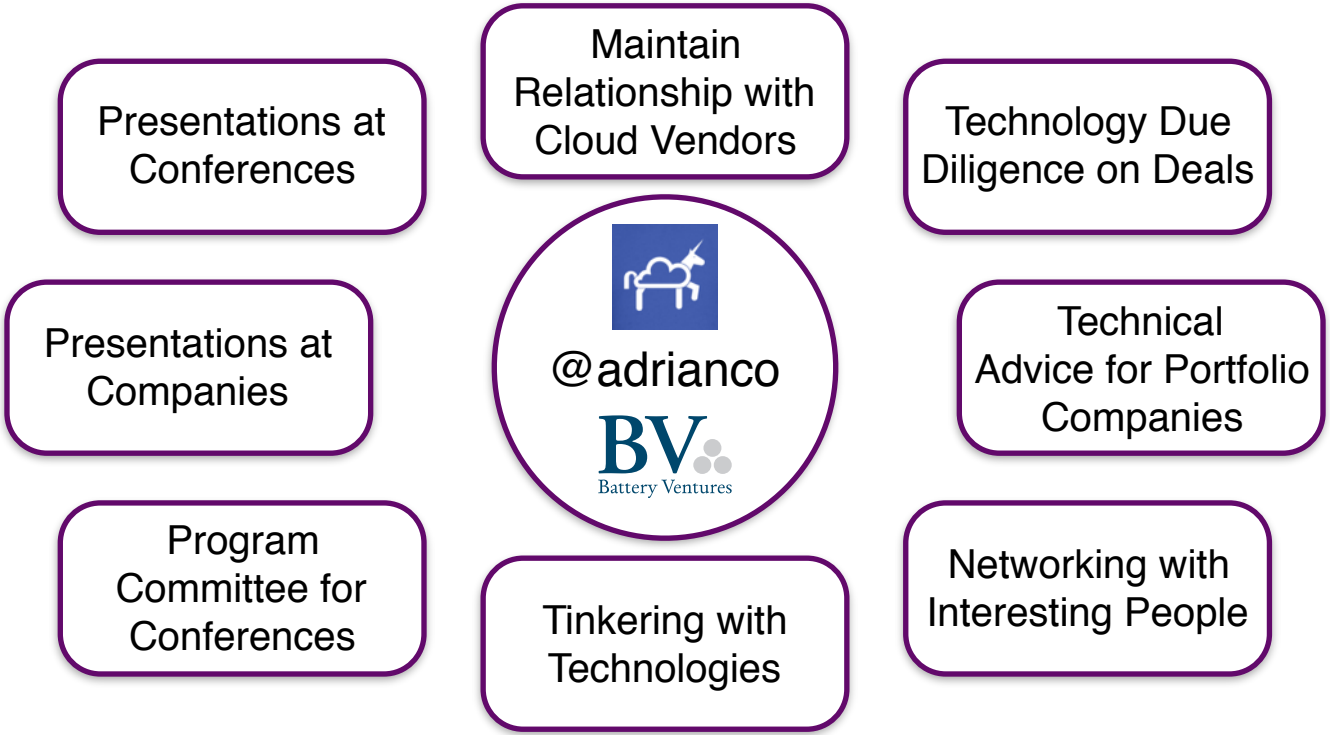
In Search of Segmentation

Adrian Cockcroft @adrianco
Technology Fellow - Battery Ventures
February 2016

BV
Battery Ventures

What does @adrianco do?



http://www.slideshare.net/adriancockcroft

Segmentation

Industry Trends

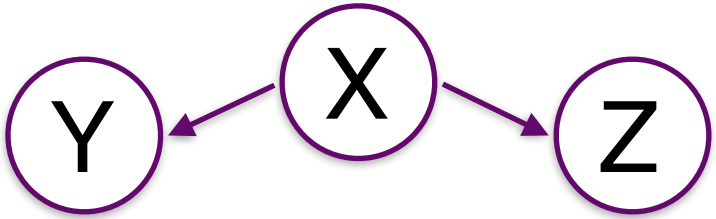
Airgaps closing
Industrial IoT
Security blanket perimeter firewalls
Datacenter to cloud transitions
New systems of engagement

http://peanuts.wikia.com/wiki/Linus'_security_blanket

Policy

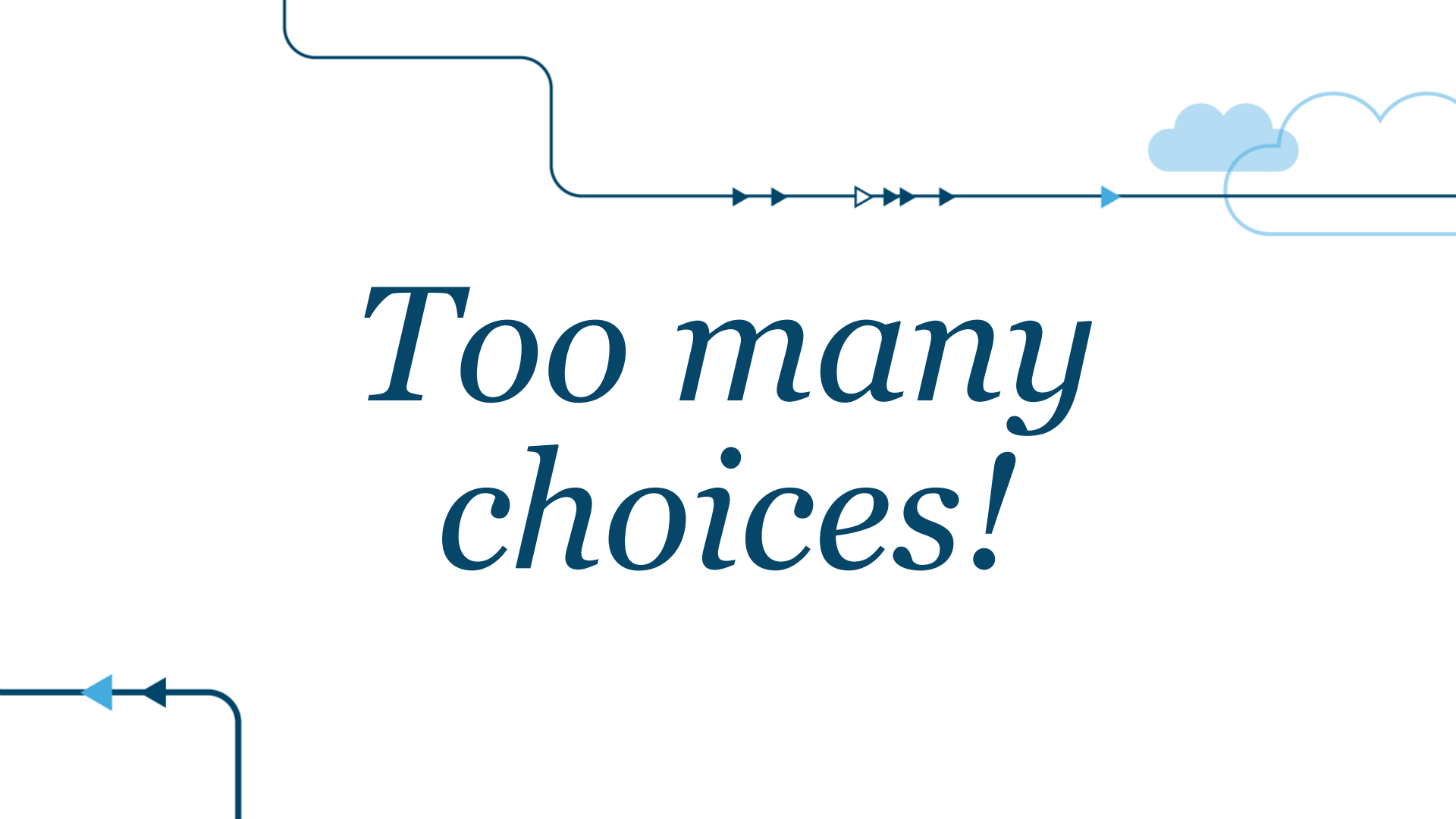
A can talk to B
B can talk to C
A must not talk to C

Y and Z failure modes must be independent so X can always succeed



Availability requirements drive a need for distributed segmentation

Choices?


Too many
choices!

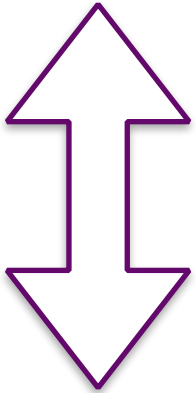
Over-reliance on one mechanism leads to abuse...

Lack of coordination across many mechanisms leads to fragility

Example segmentation mechanisms

Disclaimer:
I'm not a developer, I don't have hands-on experience with any of these mechanisms, I'm looking for input where I'm wrong or missed something.

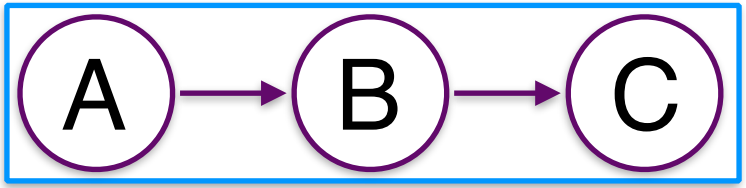
Also, apologies if I didn't namecheck your favorite project/product.



Datacenters/AWS Accounts
IAM/AD/LDAP Roles
VPC/VLAN Networks
Security Groups/Hypervisor
IPtables/Calico Policy
Docker Links/Weave Overlay

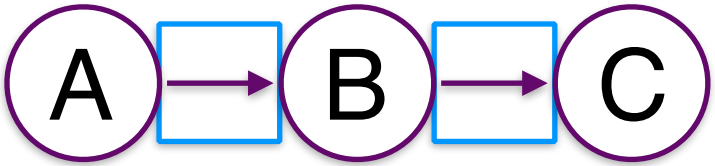
Accounts and Roles

Who can set policy for what?
Needs distributed policy management



Network Segmentation

Who controls the network?



Network Segmentation

Datacenter policies are based on separation of duties. Tickets, Network admins and VLANs

Network Segmentation

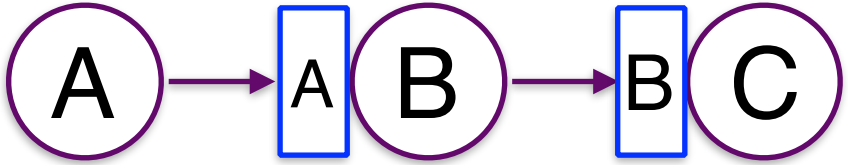
AWS VPC networking uses developer-driven automation, loses separation of duties…

VPC Abuse Antipattern

Lots of small VPC networks for microservices, end up in IP address space capacity management hell...

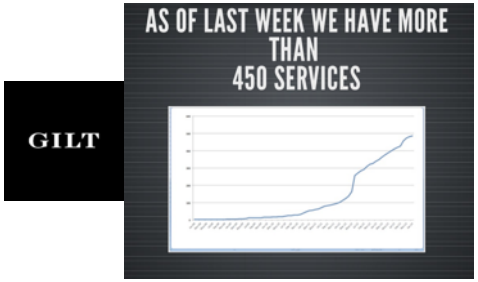
Hypervisor and Security Group Segmentation

Distributed firewall rules



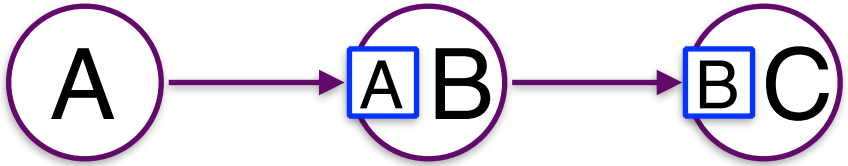
Security Group Abuse Antipattern

Too many microservices need to be in the same group, overloads configuration limitations



Kernel eBPF & Calico IPtables Segmentation

Distributed firewall rules

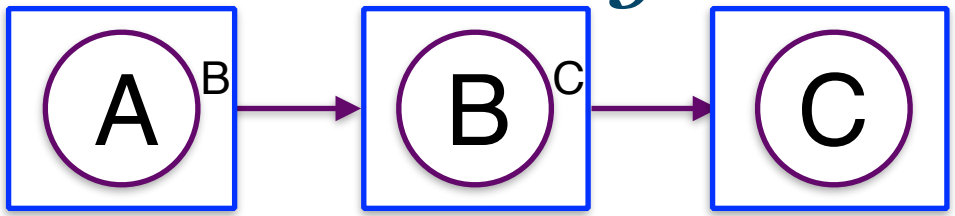


IPtables Segmentation

Can use IP Sets to scale
Managed in the container host OS
Separates routing reachability from access policy

Docker & Weave Segmentation

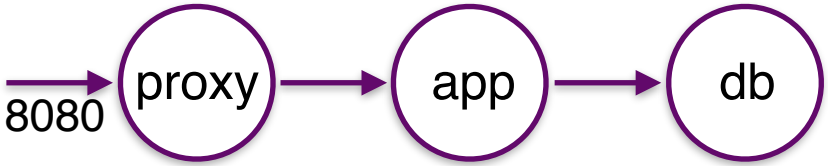
Docker daemon manages connections



Docker Compose V1

```
proxy:
  build: ./proxy
  ports:
    - "8080:8080"
  links:
    - app
app:
  build: ./app
  links:
    - db

db:
  image: postgres
```

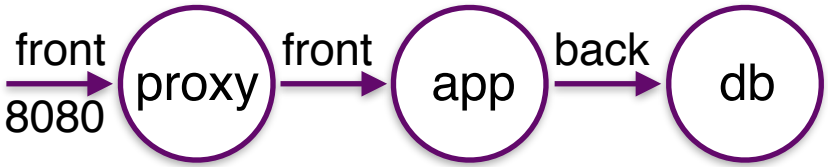


Docker Compose V2

```
version: '2'

services:
  proxy:
    build: ./proxy
    ports:
      - "8080:8080"
    networks:
      - front
  app:
    build: ./app
    networks:
      - front
      - back
  db:
    image: postgres
    networks:
      - back

networks:
  front:
  back:
```



Docker Segmentation

Overlay network created and managed by Docker or Weave.
DNS based lookups.

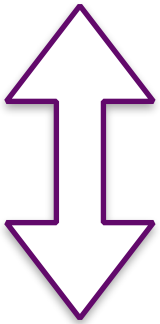
Segmentation Scalability

Real world microservices architectures have hundreds to thousands of distinct microservices

Segmentation Scalability

There's often a few very popular microservices that everyone else wants to talk to

How to coordinate across all these layers?

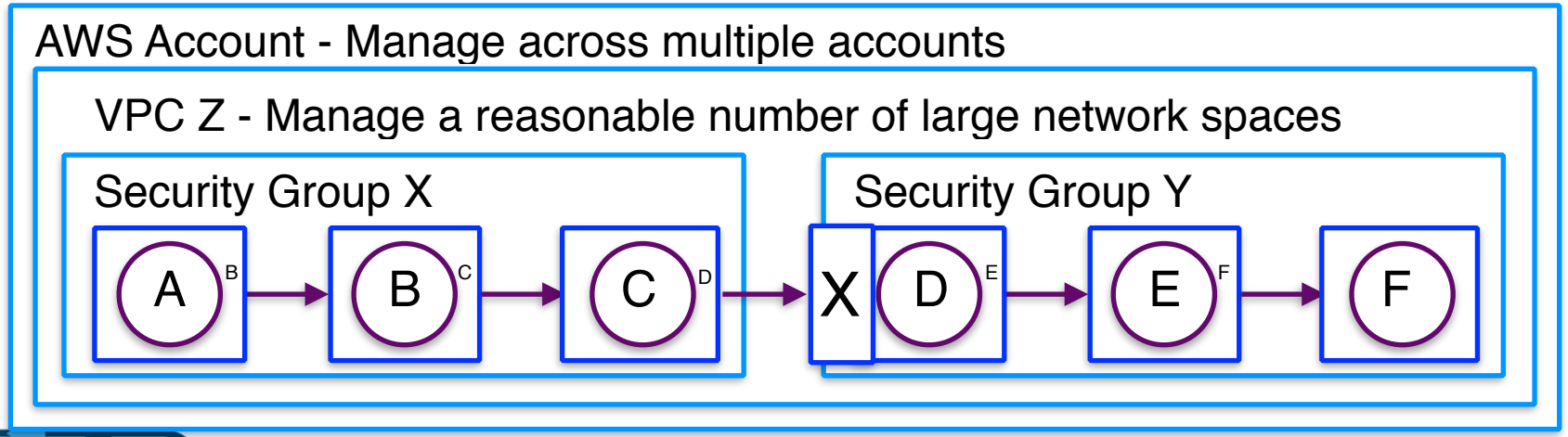


Datacenters/AWS Accounts
IAM/AD/LDAP Roles
VPC/VLAN Networks
Security Groups/Hypervisor
IPtables/Calico Policy
Docker Links/Weave Overlay

How to scale to 1000+ segments?

Hierarchical Segmentation

Enforced by IAM roles at every level



An AWS oriented example…

Policy Specification Options

How to coordinate any/all of these?

Docker Compose V2
Kubernetes/Mesos policy
Calico/Cisco Contiv
AWS IAM/AD Policies

Comments and Questions?

Adrian Cockcroft @adrianco
http://slideshare.com/adriancockcroft
Technology Fellow - Battery Ventures

See www.battery.com for a list of portfolio investments

BV
Battery Ventures

Enterprise IT

Visit http://www.battery.com/our-companies/ for a full list of all portfolio companies in which all Battery Funds have invested.