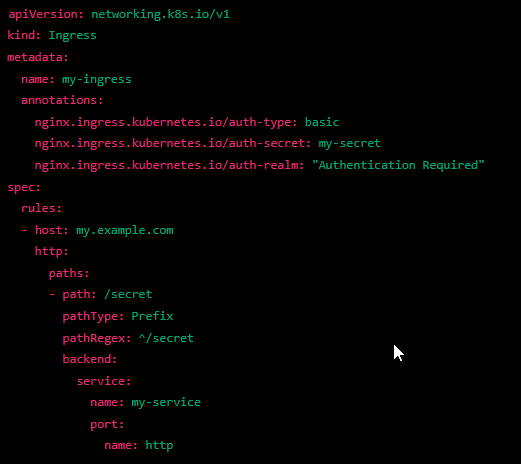
**Kubernetes Security Misconfiguration Ingress and Egress Controller**

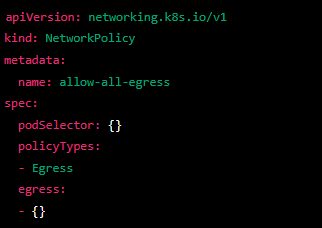
Ingress Controllers:

One common security misconfiguration in ingress controllers is exposing sensitive information in the ingress rules. For example, if the ingress rule includes a path that includes sensitive information such as a password or token, it can be easily accessed by an attacker.



Egress Controllers:

Another common security misconfiguration in egress controllers is allowing all outbound traffic by default. This can allow attackers to communicate with external systems and potentially exfiltrate data.



Additionally, not properly configuring the egress rules can also lead to a security vulnerability. For example, if the egress rules allow all traffic to a specific IP range, an attacker may be able to use that IP range to communicate with external systems.

