What Does An Ingress Controller Do?

The **Ingress controller** is a specialized load balancer that manages Layer 4 and 7 ingress and egress (“north-south”) traffic.

It can also be used for:

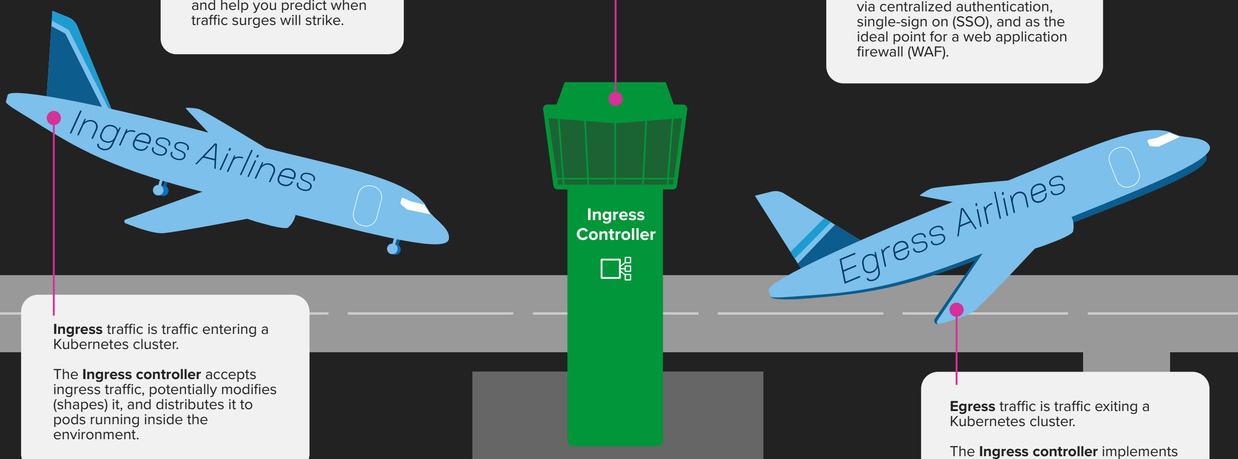
- Traffic control
- Traffic shaping
- Monitoring and visibility
- As an API gateway
- Authentication and SSO
- WAF integration

Monitoring and Visibility

The **Ingress controller** can give you insight into issues impacting app and infrastructure performance, and help you predict when traffic surges will strike.

Security

The **Ingress controller** can protect your environment from unauthorized or malicious traffic via centralized authentication, single-sign on (SSO), and as the ideal point for a web application firewall (WAF).

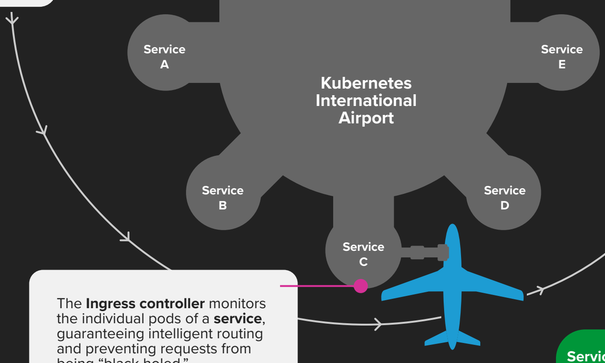


Ingress traffic is traffic entering a Kubernetes cluster.

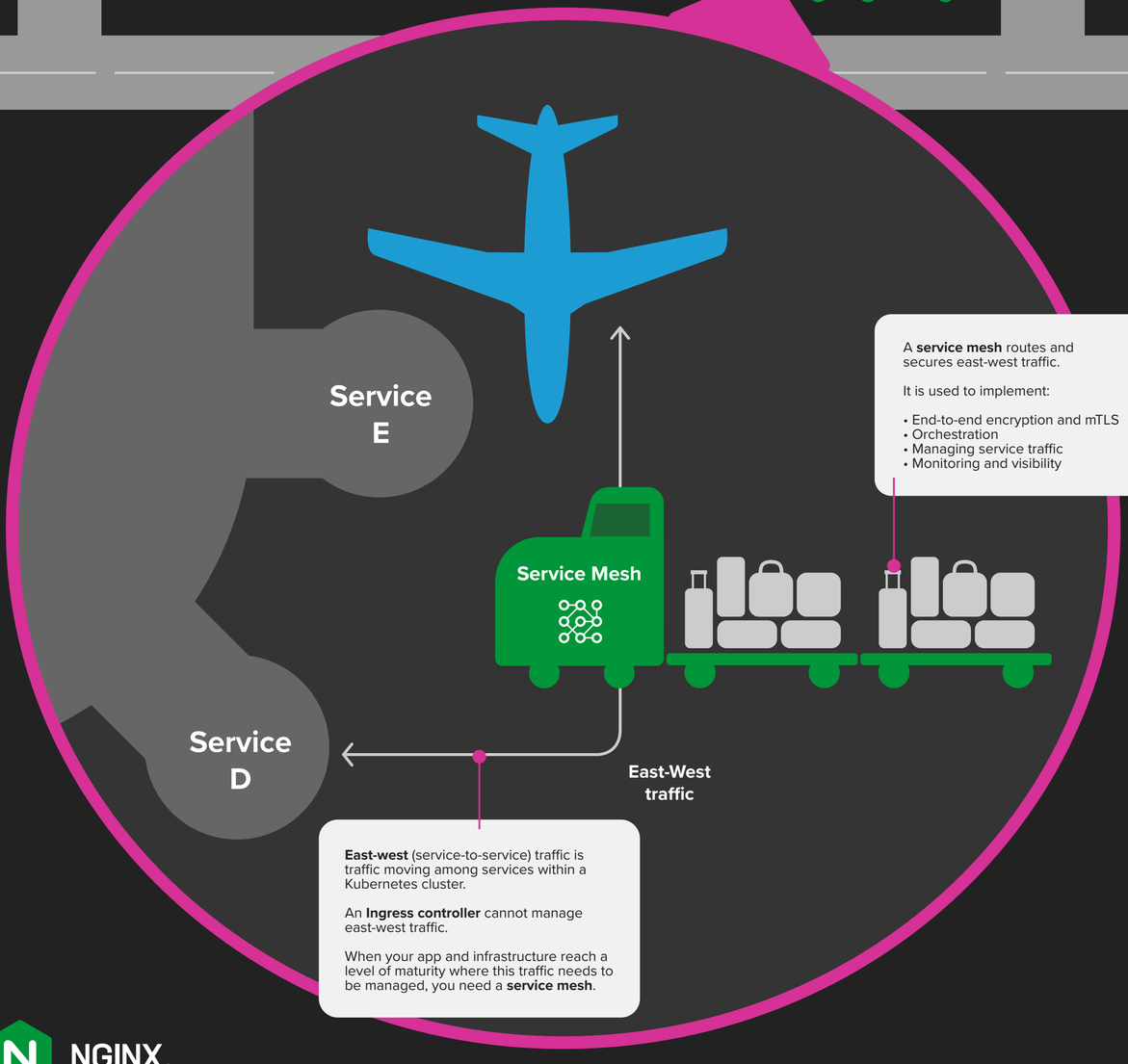
The **Ingress controller** accepts ingress traffic, potentially modifies (shapes) it, and distributes it to pods running inside the environment.

Egress traffic is traffic exiting a Kubernetes cluster.

The **Ingress controller** implements egress rules to enhance security with mutual TLS (mTLS) or limits outgoing traffic from certain pods to specific external services.



The **Ingress controller** monitors the individual pods of a **service**, guaranteeing intelligent routing and preventing requests from being “black-holed.”



A **service mesh** routes and secures east-west traffic.

It is used to implement:

- End-to-end encryption and mTLS
- Orchestration
- Managing service traffic
- Monitoring and visibility

East-west (service-to-service) traffic is traffic moving among services within a Kubernetes cluster.

An **Ingress controller** cannot manage east-west traffic.

When your app and infrastructure reach a level of maturity where this traffic needs to be managed, you need a **service mesh**.

NGINX
Part of F5

Click here to learn more at nginx.com