



# SharkFest '18 Europe



## Packet Analysis in the Cloud

I can't see in the rain

Matthew York

Advance7



# Clouds are big and getting bigger



## Azure PaaS Services

### Compute

- EC2**  
Virtual Servers in the Cloud
- EC2 Container Service**  
Run and Manage Docker Containers
- Elastic Beanstalk**  
Run and Manage Web Apps
- Lambda**  
Run Code in Response to Events

### Storage & Content Delivery

- S3**  
Scalable Storage in the Cloud
- CloudFront**  
Global Content Delivery Network
- Elastic File System** PREVIEW  
Fully Managed File System for EC2
- Glacier**  
Archive Storage in the Cloud
- Import/Export Snowball**  
Large Scale Data Transport
- Storage Gateway**  
Hybrid Storage Integration

### Database

- RDS** Preview  
Managed Relational Database Service
- DynamoDB**  
Managed NoSQL Database
- ElasticCache**  
In-Memory Cache
- Redshift**  
Fast, Simple, Cost-Effective Data Warehousing
- DMS** PREVIEW  
Managed Database Migration Service

### Developer Tools

- CodeCommit**  
Store Code in Private Git Repositories
- CodeDeploy**  
Automate Code Deployments
- CodePipeline**  
Release Software using Continuous Delivery

### Management Tools

- CloudWatch**  
Monitor Resources and Applications
- CloudFormation**  
Create and Manage Resources with Templates
- CloudTrail**  
Track User Activity and API Usage
- Config**  
Track Resource Inventory and Changes
- OpsWorks**  
Automate Operations with Chef
- Service Catalog**  
Create and Use Standardized Products
- Trusted Advisor**  
Optimize Performance and Security

### Security & Identity

- Identity & Access Management**  
Manage User Access and Encryption Keys
- Directory Service**  
Host and Manage Active Directory
- Inspector** PREVIEW  
Analyze Application Security
- WAF**  
Filter Malicious Web Traffic
- Certificate Manager**  
Provision, Manage, and Deploy S

### Internet of Things

- AWS IoT**  
Connect Devices to the Cloud

### Mobile Services

- Mobile Hub** BETA  
Build, Test, and Monitor Mobile Apps
- Cognito**  
User Identity and App Data S
- Device Farm**  
Test Android, iOS, and Windows Devices in the Cloud
- Mobile Analytics**  
Collect, View and Export App Data
- SNS**  
Push Notification Service

### Application Services

- API Gateway**  
Build, Deploy and Manage APIs
- AppStream**  
Low Latency Application Streaming
- CloudSearch**  
Managed Search Service
- Elastic Transcoder**  
Easy-to-Use Scalable Media Processing
- SES**  
Email Sending and Receiving
- SQS**

The screenshot shows the Azure portal dashboard with a grid of service tiles. The tiles are organized into several main sections: **Security & Management** (Portal, Active Directory, Multi-Factor Authentication, Automation, Key Vault, Store / Marketplace, VM Image Gallery & VM Depot); **Compute** (Cloud Services, Service Fabric, Batch, Remote App); **Web and Mobile** (Web Apps, API Apps, API Management, Mobile Apps, Logic Apps, Notification Hubs); **Developer Services** (Visual Studio, Azure SDK, Team Project, Application Insights); **Hybrid Operations** (Azure AD Connect Health, AD Privileged Identity Management, Backup, Operational Insights, Import/Export, Site Recovery, StorSimple); **Integration** (Storage Queues, Stateful Services, Hybrid Connectors, Service Bus); **Analytics & IoT** (HDInsight, Machine Learning, Data Factory, Event Hubs, Stream Analytics, Mobile Engagement); **Data** (SQL Database, SQL Data Warehouse, Redis Cache, Search, DocumentDB, Tables); **Infrastructure Services** (Virtual Machines, Containers, Blob Storage, Azure Files, Premium Storage, Virtual Network, Load Balancer, DNS, Express Route, Traffic Manager, VPN Gateway, Application Gateway).





# Cloud causing low visibility...



- SharkFest'16:

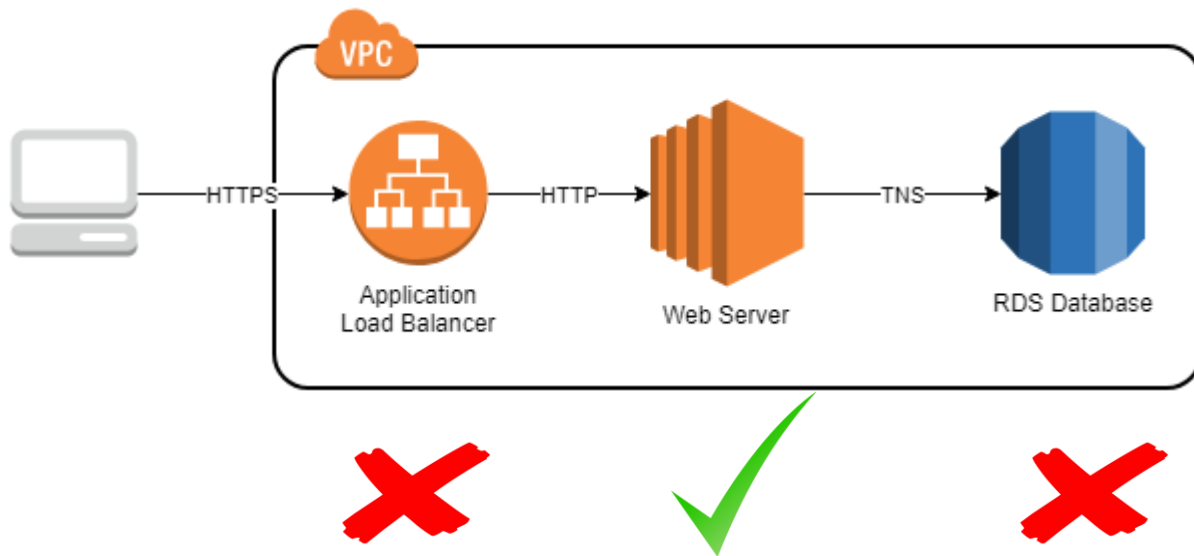
“Packet capture in the cloud is tcpdump”

- SharkFest'18 Europe:

“Packet capture in the cloud is tcpdump  
but that's OK”

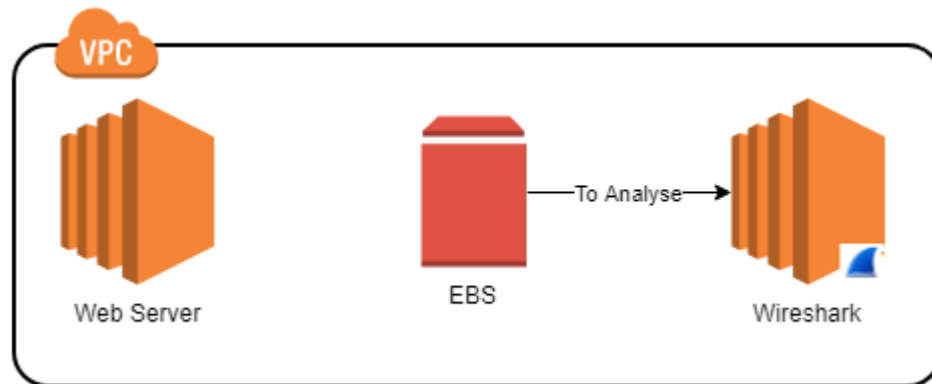
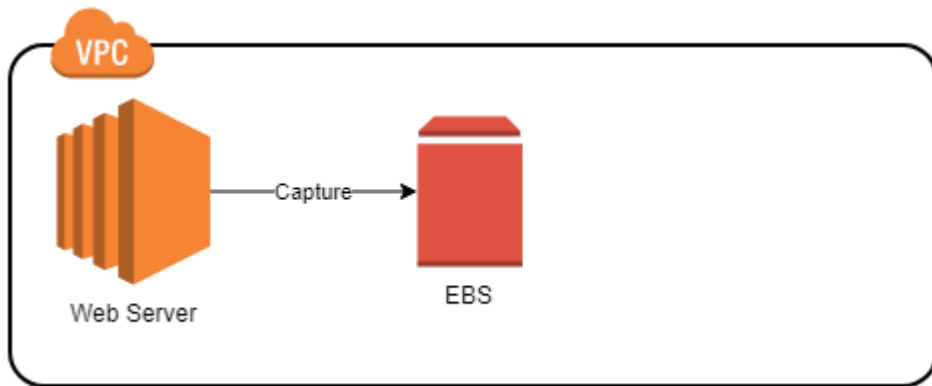


# To manage or not to manage



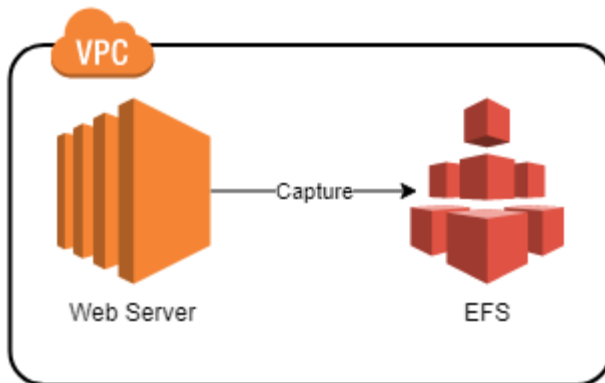


# Give me some packets





# Scale this some



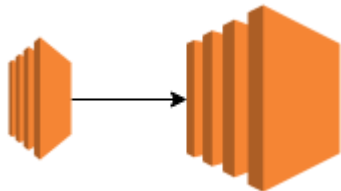
Things to Consider:  
Burst v Provision  
Lifecycle Management  
Instance Bandwidth



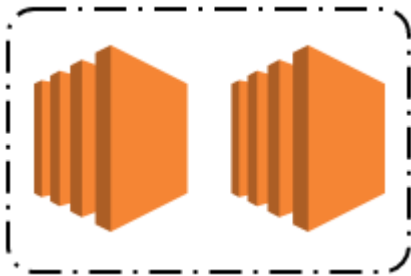
# Your captures are killing me



- You've got a bunch of options:
  - Get a bigger instance



- Use autoscaling groups

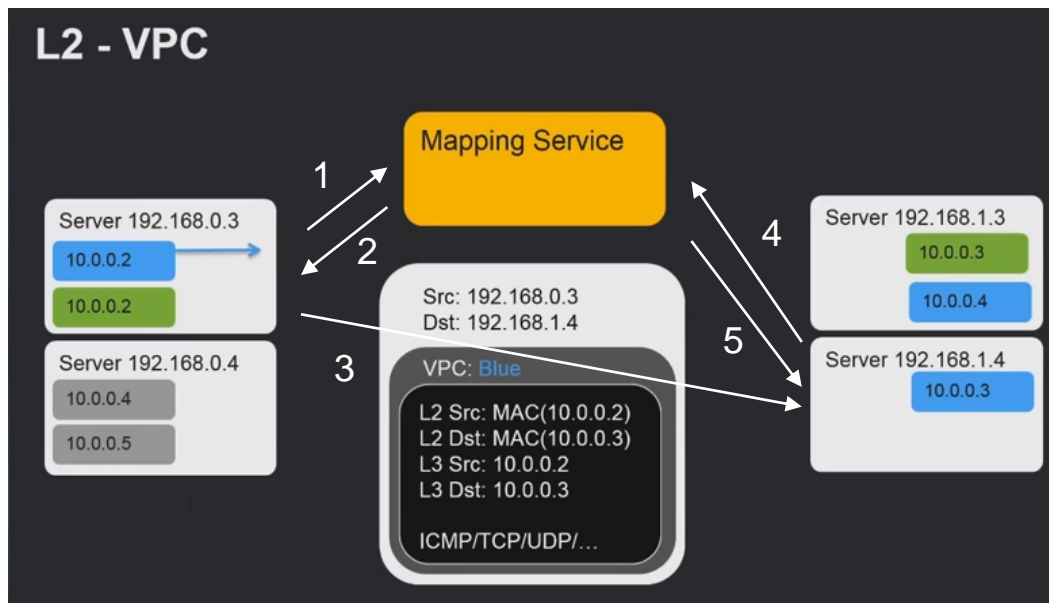




# Your captures are still killing me



- What happens in a VPC:



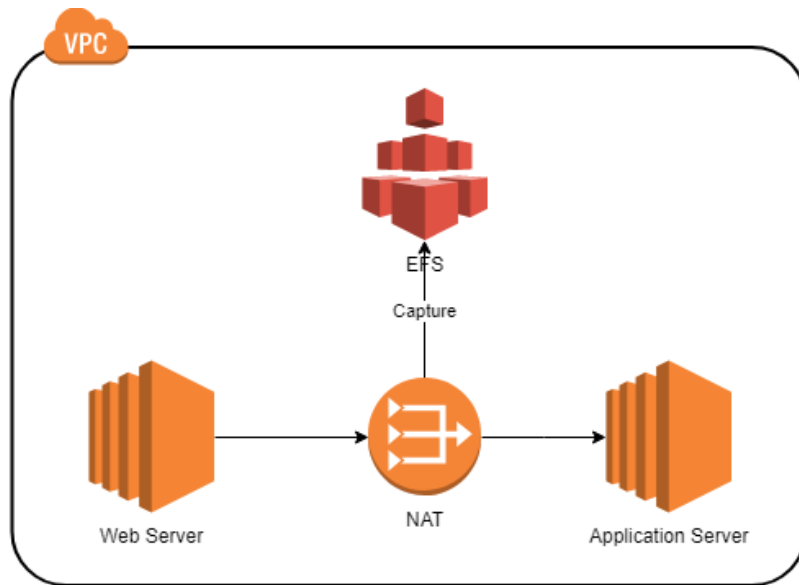




# What can we do?

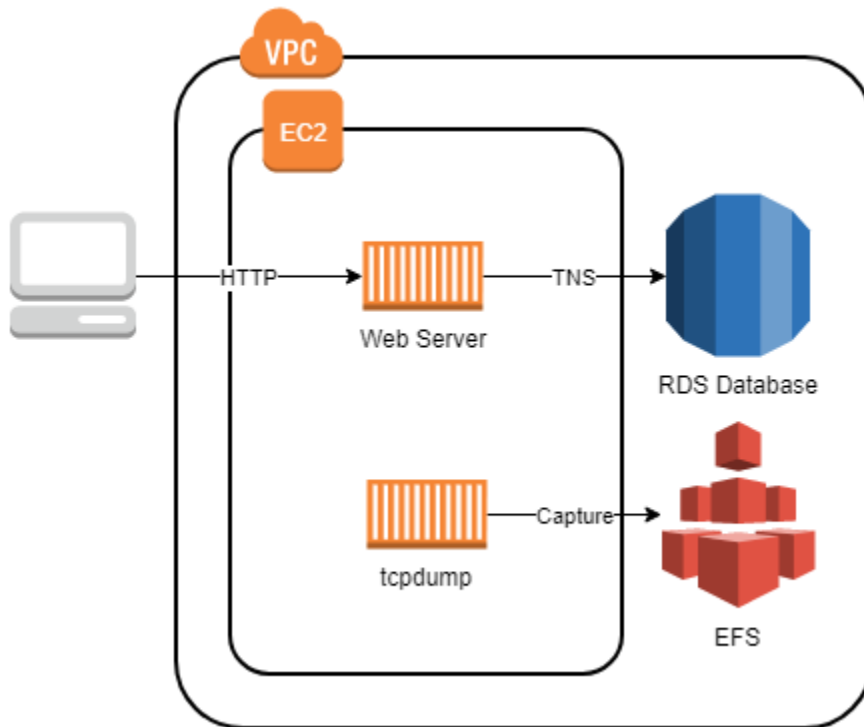
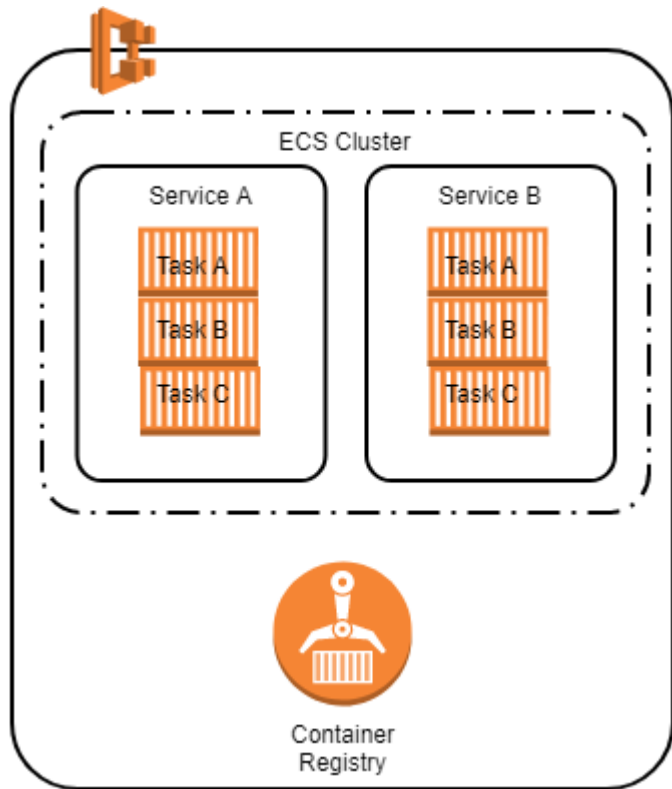


- Do some NAT'ing



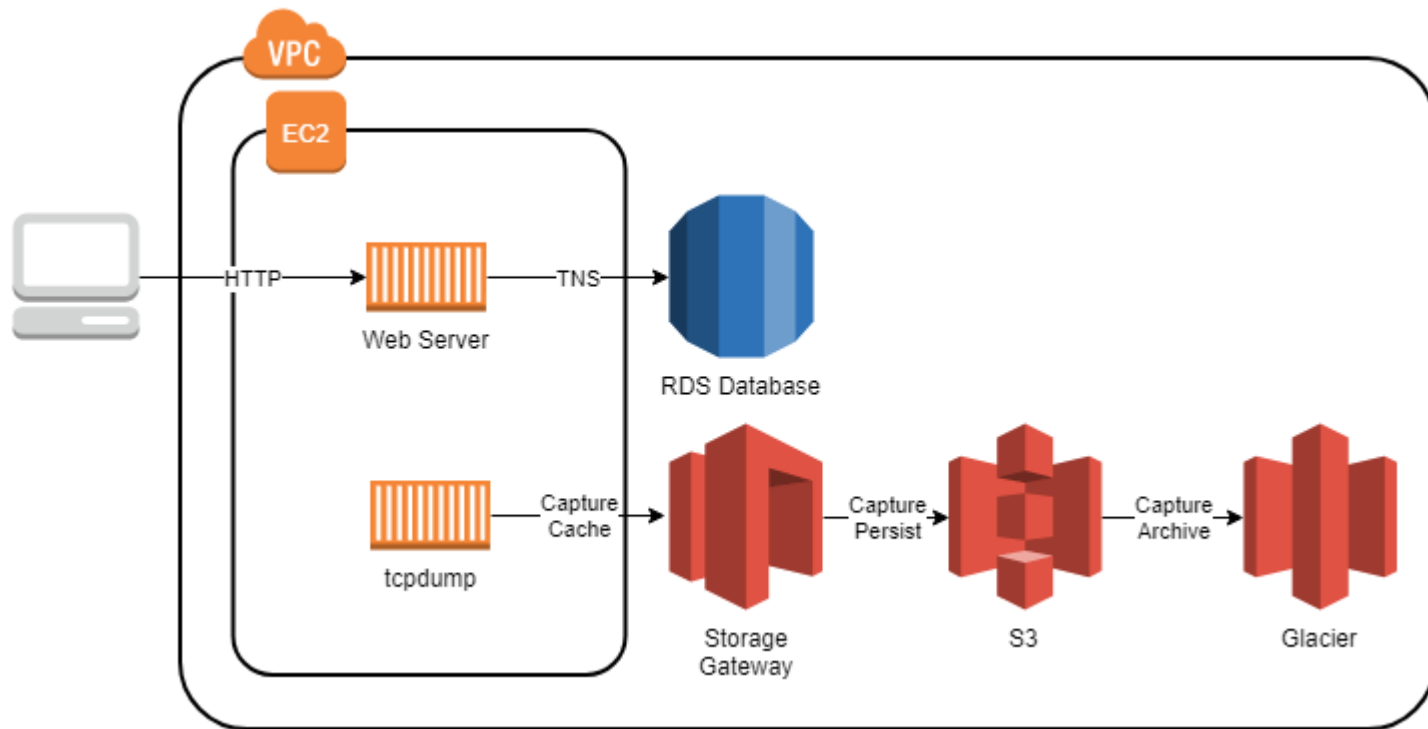


# We're using containers



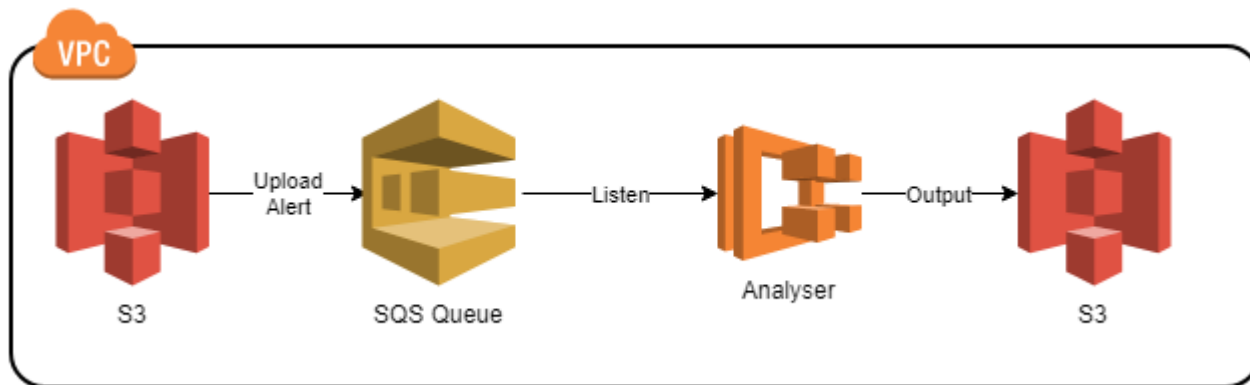


# Scale this more



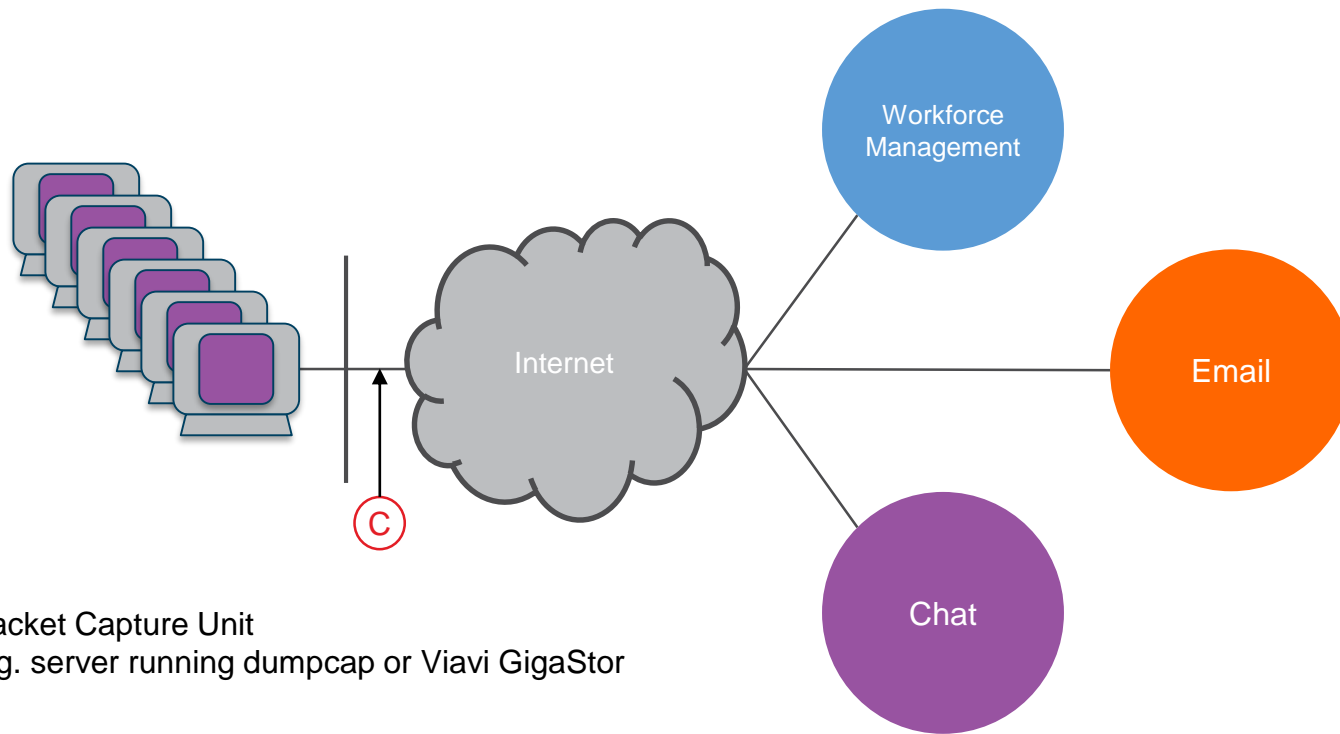



# What to do with the data





# It's not you, it's me



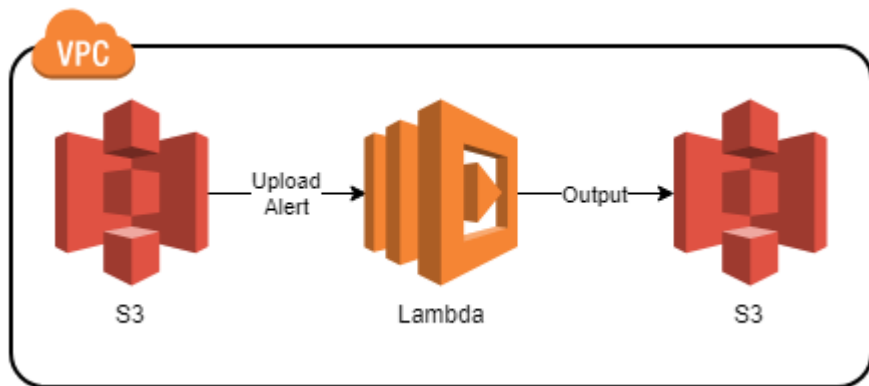
 Packet Capture Unit  
e.g. server running dumpcap or Viavi GigaStor



# What's next?



- Filling in the gaps
- Increase parallelism and reduce uptime on analysis





# Questions

