OpenSSH

OpenSSH est un outil pour la connexion à distance avec le protocole SSH. Il crypte tout le trafic pour éliminer l'eavesdropping, le détournement de connexion et d'autres attaques. OpenSSH fournit une vaste suite de fonctionnalités de tunneling sécurisé, plusieurs méthodes d'authentification et des options de configuration. La suite OpenSSH inclut les outils suivants :

-*ssh*, un remplaçant pour les clients rlogin et telnet :

-ssh utilisateur@exemple.com

-*scp*, un remplaçant pour le client rcp :
-scp utilisateur@exemple.com:~/utilisateur .

-*sftp*, un remplaçant pour le client ftp :
-sftp utilisateur@exemple.com

-*sshd*, le daemon SSH :

*sshd :

-*sftp-server*, le daemon remplaçant le serveur FTP. *sftp-server* est un sous-système lancé par *sshd* quand celui-ci reçoit une demande de connexion d'un client *sftp*.

*sftp-server :

-*ssh-keygen* **(en)**, programme de génération, gestion et conversion des clés RSA, DSA et DSA basées sur les courbes elliptiques. Par défaut, la clé privée générée par *ssh-keygen* est un fichier texte sans extension, la clé publique équivalente est un fichier texte d'extension *.pub*. Ces paires de clés servent à l'authentification des hôtes (attribut *HostKey* du serveur *sshd*) et à l'authentification des utilisateurs (attribut *IdentityFile* du client *ssh*).

-*ssh-agent*, agent d'authentification.

-*ssh-add*, agent de gestion des clés privées de l'utilisateur. *ssh-agent* et *ssh-add* font office de trousseau de clés.

-*ssh-keyscan*, utilitaire de récupération et vérification des clés publiques d'hôtes distants.

-*ssh-keysign*, Agent d'authentification servant si l'option *HostbasedAuthentication* est activée sur le serveur (option désactivée par défaut).

-*ssh-copy-id*, utilitaire servant à déposer sa clé publique sur un serveur distant.