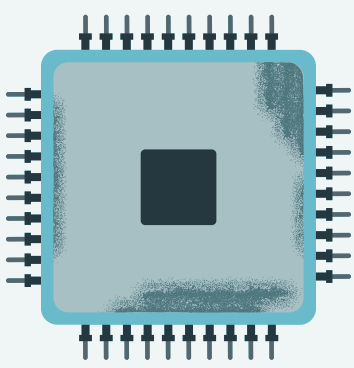
PROTOCOLO SSH

ARCHIVOS DE CONFIGURACIÓN

Los archivos de configuración de cliente y servidor son diferentes, los podemos localizar en:

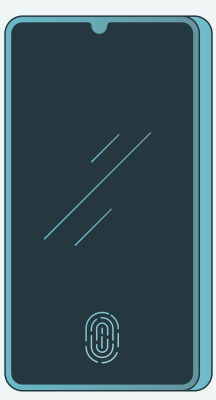
- Conf. del cliente: /etc/ssh/ssh_config
- Conf. del servidor: /etc/ssh/sshd_config

¿Qué es?



SSH es el acrónimo de Secure Shell, y es un protocolo que se utiliza en el manejo de servidores de forma remota, permitiendo a un usuario realizar toda clase de tareas sobre el mismo.

En las conexiones realizadas por medio de SSH, toda la información viaja de forma encriptada, lo cual lo convierte en uno de los medios más seguros a la hora de trabajar en un servidor.



Ejemplo de uso

Copiado de datos: con el protocolo SSH podemos copiar datos, esto se puede lograr por ejemplo mediante herramientas como rsync o scp, que tienen sintaxis sencillas y que usan una conexión vía SSH para copiar datos entre servidores, lo cual hace que toda esta información viaje entre los servidores seguros.

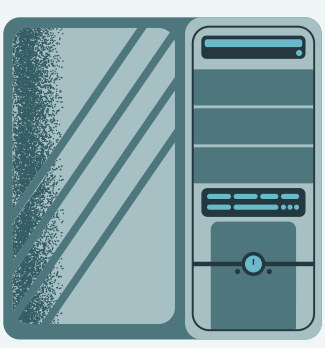
Funcionamiento

La conexión SSH usa tres ítems:
1. Un usuario
2. Un puerto (Por defecto, el 22)
3. Un servidor Con solo esos tres elementos podemos establecer una conexión segura.

Tipos de Encriptación SSH

Encriptación simétrica: es quizá la más común, y se basa en el uso de una secret key, también llamada clave secreta en español. Esta clave se usa tanto en el cifrado como en el descifrado de la conexión. Por supuesto si alguien lograra interceptar la conexión y de alguna forma obtuvo la clave secreta (prácticamente imposible pues no es algo preestablecido, es decir que es única para cada conexión) entonces podrá ver claramente la información que se está transfiriendo entre los servidores.

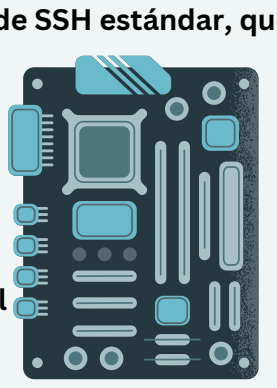
Encriptación asimétrica: en este tipo de conexión utilizamos un total de dos claves, es decir una más que en la simétrica. Se trata de una clave pública y de una clave privada. Cada clave pública está ligada a su propia clave privada, y la información encriptada solo se puede desencriptar conociendo la clave privada, así que incluso si tenemos la clave pública no vamos a poder ver los datos, para eso sí o sí se necesita la privada, la cual por supuesto no es compartida con terceros y no puede ser calculada a partir de la pública.



¿Cómo se usa?

La sintaxis básica de conexión por medio de SSH es la siguiente: ssh -p PUERTO USUARIO@SERVIDOR Como ya se ha dicho anteriormente, solo tres datos se requieren, y como podemos ver basándonos en el ejemplo se trata del puerto, del usuario y de la IP o hostname del servidor en cuestión. En algunos casos incluso no es necesario especificar un puerto si el servidor al cual vamos a conectar está usando el puerto de SSH estándar, que es el 22.

Instalación



Para la instalación ejecutamos la siguiente instrucción, con privilegios de root: apt install ssh

Una vez instalado podemos reiniciar el servicio, pararlo,etc... con la orden systemctl. Por ejemplo, para reinciar el servicio sería: systemctl restart ssh

Consta de dos componentes básicos:

- El cliente SSH que nos permite conectar con un servidor remoto.
- El demonio del servidor SSH (más conocido como sshd) que está configurado para aceptar conexiones SSH desde sistemas remotos.