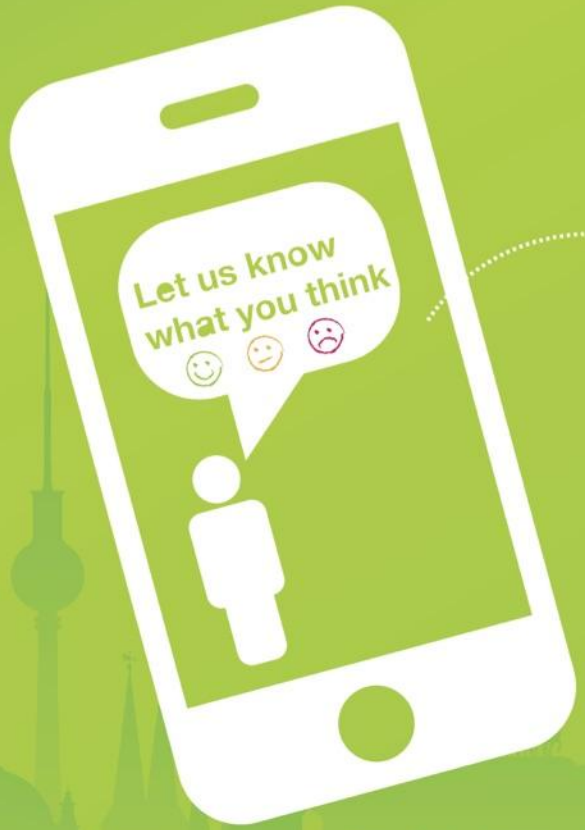
goto; conference



Click ‘Rate Session’

Rate **10** sessions to get the supercool GOTO reward

Follow us on Twitter @GOTOber

www.gotober.com

Phil Winder

Freelance Engineer
@DrPhilWinder

SECURE MY SOCKS

Exploring Microservice Security in an Open Source Sock Shop

For online orders, we accept MC, Visa, AMEX, Discover and PayPal

For mail orders, we accept check or money order

Problems with this website? Contact sock-locks@comcast.net

SOCK LOCKS

Distributed by GRT Online Promotion, LLC

Save Money! Save Socks!
Simplify your life with Sock Locks!

Read about Sock-Locks in the news!

Use Sock-Locks when you take off your socks and before putting them in the hamper. When the wash is done, simply remove the sock-lock and put your socks away or store your socks with the sock-lock on.

Also called Sock Holders, Sock Sorters, Sock Clips, Sock Rings, Sock Organizers. Doubles also sold under the names Loc-a-Sok and Sok-a-Lok.

We carry Doubles Packs and Mixed Packs of Singles and Doubles

Buy Now!

Buy Wholesale!

- **Perfect for keeping similar color (but not exactly matching) socks separate.**
- **Each member of your household could use a different color to make sorting laundry a breeze.**
- **Fewer lost and mismatched socks saves you money!**
- **Great for campers and college students.**


BBC

1.
Context

Security, PCI, devops

PCI

Who has to concern themselves with PCI compliance?

PCI Compliance Tactics (Dev)

Trust?

Assume trust, then audit like crazy

Don’t Trust?

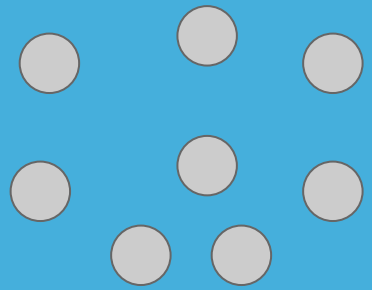
???

Top Tip

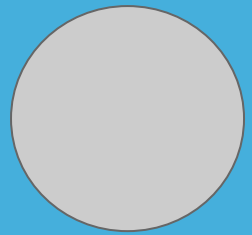
Limit the surface area

Limiting the surface area

Large surface area



Small surface area



“

PCI compliance does not mean your application is secure

Funnies

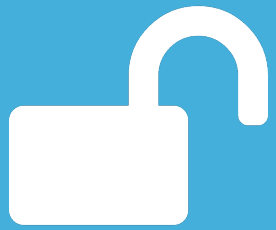
Why is docker swearing at me? (self.docker)
submitted 9 days ago * by Rkozak

I was logging into Docker hub from my Docker For Windows: Version 1.12.3-beta29.2 (8280) when I mistyped my password.

PS D:\> docker login
Login with your Docker ID to push and pull images from Docker Hub. If you don't have a Docker ID, head over to https://hub.docker.com to create one.
Username (robertkozak):
Password:
Error response from daemon: Get https://registry-1.docker.io/v2/: unauthorized:
incorrect username or password fuck you

FYI:the "fuck you" is not what I typed for password so it is not echoing back at me.

UPDATE: it is not happening anymore.



SECURITY IS HARD

Failure exploration is the beginning

One example Failure Exploration

Network segmentation and policy, Container security, Orchestrator Security

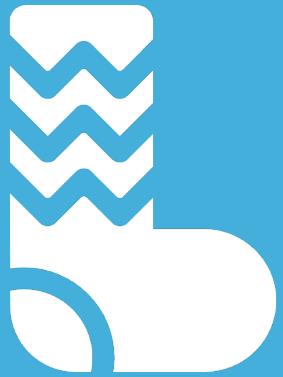
Application Security, External threats

Backup security, Organisational issues, Responsibility issues, ...

If you read this then you've read too far

Today

- Container security
- Network segmentation and policy



SOCK SHOP

An open source reference microservices architecture

Icon by http://www.flaticon.com/authors/freepik

OFFER OF THE DAY Buy 10 socks, get a pet human for free!

Login

weaveworks socks

HOME CATALOGUE

0 items in cart

WE LOVE SOCKS!

Fun fact: Socks were invented by woolly

BEST PRICES

We price check our socks with trained monkeys

100% SATISFACTION GUARANTEED

git.io/sock-shop

github.com/microservices-demo/**microservices-demo**

2.
Container Security

Container-level security aspects

- Restraint
- Immutability
- Provenance
- Hardened OS’s, modules and policies

MD front-end Dockerfile

```
FROM mhart/alpine-node:6.3

RUN mkdir -p /usr/src/app

WORKDIR /usr/src/app
COPY . /usr/src/app
RUN npm install

ENV NODE_ENV "production"
ENV PORT 8079
EXPOSE 8079

CMD ["npm", "start"]
```

MD front-end docker-compose

```
services:
  front-end:
    image:
weaveworksdemos/front-end:9093ed8f9be68d2497b
cb92587b01db6ac8197fe
    hostname: front-end
    restart: always
    environment:
      - reschedule=on-node-failure
    networks:
      - mynetwork
```

CONTAINER USER

So you haven’t set a USER?

MD front-end Dockerfile

```
FROM mhart/alpine-node:6.3

RUN mkdir -p /usr/src/app

WORKDIR /usr/src/app
COPY . /usr/src/app
RUN npm install

ENV NODE_ENV "production"
ENV PORT 8079
EXPOSE 8079

CMD ["npm", "start"]
```

Let’s add some nasties

```
apk add sl \
--update-cache \
--repository http://dl-3.alpinelinux.org/alpine/edge/testing/ \
--allow-untrust && \
export TERM=xterm && \
sl
```

READ-ONLY

So you’re filesystem isn’t read only?

Icon by http://flaticons.net/

MD front-end docker-compose

```
services:
  front-end:
    image:
weaveworksdemos/front-end:9093ed8f9be68d2497b
cb92587b01db6ac8197fe
    hostname: front-end
    restart: always
    environment:
      - reschedule=on-node-failure
    networks:
      - mynetwork
```

Let’s add some nasties

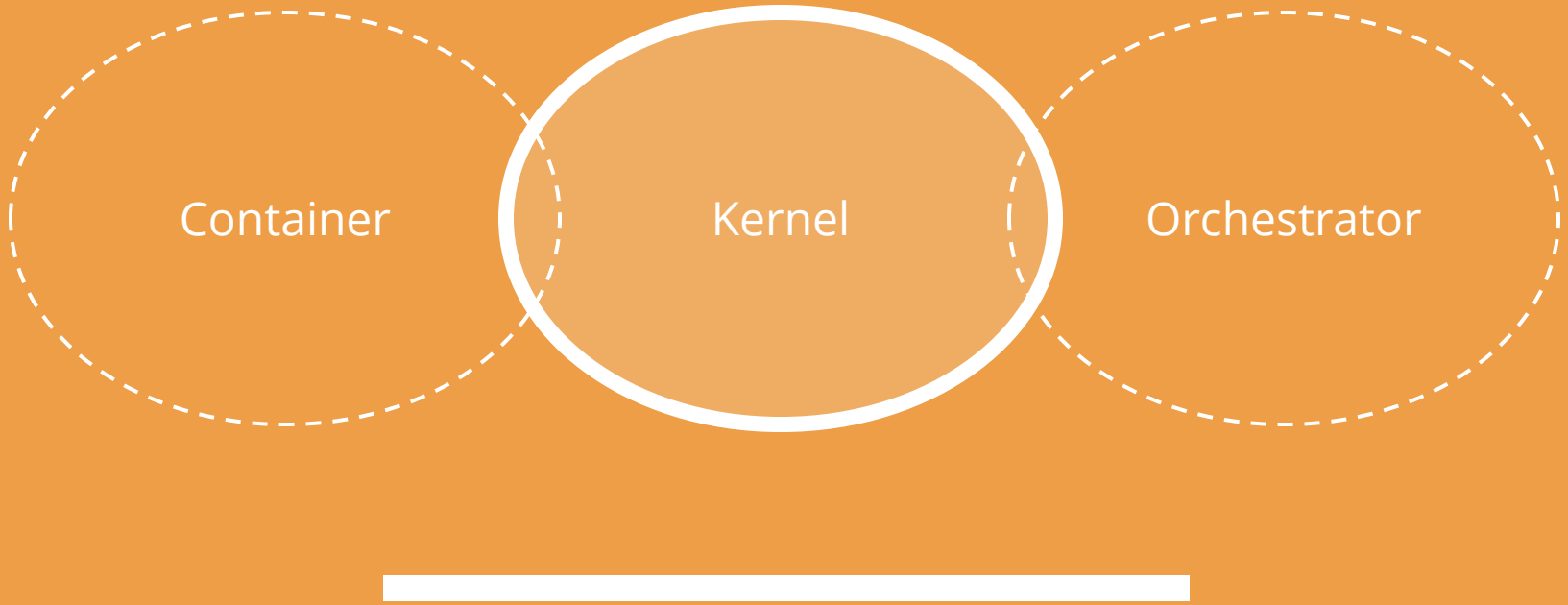
```
echo "<h1>Phil, you’re such a good presenter. Everyone is loving the talk. Even those at the back sleeping. They’re dreaming about you...</h1><img src=\"http://www.mememaker.net/static/images/memes/4395158.jpg\"/>" > public/index.html
```

Capabilities

Kernel level operation permissions


WHERE THE FUCK AM I?

Where haz caps?



MD catalogue Dockerfile

```
FROM busybox:1

EXPOSE 80
COPY app /

CMD ["/app", "-port=80"]
```

MD catalogue Dockerfile

```
FROM busybox:1
RUN  addgroup mygroup && \
     adduser -D -G mygroup myuser

USER myuser

EXPOSE 80
COPY app /

CMD ["/app", "-port=80"]
```

MD catalogue Dockerfile

```
FROM alpine:3.4

RUN  addgroup mygroup && \
     adduser -D -G mygroup myuser && \
     apk add --update libcap

EXPOSE 80
COPY app /

RUN  chmod +x /app && \
     chown -R myuser:mygroup /app && \
     setcap 'cap_net_bind_service=+ep' /app

USER myuser
CMD ["/app", "-port=80"]
```

MD docker-compose

```
services:
    catalogue:
    ...
        cap_drop:
          - all
        cap_add:
          - NET_BIND_SERVICE
        read_only: true
    ...
```

MD kubernetes

```
---
...
    spec:
      containers:
      - name: catalogue
        ...
        securityContext:
          runAsNonRoot: true
          runAsUser: 10001
          capabilities:
            drop:
              - all
            add:
              - NET_BIND_SERVICE
          readOnlyRootFilesystem: true
```

The result?

```
apk add sl \
--update-cache \
--repository http://dl-3.alpinelinux.org/alpine/edge/testing/ \
--allow-untrust && \
export TERM=xterm && \
sl

echo "This won’t work" > public/index.html

grep Cap /proc/self/status
```

Top Tip

User, read-only, caps.

11,788

People taken to hospital following accidents while putting on socks, tights or stockings in the UK, 2003

5-10

People die each year putting on socks in the UK

3.

Network Segmentation and Policy

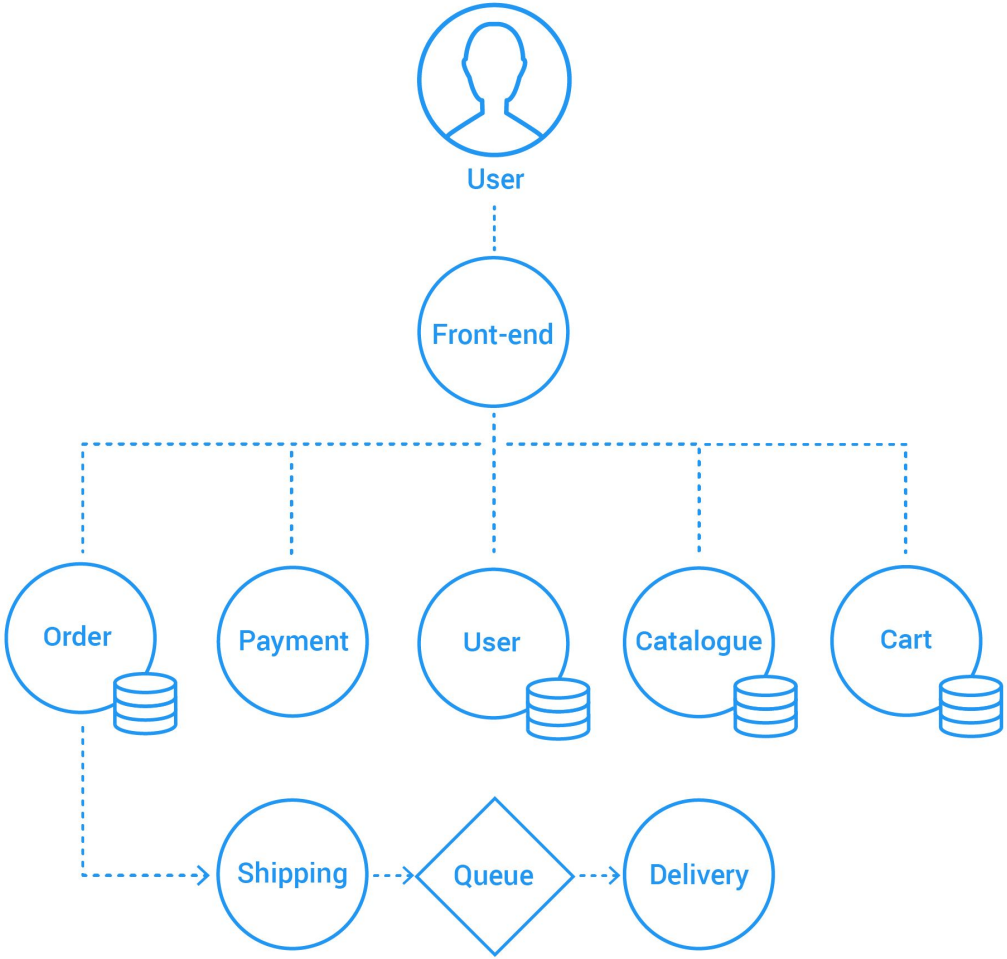
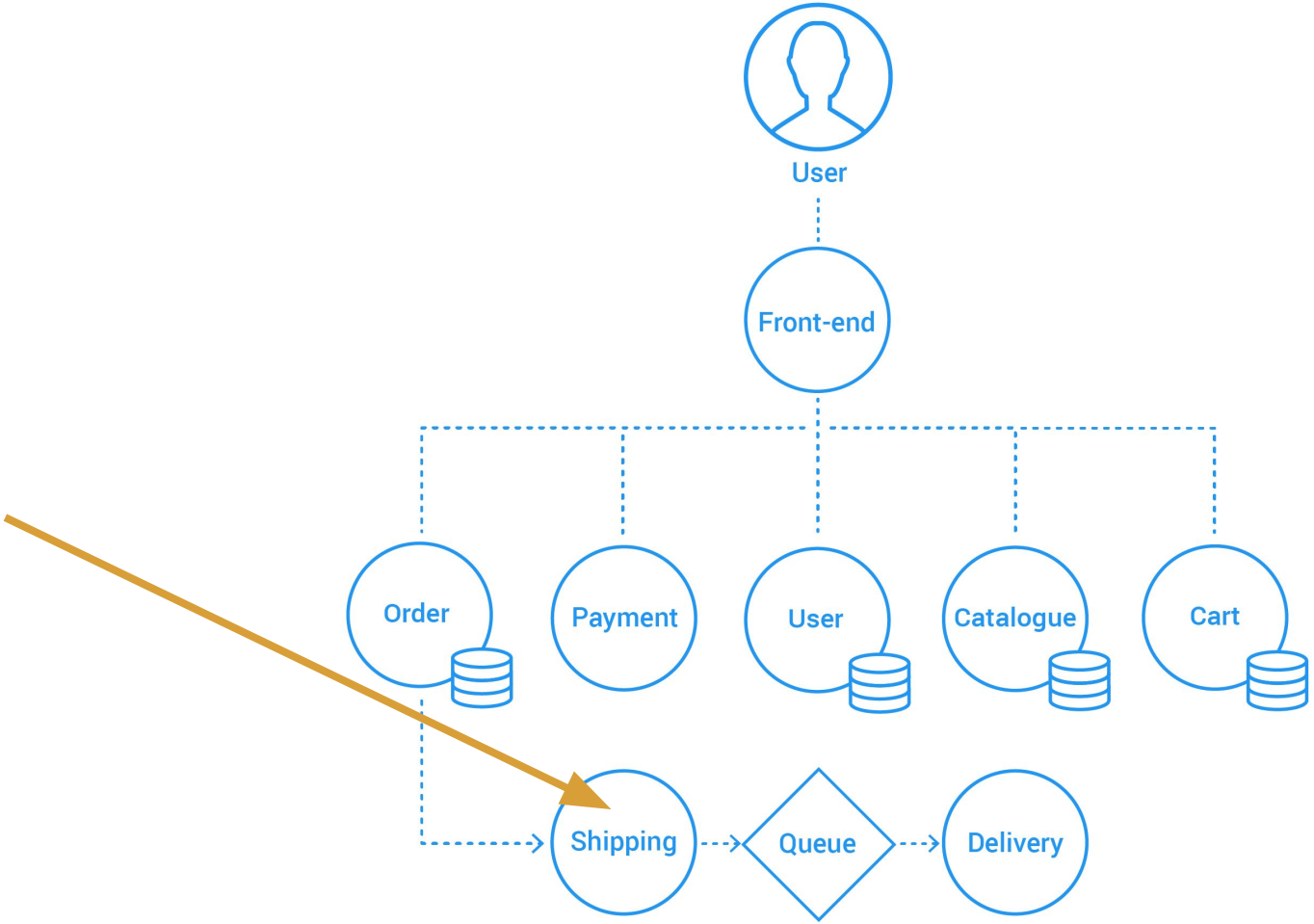
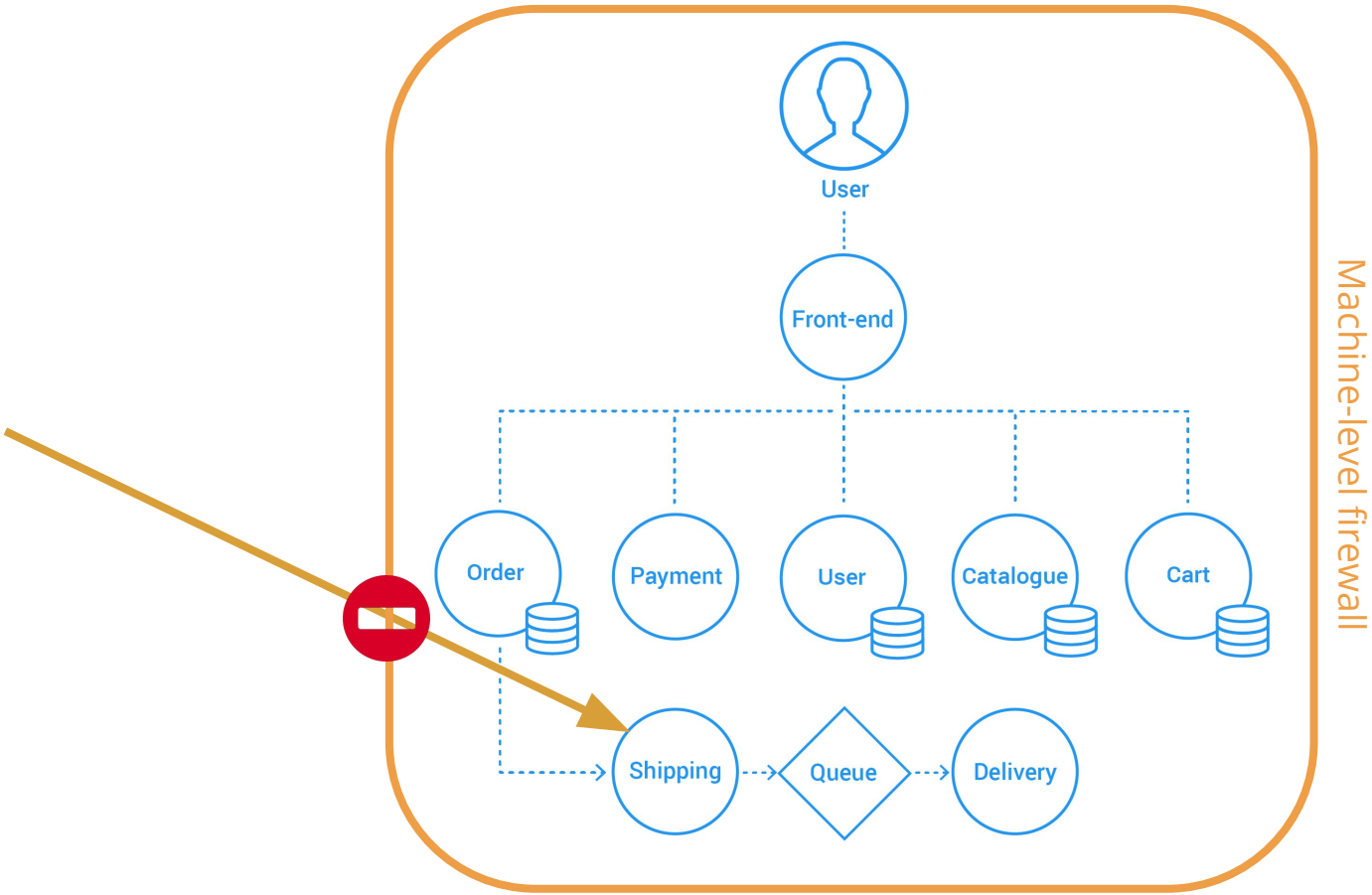


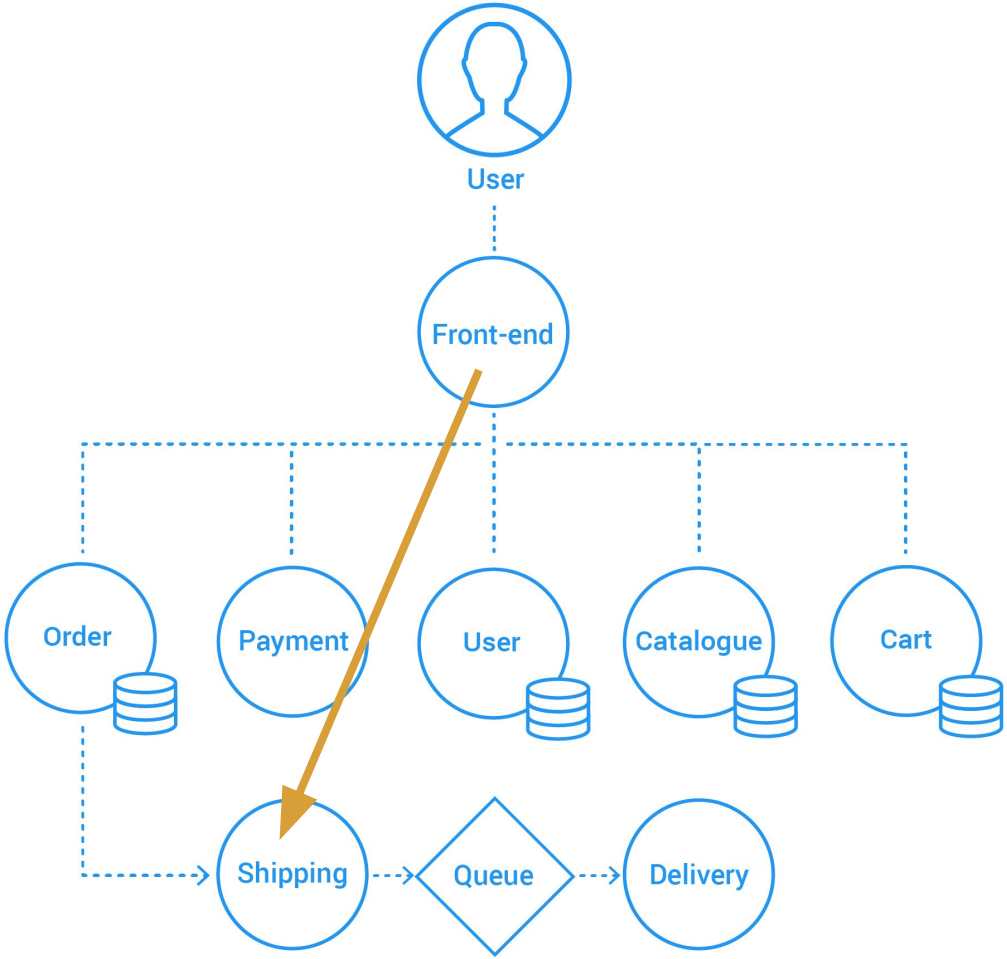
Image by Remember To Play


User
Front-end
Order
Payment
User
Catalogue
Cart
Shipping
Queue
Delivery

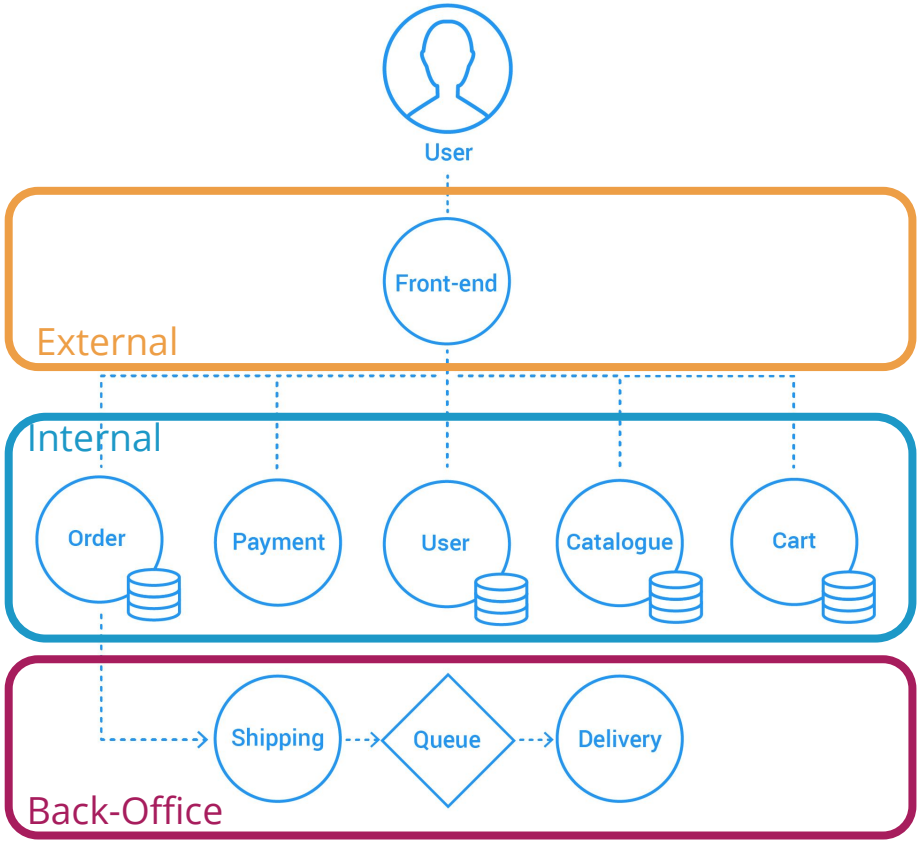

LOOK, ALL I'M SAYING IS
WE NEED TO BUILD A BIGGER FIREWALL
imgflip.com

Trump's Firewall



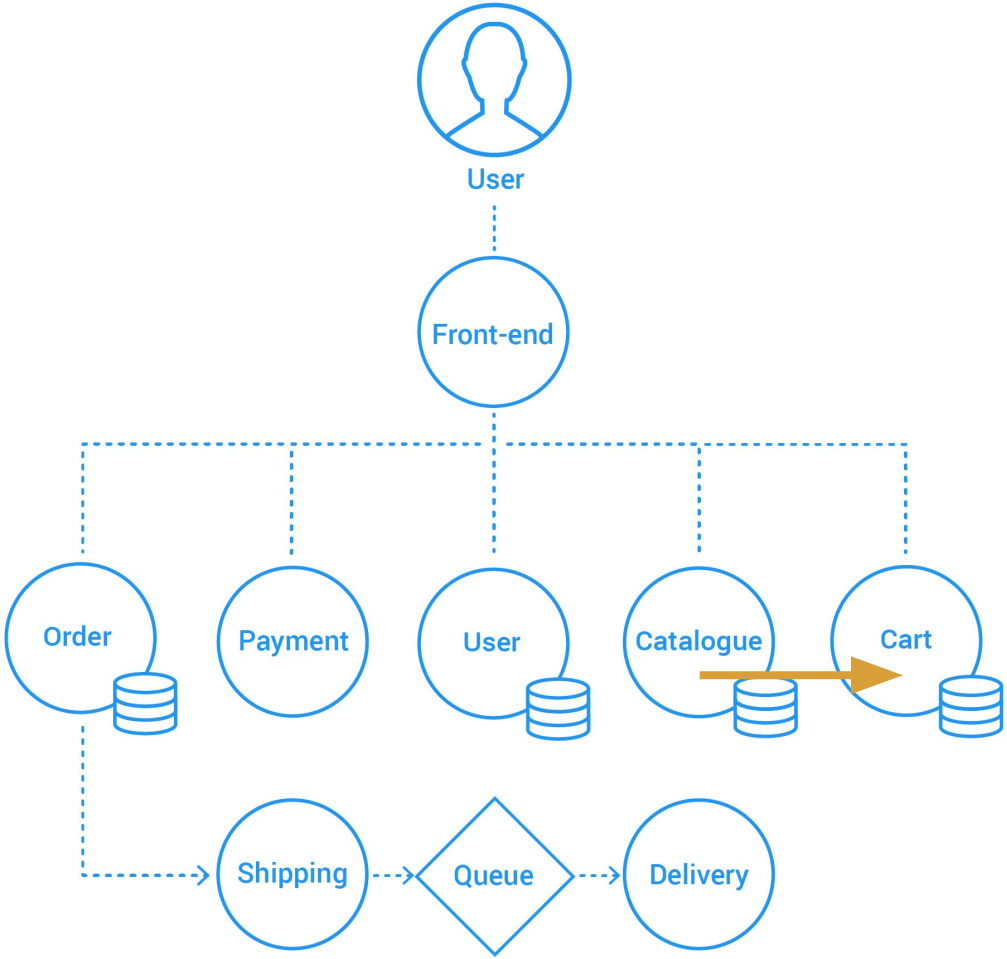

User
Front-end
Order
Payment
User
Catalogue
Cart
Shipping
Queue
Delivery

Network Segmentation

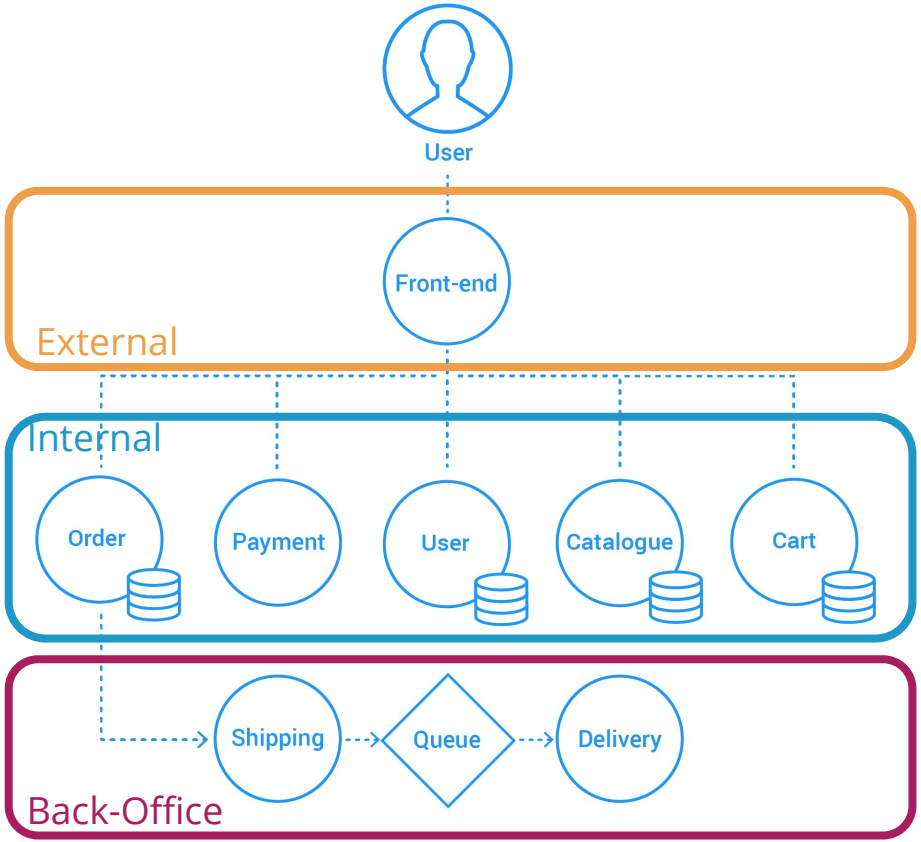


Shipping docker-compose

```
shipping:
  image: weaveworksdemos/shipping
  hostname: shipping
  ...
  networks:
    - backoffice
```


User
Front-end
Order
Payment
User
Catalogue
Cart
Shipping
Queue
Delivery

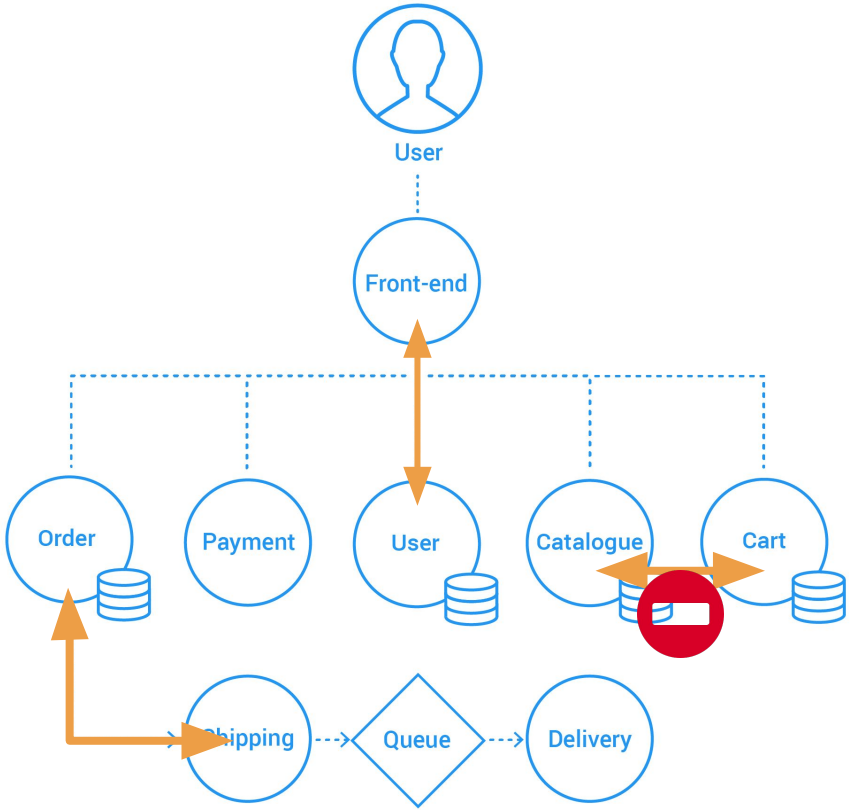
Network Segmentation



“

A Network Policy is like a bouncer that doesn’t let you in, just because you’re wearing shorts

Network Policy



Shipping K8s Network Policy

```
---
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: shipping-access
  namespace: sock-shop
spec:
  podSelector:
    matchLabels:
      name: shipping
  ingress:
    - from:
        - podSelector:
            matchLabels:
              name: orders
      ports:
        - protocol: TCP
          port: 80
```

Top Tip

You need a software defined network

4.
Wrap up

Let's review some concepts

User

Set a user in your Dockerfiles so they don't run as root

Immutable

Make the root container file system read only

Restraint

Prevent unauthorised execution

Global firewall

Block everything, minimise the surface area

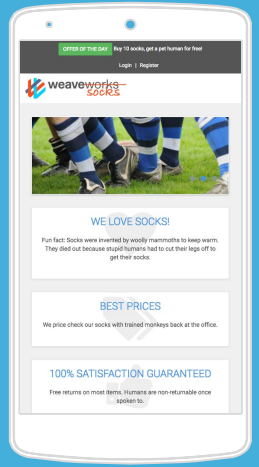
Network Segmentation

Prevent inter-network access

Network Policy

Be a bouncer, tell your containers who's allowed access

WHERE?



git.io/sock-shop

github.com/microservices-demo/**microservices-demo**

Go, try, star, contribute

DONE!

Any questions?

Contact me at:
@DrPhilWinder
phil@winderresearch.com
http://winderresearch.com

goto; conference

Please

Remember to rate session

Thank you!

Follow us on Twitter @GOTOber

www.gotober.com