Network Security Policies

Network security policies in Kubernetes are used to control and secure the network traffic between pods and external entities. Rules and restrictions are defined on how pods can communicate with each other and with external resources.

Through the use of Network Security Policies (NSP), we can override the default behavior in Kubernetes which permits all traffic.

Here are the key aspects of network security policies in Kubernetes:

- Pod Selector: Network policies are applied to pods based on specific criteria defined by pod selectors. Pod selectors can include labels, namespaces, or other attributes to target specific groups of pods.
- Ingress and Egress: Network policies can be defined for both ingress (incoming) and egress (outgoing) traffic. Ingress policies control the traffic coming into pods, while egress policies govern the traffic leaving pods.
- Allow and Deny Rules: Network policies consist of rules that specify whether to allow or

deny network traffic based on source IP, destination IP, port numbers, protocols, or pod identities, etc.

- Default Behavior: By default, Kubernetes denies all network traffic between pods. Network policies allow you to explicitly define the desired network behavior, ensuring that only authorized communication is allowed.
- Isolation and Micro-Segmentation: Network security policies enable the implementation of isolation and micro-segmentation strategies in Kubernetes clusters. They help create separate network segments and enforce strict access controls, limiting the communication between pods.
- Third-Party Network Plugins: Kubernetes supports various third-party network plugins that provide advanced network security features like cilium, calico, etc.