A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevent attackers from accessing your servers in malicious ways.
UFW (Uncomplicated Firewall) act as an interface to IP tables and is designed to simplify the process of configuring a firewall.
Sudo apt-get install ufw
sudo ufw status
sudo ufw status verbose (give the status of rules that are currently active)
sudo ufw status numbered (give the number and rules that are set)
sudo ufw enable
sudo ufw disable
sudo ufw reset (donot use it if you want to delete particular rule)
ufw by default deny all incoming connection and allow all outgoing connections
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow ssh
sudo ufw allow 22
sudo ufw deny ssh
sudo ufw allow http
sudo ufw allow 80
sudo ufw allow https
sudo ufw allow 443
sudo ufw allow proto tcp from any to any port 80,443 (to enable http and https together)
sudo ufw deny proto tcp from any to any port 80,443 (to disable http and https together)
sudo ufw allow ftp
sudo ufw allow 21/tcp
you can deny accesses to your mysql databases
ufw allow from 192.168.1.1
sudo ufw allow from 192.168.1.103 to any port 22 (if you want ip address 192.168.1.103 to access only ssh)
sudo ufw allow from 192.168.1.103/24 to any port 22 (if you want subnet addresses 192.168.1.103 to access only ssh)
sudo ufw enable
sudo ufw status
sudo ufw status verbose
sudo ufw status numbered
sudo ufw delete 1
sudo ufw reset