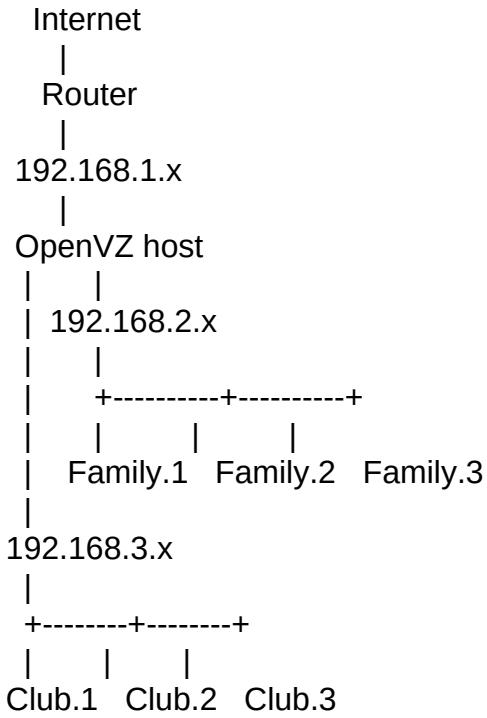
Subject: Setup for private subnets/internal LANs
Posted by jstuyts on Wed, 21 May 2014 11:20:25 GMT
View Forum Message <> Reply to Message

Note: The setup below is intended to be used for a home network. So security-wise the following things need to be considered:

I trust the users that I (might) give access to containers.
Some containers will provide public services on the internet.

I want to create containers for different purposes, for example for the family, my home company and clubs I help out. I do not want containers with different purposes to be able to see each other by default. I also want to be able to specify access rules, for example the family containers can access the home company and club containers. The implementation of the access rules will most likely require routing tables and firewalls, but I will figure that stuff out later.

To ensure containers cannot directly see containers with another purpose, I want to put containers on purpose-specific private subnets/internal LANs:



I created a test private subnet by bridging the veth devices of the containers:

```
brctl addbr vsn1
brctl addif vsn1 veth101.0
brctl addif vsn1 veth102.0
```

Using this bridge setup pings were working in all directions:

From CT0 to a CT, and vice versa

From a CT to another CT

So my questions are:

Is this the way to go forward (knowing that I need to configure IP forwarding, routing and firewalls to make it work properly)?
Will this scale and perform adequately?
Is this secure (enough)?
