Policy Object for I2NSF
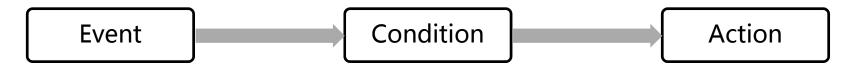
https://datatracker.ietf.org/doc/draft-xia-i2nsf-sec-object-dm/

Liang Xia

Qiushi Lin

IETF 102

Motivation

```
┌─────────────┐      ┌─────────────┐      ┌─────────────┐
│    Event    │ ───▶ │  Condition  │ ───▶ │   Action    │
└─────────────┘      └─────────────┘      └─────────────┘
```

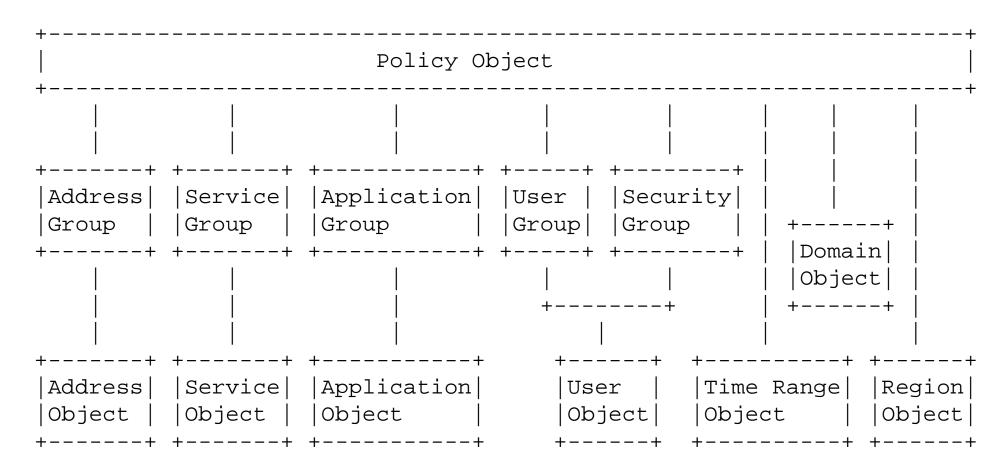- **Problems with attribute based policy rule configuration**
  - Repetitive configuration when creating new policy rules
  - Hard to maintain consistency, and time consuming to make modification
- **Object based configuration has been widely used in NSFs**
  - Re-usability: A policy object can be referenced in different policy rules as required.
  - Simplicity: The modification of a policy object will be propagated to the I2NSF policy rules that refer to this policy object.
- **Propose to introduce the "object" concept in I2NSF policy rule, and define commonly used policy objects**
  - This document is aligned with the previous information model draft and provides YANG groupings for the reusable policy objects

Policy Object Overview

- **This document provides a minimal set of commonly used policy objects :**

```
+----------------------------------------------------------------+
|                          Policy Object                         ||
+----------------------------------------------------------------+
    |           |            |          |        |     |     |
    |           |            |          |        |     |     |
+-------+   +-------+   +-----------+  +-----+  +--------+  |     |     |
|Address|   |Service|   |Application|  |User |  |Security|  |     |     |
|Group  |   |Group  |   |Group      |  |Group|  |Group   |  | +------+ |
+-------+   +-------+   +-----------+  +-----+  +--------+  | |Domain| |
    |           |            |          |        |         | |Object| |
    |           |            |       +--------+  |         | +------+ |
    |           |            |          |        |         |         |
+-------+   +-------+   +-----------+  +------+  +----------+  +------+
|Address|   |Service|   |Application|  |User  |  |Time Range|  |Region|
|Object |   |Object |   |Object     |  |Object|  |Object    |  |Object|
+-------+   +-------+   +-----------+  +------+  +----------+  +------+
```

Policy Object - Examples

```
grouping addr-objects:
+--rw addr-object* [name]
   +--rw name        address-set-name
   +  ...
   +--rw elements*  [elem-id]
      +--rw elem-id uint16
      +--rw (object-items)
         +--:(ipv4)
         | ...
         +--:(ipv6)
         | ...
         +--:(mac)
         | ...
         +--:(ipv4-range)
         | ...
         +--:(ipv6-range)
            ...

 grouping addr-groups:
+--rw addr-group* [name]
   +--rw name address-set-name
   +  ...
   +--rw elements* [elem-id]
      +--rw elem-id      uint16
      +--rw addr-object-name
                  address-set-name
```

```
grouping service-objects:
+--rw pre-defined-service* [name]
|  ...
+--rw service-object* [name]
   +--rw name        service-set-name
   +  ...
   +--rw items* [id]
      +--rw id        uint16
      +--rw (item)
         +--:(tcp-item)
         | ...
         +--:(udp-item)
         | ...
         +--:(sctp-item)
         | ...
         +--:(icmp-item)
         | ...
         +--:(icmp6-item)
         | ...
         +--:(protocol-id)
            ...
grouping services-groups:
+--rw service-group* [name]
   +--rw name service-set-name
   +  ...
   +--rw elements* [elem-id]
      +--rw elem-id      uint16
      +--rw service-object-name
                  service-set-name
```

Questions/Comments

- **Adopt "policy object" in I2NSF policy rule ?**
- **The implementation of policy object ?**
  - This document: provide policy object for NSF-facing interface
  - Does Client-facing interface also need policy object?
- **The group's opinion ?**
  - ✓ Individual draft or incorporating it into existing drafts ?
- **Please review and comment**