ngrok
Zero Trust Security

Where your paranoia is your superpower!

Mandy Hubbard
Sr. Technical Marketing Engineer

Hi, I’m Mandy!

These are a few of my favorite things:

CI/CD (in case you missed that)

Crystals

Astrology

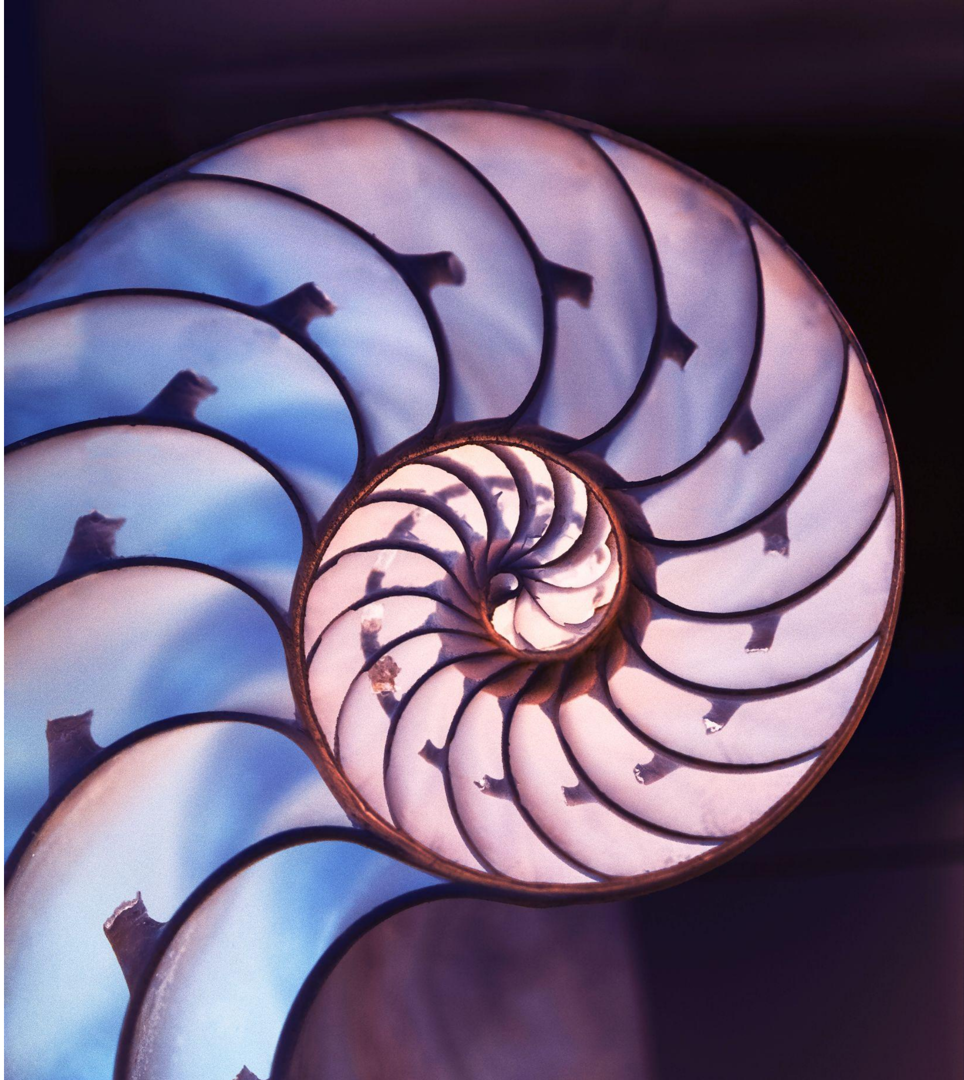
Kundalini Yoga

Creative writing

I’m The Woo in Tech ™

Let’s talk about…

- Zero Trust Security model
- Kinds of network traffic
- Kubernetes networking
- Kubernetes Services
- Kubernetes network tools



Zero Trust Security

A philosophy, a model

- Trust no one
- No safe network perimeter
- Unlisted IP addresses/undiscoverable services
- Principle of least privilege
- Reconnect and reverify frequently
- Non-root containers
- Continuous monitoring and logging of security telemetry

@DevMandy

Different types of network traffic

To the cluster

- Traffic flows to the cluster from an external endpoint
- Referred to as ingress
- Handled by Services, Ingress Controllers and API Gateways
- north-south traffic

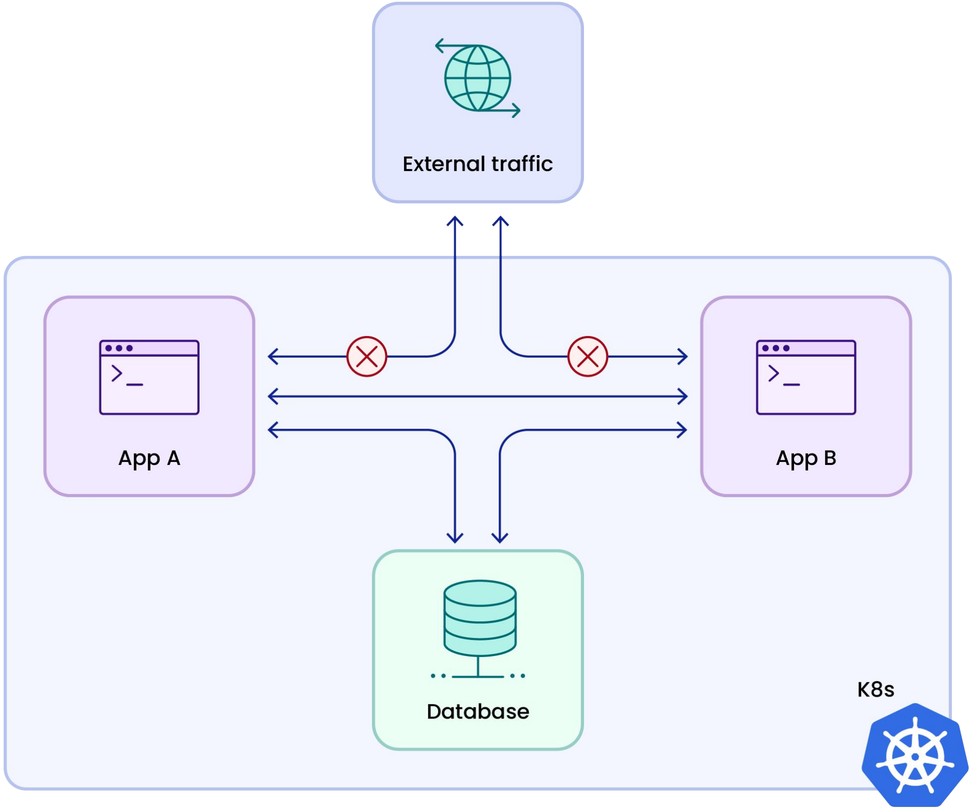
From the cluster

- Traffic flows from the cluster to an external endpoint
- Referred to as egress
- Handled by Network Policies, Egress Gateway
- north-south

Pod-to-pod

- Traffic flows within the cluster from Pods to other Pods and Services
- Referred to as ingress and egress
- Handled by Services, Network Policies and Service Meshes
- east-west traffic

Kubernetes Networking



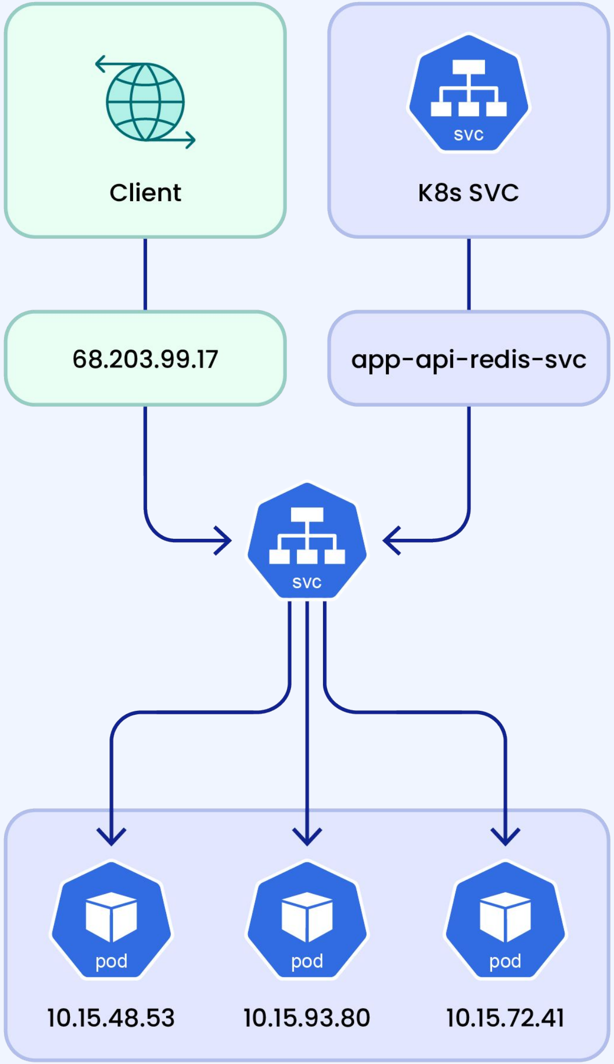
- Each Pod gets a unique IP
- All Pods can communicate with other pods using IP addresses
  - ○ Across Nodes
  - ○ Across Namespaces
  - ○ Without NAT
- Containers within a Pod can communicate with each other using localhost
- Violates Zero Trust Security micro-segmentation paradigm
- Can't rely on IP addresses as they are volatile by nature
- Cannot connect from outside world

@DevMandy

Kubernetes Service

- An abstraction representing a set of logical pods
- Acts as a single entity to the outside world
- Lives until explicitly destroyed
- Reliable point of entry
- Matches Pods based on labels
- Primarily designed for routing traffic within the cluster
- Types: ClusterIP, NodePort, LoadBalancer
- One load balancer per LoadBalancer service == $$$

@DevMandy



Kubernetes Network Policies

Policy Configuration

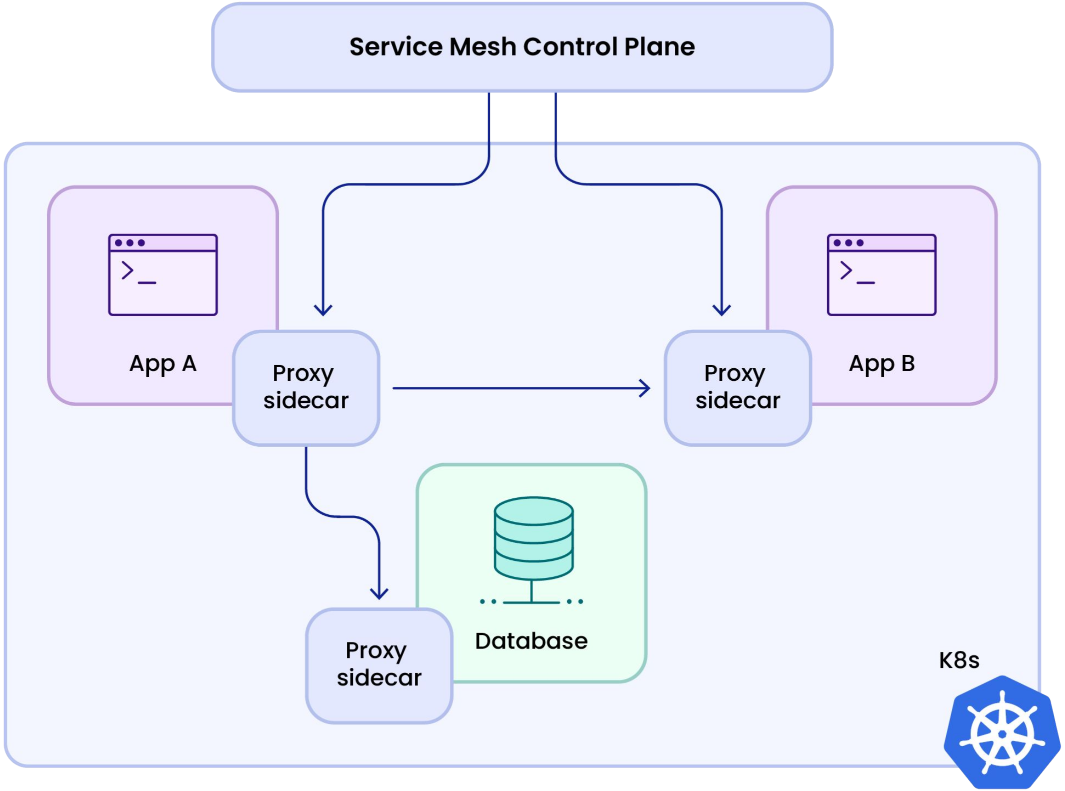
- Configure ingress and egress rules separately
- Specify traffic to/from pods, namespaces, and IP blocks
- Apply the YAML manifest to your cluster

Policy Enforcement

- Enforce the policies you define
- Conform to Container Network Interface (CNI) spec
- CNI makes container networking pluggable
- Install plugins on your cluster
- Calico and Cilium

Service Mesh

- Adds security, reliability, and observability to your east-west traffic
- Authorization, automatic mTLS, latency-aware request-level load balancing, retries, canary and blue/green deployments, high availability, dynamic request routing, and more
- Addresses cross-cutting concerns
- Predecessor to internal libraries like Netflix’s Hysterix, Google’s Stubly, and Twitter’s Finagle
- Examples: Linkerd, Istio, Kuma

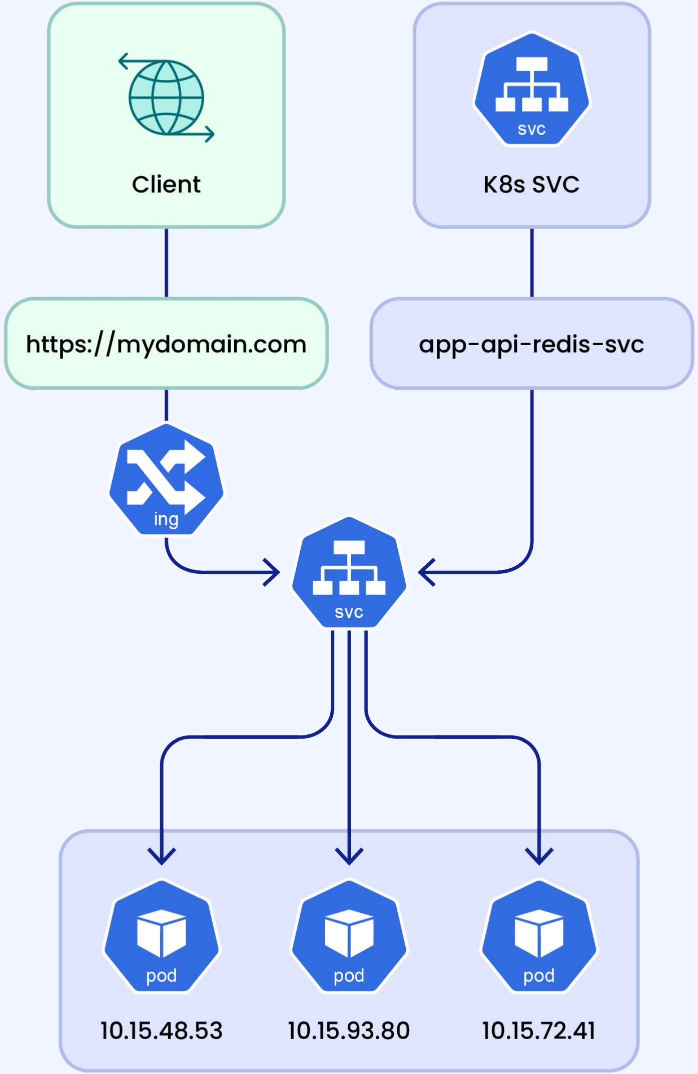


@DevMandy

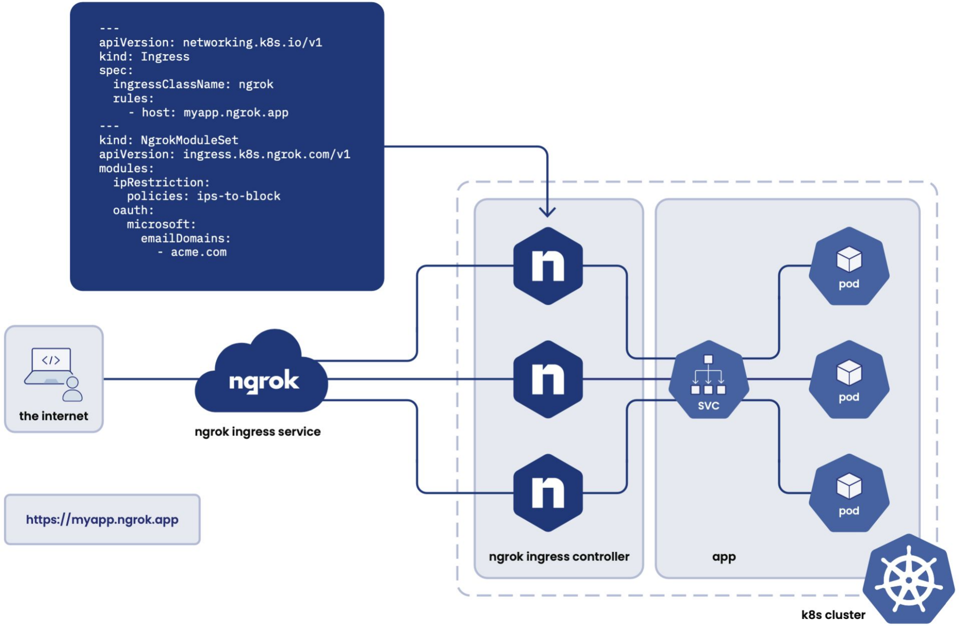
Ingress Controller

- Manages external traffic and routes it to Pods
- Load balances traffic to applications running in your cluster
- Offers advanced L7 routing capabilities (HTTP/HTTPS, headers, cookies, methods)
- Provides advanced features
  - Circuit Breaking (DDoS protection)
  - Compression
  - IP restriction
  - OAuth
  - OpenID Connect (OIDC)
  - SAML
  - TLS termination

@DevMandy



ngrok’s Ingress-as-a-Service



```yaml
---
apiVersion: networking.k8s.io/v1
kind: Ingress
spec:
  ingressClassName: ngrok
  rules:
    - host: myapp.ngrok.app
---
kind: NgrokModuleSet
apiVersion: ingress.k8s.ngrok.com/v1
modules:
  ipRestriction:
    policies: ips-to-block
  oauth:
    microsoft:
      emailDomains:
        - acme.com
```

- **Enhanced security** - intercepts and authorizes traffic and terminates TLS before it ever reaches your cluster

- **Reduced complexity** - eliminates the need to configure Load Balancers, certificate management, and DNS, and it works behind a NAT

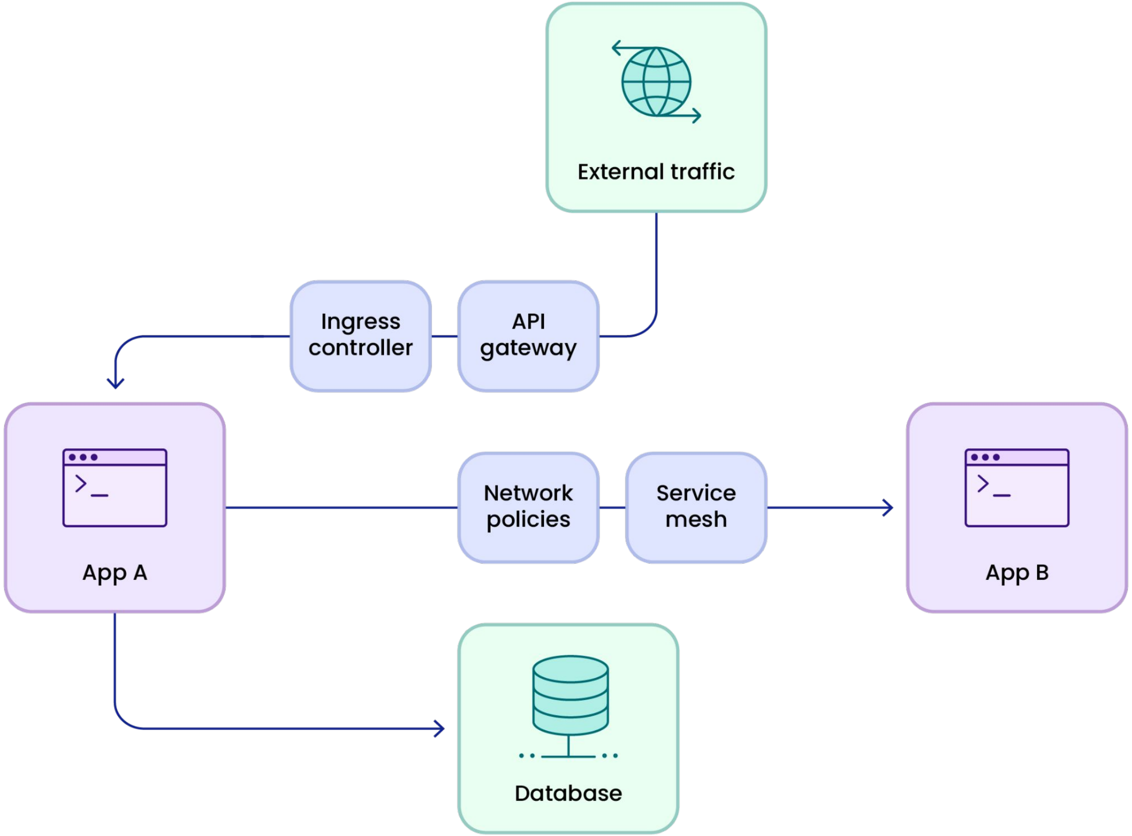
- **Works everywhere** - works in any Kubernetes cluster on any platform, regardless of the cloud provider, since the provisioning of resources is handled by the service provider

- **Improved performance** - includes GSLB

API Gateway

- Traffic routing
- Authentication and authorization
- TLS termination
- Rate limiting
- Load balancing
- Protocol translation
- Caching
- Request validation and transformation
- Metrics and logging
- API management
- Circuit breaking (DDoS prevention)
- Traffic splitting

Zero Trust Kubernetes Network



@DevMandy

That's a wrap!

- Zero Trust Security model
- Types of network traffic
- Kubernetes networking
- Kubernetes Services
- Kubernetes networking tools
    - Network Policies
    - Service Mesh
    - Ingress Controller
    - API Gateway

@DevMandy

SPECIAL THANKS TO ALL OUR AWESOME SPONSORS!

CLOUDFLARE

Unspecified

SOFTWARE CO

Join Us

WI 24

THAT®

CONFERENCE

JULY 29TH - AUG. 1ST

Thanks!
Q +A