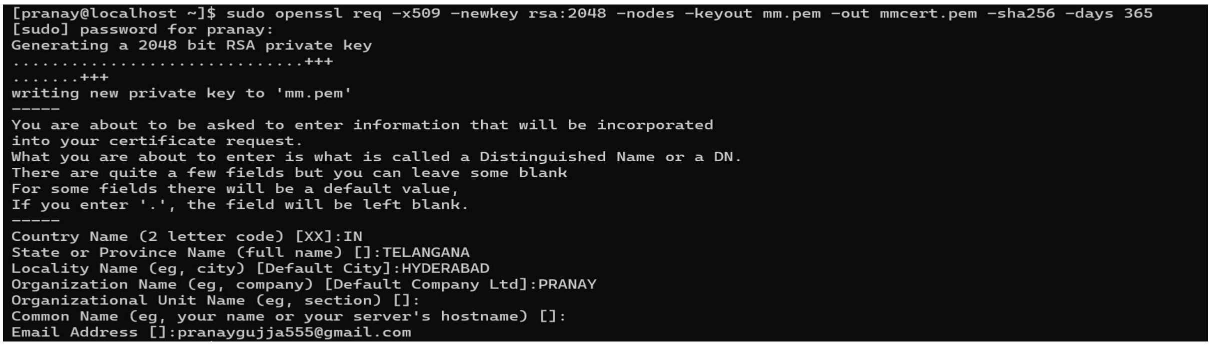
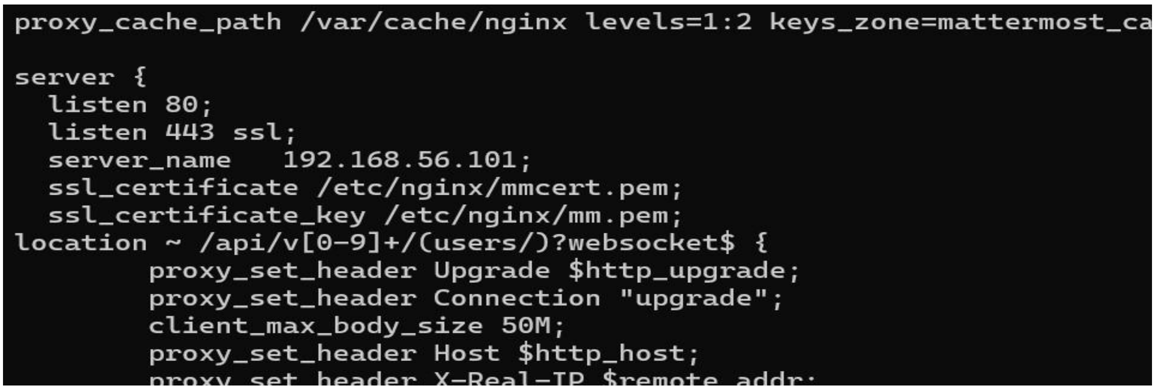
Openssl req -x509 -newkey rsa:2048 -nodes keyout mm.pem -out mmcert.pem -sha256 -days 365



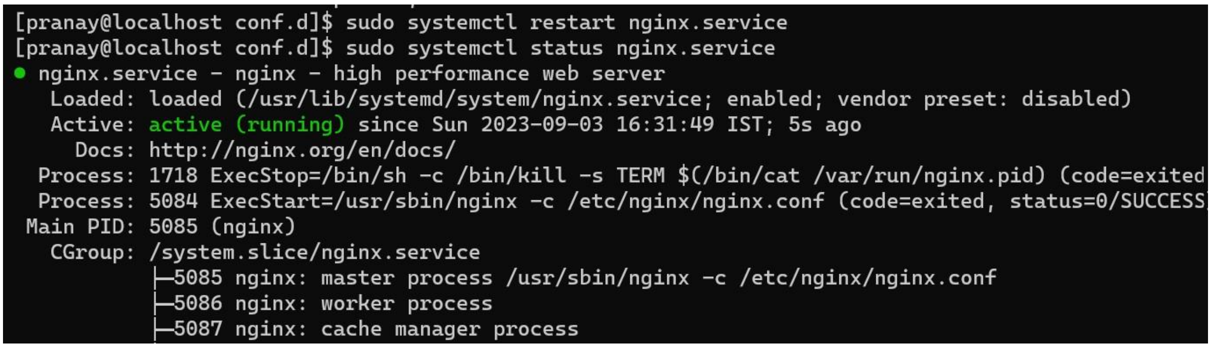
```
[pranay@localhost ~]$ sudo openssl req -x509 -newkey rsa:2048 -nodes -keyout mm.pem -out mmcert.pem -sha256 -days 365
[sudo] password for pranay:
Generating a 2048 bit RSA private key
..............................+++
.......+++
writing new private key to 'mm.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:TELANGANA
Locality Name (eg, city) [Default City]:HYDERABAD
Organization Name (eg, company) [Default Company Ltd]:PRANAY
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:pranaygujja555@gmail.com
```

Nginx configuration



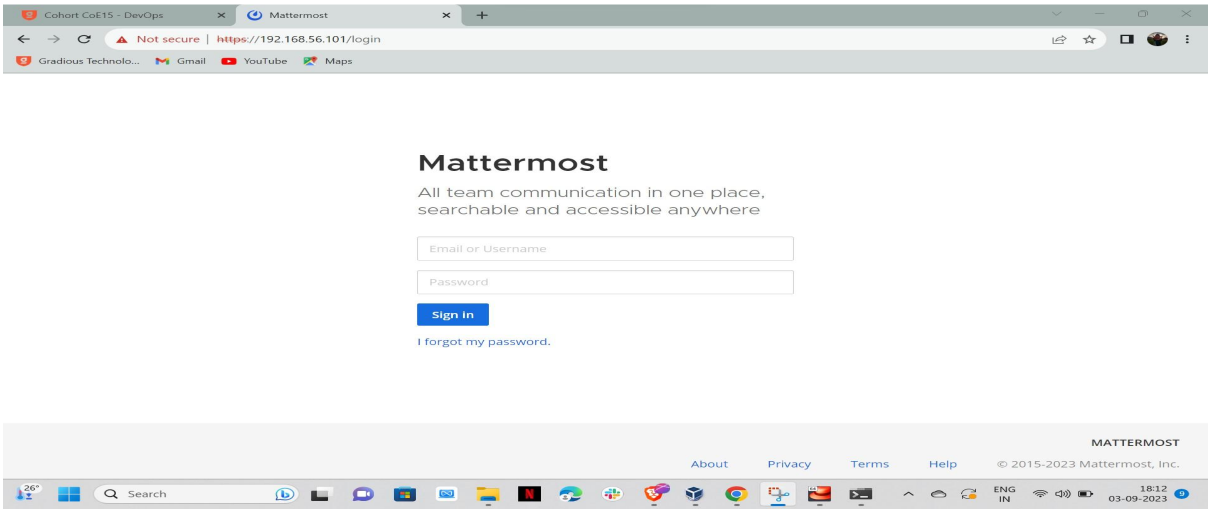
```
proxy_cache_path /var/cache/nginx levels=1:2 keys_zone=mattermost_ca

server {
  listen 80;
  listen 443 ssl;
  server_name   192.168.56.101;
  ssl_certificate /etc/nginx/mmcert.pem;
  ssl_certificate_key /etc/nginx/mm.pem;
location ~ /api/v[0-9]+/(users/)?websocket$ {
          proxy_set_header Upgrade $http_upgrade;
          proxy_set_header Connection "upgrade";
          client_max_body_size 50M;
          proxy_set_header Host $http_host;
          proxy_set_header X-Real-IP $remote_addr;
```

Restart nginx



```
[pranay@localhost conf.d]$ sudo systemctl restart nginx.service
[pranay@localhost conf.d]$ sudo systemctl status nginx.service
● nginx.service - nginx - high performance web server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2023-09-03 16:31:49 IST; 5s ago
     Docs: http://nginx.org/en/docs/
  Process: 1718 ExecStop=/bin/sh -c /bin/kill -s TERM $(/bin/cat /var/run/nginx.pid) (code=exited
  Process: 5084 ExecStart=/usr/sbin/nginx -c /etc/nginx/nginx.conf (code=exited, status=0/SUCCESS
 Main PID: 5085 (nginx)
   CGroup: /system.slice/nginx.service
           ├─5085 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
           ├─5086 nginx: worker process
           ├─5087 nginx: cache manager process
```

Site check in browser



Mattermost

All team communication in one place, searchable and accessible anywhere

Email or Username

Password

Sign in

I forgot my password.

MATTERMOST

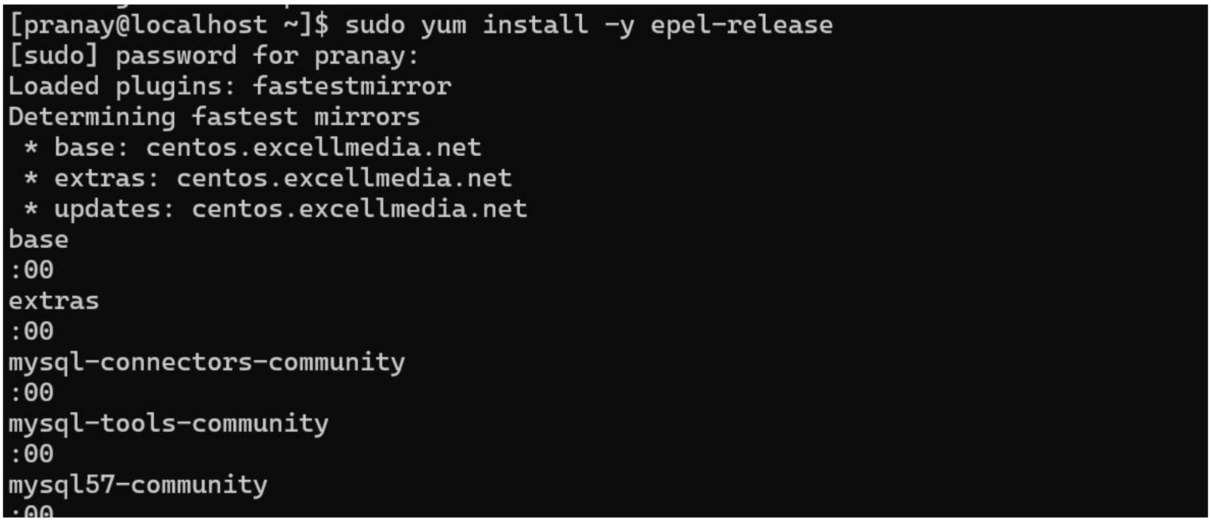
About Privacy Terms Help © 2015-2023 Mattermost, Inc.

Assignment -2 - Configure Firewall rules to prevent remote access

Instructions

Install the firewall into your terminal, run these commands in your terminal sudo yum install -y epel-release

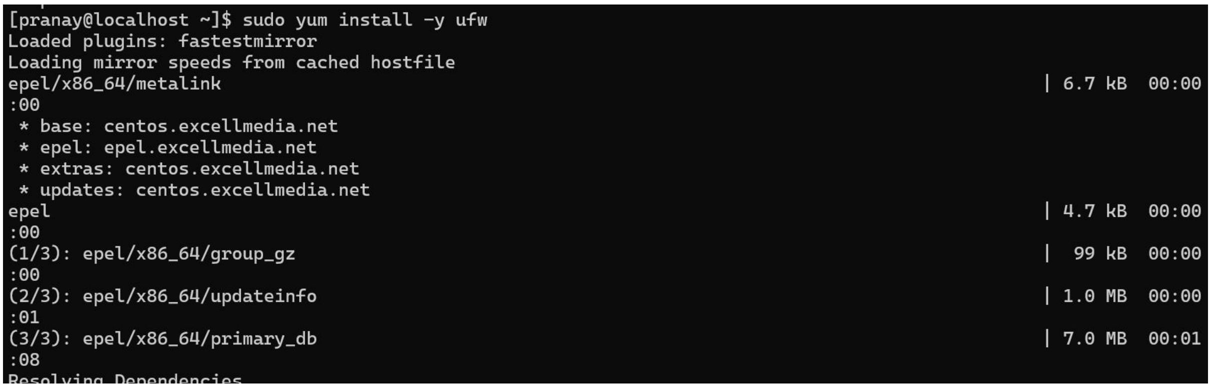
A:



```
[pranay@localhost ~]$ sudo yum install -y epel-release
[sudo] password for pranay:
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: centos.excellmedia.net
 * extras: centos.excellmedia.net
 * updates: centos.excellmedia.net
base
:00
extras
:00
mysql-connectors-community
:00
mysql-tools-community
:00
mysql57-community
:00
```

1. sudo yum install -y ufw

A:



```
[pranay@localhost ~]$ sudo yum install -y ufw
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink                                                                  | 6.7 kB  00:00
:00
 * base: centos.excellmedia.net
 * epel: epel.excellmedia.net
 * extras: centos.excellmedia.net
 * updates: centos.excellmedia.net
epel                                                                                  | 4.7 kB  00:00
:00
(1/3): epel/x86_64/group_gz                                                           |  99 kB  00:00
:00
(2/3): epel/x86_64/updateinfo                                                         | 1.0 MB  00:00
:01
(3/3): epel/x86_64/primary_db                                                         | 7.0 MB  00:01
:08
Resolving Dependencies
```

2. Check the status of ufw using "sudo ufw status" (Inactive)

3. Enable the ufw using the command "sudo ufw enable"

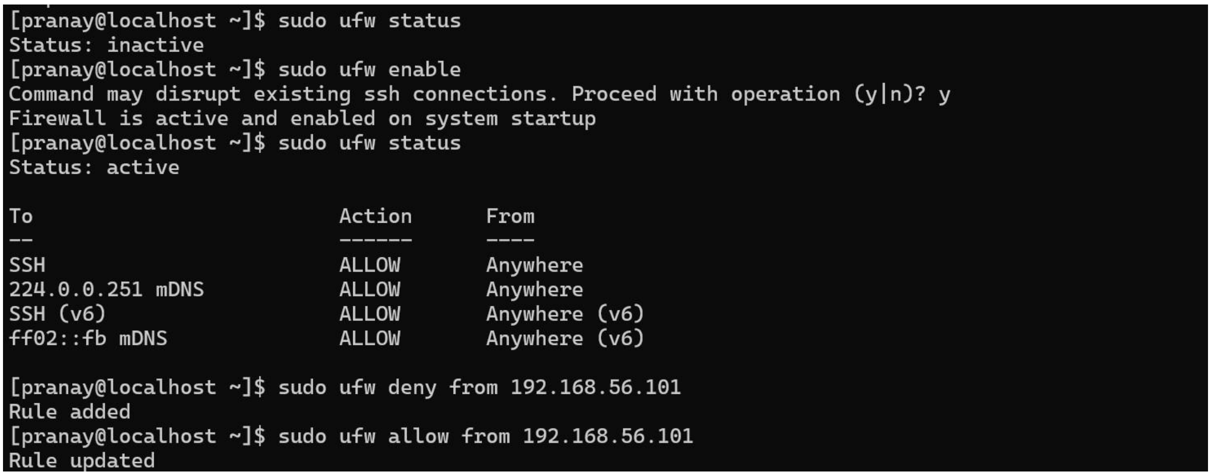
4. Check the status of ufw using "sudo ufw status" (Active)

Block an ip address using the command sudo ufw deny from "enter the ip address" (Rule added)

5. (Try to access your server (nginx) from the machine where the Ip address is blocked the site can't be reached error should display)

Allow an ip address to access server using sudo ufw allow from "enter the ip address" (Rule added)

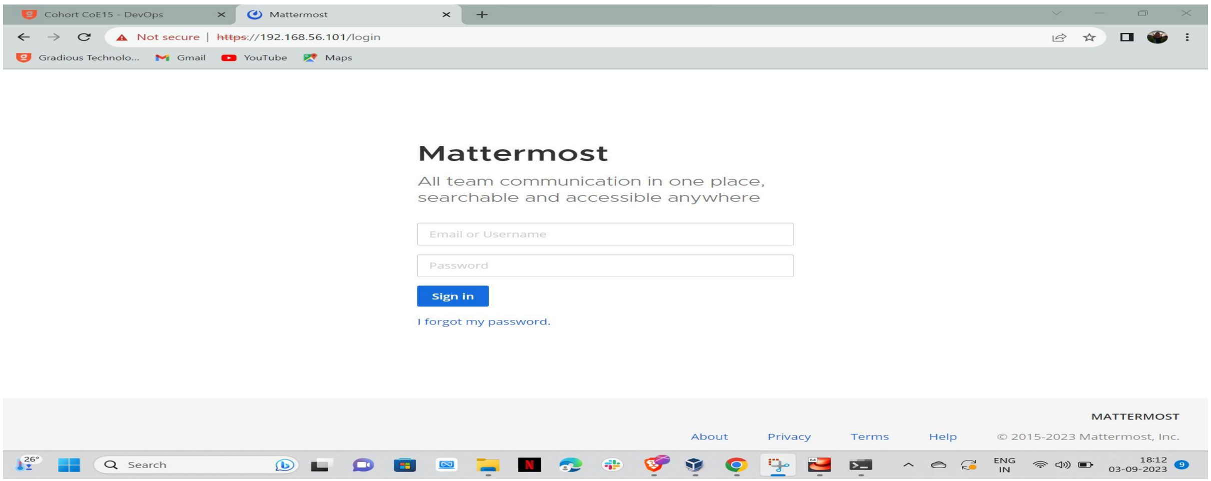
A: 2 to 5



```
[pranay@localhost ~]$ sudo ufw status
Status: inactive
[pranay@localhost ~]$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
[pranay@localhost ~]$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
SSH                        ALLOW       Anywhere
224.0.0.251 mDNS           ALLOW       Anywhere
SSH (v6)                   ALLOW       Anywhere (v6)
ff02::fb mDNS              ALLOW       Anywhere (v6)

[pranay@localhost ~]$ sudo ufw deny from 192.168.56.101
Rule added
[pranay@localhost ~]$ sudo ufw allow from 192.168.56.101
Rule updated
```

6. (Now if you try to access the server it should allow)

A:

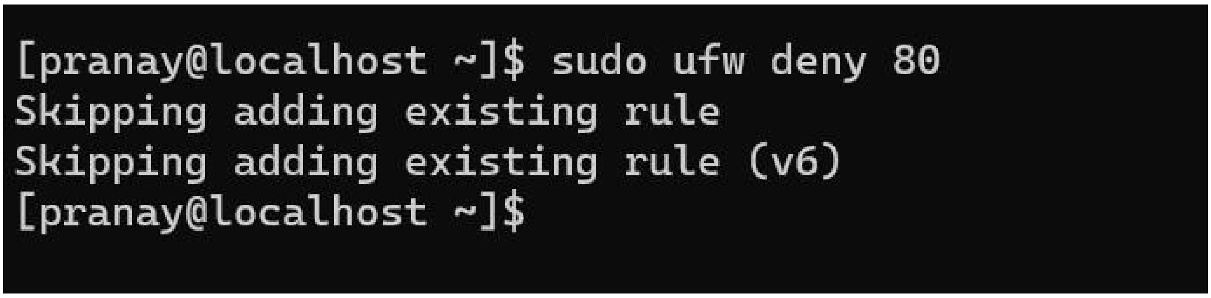


Mattermost

All team communication in one place, searchable and accessible anywhere

7. Deny a port number using command "sudo ufw deny portnumber" (rule added) (Try to access the port from outside it should be blocked)

A:



```
[pranay@localhost ~]$ sudo ufw deny 80
Skipping adding existing rule
Skipping adding existing rule (v6)
[pranay@localhost ~]$
```