ISOVALENT
now part of cisco

Kubernetes Network Policies Done the Right Way

What are the Key Challenges for Enterprises Adopting Network Policies?

Building a mission-critical, secure platform is no small task. Where do you start? How can you enforce robust security while keeping up with the rapid pace of application development? Consider these pressing challenges:

- **Balancing security with agility:** How do you implement strict security guardrails without stifling innovation? Can your developers easily onboard their applications while ensuring security?
- **Adapting to constant change:** As cloud-native applications rapidly evolve, how do you keep up with new services or features that current network policies don't support? How do you avoid policy blind spots without stalling development?
- **Managing complexity at scale:** With multiple teams and services, how do you ensure consistent policy enforcement across your entire infrastructure without introducing operational bottlenecks?
- **Proving compliance:** Are your security measures comprehensive enough to meet regulatory requirements? Can you ensure that your platform adheres to industry standards like GDPR, PCI-DSS, or HIPAA, and are you able to demonstrate compliance effectively?
- **Responding to security threats:** Can you quickly identify and respond to security incidents before they result in unauthorized access or data breaches? Are your detection and response systems robust enough to prevent potential damage?

These challenges don't appear in isolation—they stack upon one another, creating layers of friction across teams and technologies. In the face of such complexity, your strategy must allow your platform to remain secure and compliant, while empowering developers to move fast and innovate.

What You Will Learn

In this guide, we will explain the essential strategies for adopting and implementing effective network policies in Kubernetes environments. You will gain a clear understanding of how to balance security with operational agility, using advanced tools like Cilium and Hubble to enforce scalable, fine-grained policies.

Whether you are responsible for securing mission-critical applications, managing Kubernetes clusters, or ensuring compliance, this document will provide actionable insights on:

- Designing network policies that protect your infrastructure without hindering application development.
- Leveraging network observability to refine and optimize security enforcement.
- Adopting a Zero Trust architecture to minimize security risks across your cluster.
- Using Cilium and Hubble to simplify policy management, enforce compliance, and secure your Kubernetes workloads at scale.

By the end, you'll have the knowledge and tools to confidently apply network policies that align with your security and business objectives, effectively bridging the gap between strategic understanding and technical implementation.

What Are Network Policies?

In Kubernetes environments, network policies act as a critical security layer, controlling how traffic flows between pods, services, and external entities. At a high level, network policies allow you to define what is allowed—or blocked—when it comes to communication at the IP or port level (OSI layers 3 and 4).

For example, you may want to ensure that only certain pods within your cluster can communicate with specific services, or restrict access to sensitive areas of your infrastructure from external sources. Network policies give you the power to define and enforce these rules, helping to secure your applications and protect against unauthorized access.

However, defining effective network policies can be complex. Here are the main components involved in creating network policies:

- **Pod communication:** Specify which pods can interact with others, ensuring that only approved communication takes place.
- **Namespace controls:** Define rules at the namespace level to restrict or permit traffic between different parts of your application or environment.
- **IP block rules:** Set policies based on IP ranges, controlling which external IPs are allowed or blocked from accessing your cluster.

Network policies are enforced by a network plugin like Cilium, which brings enhanced visibility and security capabilities to your Kubernetes environment. While Kubernetes' standard network policies cover basic Layer 3 and Layer 4 controls, Cilium extends this to include more advanced policies, allowing control over Layer 7 traffic and enabling cluster-wide policies through CiliumClusterwideNetworkPolicy. This granularity is especially important in modern cloud-native environments, where security needs to scale alongside rapidly evolving applications.

By using Cilium, enterprises can adopt network policies with the confidence that their policies are not only enforced, but also scalable, secure, and ready to support even the most demanding cloud-native workloads.

Secure service-to-service communication based on identities

Modern distributed applications rely on container technologies for rapid deployments and scalable operations. However, traditional approaches to securing these workloads—such as IP-based firewalls—can become inefficient and slow. Some customers have reported container startup times stretching to several minutes because firewalls need to be constantly updated whenever new containers are launched. This introduces both scalability and operational challenges, particularly when numerous containers are started simultaneously.

Traditional firewalls secure workloads by filtering traffic based on source and destination IP addresses and ports. Each time a container spins up, firewall rules across the cluster must be updated, which can slow down deployments and complicate operations as the number of containers increases.

Cilium addresses these challenges by managing security at the endpoint level. In Cilium terminology, an endpoint is a group of application containers that share a common IP address.

In Kubernetes, labels are key-value pairs assigned to resources like pods and namespaces. These labels allow you to group and manage resources more easily, especially when defining security rules. Cilium assigns a security identity to groups of pods (endpoints) that share the same set of labels to simplify policy enforcement and overcome the limitations of IP-based filtering.

This security identity is attached to all network packets sent by the pods, and it's validated at the receiving node. By using these identities, Cilium ensures scalable and efficient security enforcement without the need for constant firewall updates. The management of these security identities is further streamlined through a key-value store, which keeps the enforcement lightweight and flexible.

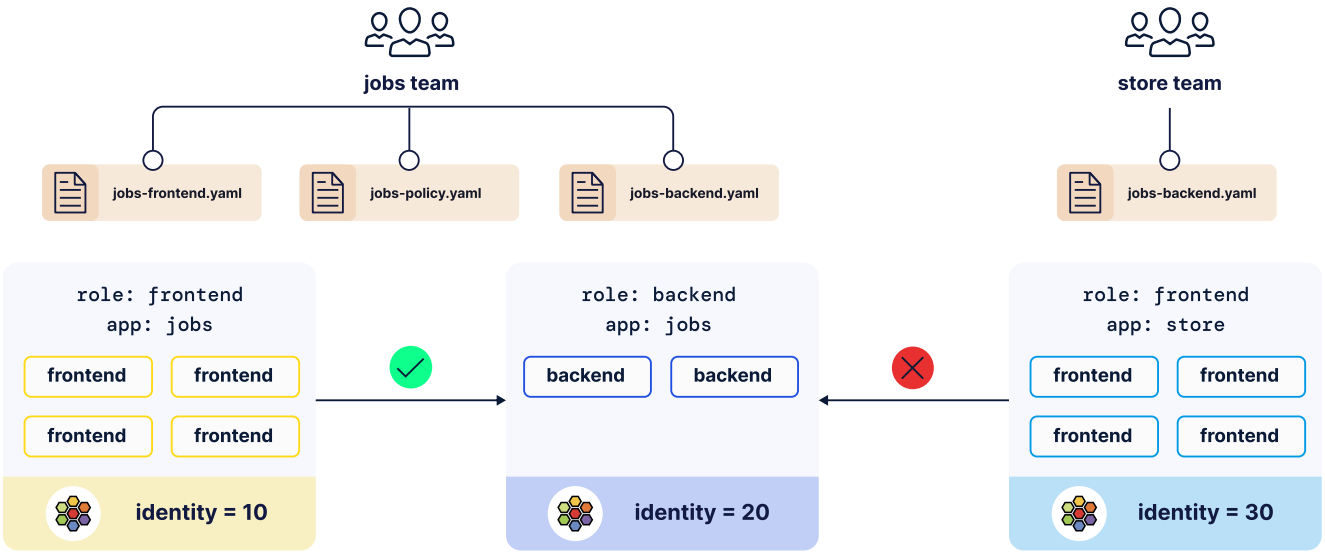

Figure 1. Cilium Identities with Network Policies