**A bit about SSH**

How does SSH work?

Works on the principle of Public/private key encryption.

1. You create a pair of public/private keys.

2. On the remote server that you want to connect to, you add the public key you created.

3. You also set a password for the private key that's saved on your computer. Setting this password is optional but highly recommended.

4. Now, later when you try to establish a connection between a remote server and the local machine using SSH, the remote server sends the saved public key to the local system.

Then, the RSA algorithm is run on the public key received and the private key saved. This is done on the local machine. And if the numbers computed from the RSA algorithm on both the public and private keys match, only then a SSH tunnel or a secure connection is established.

5. On Linux very simple to create a new SSH public/private key pair.

Linux command: ssh-keygen

6. Once that's done you set up a config file in your .ssh folder. In Linux the config file and the keys are stored in the .ssh folder under your home directory--/home/user/.ssh Do ls -la to see the .ssh folder since it's a hidden folder.

7. The config file has all the parameters which will be needed to establish a SSH connection.

*— MAR 29, 2015 —*