**Configuring the github**

SET variables:

$git config --global [user.name](http://user.name/) "YOUR NAME"  
$git config --global user.email "YOUR EMAIL ADDRESS"

Increase the Git buffer size to the largest individual file size of your repo:  
$git config --global http.postBuffer 157286400

# Attempt to SSH in to github  
Hi username! You've successfully authenticated, but GitHub does not provide  
shell access.

create file ~/.ssh/config (ssh config file located in your user directory.

Paste the following code in it ~/.ssh/config:

    Host [github.com](http://github.com/)  
    User git  
    Hostname [ssh.github.com](http://ssh.github.com/)  
    PreferredAuthentications publickey  
    IdentityFile ~/.ssh/id\_rsa  
    ForwardAgent yes  
    Port 22

Save the file.

if u follow the above procedure use :

$ssh -T [github.com](http://github.com/)

or if not then:

$ssh -T [git@github.com](mailto:git@github.com)

Warning: Permanently added the RSA host key for IP address '192.30.252.128' to the list of known hosts.  
Enter passphrase for key '/root/.ssh/id\_rsa':  
Hi telmerobertt! You've successfully authenticated, but GitHub does not provide shell access.

=========================================================================

Generate SSH key :

<https://help.github.com/articles/generating-ssh-keys/>

[1.ls](http://1.ls/) -al ~/.ssh  
# Lists the files in your .ssh directory, if they exist

2.ssh-keygen -t rsa -b 4096 -C "[your\_email@example.com](mailto:your_email@example.com)"  
# Creates a new ssh key, using the provided email as a label  
# Generating public/private rsa key pair.

3.Enter file in which to save the key (/Users/you/.ssh/id\_rsa): [Press enter]

4.Enter passphrase (empty for no passphrase): [Type a passphrase] (Give the passwards if u want else enter)  
# Enter same passphrase again: [Type passphrase again]

After you enter a passphrase, you'll be given the fingerprint, or id, of your SSH key.   
It will look something like this:

Your identification has been saved in /Users/you/.ssh/id\_rsa.  
# Your public key has been saved in /Users/you/.ssh/id\_rsa.pub.  
# The key fingerprint is:  
# 01:0f:f4:3b:ca:85:d6:17:a1:7d:f0:68:9d:f0:a2:db [your\_email@example.com](mailto:your_email@example.com)

go to the .ssh folder(/Users/you/.ssh/id\_rsa.pub) and open that file and copy the content of id\_rsa.pub (where u have generated your private key)

Go to Git >settings>ssh key > add there..

===========================================================================

If u are getting these error:  
Fatal error or connection refuse or connection timeout on port 22

ssh: connect to host [github.com](http://github.com/) port 22: Connection timed out  
while

>git push  
u ll get this error:  
fatal: The remote end hung up unexpectedly  
if u ll get 403:Forrbiden URL : change ur remote URL as SSH :

Set remote url as ssh: like this:

$git remote set-url origin git@github.com:telmerobert/DevOps728.git

$ git remote -v  
#Verify new remote URL  
# origin  git@github.com::telmerobert/DevOps728.git (fetch)  
# origin  git@github.com:telmerobert/DevOps728.git (push)

SSH is probably blocked on port 22

1.Add ports to the ACL   
2.add ip of github  192.30.252.128 to acl egress and ingress.  
3.turn off iptable:  
 chkconfig iptables off  
 service iptables status  
 service iptables stop  
 service iptables status

==========7=8=====================================================================

Commands:

NOW clone ur repo:

    git clone [git@github.com/telmerobert/DevOps728.git](mailto:git@github.com/telmerobert/DevOps728.git)  
    
    cd DevOps728/  
   
    touch ruby.txt  
    ls  
    git status  
    git add .  
    git commit -m " i am adding ruby file"  
    
    git status  
    
    git push -m "sending this file to remote repository" origin master

    git push origin master  
    
    ssh -T [git@github.com](mailto:git@github.com)  
    
    telnet [github.com](http://github.com/) 22  
    
    telnet [github.com](http://github.com/) 22