

I2NSF Data Model of Consumer-Facing Interface for Security Management

(draft-jeong-i2nsf-consumer-facing-interface-dm-05)



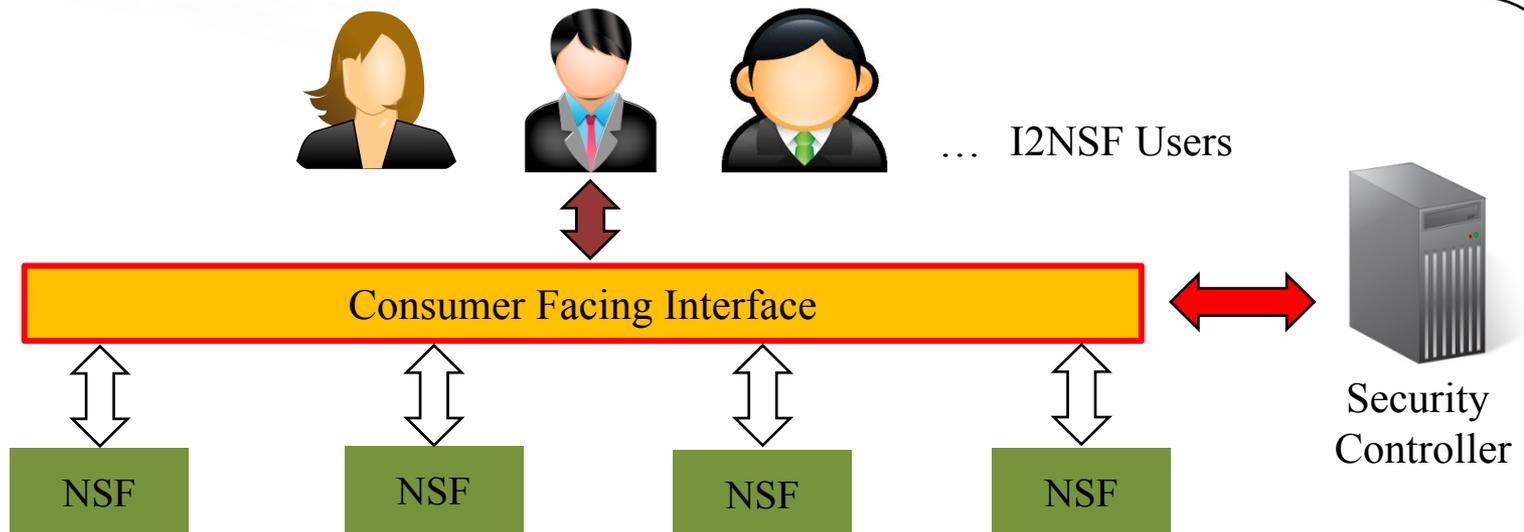
IETF 100

Presenter : Seungjin Lee (Co-author)

Jaehoon Paul Jeong, Eunsoo Kim, Tae-Jin Ahn,
Rakesh Kumar, and Susan hares

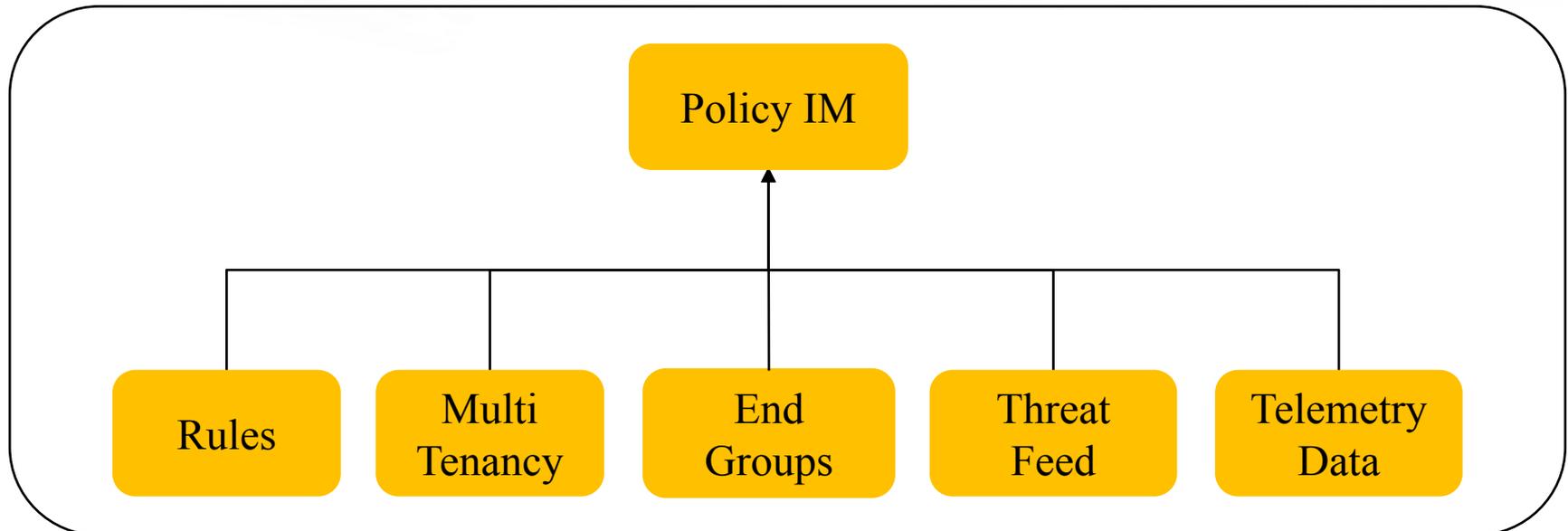
Introduction

- This document describes an YANG data model for Consumer-Facing Interface between I2NSF User and Security Controller in I2NSF system in a NFV environment
- A data model is required for enabling different users of a given I2NSF system to manage security policies for specific flows



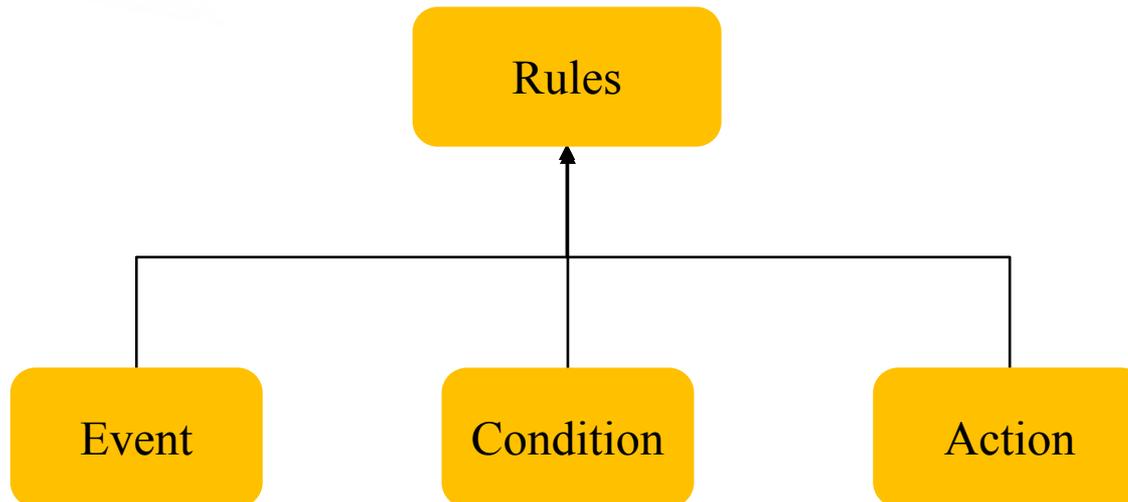
Introduction

- The data model is derived from the information model in “draft-kumar-i2nsf-client-facing-interface-im-04”
- The information model defines the managed objects and their relationship to build the interface



Introduction

- The information model is organized based on the “Event-Condition-Action” (ECA) policy model
- The main objective of this draft is to fully transform the information model into an YANG data model that can be used for delivering control via the Consumer-Facing Interface



The background of the slide features a perspective view of a city skyline with various skyscrapers. In the foreground, there is a white grid floor that recedes into the distance. In the upper left portion of the sky, a jet airplane is flying, leaving a white contrail. The sky is a light blue with a few scattered white clouds. The title 'Updates of Version' is centered in a large, bold, dark blue serif font.

Updates of Version

Update of Version

- The following changes are made from draft-jeong-i2nsf-consumer-facing-interface-dm-04
 - Data tree model has been revised according to the information model and Event-Condition-Action (ECA) based policy generation
 - YANG data model has been revised using the data tree model
 - The data tree model and the YANG data model for use case have also been modified for ECA-based policy generation
 - An example XML output for use case has been added in appendix

Major Update of Version

Data Model for Consumer-Facing-Interface

Multi Tenancy

```
+-rw multi-tenancy
  +-rw policy-domain* [policy-domain-id]
    +-rw policy-domain-id      uint16
    +-rw name                   string
    +-rw address                string
    +-rw contact                string
    +-rw date                   yang:date-and-time
    +-rw authentication-method  string
  +-rw policy-tenant* [policy-tenant-id]
```

End Group

```
+-rw policy-endpoint-groups
  +-rw meta-data-source* [meta-data-source-id]
    +-rw meta-data-source-id  uint16
    +-rw name                  string
    +-rw date                  yang:date-and-time
    +-rw tag-type?            boolean
    +-rw tag-server-information? string
    +-rw tag-application-protocol? string
    +-rw tag-server-credential? string
```

Threat Feed

```
+-rw threat-prevention
  +-rw threat-feed* [threat-feed-id]
    +-rw threat-feed-id      uint16
    +-rw name                 string
    +-rw date                 yang:date-and-time
    +-rw feed-type?          enumeration
    +-rw feed-server?        string
    +-rw feed-priority?      uint16
  +-rw custom-list* [custom-list-id]
```

Telemetry Data

```
+-rw telemetry-data
  +-rw telemetry-data* [telemetry-data-id]
    +-rw telemetry-data-id  uint16
    +-rw name                string
    +-rw date                yang:date-and-time
    +-rw logs?              boolean
    +-rw syslogs?           boolean
    +-rw snmp?              boolean
    +-rw sflow?             boolean
```

Policy

```
+-rw policy
  +-rw rule* [rule-id]
    +-rw rule-id*          uint16
    +-rw name?             string
    +-rw date?             yang:date-and-time
    +-rw event* [event-id]
      +-rw event-id        string
      +-rw name?           string
      +-rw date?           yang:date-and-time
      +-rw event-type?     string
      +-rw time-information? string
        +-rw begin-time?   yang:date-and-time
        +-rw end-time?     yang:date-and-time
      +-rw event-map-group? -> /ietf-i2nsf-consumer-facing-interface/
        threat-feed/threat-feed/
        threat-feed-id
      +-rw enable?         boolean
    +-rw condition* [condition-id]
      +-rw condition-id    string
      +-rw source?         -> /ietf-i2nsf-consumer-facing-interface/
        threat-feed/threat-feed/
        threat-feed-id
      +-rw destination?   -> /ietf-i2nsf-consumer-facing-interface/
        threat-feed/threat-feed/
        custom-list-id
      +-rw match?          boolean
      +-rw match-direction? string
      +-rw exception?      string
    +-rw action* [policy-action-id]
      +-rw policy-action-id string
      +-rw name?           string
      +-rw date?           yang:date-and-time
      +-rw primary-action? string
      +-rw secondary-action? string
    +-rw precedence        uint16
    +-rw owner?           string
```

Major Update of Version

Data Model for Consumer-Facing-Interface

```
+--rw policy
  +--rw rule* [rule-id]
    +--rw rule-id*      uint16
    +--rw name?         string
    +--rw date?         yang:date-and-time
    +--rw event* [event-id]
      +--rw event-id    string
      +--rw name?       string
      +--rw date?       yang:date-and-time
      +--rw event-type? string
      +--rw time-information? string
      | +--rw begin-time? yang:date-and-time
      | +--rw end-time?   yang:date-and-time
      +--rw event-map-group? -> /ietf-i2nsf-consumer-facing-interface/
      | threat-feed/threat-feed/
      | threat-feed-id
      +--rw enable?     boolean
    +--rw condition* [condition-id]
      +--rw condition-id string
      +--rw source?      -> /ietf-i2nsf-consumer-facing-interface/
      | threat-feed/threat-feed/
      | threat-feed-id
      +--rw destination? -> /ietf-i2nsf-consumer-facing-interface/
      | threat-feed/threat-feed/
      | custom-list-id
      +--rw match?       boolean
      +--rw match-direction? string
      +--rw exception?   string
    +--rw action* [policy-action-id]
      +--rw policy-action-id string
      +--rw name?           string
      +--rw date?           yang:date-and-time
      +--rw primary-action? string
      +--rw secondary-action? string
  +--rw precedence      uint16
  +--rw owner?          string
```

Event

Determine condition clause of the policy rule can be evaluated or not.

Condition

Action in policy rule can be executed or not.

Action

Simple permit/deny/rate-limiting, etc.

Next Step

- We will discuss with IM & DM team for
 - the consistency between IM and DM
 - the generalization of the data model for more use cases



A 3D rendering of a city skyline with a grid floor and a flying airplane. The scene is set against a light blue sky with a few clouds. A small airplane is flying in the upper left, leaving a white contrail. The city skyline is composed of various skyscrapers of different heights and styles, rendered in a dark grey color. The floor is a light grey grid that recedes into the distance, creating a sense of depth. The overall composition is clean and modern.

Thank you!