**Traffic Management**

**Request Routing –**

Examples of request match criteria that can be defined in Istio include:

* HTTP Header
* URL Path Prefix
* Query Parameters

**Sample Destination Rule:**

*apiVersion: networking.istio.io/v1alpha3*

*kind: DestinationRule*

*metadata:*

*name: notification*

*spec:*

*host: notification-service*

*subsets:*

*- name: v1*

*labels:*

*version: v1*

*- name: v2*

*labels:*

*version: v2*

**Sample Virtual Service:** Matching request header

*apiVersion: networking.istio.io/v1alpha3*

*kind: VirtualService*

*metadata:*

*name: ratings-route*

*spec:*

*hosts:*

*- ratings.prod.svc.cluster.local*

*http:*

*- match:*

*- headers:*

*end-user:*

*exact: jason*

*uri:*

*prefix: "/ratings/v2/"*

*ignoreUriCase: true*

*route:*

*- destination:*

*host: ratings.prod.svc.cluster.local*

**Sample Virtual Service:** Matching URI

*apiVersion: networking.istio.io/v1beta1*

*kind: VirtualService*

*metadata:*

*name: notification*

*spec:*

*hosts:*

*- notification-service*

*http:*

*- match:*

*- uri:*

*prefix: "/v2/notify"*

*rewrite:*

*uri: "/notify"*

*route:*

*- destination:*

*host: notification-service*

*subset: v2*

*- route:*

*- destination:*

*host: notification-service*

*subset: v1*

**Sample Virtual Service :** queryParams

*apiVersion: networking.istio.io/v1beta1*

*kind: VirtualService*

*metadata:*

*name: notification*

*spec:*

*hosts:*

*- notification-service*

*http:*

*- match:*

*- queryParams:*

*testing:*

*exact: "true"*

*route:*

*- destination:*

*host: notification-service*

*subset: v2*

*- route:*

*- destination:*

*host: notification-service*

*subset: v1*

**Security**

Istio’s JWT token authorization is configured using RequestAuthentication and AuthorizePolicy.

A **request authentication** resource defines what request authentication methods are supported by a workload, specified through a label selector. Requests which do not contain valid authentication information are rejected.

An **authorization policy** enables access control on the workloads using source principals and optionally, custom matching conditions on JWT token claims such as roles or groups.