SECURITY
Security

Network Security Policies

By default, all pods can reach each other; all ingress and egress traffic is allowed. This has been a high-level networking requirement in Kubernetes. However, network isolation can be configured and traffic to pods can be blocked. In newer versions of Kubernetes, egress traffic can also be blocked. This is done by configuring a **`NetworkPolicy`**. As all traffic is allowed, you may want to implement a policy that drops all traffic, then, other policies which allow desired ingress and egress traffic.

The **spec** of the policy can narrow down the effect to a particular namespace, which can be handy. Further settings include a **`podSelector`**, or label, to narrow down which Pods are affected. Further ingress and egress settings declare traffic to and from IP addresses and ports.

Not all network providers support the **`NetworkPolicies`** kind. A non-exhaustive list of providers with support includes Calico, Romana, Cilium, Kube-router, and WeaveNet.

In previous versions of Kubernetes, there was a requirement to annotate a namespace as part of network isolation, specifically the **`net.beta.kubernetes.io/network-policy= value`**. Some network plugins may still require this setting.

On the next page, you can find an example of a **`NetworkPolicy`** recipe. More network policy recipes can be found on GitHub.