```
hepzi@ubuntu:~$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Fetched 324 kB in 2s (130 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
243 packages can be upgraded. Run 'apt list --upgradable' to see them.



hepzi@ubuntu:~$ sudo apt install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 243 not upgraded.
Need to get 473 kB of archives.
After this operation, 2,486 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 fail2ban all 0.11.2-
6 [394 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyinotify all
0.9.6-1.3 [24.8 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 whois amd64 5.5.13 [53.4
kB]
Fetched 473 kB in 2s (289 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 201361 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-6_all.deb ...
Unpacking fail2ban (0.11.2-6) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-1.3_all.deb ...
Unpacking python3-pyinotify (0.9.6-1.3) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.13_amd64.deb ...
Unpacking whois (5.5.13) ...
Setting up whois (5.5.13) ...
Setting up fail2ban (0.11.2-6) ...
Setting up python3-pyinotify (0.9.6-1.3) ...
Processing triggers for man-db (2.10.2-1) ...



hepzi@ubuntu:~$ sudo systemctl status fail2ban
○ fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; disabled; vendor pr>
     Active: inactive (dead)
       Docs: man:fail2ban(1)
```

```
lines 1-4/4 (END)


hepzi@ubuntu:~$ sudo systemctl restart fail2ban
hepzi@ubuntu:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
hepzi@ubuntu:~$ sudo systemctl status fail2ban
 fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pre>
     Active: active (running) since Wed 2023-01-11 15:29:17 IST; 19s ago
       Docs: man:fail2ban(1)
   Main PID: 4090 (fail2ban-server)
      Tasks: 5 (limit: 2287)
     Memory: 13.1M
        CPU: 710ms
     CGroup: /system.slice/fail2ban.service
             └─4090 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 11 15:29:17 ubuntu systemd[1]: Started Fail2Ban Service.
Jan 11 15:29:18 ubuntu fail2ban-server[4090]: Server ready

hepzi@ubuntu:~$ sudo nano /etc/fail2ban/jail.local
hepzi@ubuntu:~$ cat /etc/fail2ban/jail.local
[Default]

ignoreip = 127.0.0.1/8 ::1 123.123.123.123 192.168.1.0/24
bantime = 10m
findtime = 10m
maxretry = 3



hepzi@ubuntu:~$ sudo fail2ban-client set sshd banip 127.0.0.1/8
1
hepzi@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:  /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   127.0.0.0/8

   hepzi@ubuntu:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:     sshd


hepzi@ubuntu:~$ sudo nano jail.local
hepzi@ubuntu:~$ cat jail.local
[sshd]

enabled = true
port = ssh
```

```
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
findtime = 1d
bantime = 1w
ignoreip = 127.0.0.1/8

hepzi@ubuntu:~$ sudo fail2ban-client set sshd unbanip 127.0.0.1/8
0
hepzi@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:  /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:



   UFW Firewall:

   hepzi@ubuntu:~$ sudo ufw status
Status: inactive
hepzi@ubuntu:~$ sudo ufw allow outgoing
ERROR: Could not find a profile matching 'outgoing'
hepzi@ubuntu:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
hepzi@ubuntu:~$ sudo ufw allow http
[sudo] password for hepzi:
Rules updated
Rules updated (v6)
hepzi@ubuntu:~$ sudo ufw allow 127.0.0.1/8
ERROR: Bad port
hepzi@ubuntu:~$ sudo ufw allow from 127.0.0.1/8 to any port 22
WARN: Rule changed after normalization
Rules updated

hepzi@ubuntu:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
hepzi@ubuntu:~$ sudo systemctl start ufw
hepzi@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
hepzi@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       Anywhere
22                         ALLOW       127.0.0.0/8
80/tcp (v6)                ALLOW       Anywhere (v6)

hepzi@ubuntu:~$ sudo ufw allow 2222/tcp
Rule added
Rule added (v6)
```

```
hepzi@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     ALLOW IN    Anywhere
[ 2] 22                         ALLOW IN    127.0.0.0/8
[ 3] 2222/tcp                   ALLOW IN    Anywhere
[ 4] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] 2222/tcp (v6)              ALLOW IN    Anywhere (v6)

hepzi@ubuntu:~$ sudo ufw delete 5
Deleting:
 allow 2222/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
hepzi@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     ALLOW IN    Anywhere
[ 2] 22                         ALLOW IN    127.0.0.0/8
[ 3] 2222/tcp                   ALLOW IN    Anywhere
[ 4] 80/tcp (v6)                ALLOW IN    Anywhere (v6)

hepzi@ubuntu:~$ sudo ufw deny from 127.0.0.1/8 to any port 22
WARN: Rule changed after normalization
Rule updated
hepzi@ubuntu:~$ sudo ufw delete 4
Deleting:
 allow 80/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)

hepzi@ubuntu:~$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20230111_223014'
Backing up 'before.rules' to '/etc/ufw/before.rules.20230111_223014'
Backing up 'after.rules' to '/etc/ufw/after.rules.20230111_223014'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20230111_223014'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20230111_223014'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20230111_223014'
```