Policy Enforcement Assessment: Stage 2

Definitions

Each policy is associated with a set of **rule**s.

A **rule** is one of the definitions specifying a type of network traffic. Rules for Arupa policies and Frisco policies are different.

Each Arupa rule has the following fields:

- `name` - free text
- `ip_proto` - an IP protocol number
- `source_port` - a port number
- `source_subnet` - an IP subnet in CIDR notation (for example, 192.168.0.0/24)

Arupa rule `name`s must be unique within each policy.

Each Frisco rule has the following fields:

- `name` - free text
- `ip_proto` - an IP protocol number
- `source_port` - a port number
- `source_ip` - an IP address
- `destination_ip` - an IP address

Frisco rule `name`s must be globally unique, even between policies.

Requirements

Building on the previous stage, implement create, read, update, delete, and list methods for rules.

Their interfaces should be similar to the corresponding methods for policies, except that:

- `create_rule()` should take as its first argument a policy identifier to which the rule should belong, and as its second argument a JSON string containing an object whose keys are the fields of the rule.
- `list_rules()` should take a policy identifier as its only argument, and should return all of the rules associated with that policy.