how to block external access to docker container linux centos 7

Asked 5 years, 3 months ago Modified 1 year, 5 months ago Viewed 2k times

6

I have a mongodb docker container I only want to have access to it from inside of my server, not out side. even I blocked the port 27017/tcp with firewall-cmd but it seems that docker is still available to public. I am using linux centos 7 and docker-compose for setting up docker

docker docker-compose centos7

Share Improve this question Follow

asked Nov 19, 2019 at 9:46

Ehsan Sarshar

3,221 ● 1 ● 28 ● 46

4 Answers

Sorted by: Highest score (default)

3

I resolved the same problem adding an iptables rule that blocks 27017 port on public interface (eth0) at the top of chain DOCKER:

```
iptables -I DOCKER 1 -i eth0 -p tcp --dport 27017 -j DROP
```

Set the rule after docker startup

Another thing to do is to use non-default port for mongod, modify docker-compose.yml (remember to add --port=XXX in command directive)

For better security I suggest to put your server behind an external firewall

Share Improve this answer Follow

edited Jun 12, 2020 at 9:44

answered Jun 11, 2020 at 16:37

FRa

371 ● 4 ● 8

2

If you have your application in one container and MongoDb in other container what you need to do is to connect them together by using a network that is set to be internal.

See Documentation:

> Internal
> By default, Docker also connects a bridge network to it to provide external connectivity. If you want to create an externally isolated overlay network, you can set this option to true.

See also this question

Here's the tutorial on networking (not including internal but good for understanding)

You may also limit traffic on MongoDb by Configuring Linux iptables Firewall for MongoDB

for creating private networks use some IPs from these ranges:
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

more read on Wikipedia

You may connect a container to more than one network so typically an application container is connected to the outside world network (external) and internal network. The application communicates with database on internal network and returns some data to the client via external network. Database is connected only to the internal network so it is not seen from the outside (internet)

Share Improve this answer Follow

answered Nov 19, 2019 at 10:14
Jimmix
6,556 ● 7 ● 52 ● 91

Centos7 not use iptables it use firewall-cmd instead – Ehsan Sarshar Nov 19, 2019 at 14:28

@Ehsansarshar if you would like to follow MongoDB iptables firewal configuration page you can have iptables for Centos. See here – Jimmix Nov 19, 2019 at 16:58

1

I found a post here may help Securing Docker Ports with Firewalld (CentOS7, etc). Just post it here for people who need it in future.

For security concerns, we need both hardware and OS firewalls to be enabled and properly configured. I found that firewall protection is ineffective for ports that are opened in a Docker container and listened on 0.0.0.0, even though the firewalld service was enabled at that time.

My situation is :

- A server with Centos 7.9 and Docker version 20.10.17 installed
- A docker container was running with port 3000 opened on 0.0.0.0
- The firewalld service had started with the command `systemctl start firewalld`

- Only ports 22 should be allow access outside the server as the firewall configured.

It was expected that no one others could access port 3000 on that server, but the testing result was opposite. Port 3000 on that server was accessed successfully from any other servers. Thanks to the blog post, I have had my server under firewall protected.

> Quoted from the post : Securing Docker Ports with Firewalld (CentOS7, etc)

> Tested on CentOS7 with Docker-CE 18.09.6 Docker maintains IPTABLES chain "DOCKER-USER". If you restart firewalld when docker is running, firewalld is removing the DOCKER-USER chain, so no Docker access is possible after this. Docker adds a default rule to the DOCKER-USER chain which allows all IPs to access (possibly unsecure).
>
> We can achive secured Docker ports maintained by firewalld by letting firewalld create the DOCKER-USER chain, then apply iptables direct rules to secure the docker ports in this chain. When Docker is then started, it adds its allow-all rule to the bottom of our chain, but as we add a reject-all rule before, this rule is not in effect.

Share Improve this answer Follow

edited Apr 24, 2023 at 13:36

answered Aug 23, 2022 at 13:20

Rong.l
378 ● 2 ● 14

-1

Just run your docker like:

```
sudo docker run --rm --detach -p 127.0.0.1:9000:9000
```

There will be only internal localhost access, and not for the entire Internet.

Share Improve this answer Follow

answered Oct 1, 2023 at 20:31

Kirill Parfenov
653 ● 6 ● 9

Start asking to get answers

Find the answer to your question by asking.

Ask question

Explore related questions

docker docker-compose centos7

See similar questions with these tags.