

[Skip to main content](#)

r/docker



Search in r/docker

[Log In](#)

r/docker • 3 yr. ago

KRS_33



Blocking internet access to one container in docker-compose

Hello,

I need some help on network segregation.

I have a webservice container using a database.

The webservice is reachable on port 80.

It needs to communicate with the db but should not communicate to the internet.

I would like to block it at the docker-compose level.

docker-compose.yml

```
version: '2'
```

```
services:
```

```
  db:
```

[Read more](#) ▾

18

17



Share



TradeStation • Official • Promoted



See your trade from every angle with a fully customizable trading platform.

[Learn More](#)tradestation.com[+ Add a comment](#)Sort by: **Best** ▾

Search Comments



u/xr09 • 3y ago

[Skip to main content](#)[Log In](#)

```
version: '2'

services:
  db:
    image: mariadb
    environment:
      <...>
    volumes:
      <...>
    networks:
      - no-internet

  web:
    image: myWebService
    environment:
      <...>
    depends_on:
      - db
    links:
      - db:db
    ports:
      - "80:80"
    volumes:
      <...>
    networks:
      - web
      - no-internet

networks:
  web:
    driver: bridge
  no-internet:
    driver: bridge
    internal: true # Block internet access
```

13 [Upvote](#) [Downvote](#) [Reply](#) ...



KRS_33 OP • 3y ago

Yes, it would look like this but how to be sure the internet traffic on myWebService doesn't use the web network for this ? MyWebService needs to be reached from the internet on port 80, but it shouldn't communicate to the internet.

2 [Upvote](#) [Downvote](#) [Reply](#) ...

[+](#) 5 more replies

[Skip to main content](#)[Log In](#)

- allow **inbound** traffic to the web service
- block **outbound** traffic from the web service **except** for accessing the db
- do not modify the source web container image

Is this correct?

⊖ ↑ 4 ↓ ○ Reply ...



KRS_33 OP • 3y ago

yes exactly, if possible with proper network value in a docker-compose

↑ 2 ↓ ○ Reply ...

⊕ 1 more reply



sysadmintemp • 3y ago

Docker does not have `docker network` solution that would enable what you want to do.

From your post and replies, I understand that:

1. Web container should be able to respond to requests coming from clients
2. Web container should NOT be able to access internet

You need something like a stateful firewall for this, that would track where the initial connection request came from. Because if you simply block access to all internet on your web container, then the web container will not be able to respond to client requests as well.

You can implement this using `iptables` or similar that's on the image. But this is not possible using docker.

Reverse proxy would not work by itself. You would need a proxy + reverse proxy + blocking rules kind of solution.

Also, I assume you're trying to do this to make the container more secure. It will not make it more secure. You need another security-oriented container in front to have features such as DDoS blocking, fail2ban, etc.

⊖ ↑ 3 ↓ ○ Reply ...



KRS_33 OP • 3y ago

it's just that I may not trust the container (closed source) since it could send data to the internet. Sure a firewall would fix this. Allow 80/tcp IN only. Block all OUT

↑ 2 ↓ ○ Reply ...

⊕ 1 more reply

[Skip to main content](#)[Log In](#)

about possibility, but about skills)

⬇️ 2 ⬆️ [Reply](#) ...



KRS_33 [OP](#) • 3y ago • Edited 3y ago

yes this is something I can do, but I was wondering if it was possible to block this traffic out to the internet in docker-compose. I'm using a public image. In this case I need to overload it. Feasible but docker-compose would have been a lighter change. So probably the best answer.

⬆️ 2 ⬇️ [Reply](#) ...



mb2m • 3y ago

Another question related to OP's: How can I do basic firewalling, for example:

Container A can reach 8.8.8.8 but the rest of the world is blocked.

At the moment I'm manipulating the routes in the entrypoint while giving netadmin permissions to the container but isn't there a better option?

⬇️ 2 ⬆️ [Reply](#) ...



sysadmintemp • 3y ago

[Skip to main content](#)[Log In](#)

- A linux container + `iptables` rules to block all and pass only `8.8.8.8` DNS traffic
- A complete firewall container configured to only pass traffic to `8.8.8.8` DNS

In both cases, you need to make sure your initial container uses the router container as the default GW. You might need adjust your first container's route table to do this, or you might set a static IP for your router container.

[Here's a link from serverfault that describes how to create a NAT router using `iptables`](#) . You don't need NAT specifically, just routing, so you could tweak the answer a bit.

To set a linux machine as a router you need the following 1- Enable forwarding on the box with

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Assuming your public interface is eth1 and local interface is eth0

2- Set natting the natting rule with:

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

3- Accept traffic from eth0:

```
iptables -A INPUT -i eth0 -j ACCEPT
```

4- Allow established connections from the public interface.

```
iptables -A INPUT -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

5- Allow outgoing connections:

```
iptables -A OUTPUT -j ACCEPT
```

↑ 2 ↓ ○ Reply ...

⊕ 1 more reply

New to Reddit?

Create your account and connect with a world of communities.



Continue with Google



Continue with Email



Continue With Phone Number

[Skip to main content](#)[Log In](#) r/docker • 3 mo. ago

How can you block a Docker container from being able to access the Internet, while still allowing connections from the local network?

37 upvotes · 16 comments

 r/docker • 7 mo. ago

How to restart a service in a new container via docker compose while keeping the old container?

3 upvotes · 32 comments

 r/docker • 4 mo. ago

What are some common security mistakes people make when running Docker containers?

62 upvotes · 35 comments

 r/docker • 10 mo. ago

How to update docker containers correctly?

4 upvotes · 19 comments

 r/docker • 9 mo. ago

Using docker to host multiple websites from one IP address?

20 upvotes · 47 comments

 r/docker • 3 yr. ago

Docker-compose containers not finding each other on network

4 upvotes · 10 comments

 r/docker • 8 mo. ago

Docker is not exposing ports

3 upvotes · 8 comments

 r/docker • 2 mo. ago

Portable Docker and Container in a Binary/Executable?

3 upvotes · 7 comments

 r/docker • 5 mo. ago

Best Docker Vulnerability Scanner?

11 upvotes · 10 comments

[Skip to main content](#)[Log In](#)

58 upvotes · 163 comments

 r/docker • 6 mo. ago

Docker and nftables - is there a way? (Linux)

9 upvotes · 23 comments

 r/docker • 2 mo. ago

"com.docker.socket" was not opened because it contains malware message

8 upvotes · 8 comments

 r/docker • 9 mo. ago

Can /dev/net/tun be used by multiple docker containers?

6 upvotes · 9 comments

 r/docker • 3 mo. ago

Now I finally get why everyone's using Docker to deploy apps.

188 upvotes · 83 comments

 r/docker • 5 mo. ago

Beginner Seeking Advice: When to Use Docker and When to Avoid It?

4 upvotes · 41 comments

 r/docker • 5 mo. ago

How is docker used in production?

18 upvotes · 40 comments

 r/docker • 7 mo. ago

Docker Permissions with NFS share

6 upvotes · 11 comments

 r/docker • 1 mo. ago

Is there a way to force all docker containers to use the local DNS instead of the default 8.8.8.8?

5 upvotes · 19 comments

 r/aws • 3 yr. ago

Cannot connect to HTTP from EC2 instance

[Skip to main content](#)[Log In](#)

[iptables] `telnet 127.0.0.1 6443` fails

3 upvotes · 12 comments



r/antivirus • 3 yr. ago

Comodo Firewall

1 upvote · 3 comments



r/docker • 2 mo. ago

How to backup and restore my containers

4 upvotes · 17 comments



r/docker • 4 mo. ago

How is local development done in docker ?

23 upvotes · 21 comments



r/mikrotik • 3 yr. ago

Acces to domain inside of network

1 upvote · 10 comments



r/docker • 4 mo. ago

Docker on Android device

16 comments

TOP POSTS



Reddit

reReddit: Top posts of April 9, 2022



Reddit

reReddit: Top posts of April 2022



Reddit

reReddit: Top posts of 2022



Log In