Egress Gateway for Kubernetes

Workloads in Kubernetes are dynamic and ephemeral. Organizations have struggled to secure and identify traffic from workloads due to this behavior. Kubernetes does not offer any native solution for controlling egress traffic.

Most organizations have transformed their business through digitalization but still have many legacy non-Kubernetes applications running.

How can you effectively bridge the security gap between your Kubernetes workloads and your legacy environment?

A lot of security and traditional tools still rely on static IP addresses in order to protect on-premises and other cloud applications that are not built on microservices.

Calico Egress Gateway overview

Calico's Egress Gateway enables users to assign meaningful network identity to selected traffic so that this information can be further used by traditional tools to enforce granular policies to traffic based on identity or bandwidth. It also provides advanced capabilities such as:

- Policy enforcement
- Load-balancing
- High-availability
- Policy-based routing
Benefits

Integrate with traditional tools
Provide fixed network identity to traditional tools for better security posture

Eliminate complex service-mesh
Reduce complexity by avoiding a service-mesh for egress protection

Hybrid and Multi-cloud security
Secure communication and maintain compliance across clouds

Trusted by companies worldwide

eHealth | box | ALDAGI | GoDaddy | DISCOVER

Interested in learning how you can use Calico Egress Gateway?

Contact us