NETWAYS WEB SERVICES

NetworkPolicy

Erstellt von: Justin Lamp

Erstellt am: 16 October 2023 16:07:34

Version: 1

Inhaltsverzeichnis

NetworkPolicy

To be able to use NetworkPolicies, you'll need to run Cilium as your CNI provider. Flannel does not support it.

Use cases

If you want to secure access between pods and only allow specific traffic, NetworkPolicy are the tool of choice. They basically work like a firewall and only allow the ports/traffic you specifically specified. A basic NetworkPolicy might look like this:

```
---
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: egress-namespaces
spec:
  podSelector:
    matchLabels:
      app: myapp
  policyTypes:
  - Egress
  egress:
  - to:
    - namespaceSelector:
        matchExpressions:
        - key: namespace
          operator: In
          values: ["frontend", "backend"]
```

This will allow the myapp pods to communicate with the pods found in the namespaces `frontend` and `backend`.

Types

The afore mentioned Policy is based on the vanilla `NetworkPolicy` resource that comes with Kubernetes. Cilium on the other hand as extended this resource to form a CiliumNetworkPolicy. It has advanced features like L7 and DNS traffic inspection.

```
---
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "fqdn"
spec:
  endpointSelector:
    matchLabels:
      org: empire
      class: mediabot
  egress:
  - toFQDNs:
    - matchName: "api.github.com"
  - toEndpoints:
    - matchLabels:
```

```
      "k8s:io.kubernetes.pod.namespace": kube-system
      "k8s:k8s-app": kube-dns
  toPorts:
  - ports:
    - port: "53"
      protocol: ANY
    rules:
      dns:
      - matchPattern: "*"
- toEndpoints:
  - matchLabels:
      app: nginx
  toPorts:
  - ports:
    - port: "80"
      protocol: TCP
    rules:
      http:
      - method: "GET"
        path: "/public/*"
      - method: "GET"
        path: "/secret/index.html"
        headers:
        - 'X-My-Header: true'
```

This policy for example allows any traffic to `api.github.com` and http traffic to a nginx deployment. Some routes also need to be accessed with special headers.

Another custom resource by cilium is the `CiliumClusterwideNetworkPolicy` that as the name suggests isn't namespace scoped and will be applicable for the whole cluster.
