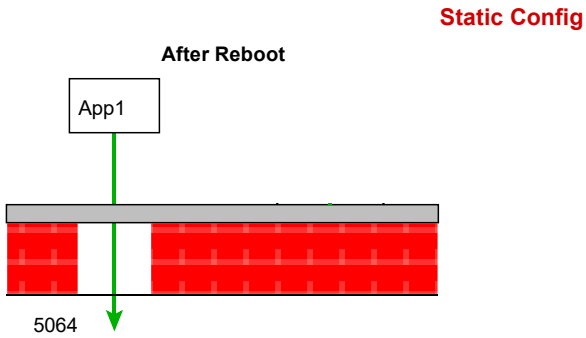
A Prototype Dynamic Firewall Manager for EPICS Channel Access

Ru Igarashi
Canadian Light Source
EPICS Collaboration
2021-07

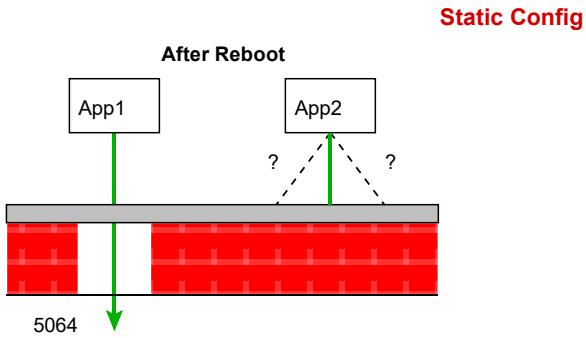
Problem

- Typically:



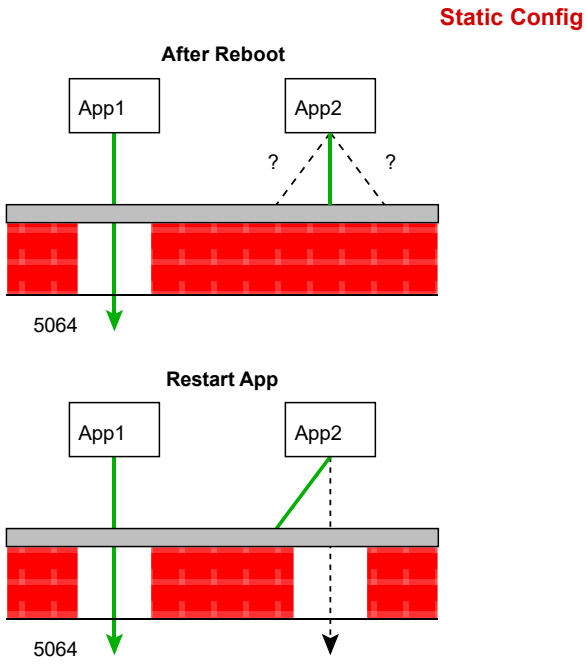
Problem

- Typically:



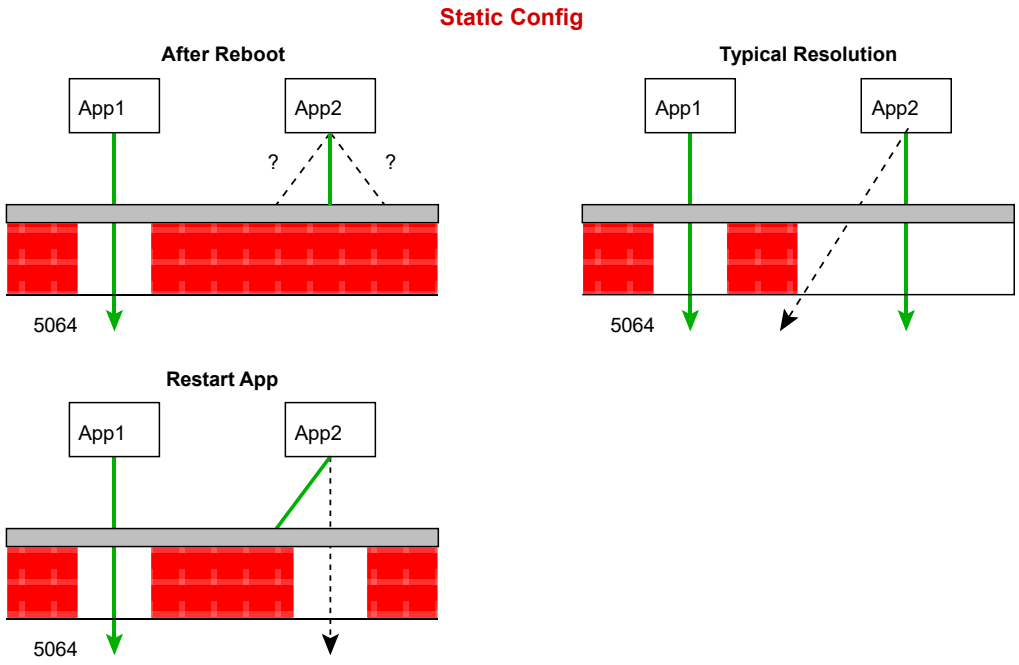
Problem

- Typically:



Problem

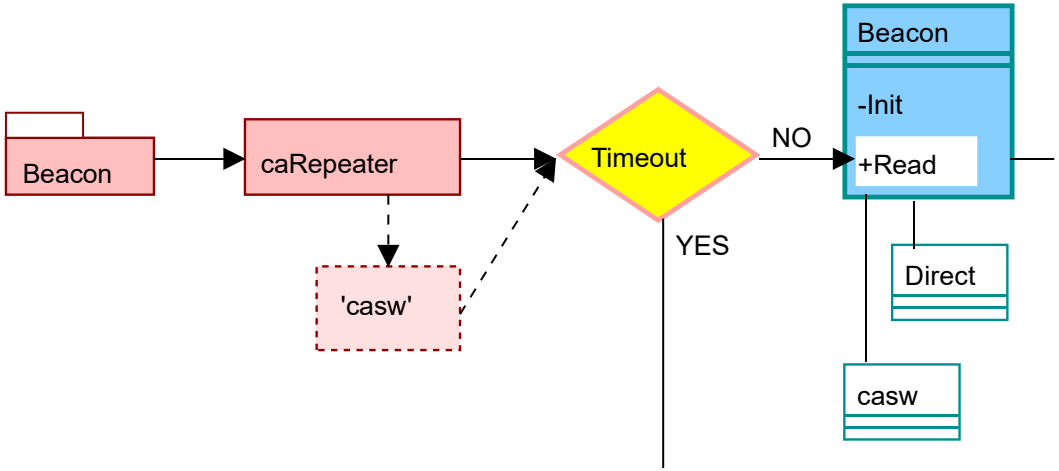
- Typically:



Requirements

- Dynamic
- Automated
- No mods/retrofit of EPICS base
- No mods/retrofit of existing apps and tools
- Multiple Linux platforms

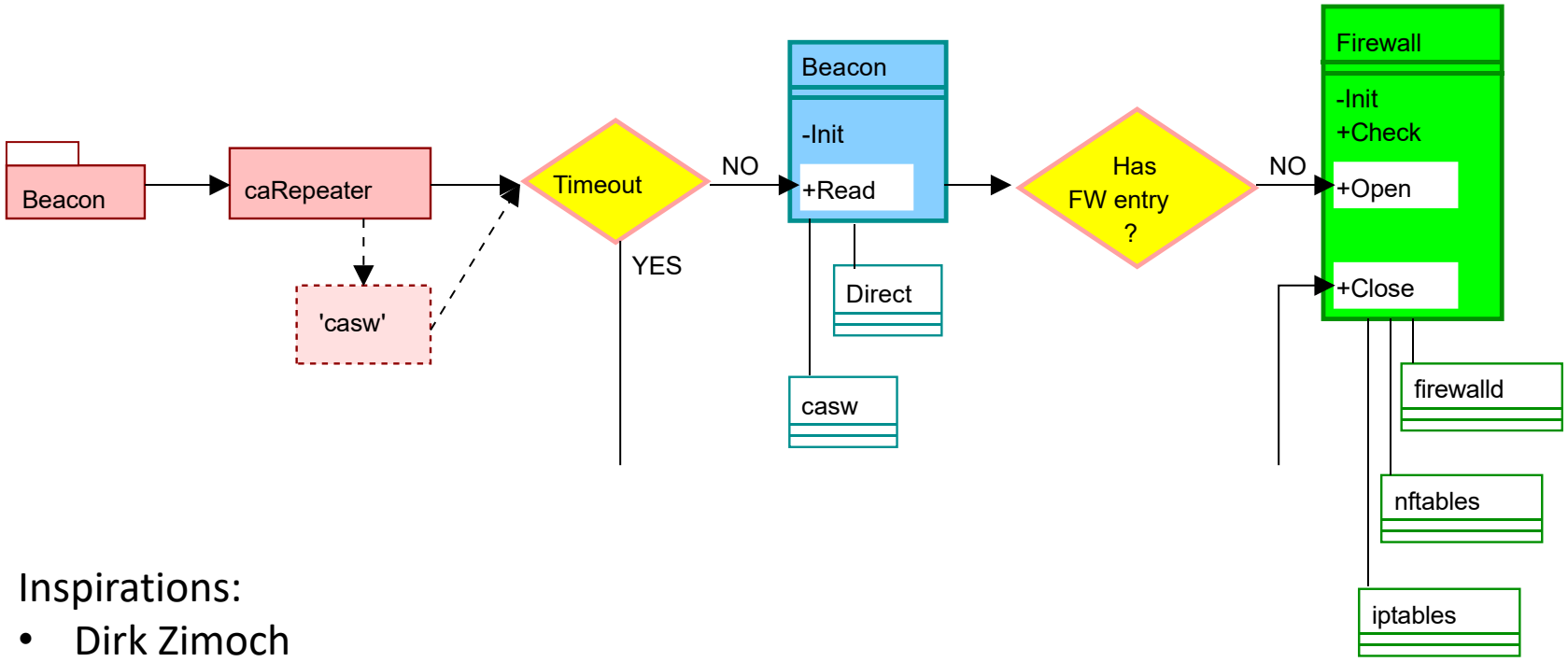
Implementation



Inspirations:

- Dirk Zimoch
  (launch script from iocsh)
- Mike Bree
  (beacons for monitors)

Implementation

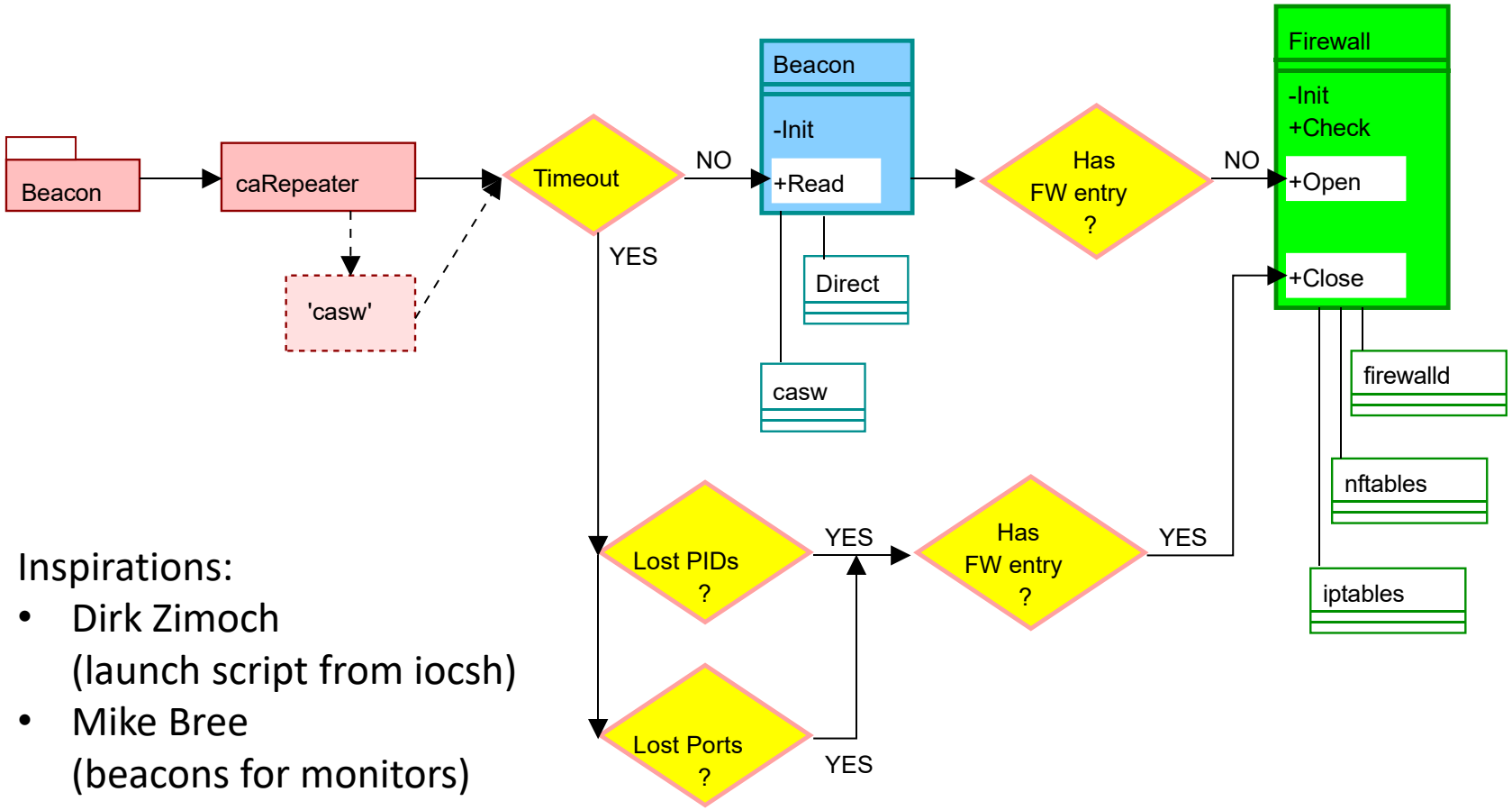


Inspirations:

- Dirk Zimoch
  (launch script from iocsh)
- Mike Bree
  (beacons for monitors)

Implementation

(sort of!)



Inspirations:

- Dirk Zimoch
  (launch script from iocsh)
- Mike Bree
  (beacons for monitors)

Tests

- Old desktop with SL 5.4 and VM with CentOS 8
- 1-50 IOC apps at once
- repeatedly restart IOC apps

	iptables		nftables		firewalld	
# apps	open	close	open	close	open	close
5	2(2)	<1	2	<1	6	5
10	2(3)	<1	2	1-2	13	10
20	2-3(5)	<1	2-3	1-2	20-25	20-25
50	4(11)	<1	4	<1	55	45

Features

```
EPICS-firewall.[pl|py] [-t fwtype] [-s sourcetype] [-b beaconport] [-l localhost] [-d debuglevel]
```

- Perl 5, Python 2 / 3
- Alternate beacon port
- Alternate hostname/IP (filter)
- Extensible firewall support
- Extensible beacon source

Drawbacks/Disadvantages

- Security: beacon spoofing
- Efficiency: relies on PID and port list scans
- Client reconnect latency: initial beacons lost
- Restart latency: beacon periods (0-15 s) to open hole

Bugs, ToDo,…

- Are you kidding?
  - “prototype” = “issues” = TONNES
- Broken / MESSY code / inefficient code
- Real-world testing
- Site dependent Firewall layout
- …

Conclusion

- Strategy: listen for beacons, issue commands to open/close holes in firewall
  - works on small (<20) scale
- Not clear how well it actually performs:
  - In long term operation – reliability, robustness
  - By scale – 100 apps, 200 apps
  - In production environment – interactions
- Don’t use firewalld for this purpose