

Unidad 3. SERVICIO DE TRANSFERENCIA DE DATOS

Servicio de acceso y control remoto. Sistema de transferencia de datos segura (SFTP)

Unidad 3. SERVICIO DE TRANSFERENCIA DE DATOS	1
Servicio de acceso y control remoto. Sistema de transferencia de datos segura (SFTP).....	1
1. ¿Qué es el servicio de acceso y control remoto?	1
2. Conexión remota segura- SSH (Secure Shell)	1
Ventajas de utilizar SSH.....	2
¿Cómo funciona SSH?	3
3. OPENSSSH.....	4

1. ¿Qué es el servicio de acceso y control remoto?

Los servicios de acceso y control remoto permiten, mediante la utilización determinadas aplicaciones de software, establecer conexiones con equipos a distancias y administrarlos de manera centralizada sin necesidad de acceder a ellos.

Cualquier equipo puede configurarse como un **servidor SSH**, instalando una pequeña aplicación y configurándola adecuadamente.

Para acceder a este equipo debemos instalar un **cliente SSH** en el equipo desde el que pretendemos comunicarnos (y tener conectividad con el servidor SSH).

2. Conexión remota segura- SSH (Secure Shell)

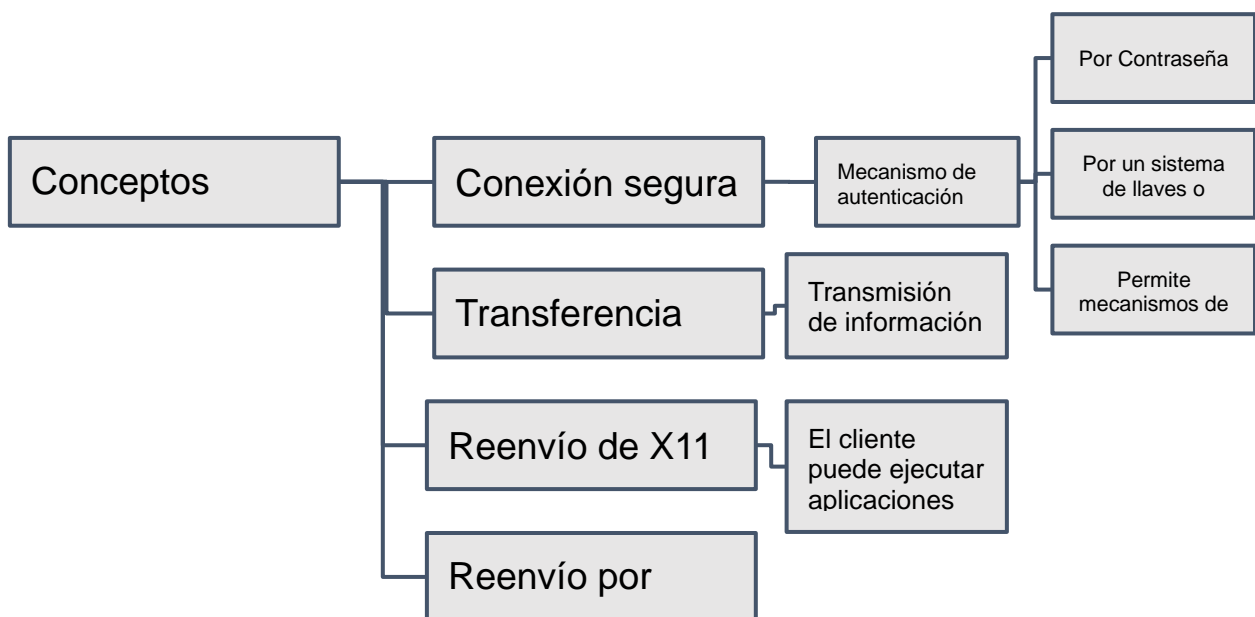
Secure Shell (Interprete de ordenes seguro, **SSH**) es una herramienta que nos permite realizar conexiones seguras entre equipos mediante una red insegura. Su objetivo es establecer conexiones remotas que permite la transmisión segura de cualquier tipo de dato como archivos, contraseñas, ejecución de órdenes de administración, sesiones login, sesiones gráficas, etc.

Cualquier equipo puede configurarse como un **servidor SSH**, instalando una pequeña aplicación y configurándola adecuadamente.

Para acceder a este equipo debemos instalar un **cliente SSH** en el equipo desde el que pretendemos comunicarnos (y tener conectividad con el servidor SSH).

Las principales características del servicio SSH son las siguientes:

- Utiliza el puerto 22 (TCP y UDP), el protocolo SSH y sigue el modelo cliente/servidor.
- Permite la autenticación de usuarios mediante contraseña o un sistema de claves.
- Permite su integración con otros sistemas de autenticación como Kerberos, PGP o PAM.
- Está implementado para la mayoría de los sistemas operativos y plataformas.

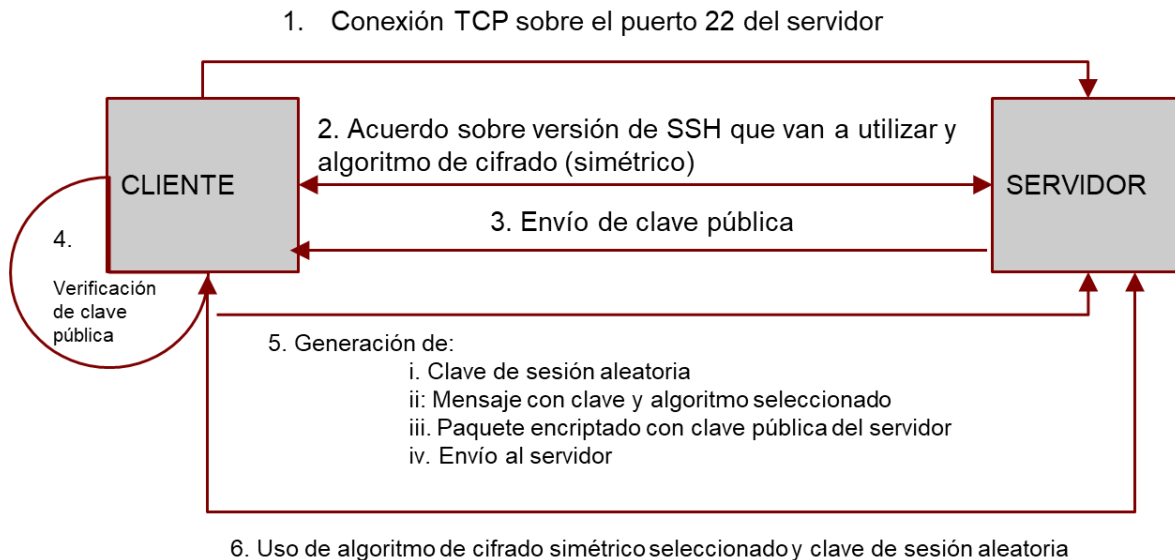


Ventajas de utilizar SSH

- Después de la primera conexión, el cliente puede saber que se conectará al mismo servidor en futuras sesiones. (Por cliente, se entiende la máquina, el equipo donde se lanza la orden SSH).
- El cliente transmite al servidor la información necesaria para su autenticación (usuario y contraseña) en formato cifrado.
- Todos los datos que se envían y se reciben durante la conexión se transfieren cifrados.
- El cliente puede ejecutar aplicaciones gráficas desde el shell (intérprete de órdenes) de forma segura.

¿Cómo funciona SSH?

La máquina cliente abre una conexión TCP sobre el puerto 22 del servidor.



1. La máquina cliente y servidor se ponen de acuerdo en la versión SSH que van a utilizar. En este momento se determina el algoritmo de cifrado (simétrico) a utilizar para la transferencia de datos.
2. El servidor tiene dos claves (pública y privada). El servidor envía su clave pública al cliente.
3. El cliente recibe la clave pública y la compara con la que tiene almacenada para verificar si es auténtica. La primera vez (como no dispone de la clave pública), SSH pide que el usuario la confirme. Se trata de su punto más débil. De hecho, se trata de un tipo de ataque bastante común conocido como “man in the middle”. En las ocasiones siguientes, cuando el cliente reciba la clave pública del servidor, la comparará con la que tiene almacenada. Se pueden prevenir ataques man in the middle contra SSH en una intranet fácilmente. Basta con publicar un listado con las claves de los servidores de la intranet, para que los usuarios puedan verificarlas antes de aceptarlas.
4. El cliente genera una clave de sesión aleatoria y crea un mensaje que contiene la clave aleatoria generada y el algoritmo seleccionado, todo ello encriptado haciendo uso de la clave pública del servidor. El cliente envía este paquete cifrado al servidor.
5. Para el resto de sesión remota utiliza el algoritmo de cifrado simétrico seleccionado y clave de sesión aleatoria.
6. Llegados a este punto se autentica el usuario y aquí pueden usarse varios mecanismos.

7. Por último, se inicia la sesión de usuario.

3. OPENSSSH

La suite OpenSSH incluye:

ssh, reemplaza a rlogin y telnet para permitir shell el acceso remoto a otra máquina. `ssh tero@ejemplo.com`

scp, reemplaza a rcp `scp tero@ejemplo.com:~/archivo .`

sftp, reemplaza a ftp para copiar archivos entre dos computadoras `sftp tero@ejemplo.com`

sshd, el servidor demonio SSH `sshd`

ssh-keygen, una herramienta para inspeccionar y generar claves RSA y DSA que son usadas para la autenticación del cliente o usuario.

ssh-agent y **ssh-add**, herramientas para autenticarse de manera más fácil, manteniendo las claves listas para no tener que volver a introducir la frase de acceso cada vez que utilice la clave.

ssh-keyscan, que escanea una lista de clientes y recolecta sus claves públicas.

El servidor OpenSSH puede autenticar a los usuarios mediante todos los métodos estándar del protocolo `ssh`

Conexión remota SSH sobre equipos Linux

Instalación del servicio `ssh`.

Configuración del servicio `ssh`

Configuración del cliente **Putty**








Configuración del cliente **Notepad++**

Utilizado para documentar ficheros de configuración.

Utilizado para modificar ficheros de configuración desde un entorno gráfico (para ello la cuenta de conexión debe tener permisos de escritura sobre el fichero... lo que nos lleva a tener que habilitar el password del root o a modificar los permisos del fichero de configuración para la cuenta que estamos utilizando).

Conexión remota desde Windows

Configuración del servidor `ssh` sobre Windows.

e equipo > Windows (C:) > Windows > System32 > OpenSSH				▼	↺	🔍
Nombre	Fecha de modificación	Tipo	Tamaño			
 scp.exe	19/03/2019 13:00	Aplicación	315 KB			
 sftp.exe	19/03/2019 13:00	Aplicación	381 KB			
 ssh.exe	19/03/2019 13:00	Aplicación	862 KB			
 ssh-add.exe	19/03/2019 13:00	Aplicación	480 KB			
 ssh-agent.exe	19/03/2019 13:00	Aplicación	376 KB			
 ssh-keygen.exe	19/03/2019 13:00	Aplicación	623 KB			
 ssh-keyscan.exe	19/03/2019 13:00	Aplicación	518 KB			

Configuración del cliente ssh: Putty, NotePad++, Netbeans, Eclipse, PHPStorm, Visual Studio code, ...

Gestión de certificados en SSH

Generar nuestro propio certificado

Utilizar nuestro propio certificado en la conexión ssh.