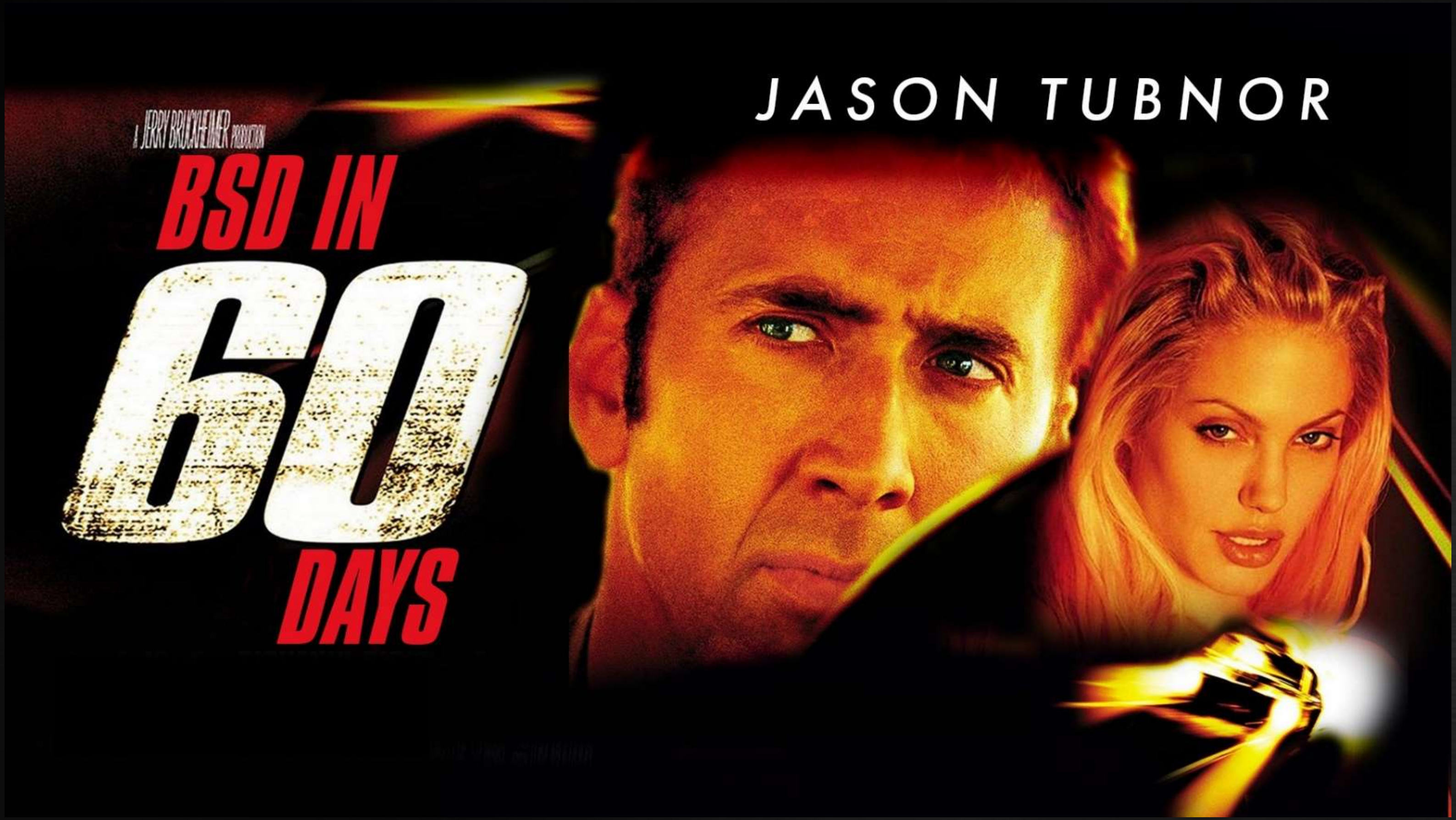
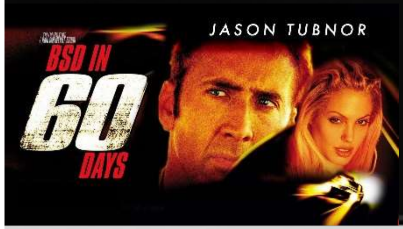
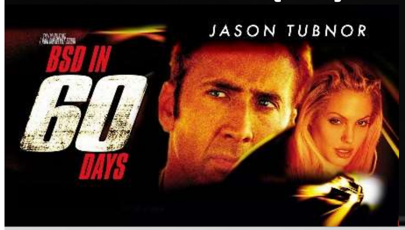


ICT Senior Security Lead
Latrobe Community Health Service Ltd.



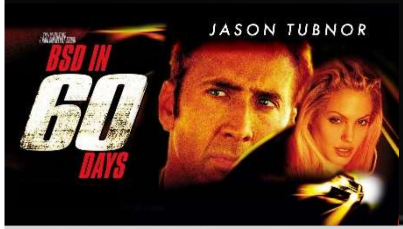
Introduction

- Use of BSD in the NFP/NGO Australian Health Sector
  - About Me
  - My employer, Latrobe Community Health Service (LCHS)
- iked(8), pf(4)
- ripd(8), Squid, spamd(8), rdomain(4), vxlan(4)
- Documentation, performance testing
- zfs(8), bhyve(8) and other cool stuff™



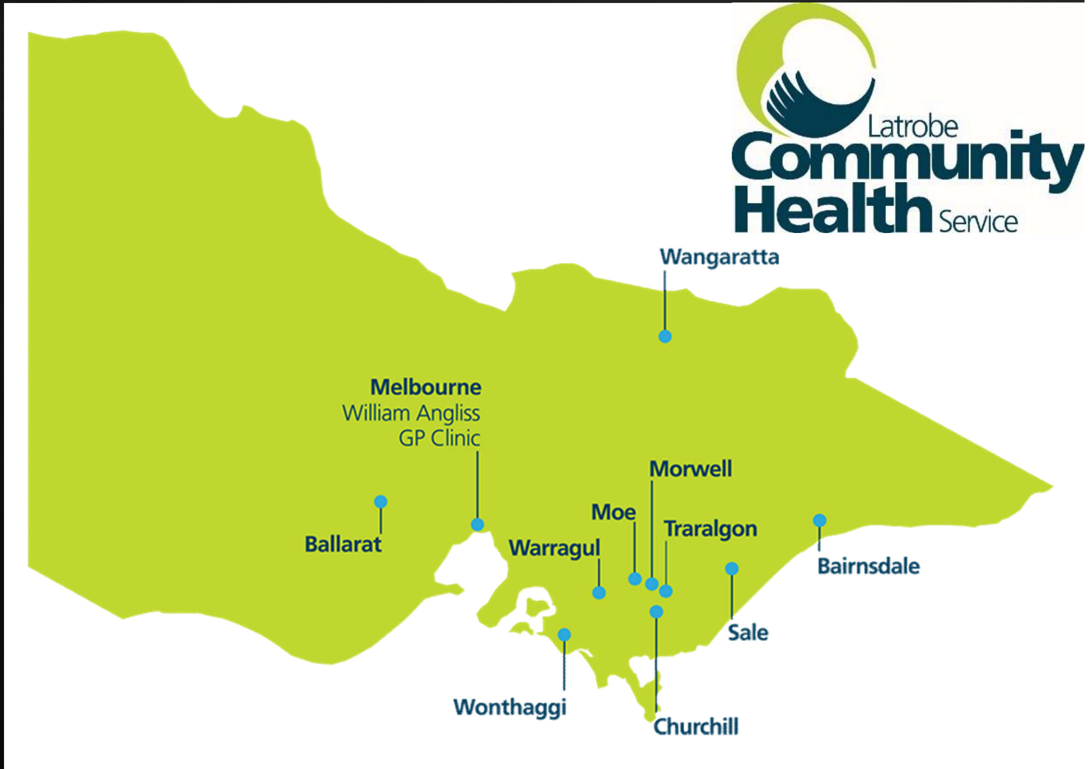
About Me

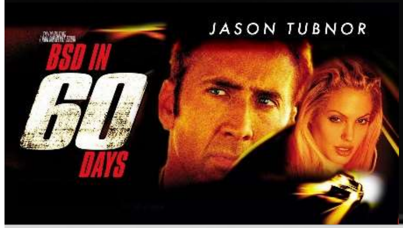
- 24 Years of ICT experience
- Introduced to Open Source in the mid 90’s
- Hey, check out this OpenBSD operating system in 2000
- A user of OpenBSD and FreeBSD since ’00 to present
- Cycle road racing
  - Twitter: @Tubsta
  - Email: jason@tubnor.net



About LCHS

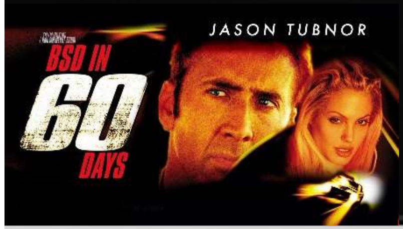
- Originally a Gippsland based NFP/NGO health service
- ICT manages 500+ users
- Servicing 12 sites growing to 49 sites over the next 3-6 months
- Covering 102,000km^2
- Which is the size of the state of Kentucky, USA





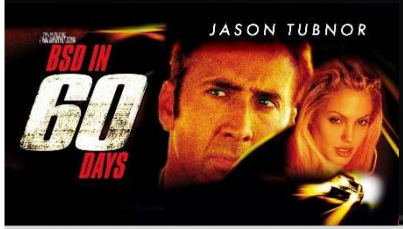
Bridge the office

- Newly acquired contract to run Headspace Morwell
- Management were welcoming to new ideas
- Problem: Bridge two networks over public Internet
- Short timeframe for implementation



OpenBSD IKEv2 – iked(8)

- Investigated multiple solutions
- OpenBSD iked(8) implementation won due to simplicity
- Enabled connectivity to the server VLAN in 2 lines of iked(8) configuration



OpenBSD IKEv2 – iked(8) cont.

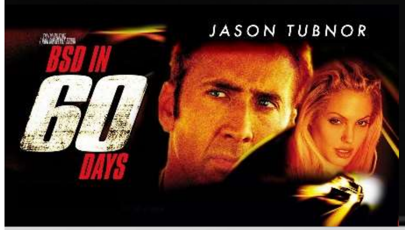
- Problems:
  - Expiration of certificates
  - NAT – use static-port with nat-to when behind a pf(8) firewall
  - Rekeying at 3hr/512MB caused issues with established connections
  - VMWare DRS and OpenBSD don’t play well together

OpenBSD IKEv2 – iked(8) cont.

- Overall:
  - Solved the problem out of the box
  - Super simple to configure and maintain
  - Authentication mechanisms are easy
  - Integrates well with pf(8)
  - Bullet proof – works like an appliance
  - Worked so good, highly recommended over commercial offerings
  - Management were happy with the results

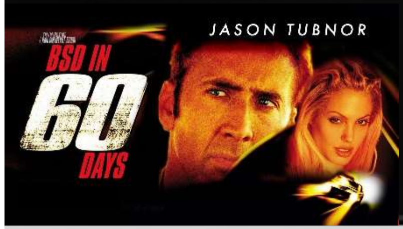
Network Migration

- Departed ways with our outsourced network provider
- New challenges
- Network provider had been already chosen to provide Internet & MPLS services
- Hardware refresh for LAN gear was in scope

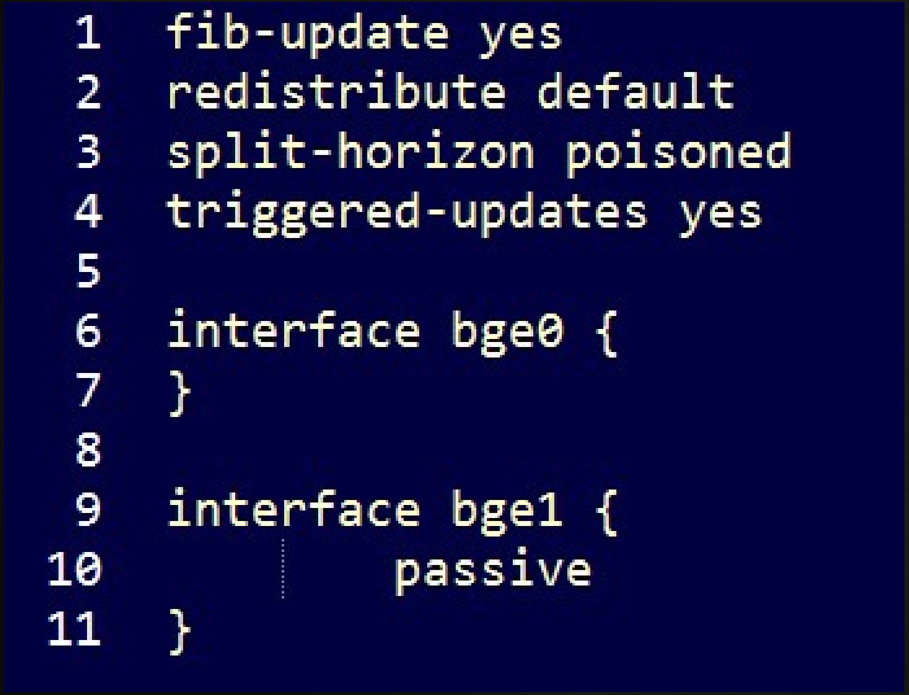


Network Migration – cont.

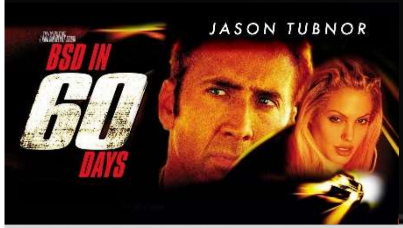
- Selecting a routing protocol – RIPv2 or EiGRP
- We chose RIPv2
- As of OpenBSD 6.1, ripd(8) plays nicely in rdomain(4)
- But why RIP?



Network Migration – cont.

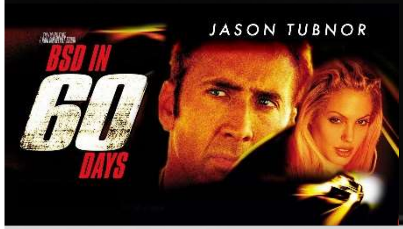


```
fib-update yes
redistribute default
split-horizon poisoned
triggered-updates yes

interface bge0 {
}

interface bge1 {
        passive
}
```



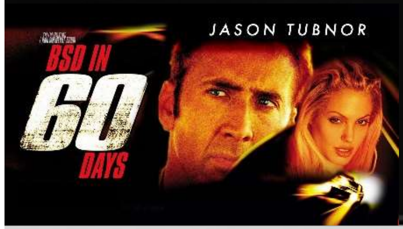
Primary External Gateway

- We chose OpenBSD with pf(4)
- Why not choose pfsense or FreeBSD with pf(4)?
- Integrates nicely with RIPv2 using only base



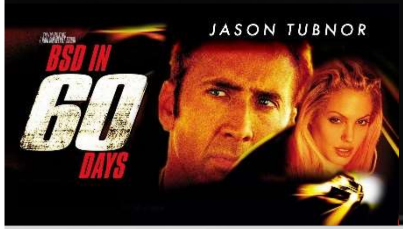
Primary External Gateway – cont.

- pf(4) was configured to block by default
- Matching against traffic type to a /28
- pf(4) tables for blocking of ips and subnets
  - also turning on and off the guest WiFi networks
- Queuing and traffic shaping
- Very durable, bare metal host barely showing signs of load on 8 core Xeon



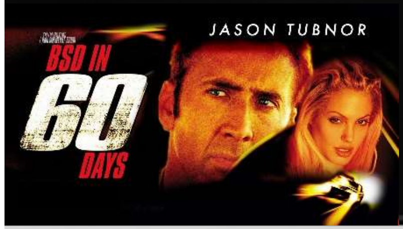
Primary External Gateway – cont.

- To compliment:
  - Squid Proxy
    - Didn’t break HTTPS traffic
    - Used Squid Blacklist
  - Spamd(8)
    - Keeps the bulk of spam from overwhelming the Spam Assassin server



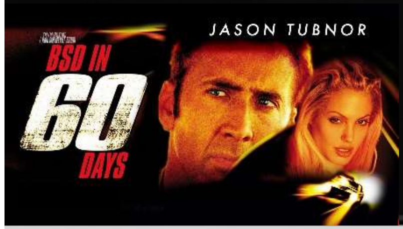
Moving beyond the boundary

- Mail Ingress
  - OpenSMTPD – spamd(8)
  - Spam Assassin
  - ClamAV



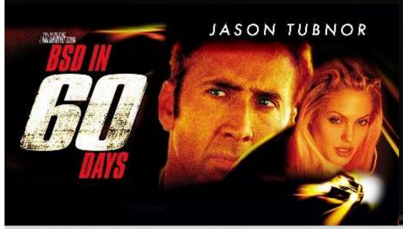
Backing up the shiny

- Initially an OpenBSD system simply to backup tftp configs from switches
- Moved to FreeBSD for ZFS (snapshot, send/recv)
- Atftp used as the TFTP daemon
- Sshd_config needed modification, using Match for Call Manager ssh backups
- Zfssnap2 and zxfer used for management and transfer to DR site



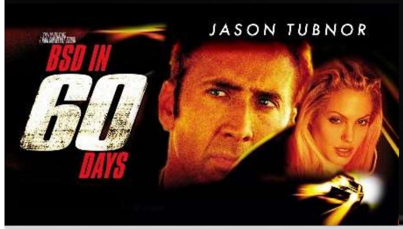
Backing up the shiny – cont.

- Benefits:
  - Easy to pull individual files from a point in time
    - Helped when we had to review mail volumes
  - Simplistic

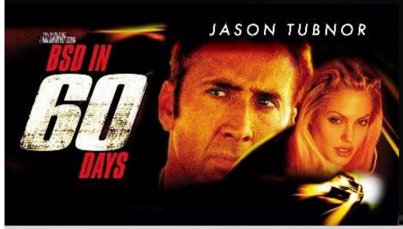


Documentation

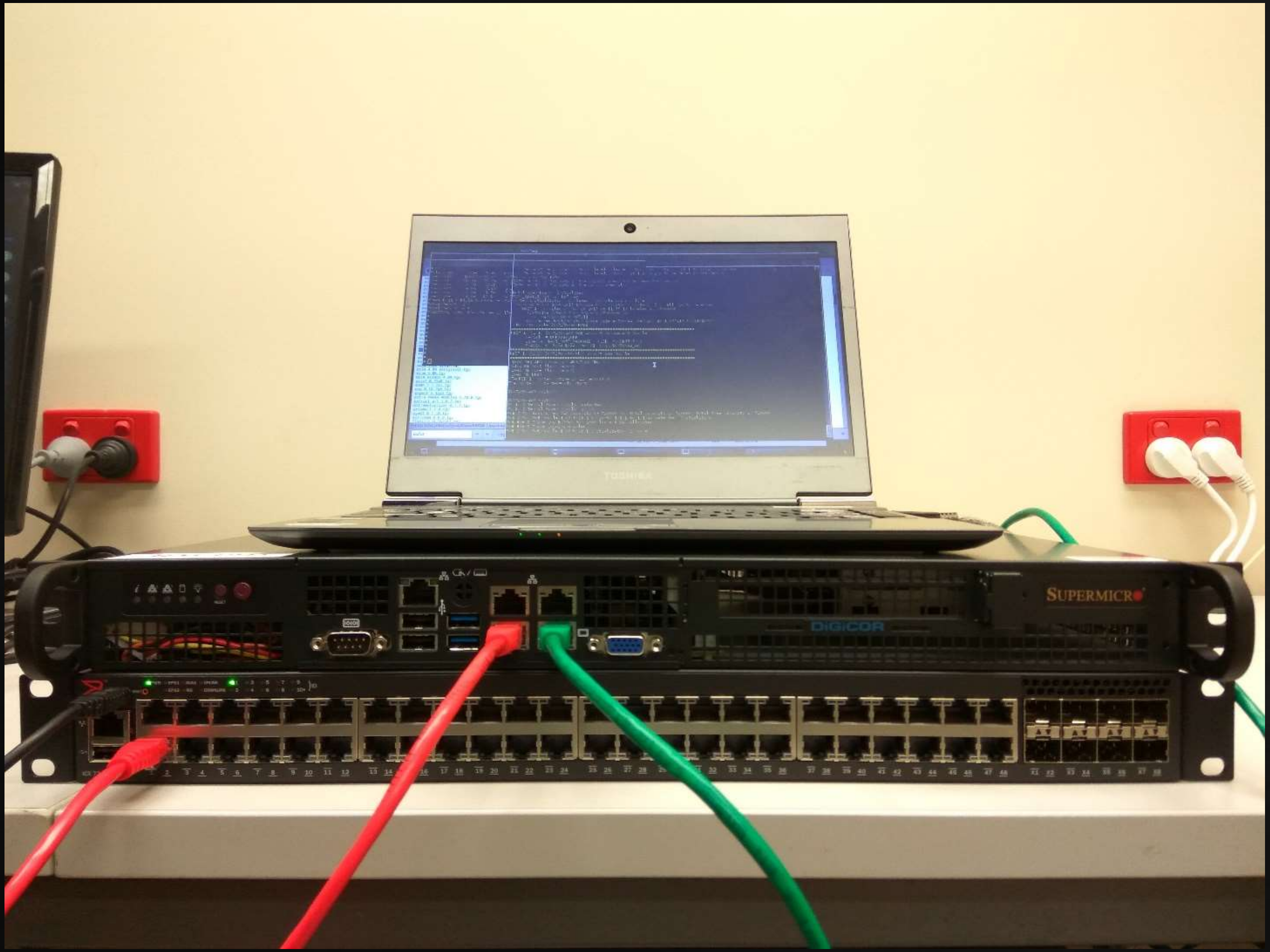
- Need for online and offline documentation
- A learning tool for team members to understand BSD
- OpenBSD virtual instance running Mediawiki
- OpenBSD physical instance in DR
- Custom scripts run daily to sync and update the DB nightly

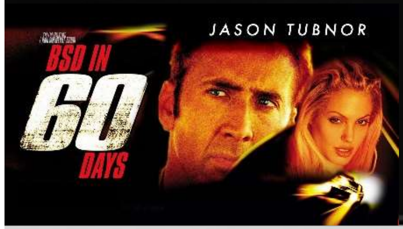


Super Duper Extra Special Bonus Section



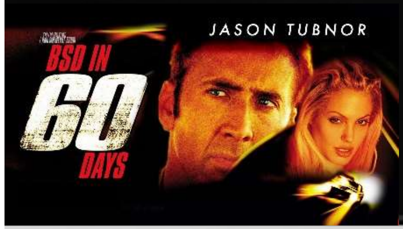
Project Point.5



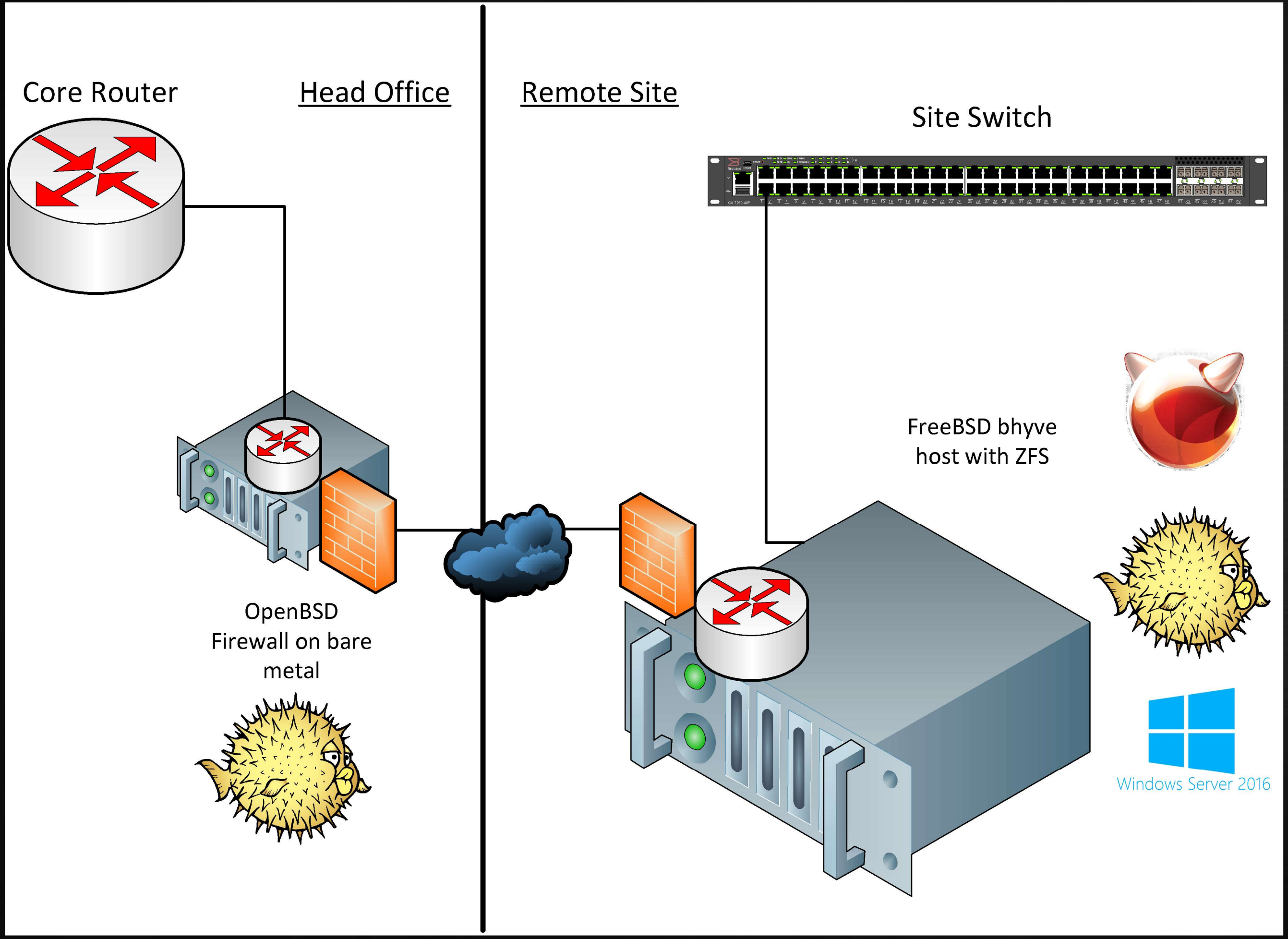


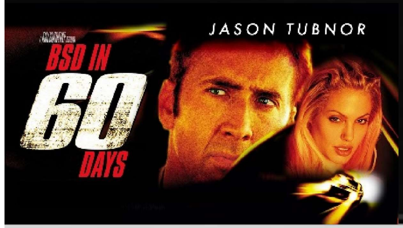
Project Point.5 – cont.

- Appliance to use as a remote site endpoint
- Router and site server
- Running FreeBSD 11.0 as host
- ZFS, bhyve with UEFI + other packages
- Chyves
- OpenBSD 6.1 and Windows Server 2016 guests



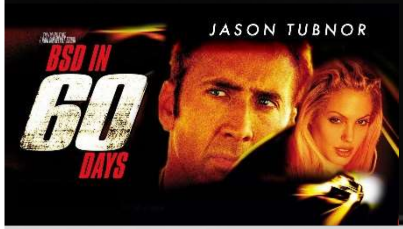
Project Point.5 – cont.





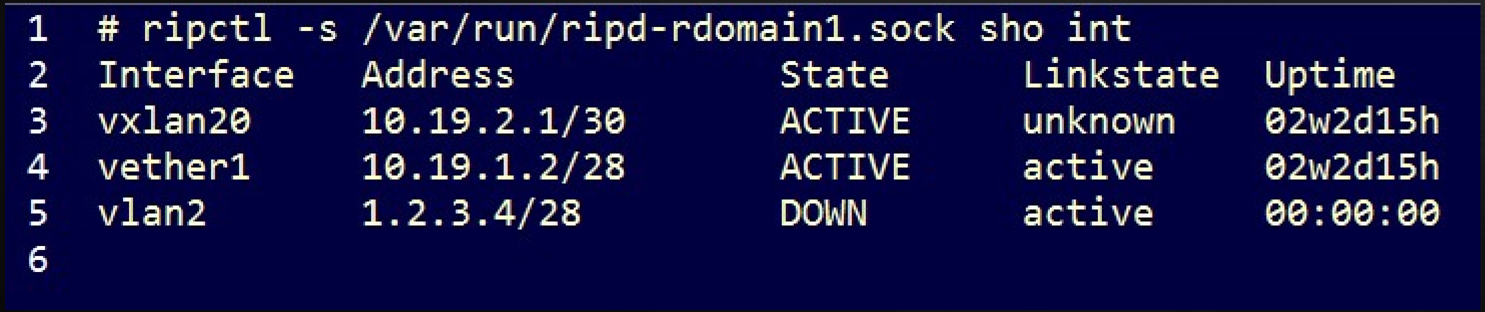
Project Point.5 – cont.

- Components:
  - IKEv2 with compression
  - PF with queues
  - vxlan
  - RIPv2
  - dhcpd
  - VLANs
  - Bridges
  - Taps

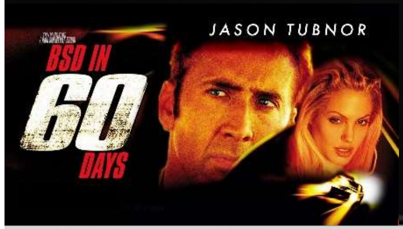


Project Point.5 – a bug – cont.

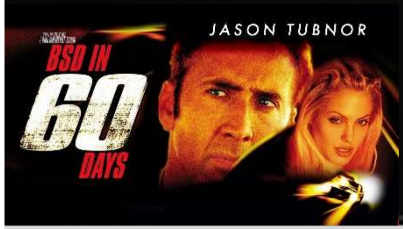
- Appeared to find a bug in ripd(8)
- Prevents the IP of the two vxlan(4) interfaces from being advertised
- Static route inserted into the core an redistributed as a workaround



```
# ripctl -s /var/run/ripd-rdomain1.sock sho int
Interface   Address            State      Linkstate  Uptime
vxlan20     10.19.2.1/30       ACTIVE     unknown    02w2d15h
vether1     10.19.1.2/28       ACTIVE     active     02w2d15h
vlan2       1.2.3.4/28         DOWN       active     00:00:00

```

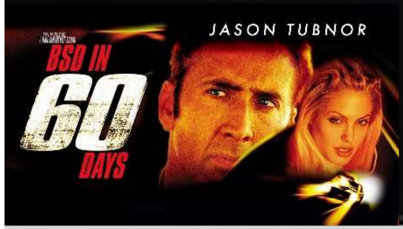


Project Point.5 – cont.



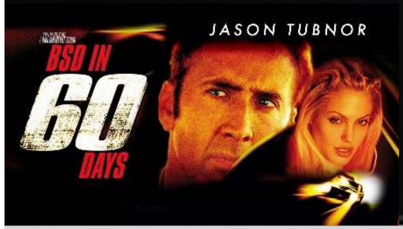
Thanks

- OpenBSD Project
- FreeBSD Project
- Michael Dexter
- Peter Grehan
- Stuart Henderson
- ….. and all those that work tirelessly on open source software



Donate

- You too can help:
  - OpenBSD Foundation
    http://www.openbsdfoundation.org/
  - FreeBSD Foundation
    https://www.freebsdfoundation.org/



Q & A