KubeCon

CloudNativeCon

Europe 2020

Making Compliance Cloud Native

Ann Wallace and Zeal Somani

Zeal Somani

Security & Compliance Specialist, Google Cloud

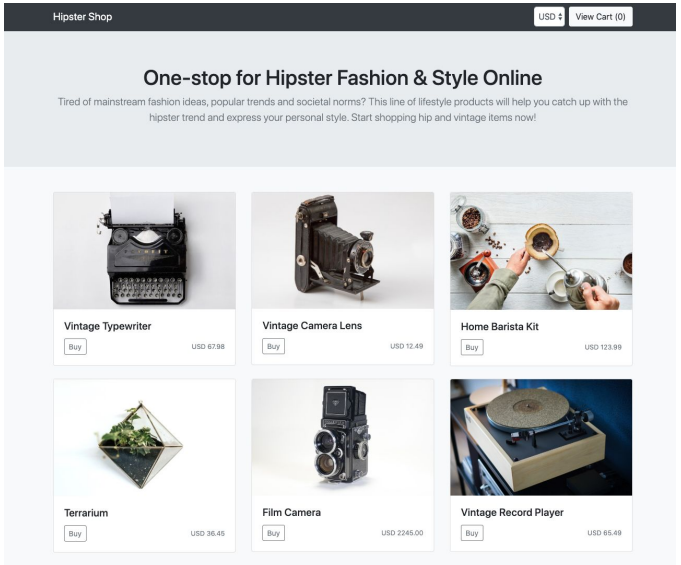
Ann Wallace

Security Solutions Manger, Google Cloud

@AnnNWallace

Google Cloud

Regulated bank or Ecommerce store



Google Cloud

Running a regulated workload...

Makers

Developers

Product Owners

Enterprise Architects

Checkers

Security

Risk and Compliance

Legal

Google Cloud

Makers love cloud-native technologies!

- Enable microservices architecture
- Allows for multi-cloud and hybrid deployments

Google Cloud

Checkers love them too!

- Inherit a lot of security defaults
- Blue / Green deployments

Google Cloud

Demonstrate compliance to your (friendly) Regulator

Google Cloud

Regulatory audits...

Google Cloud

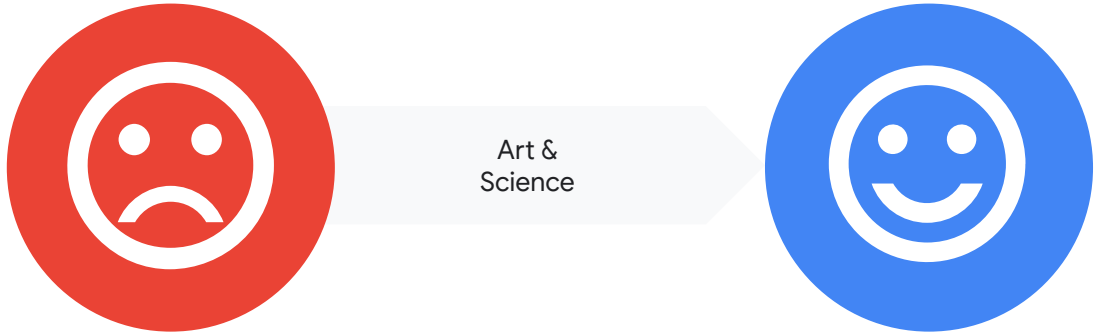
Compliance challenges with cloud native technologies

Scoping the audit

Evidencing controls

Compliance and auditing complexity increases!

Regulatory audits (in cloud) can create anxiety



Compliance Frameworks != Cloud Native

It takes a village to PASS an audit

Fear of Misconfigurations

Evidencing the shared responsibility

Pain-free and a smooth audit!!

Better brand value

Increased trust

Shift Left for Declarative Compliance

Declare your compliance outcomes.

Decoupling compliance controls from business logic with a cloud-native architecture allows the environment to adapt to new or changing compliance without rebuilding.

Google Cloud

Common Compliance Requirements

How to demonstrate compliance requirements natively through cloud - native technologies

Segmentation and Networking	How to isolate workloads with different risk profiles
Identity and Access Management	Are the right access controls in place?
Data Security and Encryption	Is my data properly secured?
Secure Supply Chain	Am I deploying trusted workloads?
Continuous Monitoring	How to detect common vulnerabilities in applications

Google Cloud

Segmentation and Networking

Google Cloud

Keep our in-scope and out-of-scope audit environments fully segmented

Limit access to the “in-scope” environment from “trusted” networks only or have a “DMZ”

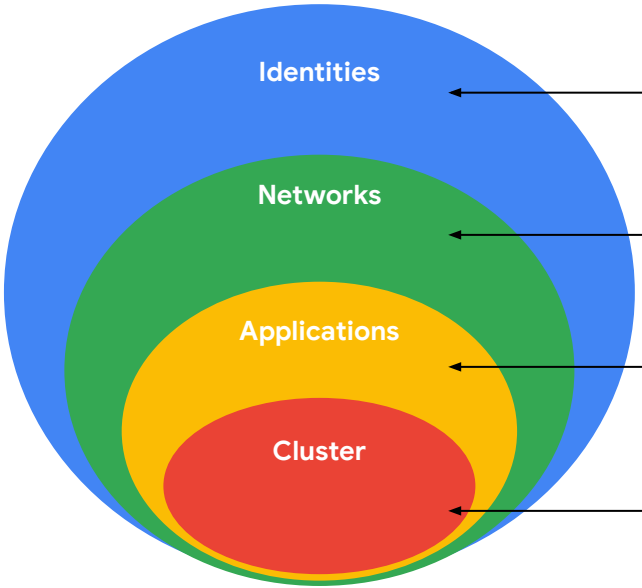
Do not expose private IP addresses from the boundary

Have an IDS / IPS at all critical points in your network

Maintain an accurate network and data-flow diagram

Google Cloud

Why is segmentation important?



User segmentation	Enforce access on “need to know” or “least privilege”
Network segmentation	Limit access from “trusted” / private networks only
Application segmentation	Isolate your “in-scope” and “out-of-scope” applications
Cluster segmentation	Limit the in-scope K8S pods

Macro-segmentation

Micro-segmentation

Google Cloud

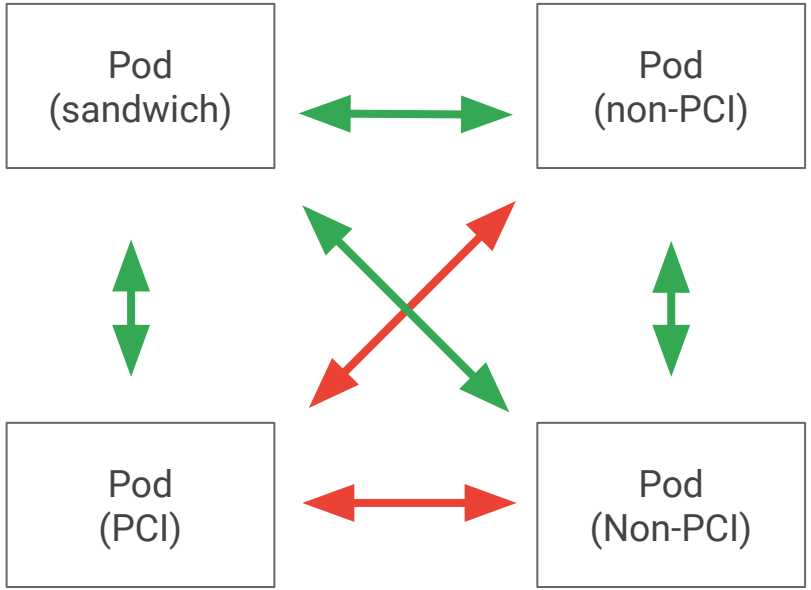
K8S: NetworkPolicy

How does K8S networking work?

- IPs are per pod, **scoped to cluster**
- **Pods can reach each other directly**, without NAT, even across nodes

With NetworkPolicy:

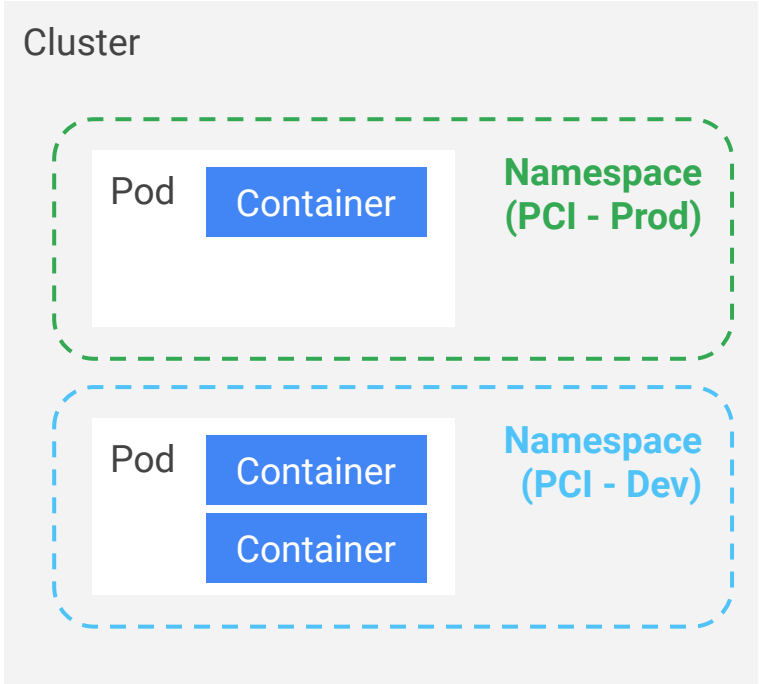
Restrict pod-to-pod traffic

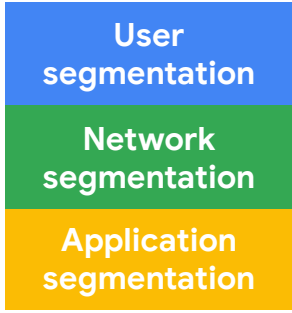


K8S: Kubernetes namespaces

Namespaces

- Create new namespaces as needed
  - Per-user, per-app, per-department, etc.
- Namespaces are just another API object
- Provide each user community with its own:
  - Resources, with consumption limits
  - Policies, with delegated management





Still need stronger isolation..

- Organizational boundary
- Monitor ingress / egress traffic at the boundary
- All access must be deny all by default
- Enforce service-to-service authentication and end user - to - service replayable authentication
- Enforce encryption in transit

Google Cloud

User segmentation

Network segmentation

Application segmentation

Service mesh: a framework for connecting, securing, managing and monitoring services

Google Cloud

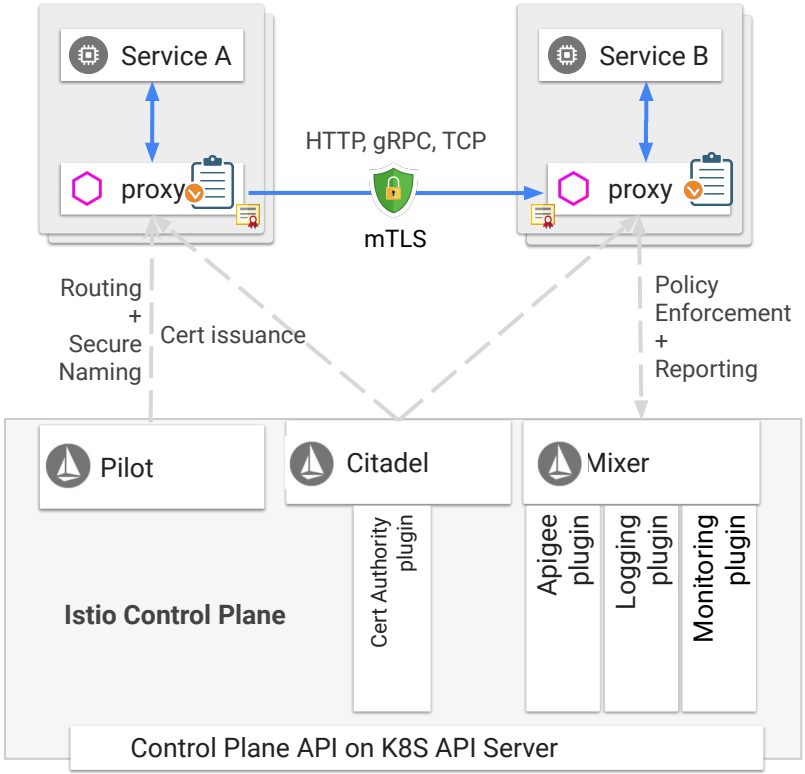
Istio Architectural Components

Envoy: Network proxy to intercept communication and apply policies.

Pilot: Control plane to configure and push service communication policies.

Mixer: Policy enforcement with a flexible plugin model for providers for a policy.

Citadel: Service-to-service auth[n,z] using mutual TLS, with built-in identity and credential management.



Security policies and compliance configurations can be implemented at different levels of granularity - Service, Namespace, Mesh.

Policies like:

- *Session timeouts: 15 minutes*
- *Conditional routing*
- *mTLS: Non replayable service authentication*

Google Cloud

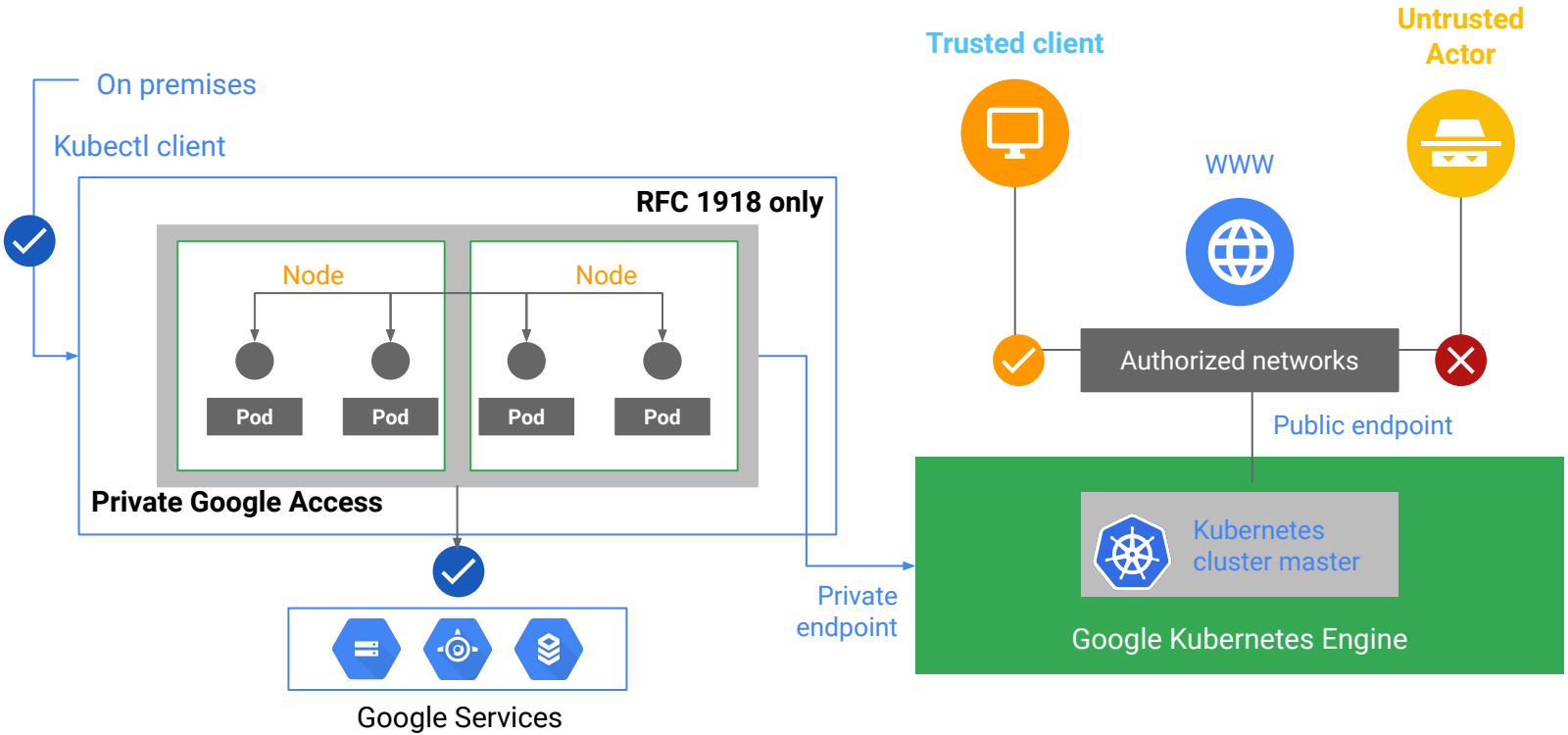
NATing into your Kubernetes footprint

Your cloud providers managed NAT

CALICO ENTERPRISE

Google Cloud

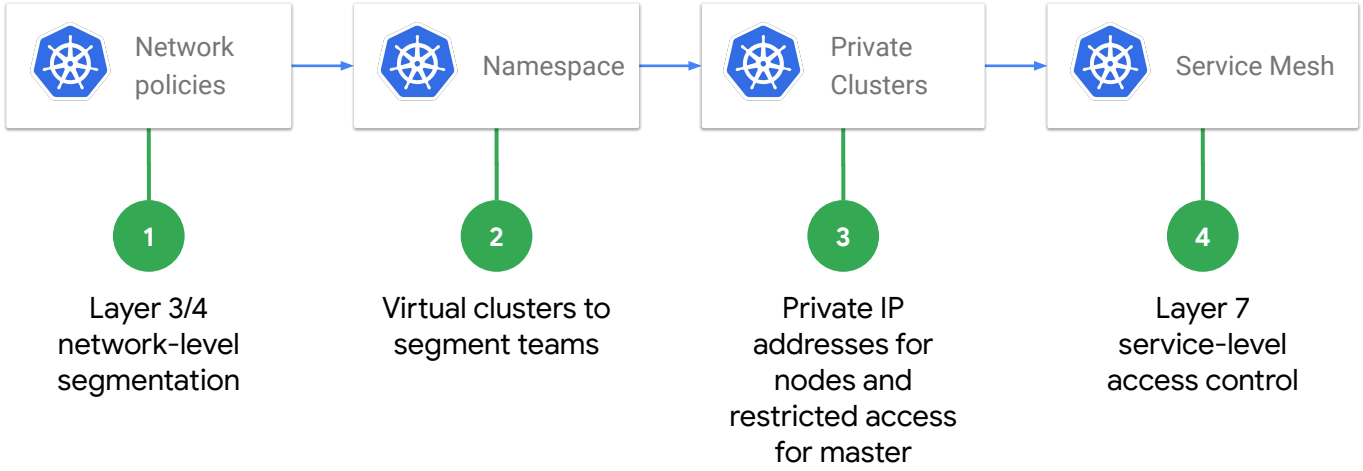
Kubernetes private clusters



Google Cloud

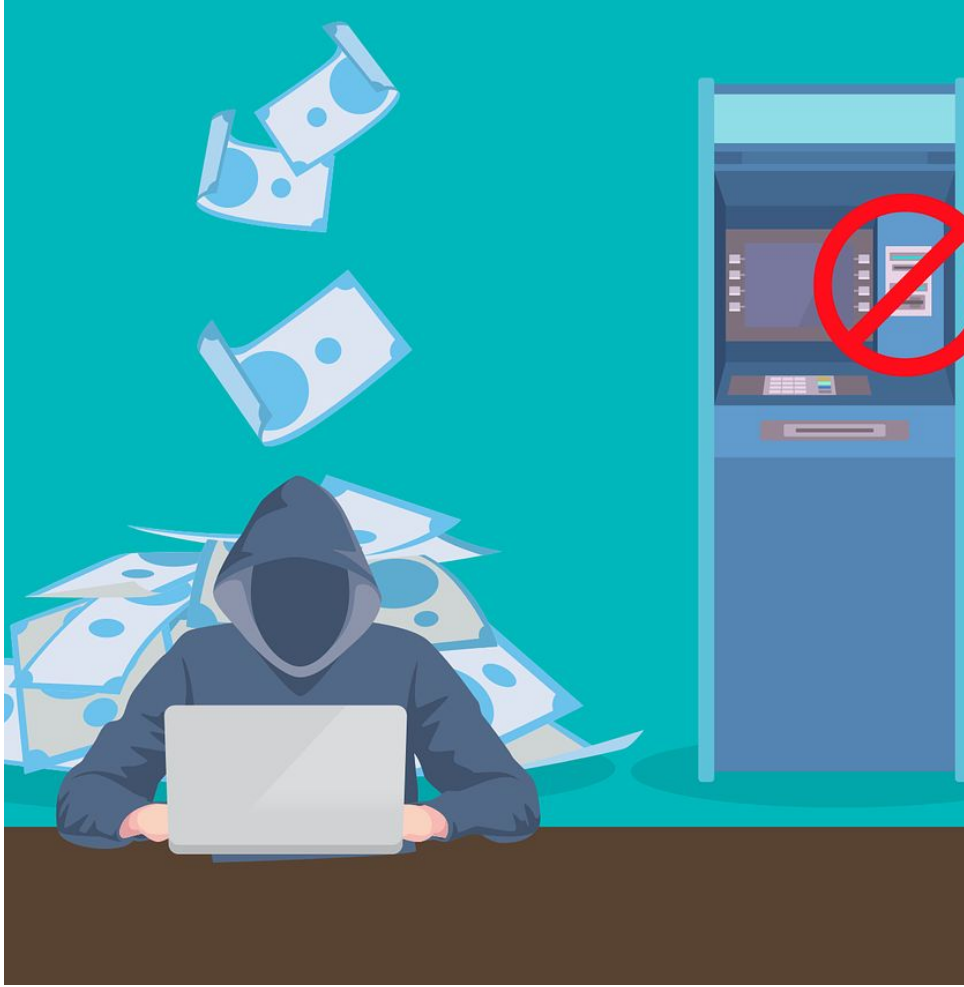
Kubernetes segmentation

A defense-in-depth architecture for securely isolating workloads



Google Cloud

Data Protection



Google Cloud

Ensure that encryption ecosystem meets FIPS 140-2 requirements

Evidence the key management procedures I.e., rotation, dual controls,

Encryption for data at rest and in transit, secrets

Google Cloud

Areas of data protection

In flight

At rest

Secrets

A default OSS Kubernetes setup is not encrypted by default.
Secrets are stored in plaintext.

Use envelope encryption

Data protection Dos

Have a TTL on your data

- Delete the data and make it unrecoverable - shred the keys
- Understand how data deletion works with your cloud provider

Maintain an Asset Inventory

- Track data consistently across the organization -- apply appropriate data protection technique
- Identify assets on-prem vs. public cloud

Familiarize with Shared Responsibility

- Understand difference in responsibilities as you consume KMS and HSMs
- FIPS 140-2 related responsibility.

Key Management

- Set rotation policies for your keys.
- Make sure your DEKs and KEKs are separate

Google Cloud

Secure and Compliant Supply Chain

Google Cloud

Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking

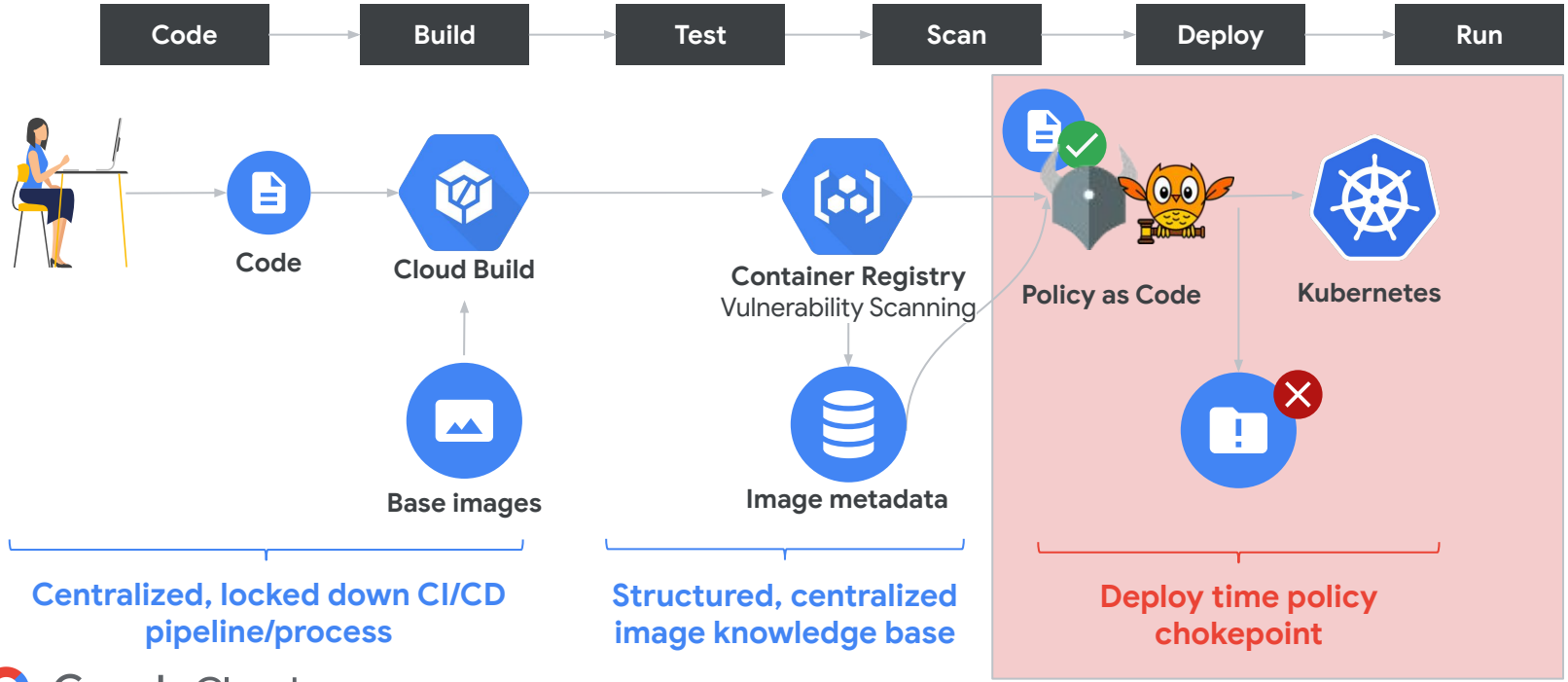
Ensure that all systems and software are protected from known vulnerabilities.

Enable only necessary services, protocols, daemons, etc

Configure system security parameters to prevent misuse.

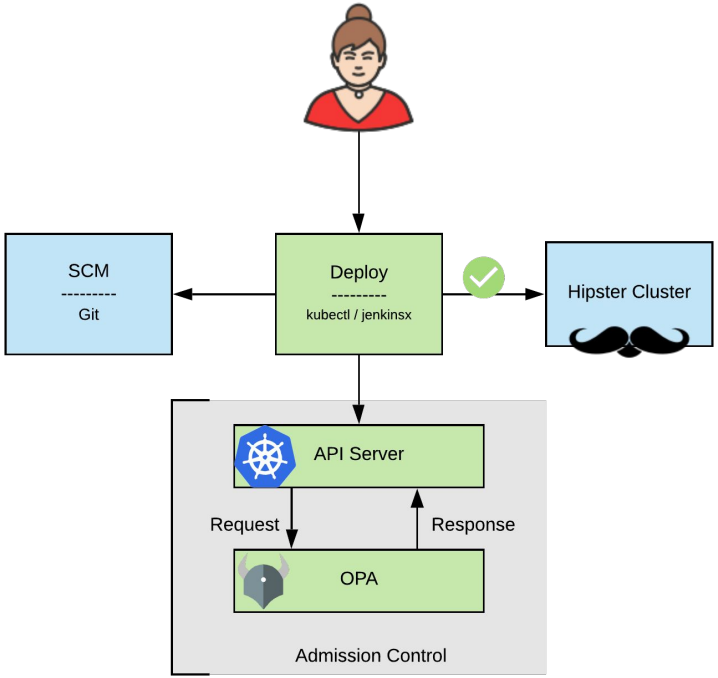
Google Cloud

Stages of the Software Supply Chain



Google Cloud

Software Supply Chain with OPA & Kubernetes



Google Cloud

OPA & Kubernetes

```
package kubernetes.admission

import data.kubernetes.namespaces

deny[msg] {
    input.request.kind.kind = "Service"
    input.request.operation == "CREATE"
    port := input.request.object.spec.ports[_].port
    port != 443
    msg := sprintf("Port %d is not permitted. Only 443 is permitted", [port])
}
```

```
kind: Service
apiVersion: v1
metadata:
  name: http-service
spec:
  type: LoadBalancer
  selector:
    app: http-app
  ports:
  - protocol: TCP
    port: 80
    targetPort: 8888
```

Google Cloud

Infrastructure & Policy as Code

Open Policy Agent

HashiCorp Terraform

Governance & Audit of Hipster Store's IaC

- Pre-deployment checks of Terraform Plan
- Audits of Terraform State Files

```
package tfstate.analysis

# allowed location / country
allowed_location = "eu-"

# Allow only if there are no differences between
# expected and actual
location_test[passed] {
        passed := startswith(actual[location], allowed_location)
}

# Get service names from resources where the type
# is google_container_cluster and set location
actual[location] {
        some i
        res := input.resources
        res[i].type == "google_container_cluster"
        location := res[i].instances[_].attributes.location
}
```

Google Cloud

Grafeas and Kritis

Governance & Audit of Hipster Store's Container Images

Grafeas (Container Analysis)

- Pulls security relevant info from container images, Virtual Machine (VM) images, JAR files, and scripts

Kritis (Binary Authorization)

- Enforces user-defined policies using the data provided by Grafeas
- Also uses a PGP key to sign attestations for Grafeas

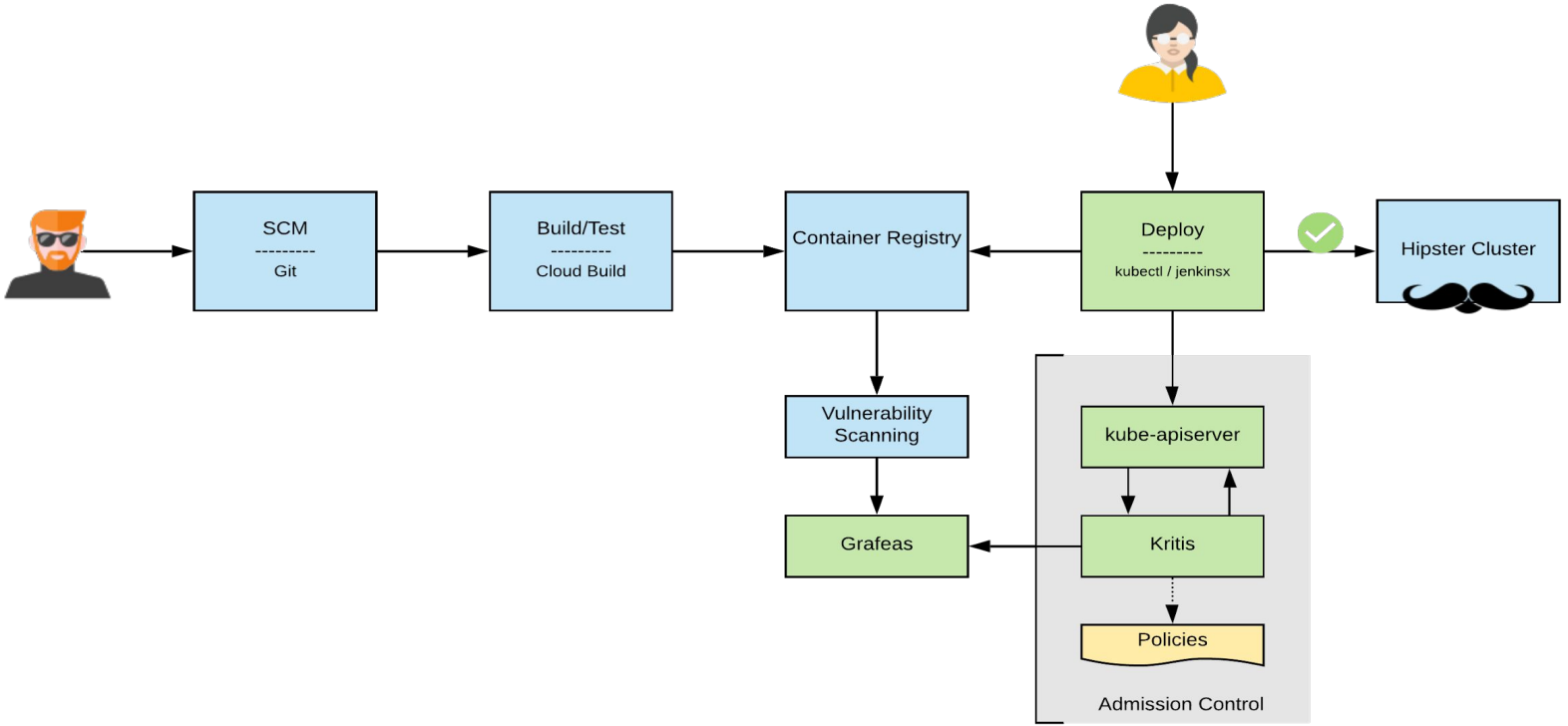
Grafeas Kritis

```
imageWhitelist:
- gcr.io/my-project/whitelist-image@sha256:<DIGEST>
packageVulnerabilityPolicy:
  maximumSeverity: HIGH
  whitelistCVEs:
    providers/goog-vulnz/notes/CVE-2017-1000082
```

example Kritis policy

Google Cloud

Software Supply Chain with Grafeas & Kritis



Google Cloud

Run Time Security

Google Cloud

- Implement audit trails to link all access to system components to each individual user
- Routinely monitor event logs
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
- Audit trails include: User, Type of Event, Date and Time, Success or Failure...

Google Cloud

Logs

1. **Infrastructure logs:** what the infrastructure does, and what a human does to the infrastructure
2. **Kubernetes logs**: what the control plane does, what a container does to the control plane, and what a human does to the control plane
3. **Operating system logs:** what a container does to the node
4. **Application logs:** what an application does (in a container)

Kubernetes :: Audit logging

Kubernetes audit policy

None <
Metadata <
Request <
RequestResponse

```
- level: Request
  verbs: ["get", "list", "watch"]
  resources: ${known_apis}
  omitStages:
    - "RequestReceived"
- level: RequestResponse
  resources: ${known_apis}
  omitStages:
    - "RequestReceived"
- level: Metadata
  omitStages:
    - "RequestReceived"
```

‘get’ responses can be large

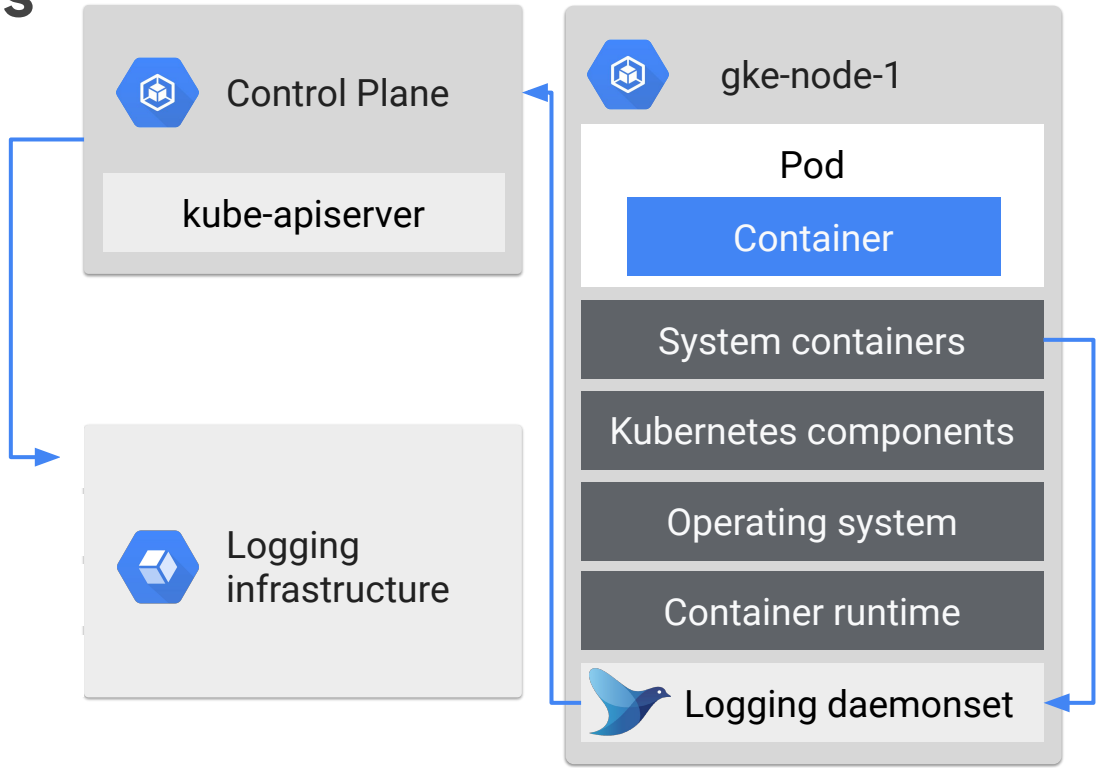
‘RequestResponse’ default for known APIs

‘Metadata’ default for all other requests

Google Cloud

Collecting all the logs

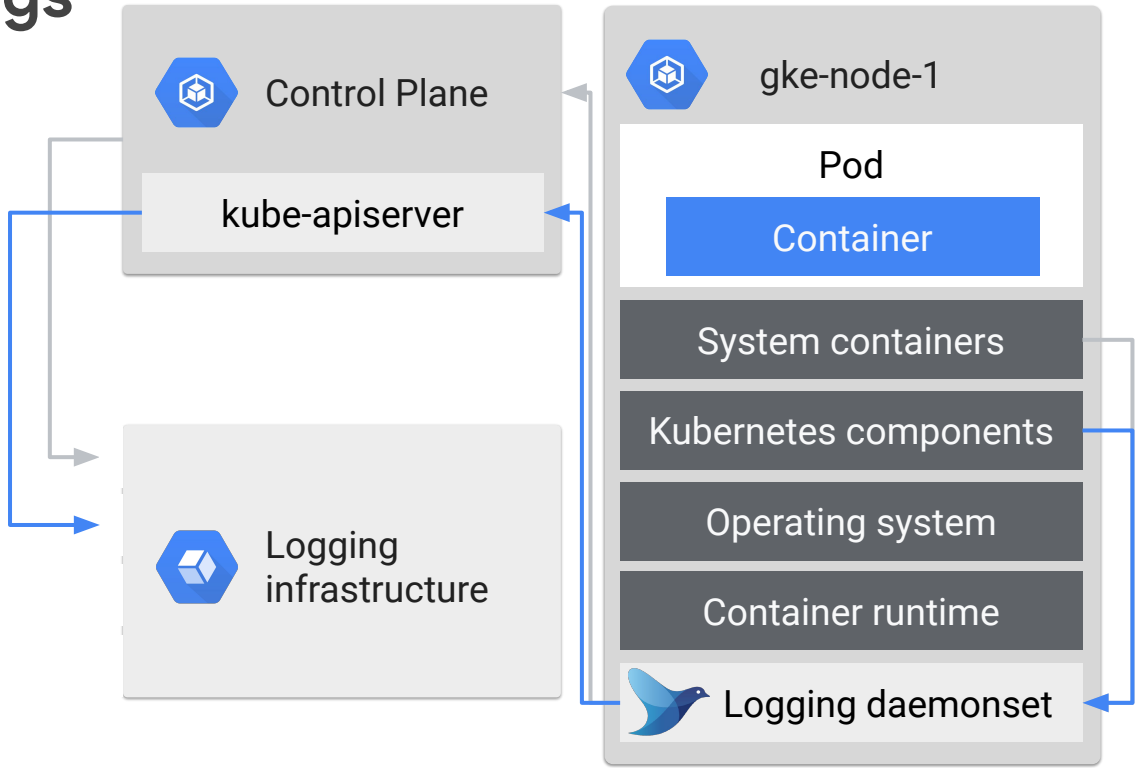
Infrastructure logs



Collecting all the logs

Infrastructure logs

Kubernetes logs



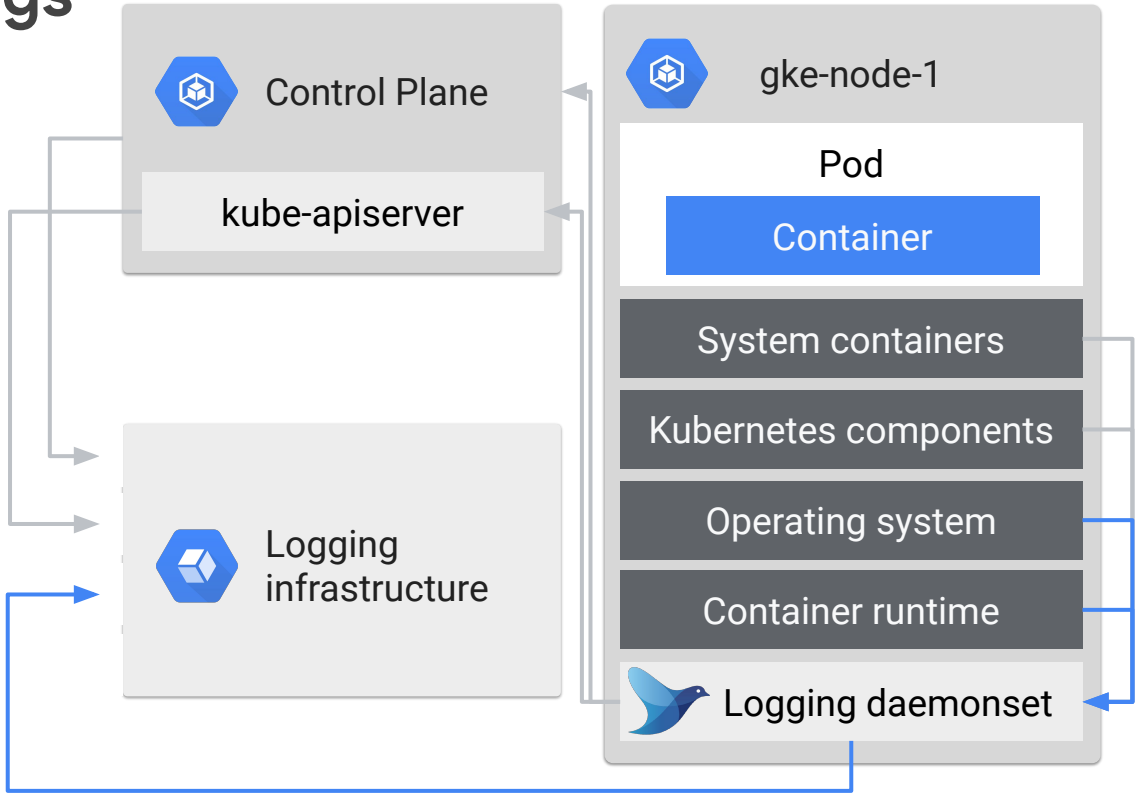
Google Cloud

Collecting all the logs

Infrastructure logs

Kubernetes logs

OS logs



Google Cloud

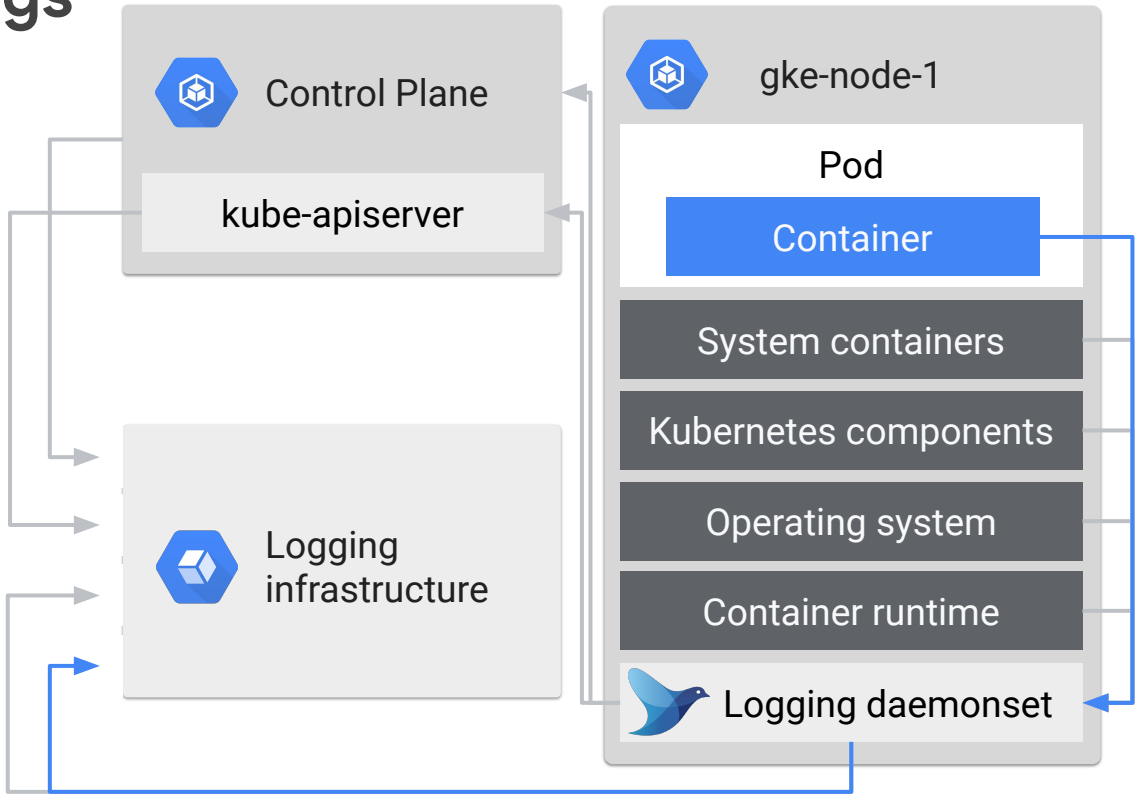
Collecting all the logs

Infrastructure logs

Kubernetes logs

OS logs

Application logs



Google Cloud

K8S: Monitoring & logging

K8s audit logs

Logging Infrastructure

- Review, monitor and alert on audit logs centrally
- “jamie@hipsterstore.com deployed a new frontend version @ time T”

Prometheus

Grafana

- Runtime metrics gathered
- “Add to cart latency in the last 10 minutes was 1.3s”

Google Cloud

Anomalous activity detection

Aqua Security

Capsule8

Google

Twistlock

StackRox

Sysdig

(and more)

People & Process

Google Cloud

Diagrams!

Applications & Projects Detailed View

In PCI Scope

network

Virtual Private Cloud

Cloud Firewall Rules

management

Forseti Security on Compute Engine

Cloud Storage

Stackdriver Logs

in-scope

Public Cloud Load Balancer

Frontend Kubernetes Engine

Payment Service Kubernetes Engine

Checkout Service Kubernetes Engine

in-scope Kubernetes Engine

1

out-of-scope

Internal (Private) Cloud Load Balancing

Cart Service Kubernetes Engine

Ad Service Kubernetes Engine

Recommendation Service Kubernetes Engine

Currency Service Kubernetes Engine

Catalog Service Kubernetes Engine

Email Service Kubernetes Engine

Shipping Service Kubernetes Engine

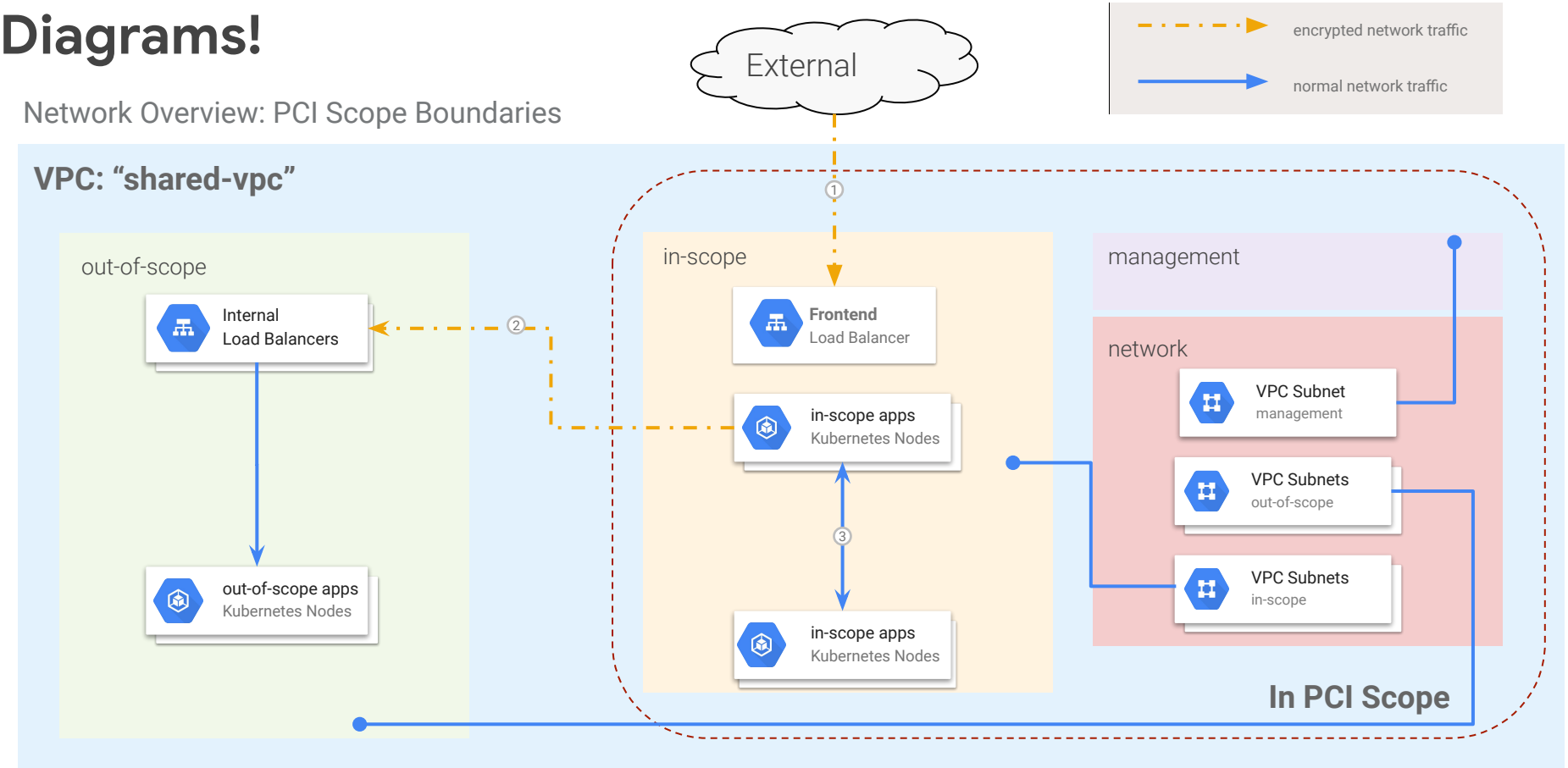
Redis Kubernetes Engine

out-of-scope Kubernetes Engine

1. Log data from Kubernetes clusters sent to Stackdriver

Diagrams!

Network Overview: PCI Scope Boundaries

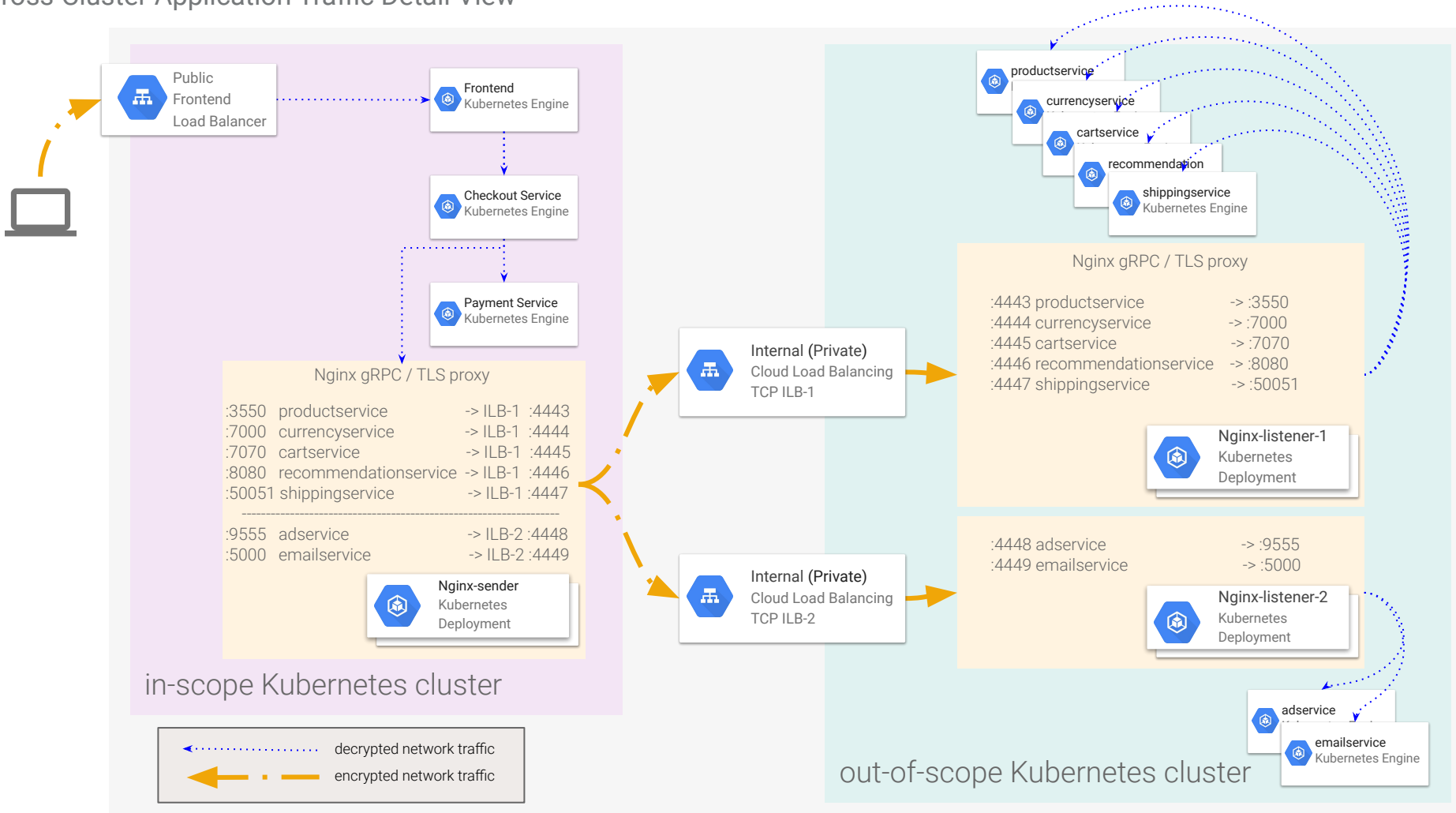


1. HTTPS traffic from outside VPC to in-scope Public Load Balancer

2. TLS-encrypted traffic between in-scope Kubernetes Cluster nodes to Internal Load balancers

3. Intra-cluster communication is unencrypted

Cross-Cluster Application Traffic Detail View



YAML FTW!

```yaml
apiVersion: networking.gke.io/v1beta1
kind: ManagedCertificate
metadata:
   name: example-certificate
spec:
   domains:
       - example.com
```

```yaml
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
   name: example-ingress
   annotations:
     kubernetes.io/ingress.global-static-ip-name:example-ip-address
     networking.gke.io/managed-certificates: example-certificate
spec:
   backend:
      serviceName: example-nodeport-service
      servicePort: 443
```

Google Cloud

Advocacy and Empathy

Makers

Internal Checkers

External Checkers

Google Cloud

Advocacy and Empathy

Makers

- Developers
- Product Owners
- Enterprise Architects

Google Cloud

Advocacy and Empathy

- Security
- Legal
- Governance, Risk & Compliance

Internal Checkers

Advocacy and Empathy

- Regulators
- Auditors

External Checkers

TL;DR :: You've got this!

- K8S & Cloud Native Tech can make compliance a lot easier
- Practice Advocacy and Empathy
- Document the hell of everything
- Automation - IaC and PaC
- Understand the shared responsibility model
- **We're here to help!**

Google Cloud