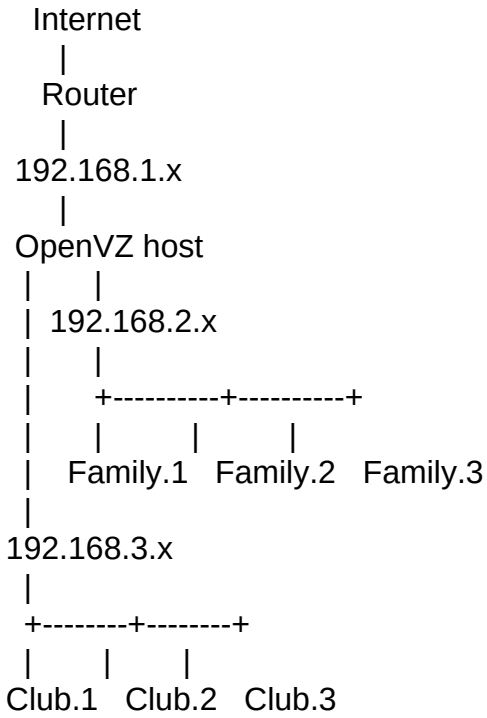
Subject: Setup for private subnets/internal LANs
Posted by jstuyts on Wed, 21 May 2014 11:20:25 GMT
View Forum Message <> Reply to Message

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)?

Subject: Re: Setup for private subnets/internal LANs
Posted by jetlee on Fri, 23 May 2014 09:51:56 GMT
View Forum Message <> Reply to Message

Id like to piggy back on this question, as I am currently trying to do exactly the same thing, and I think a thread (that is actually resolved) might be a good place to keep a simple discussion on the matter.

Some of my machines on the same network are windows based, and will access the containers, and here is a summary of what I tried / investigated, and some of the things I discovered.

Physical network isolation is very difficult / not very well documented in Openvz
In other virtual machine / hyperviser or similar software has a mechanism for virtual switches or similar allowing your network to behave as if it physically connected to a different switch. I cannot find a way to reliably do this in openvz. My next attempt at this will be to create multiple bridges, and try to use iptables to deny traffic across bridges, and am not sure how this may work, as I dont fully understand the v-nic traversal path with veth networking.

Broadcast protocols require Veth
There are some things than can be used, but most documentation seems to ignore veth (by other vendors) when searching on OpenVZ topics. When using something like samba or dhcp, veth is required.

VLANs dont solve all problems
I tried implementing VLANs, which worked brilliantly in Linux, but some of the network cards / drivers in windows did not support VLAN's, so the traffic from those machines could not see VLAN machines.

IP Subnets dont solve all isolation problems
IP Subnets were my last attempt at this separation. As per the previous diagram, IP subnet separation only works, if a host inside your network is not compromised. Having 2 ranges (192.168.0.0 and 192.168.1.0) does not preotect against an intruder gaining access to one network, and changing the mask to 255.255.0.0) and immediately allowing access to both subnets.

I hope that there is something obvious I have missed, and I hope my previous attempts, will assist

somene else in making decisions around structures / designs similar to the one posted.

Justin

Subject: Re: Setup for private subnets/internal LANs
Posted by jstuyts on Fri, 23 May 2014 16:45:01 GMT
View Forum Message <> Reply to Message

Hi Justin,

Thanks for sharing your experiences. I will see if I can use them.

You also got me in a bit of a pessimistic mood though.
