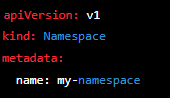
**Kubernetes Security Misconfiguration Networking Controls**

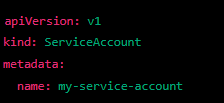
Inadequate Network Segmentation: Kubernetes allows for the creation of multiple namespaces, which can be used to segment network traffic and limit access between different parts of the cluster. However, if the network segmentation is not properly configured, it can lead to unauthorized access between namespaces.



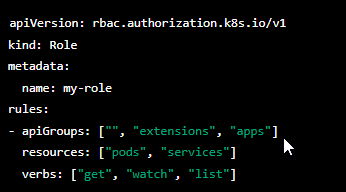
Inadequate Pod Security: Pods are the basic building blocks of a Kubernetes cluster, and they can be configured with various security options such as limiting resource usage and restricting access to network ports. If these security options are not properly configured, it can lead to unauthorized access to pods and services.



Inadequate Service Accounts: Service accounts in Kubernetes are used to control access to the API server. If these accounts are not properly configured, it can lead to unauthorized access to the API server and cluster resources.



Inadequate Role-Based Access Control (RBAC): Kubernetes uses RBAC to control access to resources in the cluster. If RBAC is not properly configured, it can lead to unauthorized access to resources and services.



Inadequate Network Policies: Network policies in Kubernetes are used to control access to resources in the cluster. If network policies are not properly configured, it can lead to unauthorized access to resources and services.

