Secure Systems Group, Aalto University

Aarni Halinen, José Luis Martin Navarro, Jacopo Bufalino

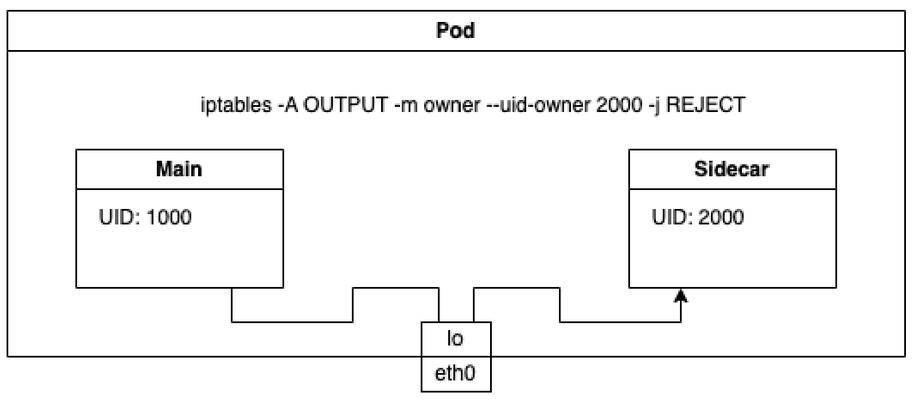
Zero Trust Architecture on K8s sidecars

Problem

- Kubernetes applications often use co-scheduled sidecar containers for peripheral tasks like logging, observability...
- Sidecar containers reside in same Pod with the main container for co-scheduling, and communicate via loopback device
- Network policies can only be applied to Pod-to-Pod communication
  - Sidecar receives same network access rules as the main application container
  - No built-in tooling for filtering traffic between the main container and the sidecar
- Egress traffic from the sidecar is indistinguishable from the main container

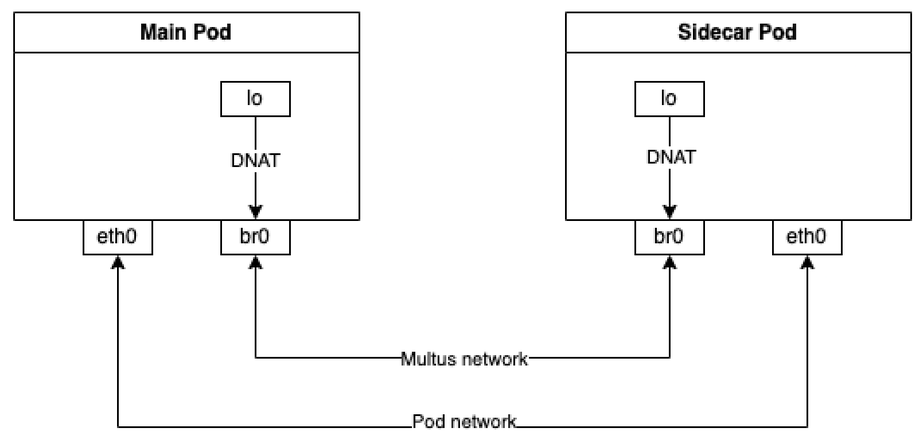
Solution 1

On Linux systems,



Solution 2

Another approach With macvlan CNI and Multus, a CNI plugin that allows creation of multiple network interfaces per Pod, a new bridge network can be created between the Pods. This network has own IP address space, and is independent from Network Policies applied on the default cluster network. For forwarding all localhost traffic to the new network, a DNAT routing rule can be attached to the loopback devices. The functionality of Network Policies can be implemented on the bridge network with MultiNetworkPolicy, a custom resource definition provided by the same team behind the Multus CNI.



Colors

- Use blue for emphasis
- Use red for negative points
- Use green for positive points

Aalto University
School of Science

Contact: aarni.halinen@aalto.fi, jose.martinnavarro@aalto.fi, jacopo.bufalino@aalto.fi