Dodging Raindrops: Escaping the Public Cloud

A User Story of De-Google-ication Using FreeBSD and Other Open Source Software

Michael "Ike" Eichorn

BSDCan 2016

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

From Windows Fanboy to BSD User

- Windows Vista and my college laptop the Thinkpad X61t
- Windows 7 not enough configuration options
- Ubuntu was my gateway, but upgrades were terrible
- Mangling .deb and .rpm distros
- Archlinux gateway to the terminal
- The crash that brought me to BSD
- FreeBSD to OpenBSD to PCBSD to FreeBSD

The Day Job

- Mechanical Test Engineer
- 'Data Engineer'
- And by Mechanical I mean Aerospace
- Not Admin, Not Programmer, but an 'Operator'
- FORTRAN 77 with bad comments
- 'Like we did it last time'
- (And by 'last time' they mean 10-15 years ago)
- A member of the TEX faction
- Hater of Excel

Yea, but Why Should I Listen to You

- I am in front of you
- I have the podium
- I like to hear myself talk
- IANALawyer
- IANADev
- IANASysAdmin
- IANANetAdmin
- I am a User

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

A *Reasonable* Expectation of Privacy

- Everyone has the right to record anything that is public
- Most legal systems recognize a right to privacy
- In the USA the 4th Amemendment restriction on searches and seisures uses the "Reasonable Expectation of Privacy" test
- This is a problem because it can be twisted by denying that there is an expectation of privacy in some way long enough that the expectation becomes lost
- Some thought in the liberal tradition held that mearely searching one's papers was potentially on par with a violation of freedom of thought.
- The nothing to hide argument is short sighted and lazy

The Third Party Doctrine and the ECPA (USA)

- The Third Party Doctrine – If you voluntarily give information to third parties you have no reasonable expectation of privacy over that information.
- 1967 – US v. Katz – wiretapping a public phone booth is a search and requires a warrant.
- 1976 – US v. Miller – No privacy in banking records – Third Party Doctrine Established
- 1979 – Smith v. Maryland – No privacy in phone records
- 1982 – RFC 821 – SMTP Standardized
- 1984 – RFC 918 – POP Standardized
- 1986 – The Electronic Communications Privacy Act – Emails left unopened for 180 days are abandoned and not private, Opened Emails are not private
- 1988 – RFC 1064 – IMAP Standarized

So Who 'Owns' that Data

- Possession is 9/10 of the Law
- If your neighbor was keeping your lawnmower and sold it, you could sue them.
- All of those Terms of Service really make you abandon most of your rights.
- Are you really the customer or is it really some advertiser who is the customer?

Digital Data Wants to be Copied

- DRM does not work well if at all
- Copies are economically almost free
- Coping does not harm the original
- The cost is all in creation, transmission, and storage.
- Privacy and Copyright are human notions we put on data, not an inherent property of data.

To Companies and Governments You are Data

- With friends and family we interact as individuals, actions are based on personal knowledge
- Beyond that scope social and commerical interaction must use less personal knowledge
- At some scope you and your preferences can be aggregated with other individuals
- While one person may be unpredictable a sufficient number will be.
- Credit Scores and other Single Numbers

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

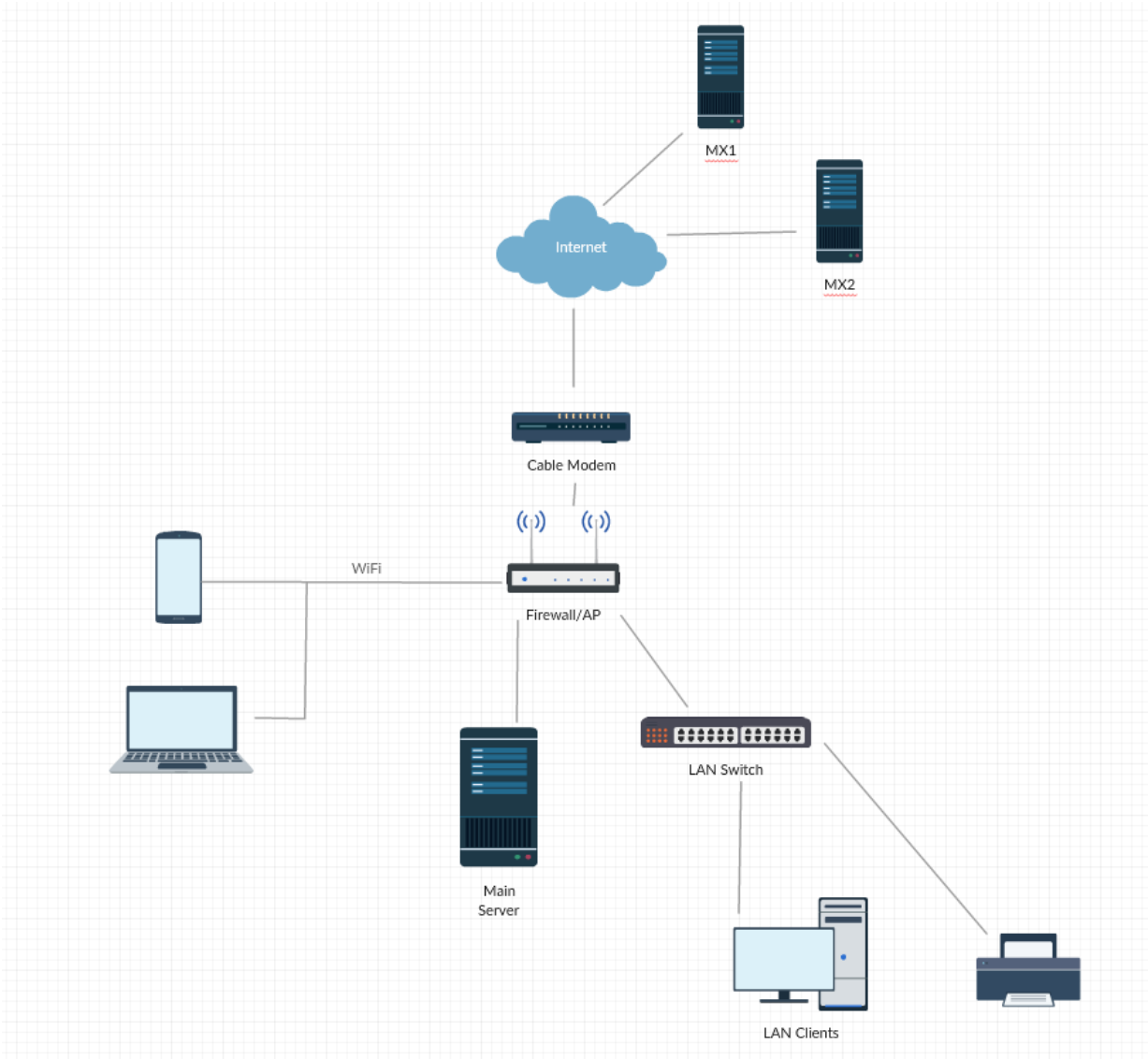
The Hardware

- Athlon 64 X2 on a Socket AM2+ Board
- Purchased in mid to late 2000's
- 4 GiB DDR2 RAM
- Pair of 3TB WD Reds mirrored with ZFS root
- No performance tuning at all

My ISP

- A large cable company
- 30/5 Mbit/s Residential Service
- Dynamic IP Address
- No ports blocked

The Network


MX1
Internet
MX2
Cable Modem
WiFi
Firewall/AP
LAN Switch
Main
Server
LAN Clients

Jails, Jails, and Even More Jails

- fileserver
- http(s) reverse proxy (nginx)
- wordpress (Apache-MariaDB-PHP)
- mediawiki (Apache-MariaDB-PHP)
- PHP website (Apache-PHP)
- PHP website (Apache-PHP)
- Static website (nginx)
- Static website (nginx)
- SMTP (OpenSMPTD)
- LDAP (Dovecot)
- Webmail (Roundcube)
- CalDav/CardDav (Radicale)
- Owncloud
- Experiment of the week

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

SMTP

- In my case no ports were blocked so the home email server is the first MX
- ISP has an outgoing relay that I once used
- MTA/MSA was Postfix, moved to OpenSMTPD about a year ago
- Two backup MXs using DigitalOcean in NY and CA
- I have never had a problem receiving mail
- Mail is delivered to Dovecot via LMTP
- SMTPS on port 465 is DEPRECIATED and IANA has reassigned it!

IMAP

- Dovecot – WARN: Monoculture
- IMAP + STARTTLS Only
- Works great with Evolution/Thunderbird/K9
- Sieve Filtering is great but the documentation was rough

Spam and Avoiding Blacklists

- Do not send directly from a dynamic IP, use a relay
- Backup MXs are already there and make great relays
- Spam has not really been a problem, Spammers do not seem to target domains where the first MX is dynamic
- Per-website emails e.g. google@yourdomain.tld allow you to throw away emails if they are compromised
- Will soon be adding spam filtering thanks to Aaron Poffenberger's OpenSMTPD Tutorial

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

Requirements

- Public or Private
- Level of Security
- Ease of Use
- Ease of Setup
- Robustness

FTP

- No security.
- Does not behave well with firewalls.
- Works in a web browser
- Old and durable

SFTP

- Secured with SSH
- Easy to setup
- May not be easy to use for un-savy
- SSHFS is nice
- SSH is robust

Plain Old Apache

- Built-in .htpasswd is probably fine for most security needs
- Made for serving files
- Works in all web browsers
- Robust
- Populating files would seem to be a problem
- Unless you do something like SSHFS mount that server directory as /home/user/public

Owncloud et al.

- Web-app style login security
- Fine grained sharing control
- Desktop sync apps
- Has been known to loose files
- *AMP deployment
- Easy to use and pretty

Syncthing et al.

- No easy to use config files
- Works well
- No way family will use this unless you set it up

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

Fixing Things I Broke

- CalDav/CardDav
- Taskd (Taskwarrior)
- Owncloud
- Local Backup
- VPN
- LDAP/Kerberos

Adding New Tools That Exist

- XMPP or similar IM solution
- Nagios/Icinga or similar monitoring solution
- TinyTinyRSS or similar RSS feed reader
- Improved Remote Backup (Tarsnap)
- VOIP

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

Mobile Problems

- Outside Location tracking generally is too easy on phones
- Google Maps dominant in navigation.
- Whole sandboxes are geared to forcing the use of 'thier' cloud solutions
- Remember Google bought Android to dominiate mobile search.
- Google Now / Siri are nice, but I want to control my personal assistant not have it be a spy for an advertising company.

Simple Deployments

- Having lots of knobs is nice, it is a major draw for me.
- Sane defaults are better.
- Most users do not want to change all of the knobs and will accept mediocre performance
- Consider Sendmail vs Postfix vs OpenSMTPD
- More options are more things to support and test

Table of Contents

Who is the Guy? And Why Should I Listen?

What Does He Have Against Google and the Cloud?

Three Domains Served From Home

Email with a Residential ISP

File Sharing - Many Solutions

My To Do List

What is Missing? (Or at least hard to find)

What was Painful?

Multiple Computer Multidirectional File Syncing

- Trying to keep local copies in sync is bad everwhere
- Microsoft Offline Files
- Unison
- Owncloud - sometimes looses files
- Syncthing - sometimes fails to connect
- Permissions and UIDs not always part of sync solution

NFS

- I cannot make it work
- Documentation often skips firewall config
- Lots of documentation confusion about NFSv3 vs NFSv4
- I am a rocket scientist and I cannot make it work

Spam Filtering

- Lots of solutions but often described as chained together
- Most documentation seems to assume that all of the components are on the same machine, I want to jail them all separately and connect them on lo0.
- Thanks to Aaron Poffenberger's OpenSMTPD Tutorial I may be able to finish figuring this out.

FreeBSD-update Related Booting Problems

- I have lost my system multiple times to boot problems
- Would not boot off the ZFS root pool
- Usually happened after a freebsd-update
- Never had time to fully diagnose, I only had one server so I restored from backups.
- There seem to be some ways to shoot your foot off with regard to booting in the update procedure