerto TCP o UDP → fácil para firewalls
- Multiplataforma → misma herramienta funcionando sobre distintos SO vs implementaciones diferentes de un mismo estándar en distintas arquitecturas
- Compresión de datos LZO

# Algunos problemas

- No es compatible con IPSec, el estándar para soluciones VPN
- Comunidad no muy amplia
- Faltan dispositivos con clientes OpenVPN integrados

## COMPARATIVA: OpenVPN - IPSec

# Modos de funcionamiento

- **Modo túnel**: Emplea el driver tun y es utilizado para crear túneles virtuales operando con el protocolo IP
- **Modo puente**: Utiliza el driver tap y es empleado para túneles que encapsulan directamente paquetes Ethernet. Se recomienda en las siguientes situaciones:
  - La VPN necesita encapsular protocolos no-IP
  - Se ejecutan aplicaciones que necesitan network broadcasts
  - No se cuenta con un servidor Samba y se necesita que los usuarios puedan navegar por los ficheros compartidos

# Autenticación

- La autenticación de los extremos remotos de una conexión SSL/TLS está basada en el modelo de claves asimétricas RSA
- Los participantes intercambian sus claves públicas a través de certificados digitales X.509, que han sido firmados previamente por una Autoridad de Certificación en la que se confía