

## hack4glarus-2019-winter - Task #7378

### Document / explore on how to sensibly run docker with a /64

11/29/2019 06:08 PM - Nico Schottelius

<b>Status:</b>	Closed	<b>Start date:</b>	11/29/2019
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>		<b>% Done:</b>	0%
<b>Category:</b>		<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>			
<b>PM Check date:</b>			
<b>Description</b>			
<b>draft 1: "https only"</b>			
<ul style="list-style-type: none"><li>• Block everything incoming besides https</li><li>• Reasoning:<ul style="list-style-type: none"><li>◦ containers by default insecure</li><li>◦ if https open -&gt; it is likely intended</li></ul></li><li>• container types (brainstorming)<ul style="list-style-type: none"><li>◦ databases</li><li>◦ message broker</li><li>◦ workers (probably not even reachable)</li><li>◦ a lot of http only stuff</li></ul></li></ul>			
<b>draft 2: tls/ssl in a container</b>			
<ul style="list-style-type: none"><li>• get a name</li><li>• get a cert</li><li>• TBD</li></ul>			
<b>draft 3: "NAT66 + firewall"</b>			
<ul style="list-style-type: none"><li>• Use the same approach as in IPv4 world</li><li>• We use a site local IPv6 addresses</li><li>• Do a NAT66 to the one IPv6 address of the host</li><li>• People can behave/have similar mechanisms as before</li></ul>			

### History

#### #1 - 11/29/2019 06:36 PM - Den Ivanov

Is that related to <https://redmine.ungleich.ch/issues/7359> ?

#### #2 - 11/30/2019 12:34 PM - Nico Schottelius

- Description updated

- Status changed from New to In Progress

#### #3 - 11/30/2019 12:38 PM - Nico Schottelius

- Description updated

#### #4 - 11/30/2019 12:46 PM - Nico Schottelius

- Description updated

#### #5 - 11/30/2019 12:48 PM - Nico Schottelius

- Description updated

#### #6 - 11/30/2019 09:18 PM - Den Ivanov

Some advices -> maybe that would help (\*may be dependent on docker version):

1) Run docker with: `` --ipv6 --fixed-cidr-v6={{ our net }} ``

2) Change sysctl options:

```

```
net.ipv6.conf.all.forwarding=1
net.ipv6.conf.default.forwarding=1
net.ipv6.conf.eth0.accept_ra=2
```

```

3) Remove IPv4-only embedded docker DNS server (useful when using custom networks created with "docker network create"):

```

```
RESOLV_CONF=$(sed 's/nameserver 127.0.0.11//g' /etc/resolv.conf)
echo "$RESOLV_CONF" > /etc/resolv.conf
```

```

**#7 - 11/30/2019 09:47 PM - Evil Ham**

This might benefit from [#7379](#) :-D

**#8 - 01/02/2024 12:35 PM - Nico Schottelius**

- Status changed from *In Progress* to *Closed*