

UFW and Docker

When running containers in Docker, you will come across the need for a container to gain access to a resource on the host.

If you have UFW firewall enabled, you will need to allow ingress from the docker network, running on the host.

To identify the docker network, run this:

```
sudo docker network ls
```

It will return the list of docker networks:

```
root@redtoade:/etc/postgresql/14/main# sudo docker network ls
NETWORK ID      NAME          DRIVER       SCOPE
8c5a405ea9cc   bridge       bridge       local
c09callcb4b1   host         host         local
fa674ab962ab   none         null         local
root@redtoade:/etc/postgresql/14/main#
```

Next, you need to identify the docker network where your containers are addressed.

To do this, run the following on each network name:

```
sudo docker network inspect bridge
```

The above command will give you a list of containers and their addresses and subnets.

Next, you will update the ufw firewall rules to allow incoming connection from the docker subnet, like this:

```
sudo ufw allow from 172.17.0.0/16
```

You can check the status and rules with:

```
sudo ufw status
```

This will return something like this:

```
root@redtoade:/etc/postgresql/14/main# sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443 ALLOW Anywhere
62168 ALLOW Anywhere
80 ALLOW Anywhere
Anywhere ALLOW 172.17.0.0/16
80/tcp (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)
62168 (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)

root@redtoade:/etc/postgresql/14/main#
```

Now, you should be able to access host resources from a docker container, with UFW enabled.

Revision #1

Created 6 July 2025 19:27:55 by glwhite

Updated 6 July 2025 19:29:43 by glwhite