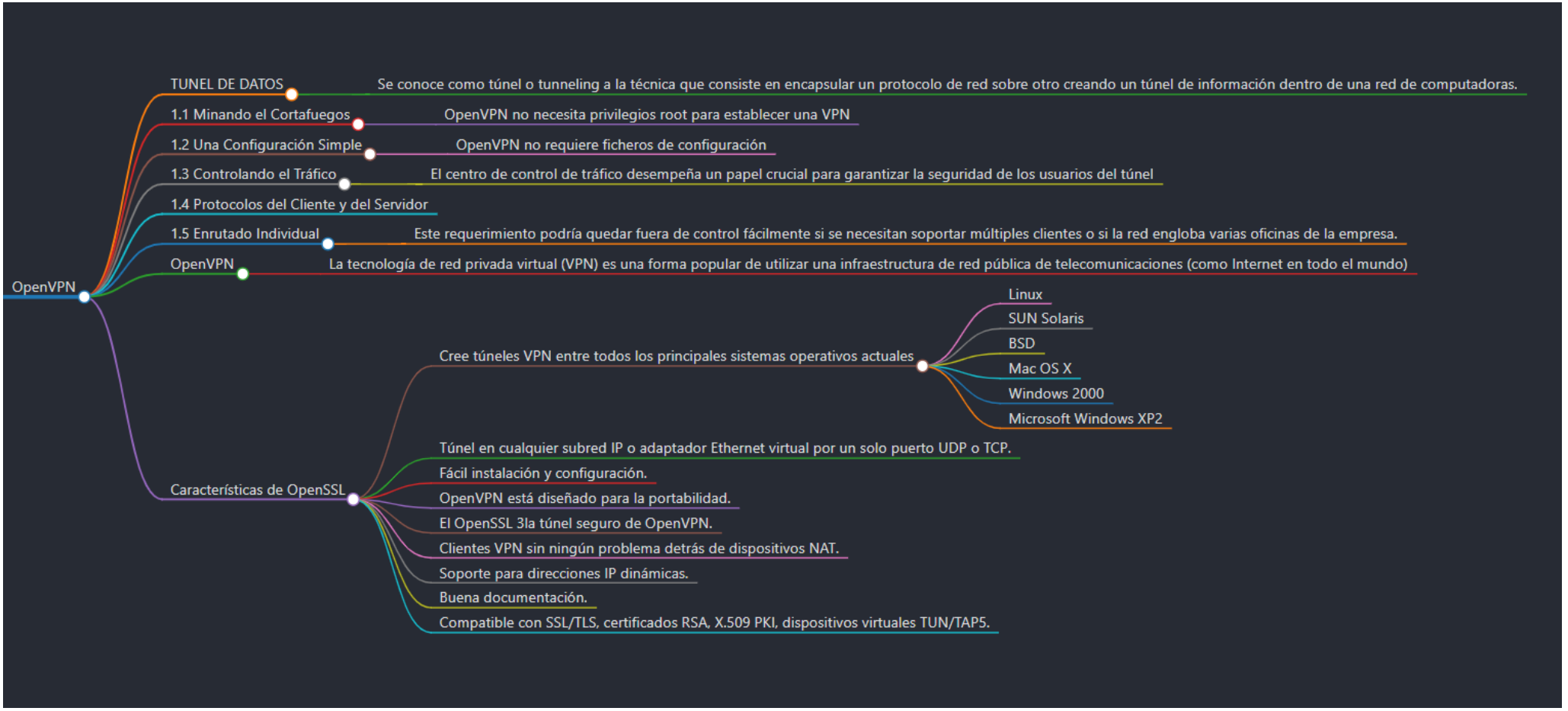

 # OpenVPN

TUNEL DE DATOS

- Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro creando un túnel de información dentro de una red de computadoras.

1.1 Minando el Cortafuegos

- OpenVPN no necesita privilegios root para establecer una VPN

Si tenemos acceso a dispositivos virtuales TUN/TAP, será suficiente para funcionar con los privilegios de usuario.
Todo lo que se necesita son unos cuantos parámetros para configurar la VPN, En un escenario.

Necesitamos el fichero que contiene la clave secreta, que se puede crear en la máquina cliente con el comando openvpn --genkey --secret secret.key para posteriormente copiarlo en el servidor.

El protocolo UDP, es la mejor opción para realizar el túnel con TCP/IP: esto evita que se dé el escenario en el que pueda producirse un timeout simultáneo entre OpenVPN y la conexión TCP.

La mayoría de los cortafuegos no permiten que los clientes puedan recibir paquetes UDP desde Internet. La única alternativa es optar por una conexión TCP. Esto implica que el servidor ha de estar escuchando en un puerto determinado a la espera de conexiones entrantes para establecer la conexión VPN.

1.2 Una Configuración Simple

- OpenVPN no requiere ficheros de configuración

Por lo que, la mejor opción para el establecimiento de la configuración del túnel que se realiza a través de la línea de comandos mediante sus parámetros. El servidor no necesita mucha información, requiere la dirección ip del servidor y de la máquina del cliente.

1.3 Controlando el Tráfico

- El centro de control de tráfico desempeña un papel crucial para garantizar la seguridad de los usuarios del túnel

Especialmente en caso de catástrofe. Por lo tanto, resultan esenciales la redundancia multicapa, la ciberseguridad, la integración con los servicios de emergencia y el control sin fisuras de los sistemas de emergencia en el túnel. Para garantizar un correcto funcionamiento, los túneles se monitorizan desde los puestos de control centrales. En función de su tipo y tamaño, los túneles tienen sus propias instalaciones de control conectadas a centrales de control de nivel superior.

1.4 Protocolos del Cliente y del Servidor

El parámetro (protocolo tcp) server habilita OpenVpn en el servidor e indica la escucha de las conexiones tcp entrantes

1.5 Enrutado Individual

- Este requerimiento podría quedar fuera de control fácilmente si se necesitan soportar múltiples clientes o si la red engloba varias oficinas de la empresa.

Para los usuarios que consideren requerimientos mayores, VPN versión 2.0 o posterior proporcionan infraestructura de Clave Pública, CAs y soporte para múltiples clientes para escenarios más avanzados

Protocolos del cliente y del servidor:

el parámetro (protocolo tcp) server habilita OpenVpn en el servidor e indica la escucha de las conexiones tcp entrantes.

OpenVPN

- La tecnología de red privada virtual (VPN) es una forma popular de utilizar una infraestructura de red pública de telecomunicaciones (como Internet en todo el mundo)

para interconectar redes privadas y remotas y proporcionar acceso seguro (remoto) a oficinas o redes. Esto se puede hacer usando varios protocolos de tunelización y cifrando, descifrando y autenticando el tráfico. Proporciona más o menos las mismas capacidades que (p. ej.) una línea arrendada pero a un costo menor.

Características de OpenSSL

Cree túneles VPN entre todos los principales sistemas operativos actuales
Linux
SUN Solaris
BSD
Mac OS X
Windows 2000
Microsoft Windows XP2
Túnel en cualquier subred IP o adaptador Ethernet virtual por un solo puerto UDP o TCP.
Fácil instalación y configuración.
OpenVPN está diseñado para la portabilidad.
El OpenSSL 3la túnel seguro de OpenVPN.

Clientes VPN sin ningún problema detrás de dispositivos NAT.
Soporte para direcciones IP dinámicas.
Buena documentación.
Compatible con SSL/TLS, certificados RSA, X.509 PKI, dispositivos virtuales TUN/TAP5.