OpenBSD vmm at bsd.network and conference tutorials

Peter Hessler

phessler@openbsd.org

14 May, 2019

- OpenBSD has a native hypervisor
- ... development started in 2015
- ... enabled by default in 6.1 (released in Apr 2017)

- bsd.network is a social network connected to the activitypub fediverse
- owned by me and a friend of mine
- opened for registrations 2 Jan 2018
- 1249 users, 405 monthly active, 122,849 statuses, 4243 connections
- around 30 statuses per hour.
- has, and enforces, a code of conduct

- vmm was chosen because I'm an OpenBSD developer
- and wanted to dogfood our hypervisor
- … was already using it for my bgp tutorial
- first public production service of vmm(4) in the world
- … to the best of our knowledge

- 1 physical server
- 12x xeon e5 cores, 64G ram, two ssd disks
- 3 vmm guests
- has always been OpenBSD-on-OpenBSD

- 1 vcpu
- 8G ram
- two nics, one external, one internal

- external interface has public v4 and public v6
- ... all services are dual stack
- external interfaces are bridged together
- ... and to the egress interface

- internal interface has private v4 and private v6
- … all services are still dual stack
- … orignally was v6-only, but go is stupid
- internal interfaces are bridged together
- … and heavily firewalled from the outside world

- ruby web app
- … with a nodejs service
- uses sidekiq as a queue runner

- very cpu heavy
- fork heavy
- ruby isn't too terrible
- but nodejs is a trashfire
- … npm makes me consider never using electricity again

- originally ran all services on a single vmm guest
- was alright until around 400 user accounts
- grew to 3 VMs
- ... web front end
- ... databases
- ... queue runners and media server (mostly developers artwork)

- since June 2017 I teach a tutorial on BGP
- … intended for non-experts
- (happening on Thursday, wink wink)
- just talking isn't very interesting
- … I wanted labs

- connecting networks together is the entire point
- simple home labs are insufficient
- connect all of the students together
- … real tests they can see
- … free experimentation with (minimal) consequences

- 1 Thinkpad t430s
- ... already owned it
- ... 16G of ram
- ... very silly things with disks

- each student gets two VM guests
- 1 vcpu, 192M ram, small disk
- side-left and side-right
- ... interfaces are bridged together
- side-right is also connected to a shared LAN

- each guest runs openbsd
- ... acts as a BGP router
- pre-configured in simple ways
- ... students are expected to grow the configuration through the class

- side-right is connected to everyone
- … started with only connected to a router I control
- they add connections to other students throughout the lab sessions

- 1 vcpu, 512M ram, slightly larger disk
- first router they connect to

- 5 teaching VMs
- … one central router
- … two teacher routers
- … two attacker routers
- 2x VMs per student
- max of 30 people per class
- up to 65 guests
- at the time, largest single system deployment of vmm(4)

- ttyd
- web accessible terminals
- … connects to each guest and re-attaches to a tmux session

- each student does the lab work from a web page
- ... contains two terminals they can type into
- ... reminders of their Internet Numbers for doing BGP things
- students only need a web browser on the correct wifi