Defense In Depth

Building networks that survive first contact

BSides Delaware 2012

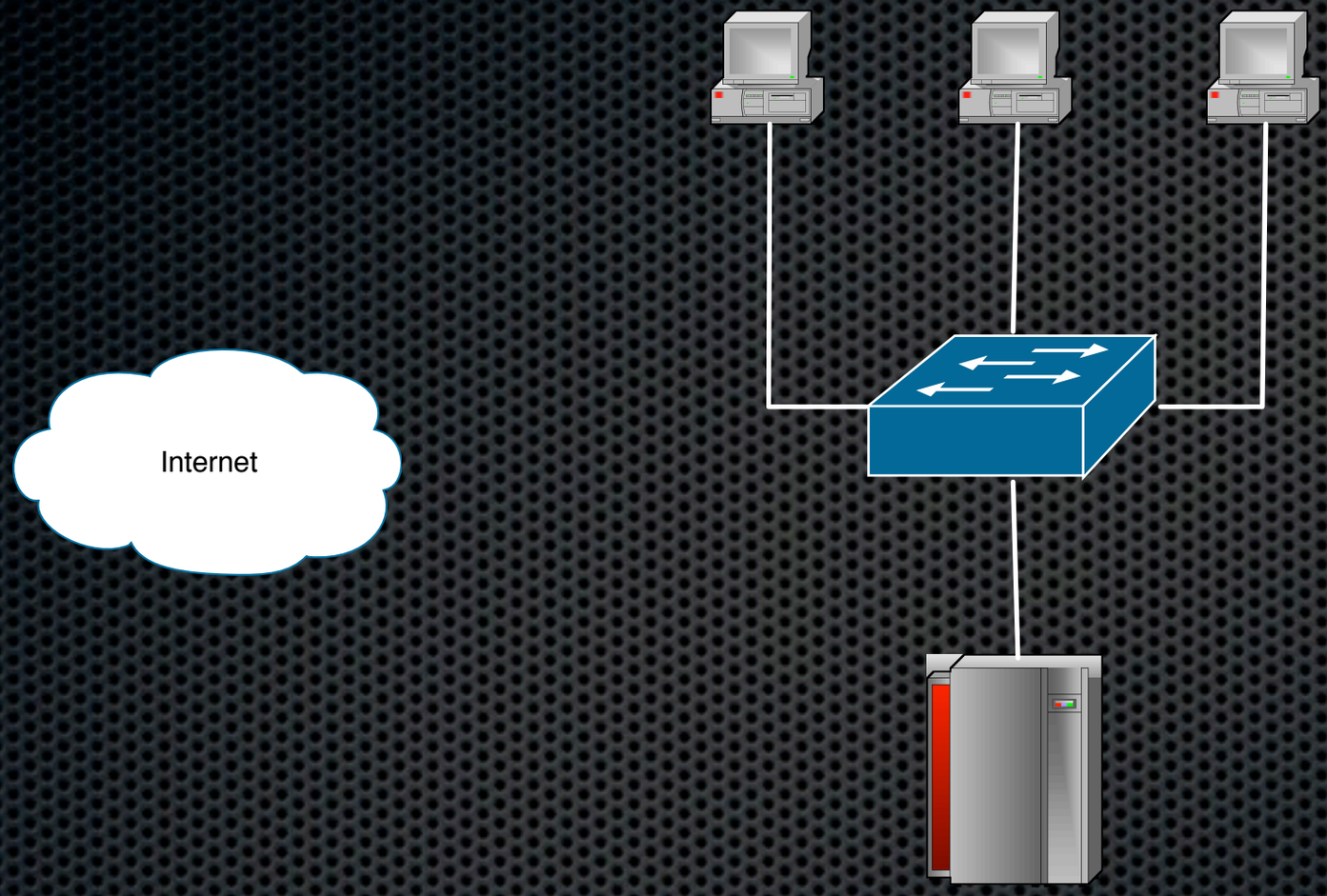
Who the hell is this guy?

- Not a security guy
- Hi, I'm Jason Frisvold
- Senior Network Engineer, Lafayette College
- But if I'm not a "security" guy, WTF am I here for?
- Like you, I'm here to learn

friz@godshell.com
@XenoPhage

Let’s start with a story

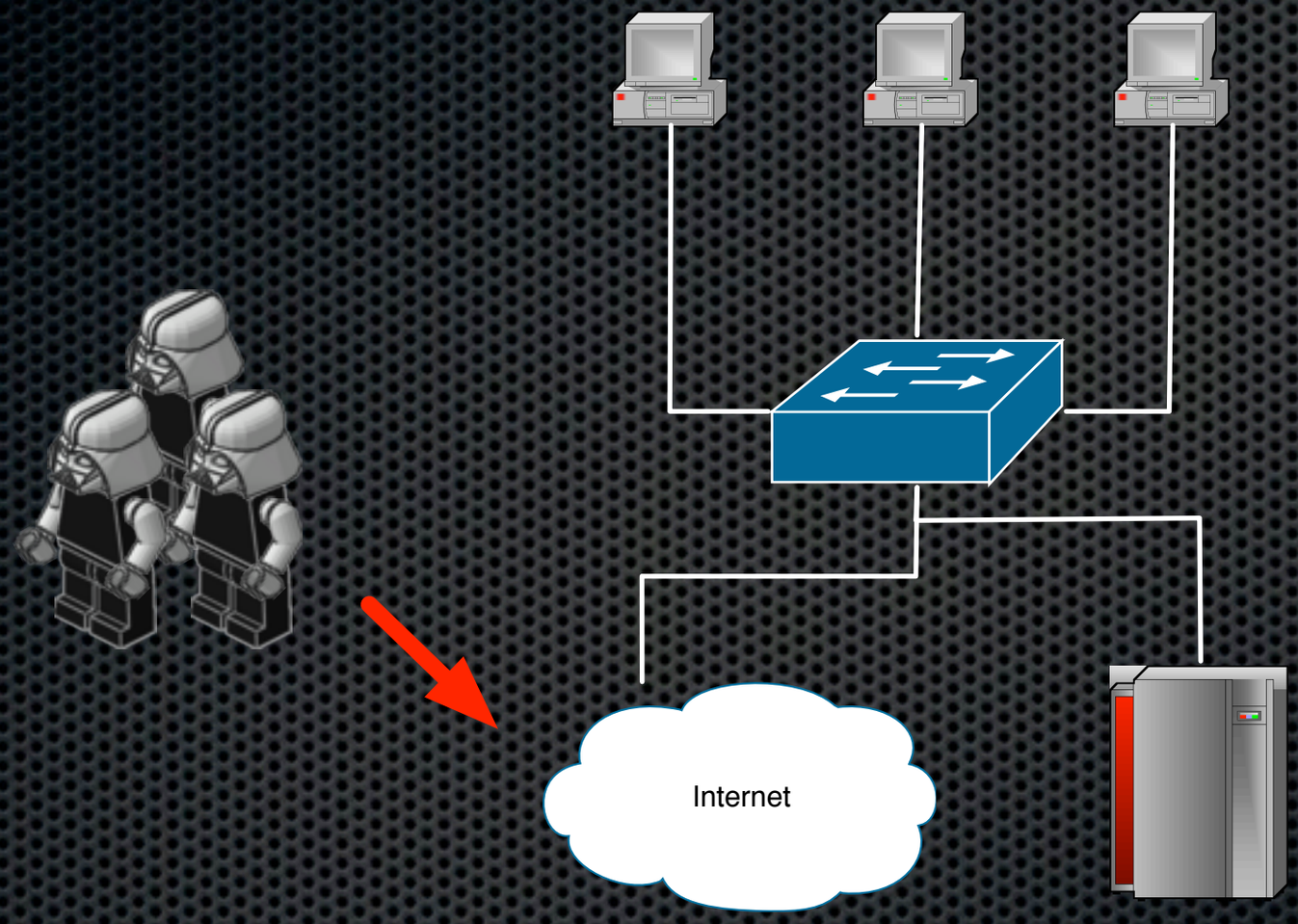
Once Upon A Time ...



It was a dark and stormy night.

And then another time.

So, we connected.



And so did they ...

802.1x

Firewalls

Routers

NAC

Traffic Shaping

WAF

Netflow

And the race was on

DPI

IPS

DLP

IDS

Anomaly Detection

What if we started with a clean slate?

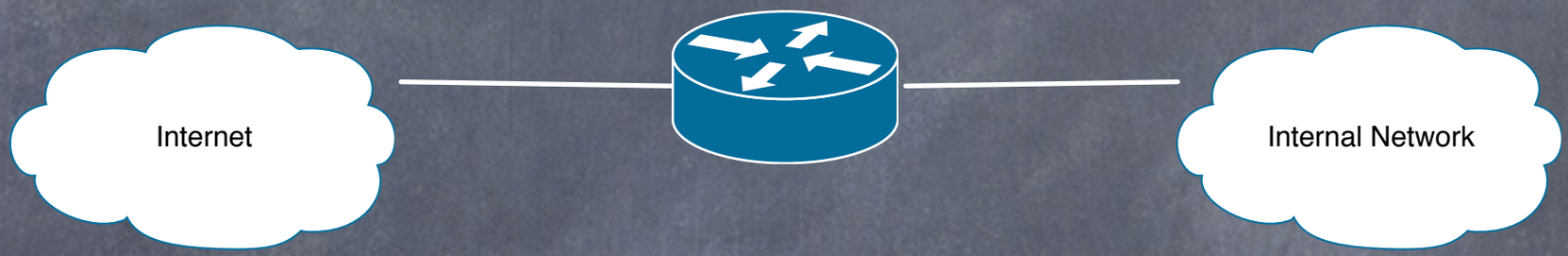
What if we started with a clean slate?

What could we do differently?

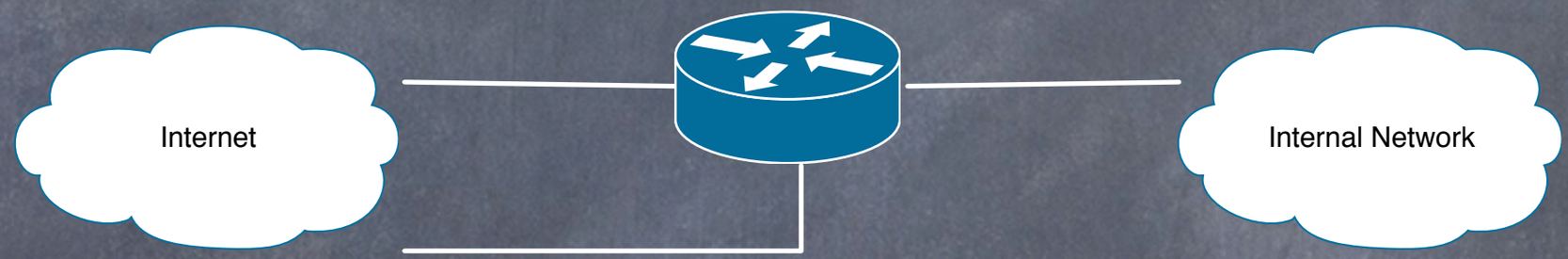
Some Basic Principles

- Redundancy and Resiliency
- Network Segmentation
- Principle of least privilege
- Monitoring
- Security

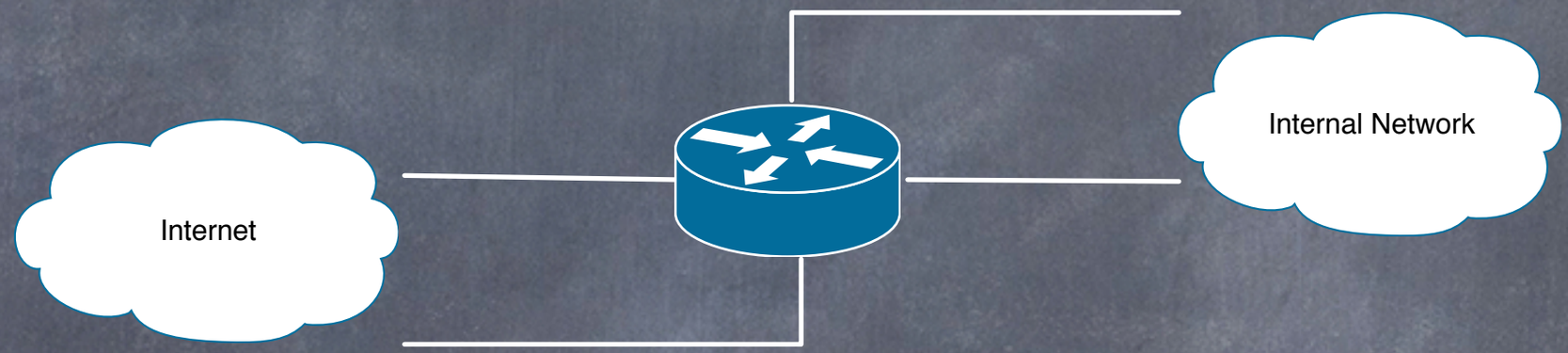
Redundancy & Resiliency



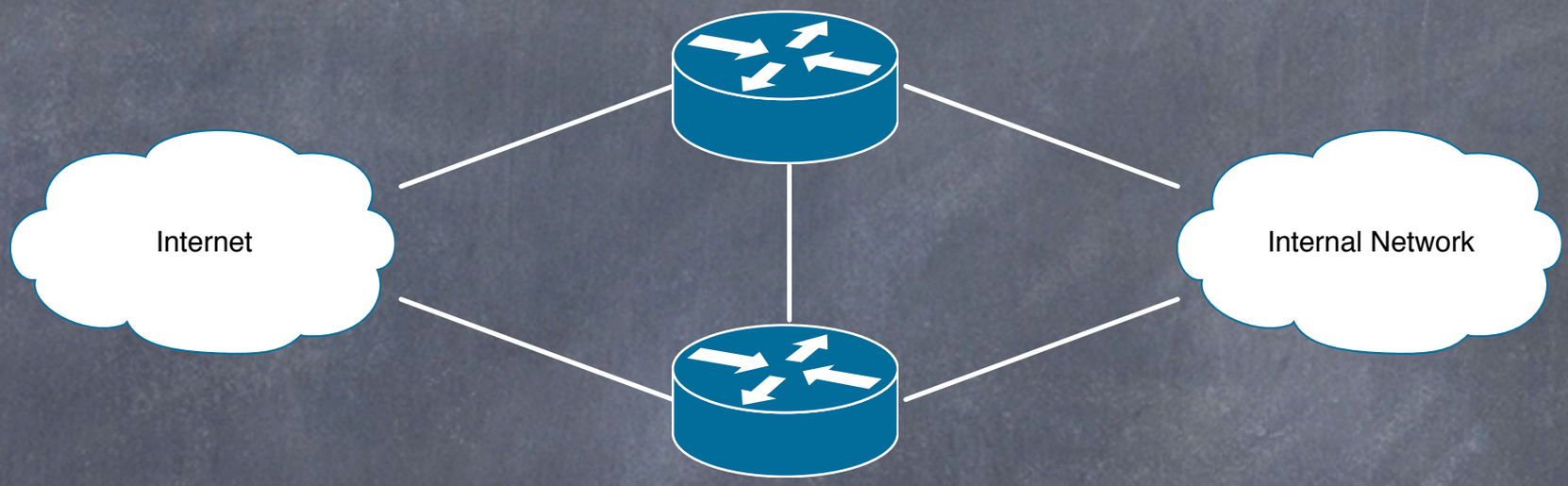
Redundancy & Resiliency



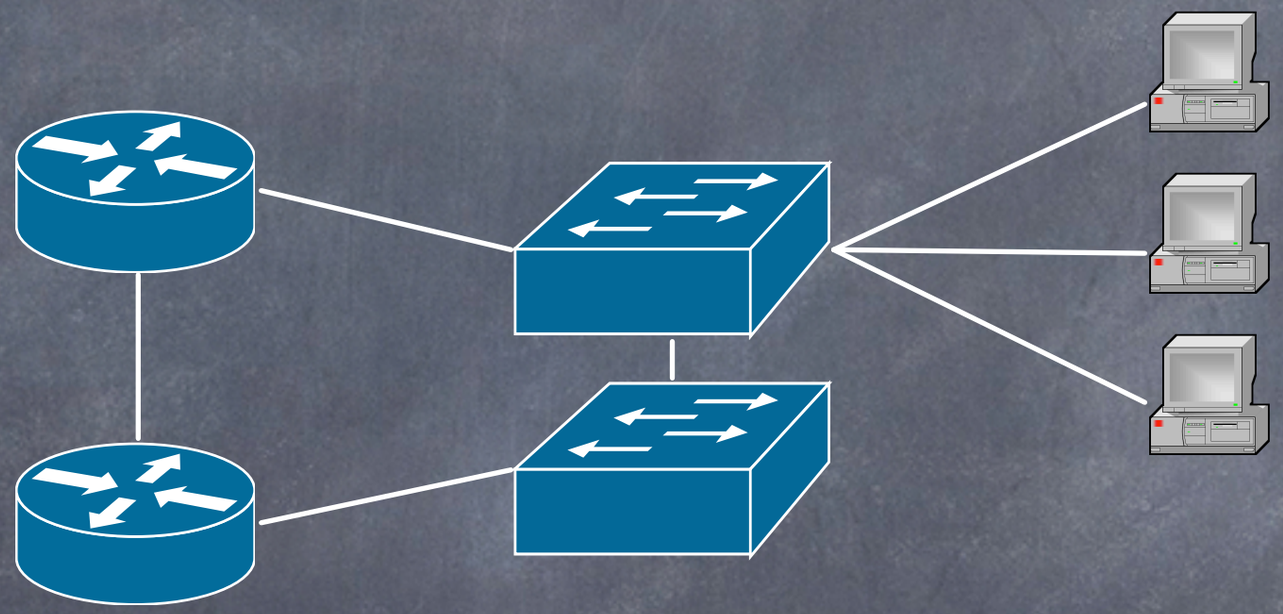
Redundancy & Resiliency



Redundancy & Resiliency



Redundancy & Resiliency



Redundancy & Resiliency

Other areas?

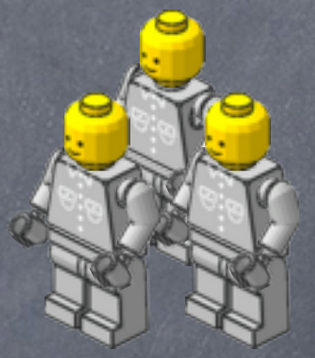
Audience Participation Time !

Network Segmentation

Sales

Tech Support

Marketing



Engineering

Web Servers

Security

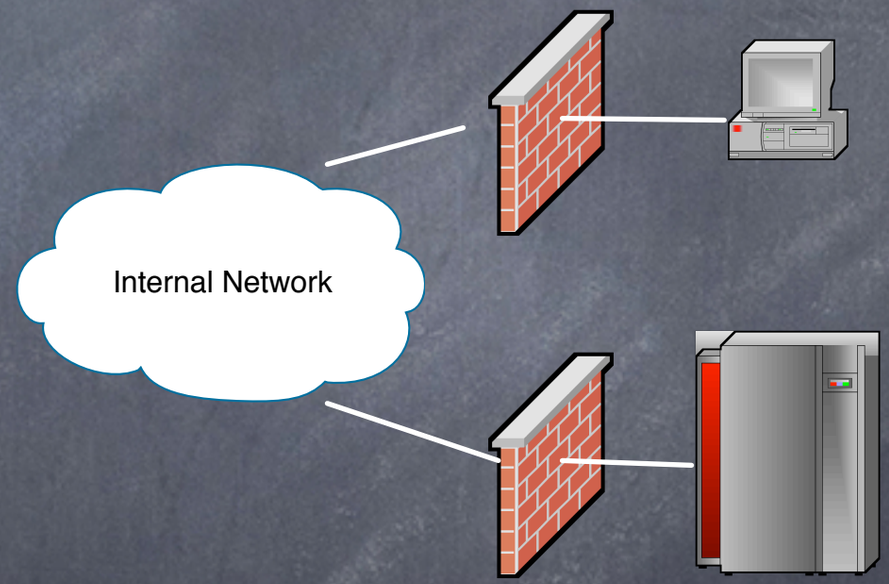
Databases

Network Segmentation

- Some questions to ask :
  - Where does it belong?
  - What access does it need?
  - How do we decide?
- It's OK to add new networks
- But don't go overboard...

Principle of Least Privilege

- At the network level?
- But, how?
- What about a firewall?
- Really least privilege?



Principle of Least Privilege

How else?
Audience Participation Time !

Monitoring

- Part of network building?
- ABSOLUTELY!
- Insight into what's going on
- EXTREMELY useful for troubleshooting
- Historical data
- Oh yeah, and security too...

Monitoring

- Really Awesome New Cisco confIg Differ (RANCID)
- Simple Network Monitoring Protocol (SNMP)
- Traps (In Soviet Russia, Network Monitors You!)
- Ping!
- Syslog

Monitoring

Monitor ALL the things

Audience Participation Time !

Security

- A recap of the security we've built in :
  - Network Segmentation
  - Firewalling
  - Monitoring
  - Logging

Security

What else can we add?
Audience Participation Time!

How about those fancy toys?

Questions?

friz@godshell.com
@XenoPhage
http://www.godshell.com