OpenVPN

OpenVPN

OpenVPN es una herramienta de conectividad basada en software libre: **SSL (Secure Sockets Layer)**, VPNVirtual Private Network (red virtual privada). OpenVPN ofrece conectividad **punto-a-punto** con validación jerárquica de usuarios y host conectados remotamente.

CANÓ ACADEMY

OpenVPN

OpenVPN es una solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria **SSL/TLS** para cifrar y combina todas las características mencionadas anteriormente en las otras soluciones VPN.

Su principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. Sin embargo, en sistemas basados en **Linux(Mikrotik)** se puede implementar sin problemas mediante software.

OpenVPN

Para cifrar datos se usan Passwords o claves de cifrado.

OpenVPN tiene dos modos considerados seguros, uno basado en **claves estáticas pre-compartidas** y otro en **SSL/TLS usando certificados** y claves RSA.

Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, estamos usando el mecanismo conocido como “**clave simétrica**” y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN.

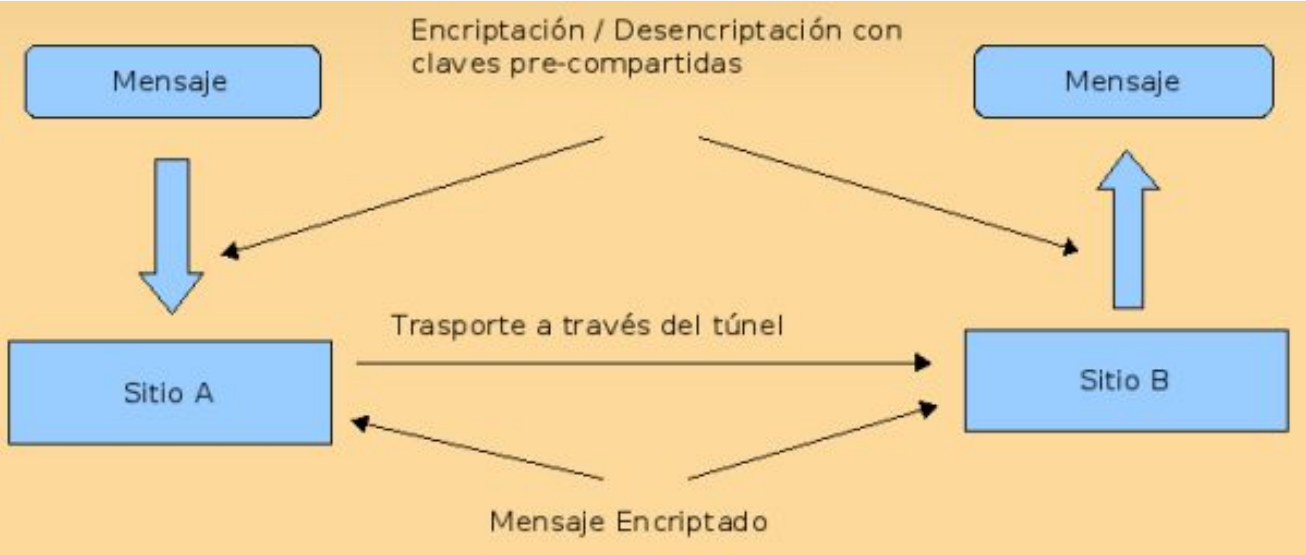
Si bien **SSL/TLS + claves RSA** es por lejos la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad.

Cifrado simétrico con llaves compartidas

Para cifrar datos se usan Passwords o claves de cifrado.

Mecanismos como IPsec **cambian** las claves cada **cierto período**, asociando a las mismas ciertos períodos de validez, llamados “**tiempo de vida**” o “**lifetime**”. Una buena combinación de tiempo de vida y longitud de la clave asegurarán que un atacante **no pueda descifrar la clave a tiempo**, haciendo que cuando finalmente la obtenga (porque lo hará), ya no le sirva por estar fuera de vigencia. IPSec utiliza su propio protocolo para intercambiar claves llamado IKE9 que ha sido desarrollado desde mediados de los noventa y aún no ha sido terminado.

OpenVPN



OPENVPN™

CANÓ ACADEMY

Cifrado asimétrico con SSL/TLS

OpenVPN

SSL/TLS usa una de las mejores tecnologías de cifrado para asegurar la identidad de los integrantes de la VPN.

Cada integrante tiene **dos claves**, una **pública y otra privada.**

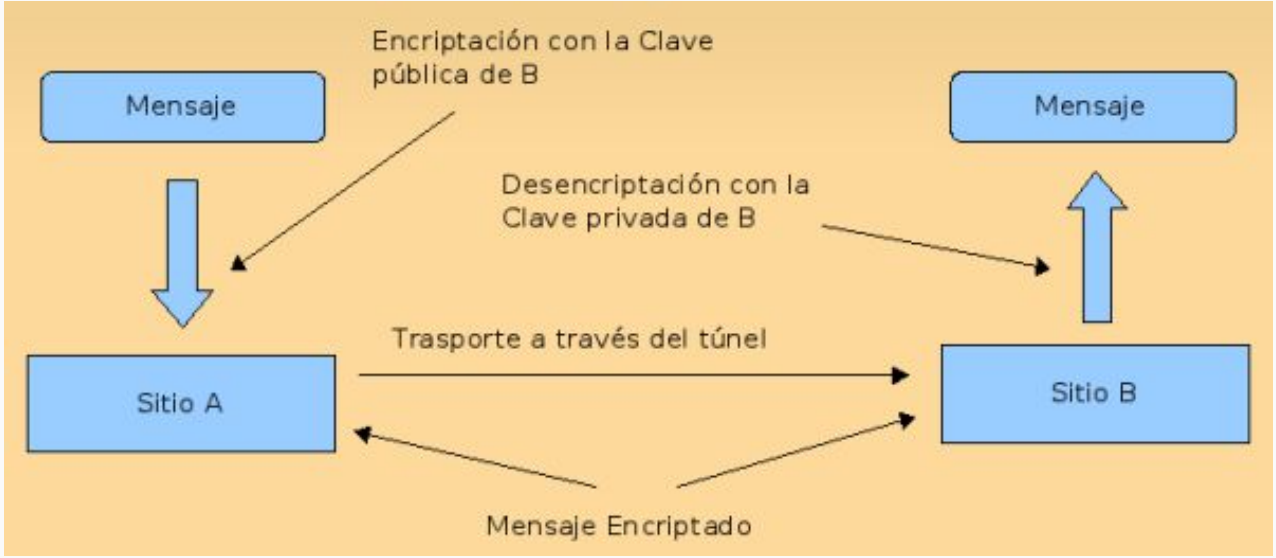
La **pública** es distribuida y usada por cualquiera **para cifrar los datos** que serán enviados a la contraparte quien conoce la clave **privada que es imprescindible para descifrar los datos**. El par de clave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la clave privada es posible leer los datos originales.

CANÓ ACADEMY

OpenVPN

Las bibliotecas **SSL/TLS** son parte del software **OpenSSL** que viene instalado en cualquier sistema moderno e implementa mecanismos de cifrado y autenticación basados en certificados. Los certificados generalmente son emitidos por entidades de reconocida confiabilidad aunque también podemos emitirlos nosotros mismos y usarlos en nuestra propia VPN. Con un certificado firmado, el dueño del mismo es capaz de demostrar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió.

OpenVPN



OPENVPN™

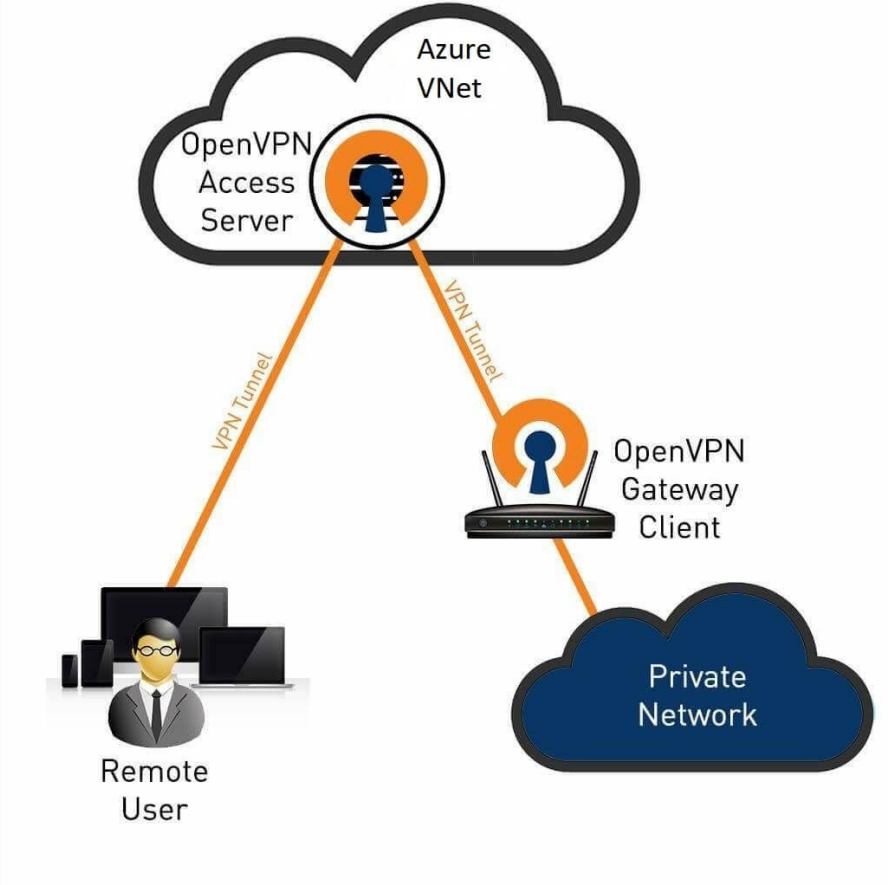
CANÓ ACADEMY

Ventajas de OpenVPN

Ventajas

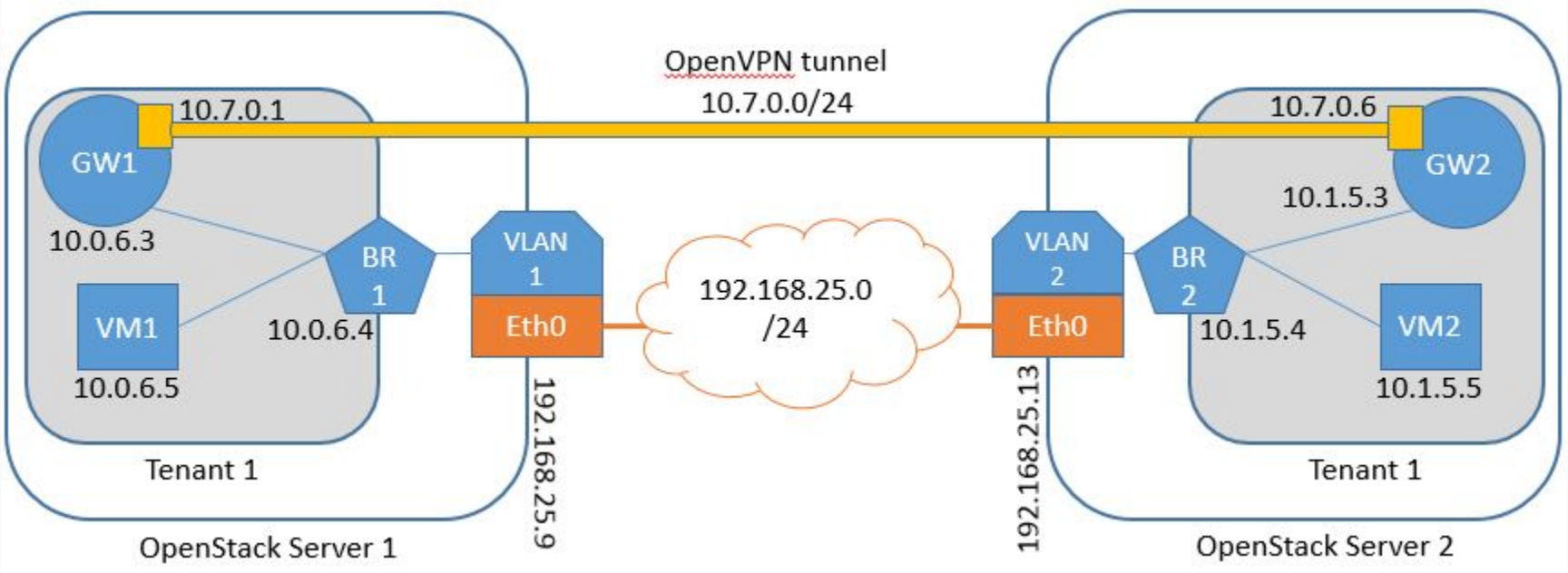
- Tecnologías de cifrado estandarizadas
- Fácil de implementar
- Utiliza solo un puerto del firewall(**1194 UDP**)
- Trabaja con servidores de nombres dinámicos como **DynDNS** o **No-IP** con reconexiones rápidas y transparentes
- **SSL/TLS** como estándar de criptografía
- No ofrece problemas con NAT(Las 2 redes pueden estar nateadas)
- Control de tráfico
- Posibilidad para los Road Warriors

Escenario



CANÓ ACADEMY

Escenario



CANÓ ACADEMY